ExtraHop 9.9
Guide de l'utilisateur du système ExtraHop

Pour plus de documentation, voir https://docs.extrahop.com.

Publié: 2025-01-05

ExtraHop Networks
Seattle, WA 98101
877-333-9872 (US)
+44 (0)203 7016850 (EMEA)
+65-31585513 (APAC)
www.extrahop.com

Table des matières

À propos de ce guide

Ce guide fournit des informations sur le système ExtraHop pour les appareils ExtraHop Discover et Command.

Le but de ce guide est d'aider les utilisateurs à comprendre l'architecture et les fonctionnalités du système ExtraHop ainsi qu'à apprendre à utiliser les commandes, les champs et les options disponibles dans l'ensemble du système.

Des ressources supplémentaires sont disponibles via les liens suivants :

- Consultez les informations sur les fonctionnalités et fonctions d'administration des appareils ExtraHop Discover et Command dans le Guide de l'interface utilisateur d'ExtraHop
- Consultez la documentation complète d'ExtraHop : https://docs.extrahop.com.
- Voir les modules de formation en ligne sur le site Web d'ExtraHop : https://www.extrahop.com/go/training/.

Nous contacter

Vos commentaires sont importants pour nous.

Merci de nous indiquer comment nous pouvons améliorer ce document. Envoyez vos commentaires ou suggestions à documentation@extrahop.com.

- **Site Web du portail d'assistance:** https://customer.extrahop.com/s/
- **Téléphone:**
  - 877-333-9872 (ÉTATS-UNIS)
  - +44 (0) 203 7016850 (EMEA)
  - +65-31585513 (APAC)

Présentation du système ExtraHop

Ce guide explique comment le système ExtraHop collecte et analyse vos données et comment les principaux composants et fonctionnalités du système vous aident à accéder aux détections, aux mesures, aux transactions et aux paquets concernant le trafic sur votre réseau.

Les flux de travail de surveillance des performances réseau vous permettent de surveiller la manière dont les services et les appareils interagissent entre eux et comment les transactions circulent entre la couche liaison de données (L2) et la couche application (L7) de votre réseau. Les workflows de détection et de réponse du réseau vous permettent d' examiner les données détectées, qu'il s'agisse de performances dégradées ou de comportements suspects, et fournissent une visibilité sur les appareils qui ont participé aux tactiques, techniques et procédures (TTP) MITRE ATT&CK associées à des campagnes d'attaque avancées en plusieurs étapes.

Vidéo: Consultez la formation associée : Présentation du système ExtraHop

Architecture de plateforme

Le système ExtraHop est personnalisé avec des composants modulaires qui se combinent pour répondre à vos besoins environnementaux uniques.

Modules

Les modules ExtraHop offrent une combinaison de solutions, de composants et de services basés sur le cloud qui offrent de la valeur pour de multiples cas d'utilisation.

Des modules sont disponibles pour la détection et la réponse du réseau (NDR) et la surveillance des performances du réseau (NPM), ainsi que des modules supplémentaires pour les systèmes de détection d'intrusion (IDS) et la criminalistique des paquets.

Les administrateurs peuvent activer le contrôle d'accès basé sur les rôles (RBAC) en accordant aux utilisateurs l'accès au module NDR, au module NPM ou aux deux.

Surveillance des performances du réseau

Le module NPM permet aux utilisateurs privilégiés d'effectuer les types de tâches système suivants.

- Affichez, créez et modifiez des tableaux de bord personnalisés. Les utilisateurs peuvent également sélectionner un tableau de bord pour leur page de destination par défaut.
- Configurez les alertes et les notifications par e-mail pour ces alertes.
- Afficher les détections de performances.

Détection et réponse du réseau

Le module NDR permet aux utilisateurs privilégiés d'effectuer les types de tâches système suivants.

- Consultez la page de présentation de la sécurité.
- Afficher les détections de sécurité.
- Consultez, créez et modifiez des enquêtes.
- Consultez les briefings sur les menaces.

Les utilisateurs autorisés à accéder aux deux modules sont autorisés à effectuer toutes ces tâches. Consultez les Guide de migration pour en savoir plus sur la migration des utilisateurs vers un accès basé sur les rôles à l' aide de ces modules.

Ces modules supplémentaires sont également disponibles pour des cas d'utilisation spécifiques :

Packet Forensics

Le module Packet Forensics peut être combiné au module NDR ou NPM pour fournir une capture, un stockage et une récupération complets des paquets.

Systèmes de détection d'intrusion

Le module IDS doit être combiné au module NDR et fournit des détections basées sur des signatures IDS conformes aux normes de l'industrie. La plupart des capteurs de paquets ExtraHop sont éligibles au module IDS, à condition que le capteur soit autorisé pour le module NDR.

Note: Débit peut être affectée lorsque plusieurs modules sont activés sur la sonde.

Caractéristiques

Le système ExtraHop fournit un ensemble complet de fonctionnalités qui vous permet d'organiser et d'analyser les détections, les mesures, les enregistrements et les paquets associés au trafic sur votre réseau.

L'accès au module et au système est déterminé par privilèges d'utilisateur qui sont gérés par votre administrateur ExtraHop.

Caractéristiques globales

Les fonctionnalités suivantes sont disponibles dans tous les systèmes ExtraHop et ne nécessitent pas de modules spécifiques.

- Vue d'ensemble du réseau
- Vue d'ensemble du périmètre
- Cartes d'activités
- tableau de bord Active Directory
- tableau de bord génératif de l'IA
- Rapports de tableau de bord planifiés
- Suivi des détections
- Actifs
- Disques
- Paquets
- Intégrations (RevealX 360 uniquement)
- Accès à l'API
- Priorités d'analyse
- Catalogue métrique
- Lots
- éléments déclencheurs
- Assistant de recherche IA (actifs et dossiers)

Caractéristiques du module NDR

Les fonctionnalités suivantes sont disponibles dans les systèmes ExtraHop dotés du module Network Detection and Response (NDR).

- Aperçu de la sécurité
- Assistant de recherche IA
- Rapports sur les opérations de sécurité
- Tableaux de bord de sécurité intégrés
- Détections de sécurité
- Carte MITRE
- Enquêtes
- Règles de réglage pour les détections de sécurité

- Règles de notification pour les détections de sécurité et les briefings sur les menaces
- Exposés sur les menaces
- Renseignements sur les menaces
- Analyse de fichiers
- Extraction de fichiers (analyse des paquets requise)

Caractéristiques du module NPM

Les fonctionnalités suivantes sont disponibles dans les systèmes ExtraHop dotés du module Network Performance Management (NPM).

- Tableaux de bord personnalisés
- Tableaux de bord de performance intégrés
- Détections de performances
- Règles de réglage pour les détections de performances
- Règles de notification pour les détections de performances
- Alertes

Fonctionnalités de Packet Forensics

Les fonctionnalités suivantes sont disponibles dans les systèmes ExtraHop dotés du module Packet Forensics.

- Capture de paquets
- Assistance pour Packetstore
- Extraction de fichiers (NDR requis)

Caractéristiques de l'IDS

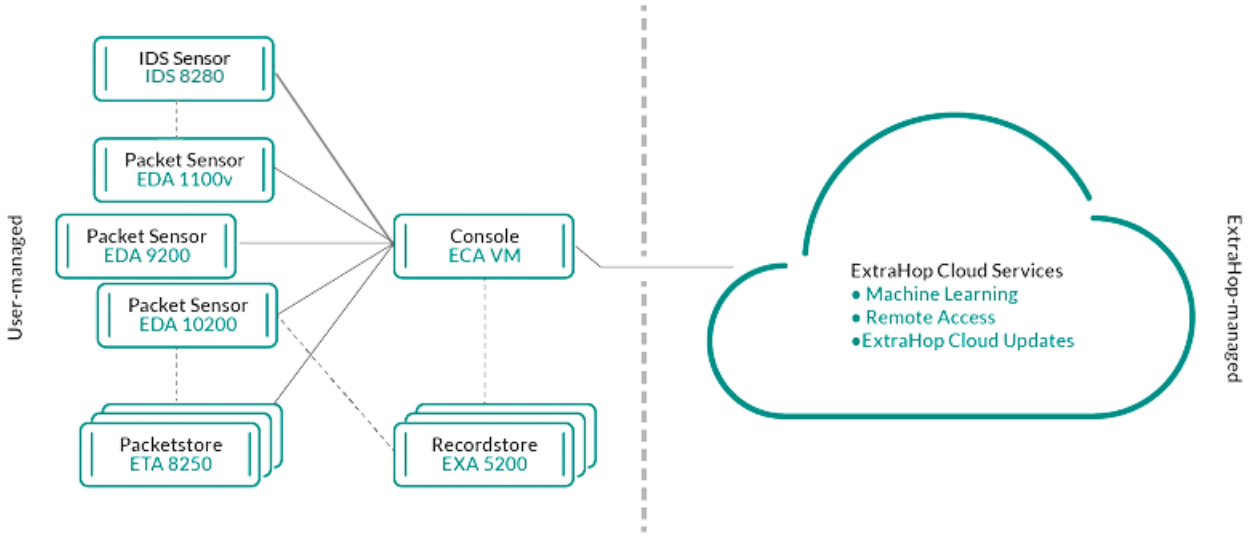
Les fonctionnalités suivantes sont disponibles dans les systèmes ExtraHop dotés du module Intrusion Detection System (IDS).

- Détections IDS

Des solutions

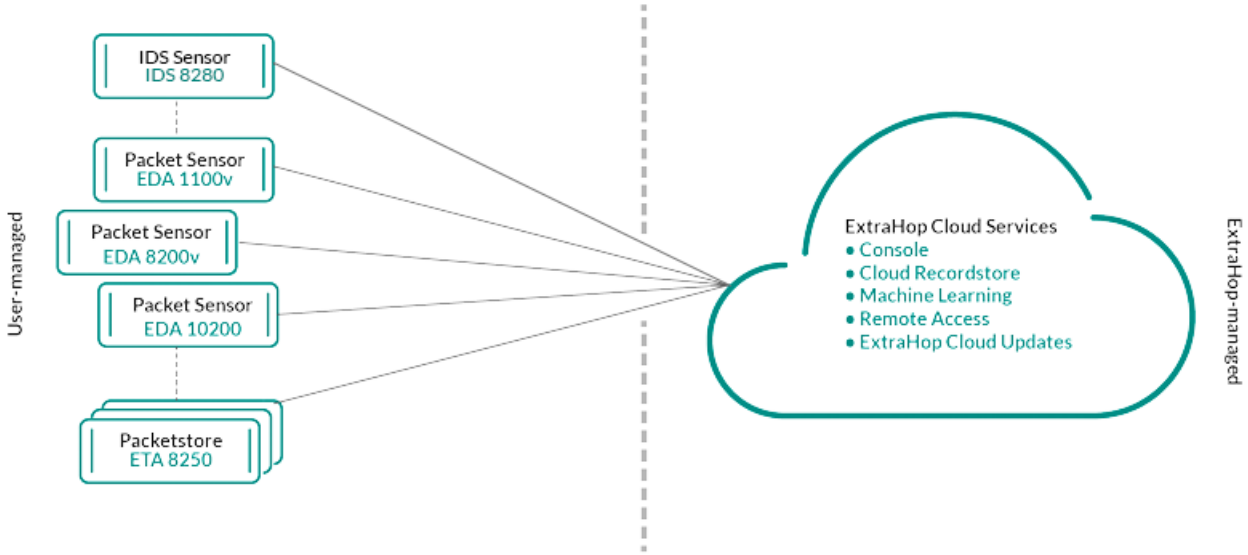
RevealX Enterprise

RevealX Enterprise est une solution autogérée qui comprend capteurs, consoles, les magasins de paquets, les magasins de disques et l'accès aux services cloud ExtraHop.



RevealX 360

RevealX 360 est une solution logicielle en tant que service (SaaS) qui comprend capteurs et packetstores et comprend un espace de stockage des enregistrements basé sur le cloud avec Standard Investigation, un console, et accès aux services cloud ExtraHop.



Composantes

Chaque solution propose un ensemble de composants en fonction de vos besoins environnementaux : capteurs, magasins de paquets, magasins de disques et console pour une gestion centralisée et des vues de données unifiées.

Capteurs de paquets

Les capteurs de paquets capturent, stockent et analysent les données métriques relatives à votre réseau. Plusieurs niveaux d'analyse, de collecte et de stockage des données sont disponibles en fonction de la taille de la sonde. Ces capteurs sont disponibles dans les modules NPM et NDR en tant qu'options physiques, virtuelles et basées sur le cloud, dans des tailles adaptées à vos besoins d'analyse.

Capteurs IDS

Les capteurs du système de détection d'intrusion (IDS) s'intègrent aux capteurs de paquets pour générer des détections basées sur la signature IDS standard de l'industrie. Les capteurs IDS sont déployés en tant que module complémentaire au module NDR. Les capteurs IDS sont une appliance physique associée à une sonde réseau d'analyse de paquets et sont disponibles pour les environnements RevealX 360 ou RevealX Enterprise.

Capteurs de débit

Les capteurs de flux sont disponibles pour RevealX 360 uniquement et collectent exclusivement les journaux de flux VPC afin que vous puissiez voir le trafic géré par les services AWS SaaS.

Disquaires

Les magasins de disques intègrent des capteurs et consoles pour stocker les enregistrements de transactions et de flux qui peuvent être interrogés depuis l'ensemble du système ExtraHop. Les magasins d'enregistrements peuvent être déployés en tant qu'options physiques ou virtuelles autonomes et peuvent être pris en charge en tant que connexions tierces à Splunk ou BiqQuery depuis RevealX Enterprise. RevealX 360 avec Standard Investigation fournit un espace de stockage des enregistrements entièrement hébergé et basé sur le cloud. Les magasins de disques sont disponibles dans des packages avec les modules NPM et NDR.

Magasins de paquets

Les magasins de paquets s'intègrent à des capteurs et consoles pour fournir PCAP en continu et un espace de stockage suffisant pour des enquêtes plus approfondies et des besoins en matière de criminalistique. Les Packetstores peuvent être déployés en tant qu'options physiques ou virtuelles autonomes et sont disponibles en tant que module complémentaire Packet Forensics pour les modules NPM et NDR.

Consoles

Les consoles fournissent une interface basée sur un navigateur qui fournit un centre de commande pour tous les composants connectés. Consoles peuvent être déployés en tant qu'options autonomes virtuelles ou basées sur le cloud pour RevealX Enterprise et sont inclus dans RevealX 360.

Le tableau suivant donne un aperçu des options disponibles pour chaque solution.

	RevealX Enterprise		RevealX 360	
	Physique	Virtuel/Cloud	Physique	Virtuel/Cloud
sonde à paquets	ANNÉE 1200 ÉD. 6200 ÉD. 8200 ÉD. 8320 ÉD. 9200 ÉD. 9300 ÉD. 10200	AWS EDA 1100 v EDA 1100v Azure GCP EDA 1100 V GCP EDA 6320v GCP EDA 8370 V KVM Linux EDA 1100 v VMware EDA 1100 v	ANNÉE 1200 ÉD. 6200 ÉD. 8200 ÉD. 8320 ÉD. 9200 ÉD. 9300 ÉD. 10200	AWS EDA 1100 v EDA 1100v Azure GCP EDA 1100 V GCP EDA 6320v GCP EDA 8370 V KVM Linux EDA 1100 v VMware EDA 1100 v

	RevealX Enterprise		RevealX 360	
	ÉD. 10300	VMware EDA 6100 v AWS EDA 6100v EDA 6100v Azure AWS EDA 8200v RevealX Ultra AWS à 1 Gbit/s et 10 Gbit/s RevealX Ultra GCP 1 Gbit/s et 10 Gbit/s	ÉD. 10300	AWS EDA 6100v EDA 6100v Azure VMware EDA 6100 v AWS EDA 8200v RevealX Ultra AWS à 1 Gbit/s et 10 Gbit/s RevealX Ultra GCP 1 Gbit/s et 10 Gbit/s
sonde IDS	ID 8280 ID 9380	IDS 1280v pour VMware IDS 6280 v pour VMware	ID 8280 ID 9380	IDS 1280v pour VMware IDS 6280 v pour VMware
sonde de débit	N/A	N/A	N/A	EFC 1291v AWS (PVC) EFC 1292 v (NetFlow)
Magasin de paquets	ET 6150 ÉTÉ 8250	AWS ETA 1150 v ETA 1150v Azure GCP ETA 1150 V VMware ETA 1150 v VMWare ETA 6150v	ET 6150 ÉTÉ 8250	AWS ETA 1150 v ETA 1150v Azure GCP ETA 1150 V VMware ETA 1150 v VMWare ETA 6150v

	RevealX Enterprise		RevealX 360	
				Inclus dans les abonnements Ultra
Disquaire	EXAMEN 5200	AWS EXA 5100 v EXA 5100 v Azure Hyper-V EXA 5100 V KVM Linux EXA 5100 v VMWare EXA 5100 v	N/A	Inclus dans les abonnements Premium et Ultra
Console	N/A	LOIS DE LA CEA ECA Azure ECA GCP ECA Hyper-V KVM ECA Linux ECA VMware	N/A	Inclus dans tous les abonnements

Services cloud ExtraHop

Services cloud ExtraHop met automatiquement à jour les capteurs en fonction des nouvelles détections et des renseignements sur les menaces critiques, ainsi que des améliorations apportées aux fonctionnalités, et permet aux équipes chargées de votre compte d'accéder à une assistance à distance et à des services professionnels.

Analyse des capteurs intelligents

Le système ExtraHop propose une interface basée sur un navigateur avec des outils qui vous permettent d' explorer et de visualiser les données, d'étudier les résultats dans des flux de travail ascendants et descendants, et de personnaliser la manière dont vous collectez, visualisez et partagez les données de votre réseau. Les utilisateurs avancés peuvent automatiser et écrire des scripts pour les tâches administratives et les tâches utilisateur via API REST ExtraHop et personnalisez la collecte de données via API ExtraHop Trigger, qui est un outil IDE JavaScript.

Au cœur du système ExtraHop se trouve un sonde qui capture, stocke et analyse les données métriques relatives à votre réseau et propose différents niveaux d'analyse, de collecte et de stockage des données en fonction de vos besoins. Sondes sont dotés d'un espace de stockage prenant en charge 30 jours de rétrospective métrique. Notez que la rétrospective réelle varie en fonction des modèles de trafic, des taux de transaction, du nombre de points de terminaison et du nombre de protocoles actifs.

Les consoles font office de centre de commande avec des connexions à plusieurs capteurs, des magasins de disques et des magasins de paquets répartis dans les centres de données et les succursales. Tous les déploiements de RevealX 360 incluent une console ; RevealX Enterprise peut déployer des variantes virtuelles ou cloud.

Les consoles fournissent des vues de données unifiées sur tous vos sites et vous permettent de synchroniser certaines configurations avancées (telles que déclencheurs et alertes) et paramètres (paramètres de réglage, priorités d'analyse, et disquaires).

Les sections suivantes décrivent les principaux composants fonctionnels du système ExtraHop et la manière dont ils fonctionnent ensemble.

Types de capteurs

Le type de sonde vous déployez détermine le type de données collectées, stockées et analysées.

Données filaires
Les capteurs de paquets et les capteurs du système de détection d'intrusion (IDS) observent passivement les paquets non structurés via un miroir de ports ou tapent et stockent les données dans la banque de données locale. Les données des paquets sont soumises à un traitement de flux en temps réel qui transforme les paquets en données filaires structurées selon les étapes suivantes :

1. Les machines à états TCP sont recréées pour effectuer un réassemblage complet.
2. Les paquets sont collectés et regroupés en flux.
3. Les données structurées sont analysées et traitées de la manière suivante :
   - Les transactions sont identifiées.
   - Les appareils sont automatiquement découverts et classés en fonction de leur activité.
   - Des métriques sont générées et associées à des protocoles et à des sources, et les données métriques sont ensuite agrégées en cycles métriques.
4. Au fur et à mesure que de nouvelles métriques sont générées et stockées et que la banque de données est pleine, les plus anciennes métriques existantes sont remplacées selon le principe du premier entré, premier sorti (FIFO).

Données de flux
Un flux est un ensemble de paquets qui font partie d'une connexion unique entre deux terminaux. Flux capteurs sont disponibles pour RevealX 360 et offrent une visibilité continue du réseau sur la base des journaux de flux VPC afin de sécuriser les environnements AWS. Les journaux de flux VPC vous permettent de capturer des informations sur le trafic IP entrant et sortant des interfaces réseau de votre VPC et sont enregistrés sous forme d'enregistrements de journaux de flux, qui sont des événements de journal composés de champs décrivant le flux de trafic. Ces données de journal vous permettent de rechercher des menaces à l'aide de détections avancées par apprentissage automatique.

Les journaux de flux sont ingérés, dédupliqués, puis regroupés en flux. Les flux sont ensuite enrichis avec des données (telles que des adresses MAC) demandées à partir des API AWS EC2.

Les flux sont ensuite analysés et traités de la manière suivante :

- Les appareils sont automatiquement découverts et classés en fonction de leur activité observée sur des ports spécifiques.
- Les métriques L2-L4 de base sont générées et agrégées en cycles métriques.
- Les types d'enregistrement ExFlow sont générés et publiés.

Métriques, enregistrements et paquets

Les capteurs ExtraHop collectent et stockent plusieurs niveaux d'interaction réseau sous forme de métriques. Les métriques sont des observations agrégées concernant les interactions entre les points de terminaison au fil du temps. Les packetstores collectent et stockent les données brutes transférées entre deux points de terminaison sous forme de paquets. Magasins de disques collectez et stockez des enregistrements, qui sont des informations structurées sur les transactions, les messages et les flux réseau.

Vous pouvez visualiser et interroger toutes ces interactions à partir de capteurs individuels ou d'un console qui est lié à un déploiement complexe de capteurs, de magasins de paquets et de magasins de disques.

Par exemple, lorsqu'un client envoie une requête HTTP à un serveur Web, voici le contenu de chaque type de données :

- Le paquet contient les données brutes qui ont été envoyées et reçues lors de l' interaction.
- L'enregistrement associé contient les métadonnées horodatées relatives à l' interaction : date à laquelle la demande a eu lieu, adresse IP du client et du serveur, URI demandé, éventuels messages d'erreur.
- La métrique associée (requêtes HTTP) contient un agrégat de cette interaction avec les autres interactions observées au cours de la période spécifiée, telles que le nombre de demandes effectuées, le nombre de demandes réussies, le nombre de clients ayant envoyé des demandes et le nombre de serveurs ayant reçu les demandes.

Les métriques et les enregistrements peuvent être personnalisés pour extraire et stocker des métadonnées spécifiques à l'aide de JavaScript déclencheurs. Alors que le système ExtraHop est terminé 4600 métriques intégrées, vous souhaiterez peut-être créer un métrique personnalisée qui collecte et agrège les erreurs 404 uniquement à partir de serveurs Web critiques. Et vous souhaiterez peut-être maximiser votre espace de stockage d'enregistrements uniquement collecte des transactions survenues via un port suspect.

Découverte des appareils

Une fois qu'un équipement est découvert, le système ExtraHop commence à collecter des métriques en fonction du niveau d'analyse configuré pour cet équipement. Tu peux Trouvez un équipement par leur adresse MAC, leur adresse IP ou leur nom (tel qu'un nom d'hôte observé à partir du trafic DNS, le nom NetBIOS, le nom du Cisco Discovery Protocol (CDP), le nom DHCP ou un nom personnalisé que vous avez attribué à l'équipement).

Le système ExtraHop peut découvrir et suivre les appareils par leur adresse MAC (L2 Discovery) ou par leur adresse IP (L3 Discovery). L2 Discovery offre l'avantage de suivre les métriques d'un équipement même si l'adresse IP est modifiée ou réattribuée par le biais d'une requête DHCP. Par défaut, le système ExtraHop est configuré pour L2 Discovery.

Les adresses IPv4 et IPv6 des appareils sont découvertes à partir des messages ARP (Address Resolution Protocol), des réponses du protocole NDP (Neighbor Discovery Protocol), des diffusions locales ou du trafic de multidiffusion du sous-réseau local. L'adresse MAC et l'adresse IP des appareils apparaissent dans les résultats de recherche sur l'ensemble du système avec les informations relatives à l'équipement.

Découverte L2

Dans L2 Discovery, le système ExtraHop crée une entrée d'équipement pour chaque adresse MAC locale découverte via le fil. Les adresses IP sont mappées à l'adresse MAC, mais les métriques sont stockées avec l'adresse MAC de l'équipement même si l'adresse IP change.

Les adresses IP observées en dehors des domaines de diffusion surveillés localement sont agrégées sur l'un des routeurs entrants de votre réseau. Si un équipement envoie une demande DHCP via un routeur agissant en tant qu'agent de relais DHCP, le système ExtraHop détecte et mappe l'adresse IP à l'adresse MAC de l'équipement. Si l'adresse IP de l'équipement change lors d'une demande ultérieure via l'agent de relais DHCP, le système ExtraHop met à jour son mappage et continue de suivre les métriques de l'équipement par adresse MAC.

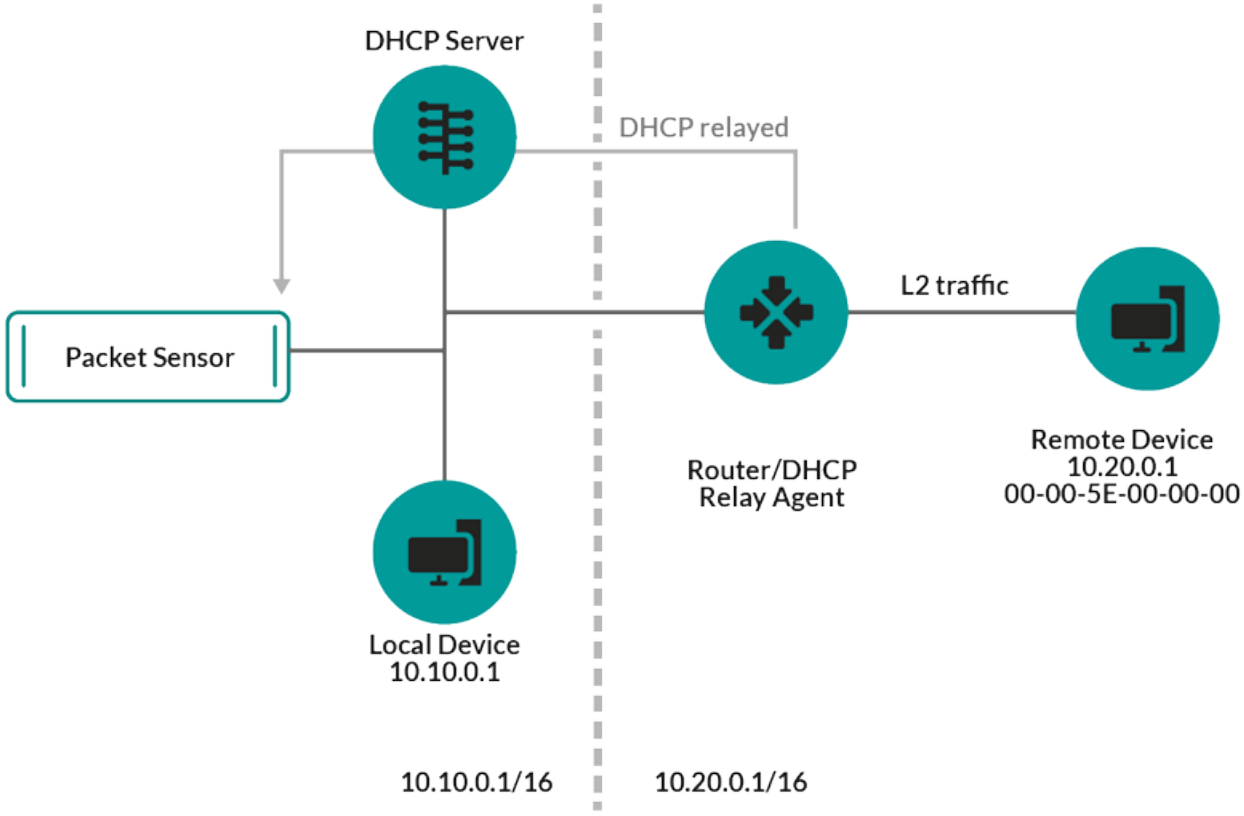


Figure 1: L'adresse MAC et l'adresse IP de l'équipement distant sont découvertes.

Si aucun agent de relais DHCP n'est configuré, les périphériques distants peuvent être découverts par leur adresse IP via Découverte L3 à distance.

L3 Discovery

Dans L3 Discovery, le système ExtraHop crée et lie deux entrées pour chaque équipement local découvert : une entrée parent L2 avec une adresse MAC et une entrée enfant L3 avec les adresses IP et l'adresse MAC.

Voici quelques considérations importantes concernant la découverte de la L3 :

- Si le proxy ARP est activé sur un routeur, le système ExtraHop crée un équipement L3 pour chaque adresse IP pour laquelle le routeur répond aux demandes ARP.
- Si un proxy ARP est configuré sur votre réseau, le système ExtraHop peut détecter automatiquement les appareils distants.
- Les métriques L2 qui ne peuvent pas être associées à un équipement enfant L3 particulier (par exemple, le trafic de diffusion L2) sont associées à l'équipement parent L2.

Découverte L3 à distance

Si le système ExtraHop détecte une adresse IP à laquelle aucun trafic ARP ou NDP n'est associé, cet équipement est considéré comme un équipement distant. Les appareils distants ne sont pas automatiquement découverts, mais vous pouvez ajouter une plage d'adresses IP distantes et découvrir les appareils situés en dehors du réseau local. Une entrée d'équipement est créée pour chaque adresse IP observée dans la plage d' adresses IP distantes. (Les appareils distants ne possèdent pas d'entrées parent L2.)

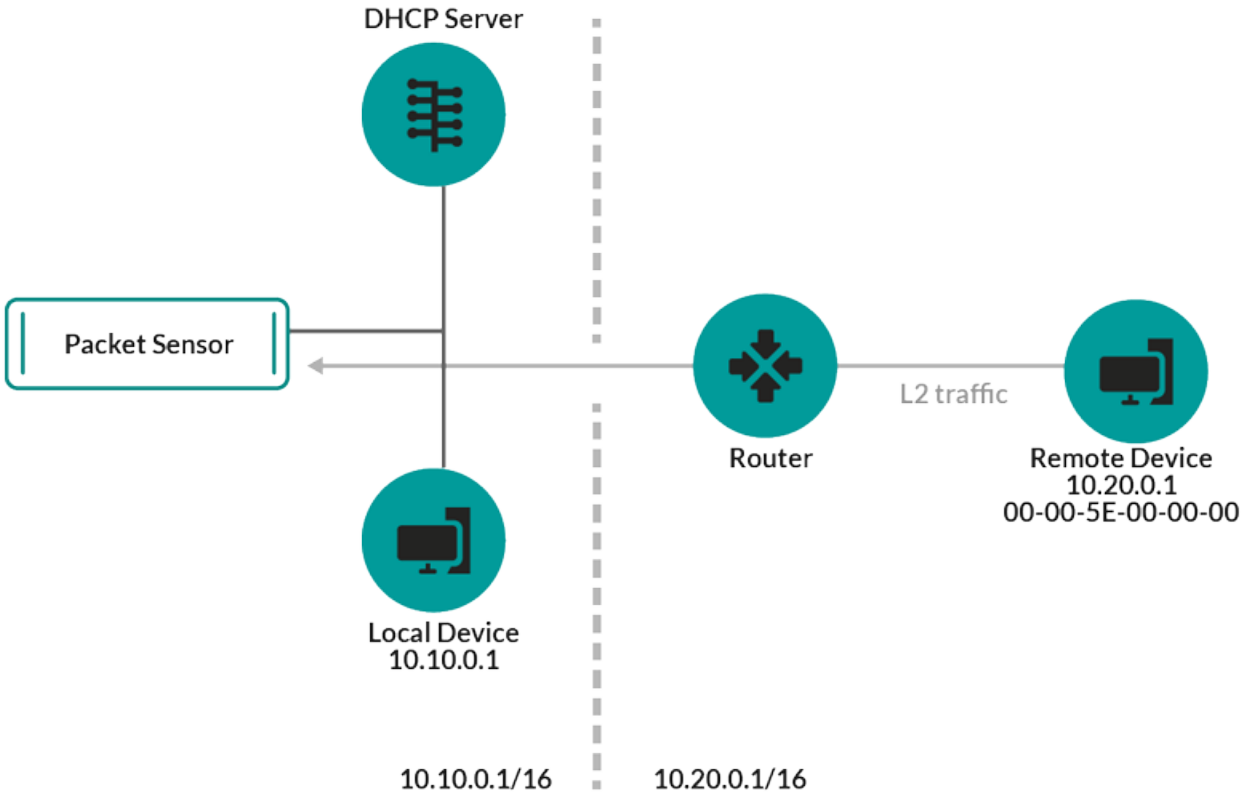


Figure 2: Seule l'adresse IP de l'équipement distant est découverte.

Voici quelques recommandations concernant le moment où configurer Remote L3 Discovery :

- Les appareils de vos clients se trouvent sur un segment du réseau qui n'est pas directement connecté.
- Votre organisation dispose d'un bureau distant sans système ExtraHop sur site, mais les utilisateurs de ce site accèdent aux ressources du centre de données central qui sont directement surveillées par un système ExtraHop . Les adresses IP du site distant peuvent être découvertes en tant que périphériques.
- Un service cloud ou un autre type de service hors site héberge vos applications distantes et possède une plage d'adresses IP connue. Les serveurs distants compris dans cette plage d'adresses IP peuvent être suivis individuellement.

Découverte du VPN
Découverte du VPN permet au système ExtraHop de corréler les adresses IP privées RFC-1918 attribuées aux clients VPN avec leurs adresses IP externes publiques. Cette visibilité accrue sur le trafic nord-sud réduit les obstacles lors de l'enquête sur les incidents de sécurité et les problèmes de performance impliquant des clients VPN externes. (Cette fonctionnalité nécessite une passerelle VPN assignée manuellement par l'utilisateur.)

Déduplication des trames logicielles

Le système ExtraHop supprime les trames et paquets L2 et L3 dupliqués lorsque les métriques sont collectées et agrégées à partir de l'activité de votre réseau par défaut.

Le État de santé du système La page contient des graphiques qui affichent les paquets dupliqués L2 et L3 qui ont été supprimés par le système ExtraHop. La déduplication fonctionne par défaut sur les ports 10 Gbit/s.

déduplication L2

La déduplication L2 supprime les trames Ethernet identiques, où l'en-tête Ethernet et la charge utile doivent correspondre. Le système ExtraHop vérifie la présence de doublons et supprime uniquement le paquet immédiatement précédent dans le monde entier si le doublon arrive à moins d'une milliseconde du paquet d'origine. La duplication L2 n'existe généralement que si le même paquet est vu dans le flux de données, ce qui est généralement lié à un problème de port de duplication.

déduplication L3

La déduplication L3 supprime les paquets TCP ou UDP avec des champs d'identification d'adresse IP identiques sur le même flux, où seul le paquet IP doit correspondre. Le contenu de tous les en-têtes qui précèdent l' en-tête IP en cours de vérification peut être différent. La déduplication L3 n'est actuellement prise en charge que pour IPv4, et non pour IPv6. Le système ExtraHop recherche les doublons et supprime uniquement le paquet immédiatement précédent du flux si le doublon arrive à moins d'une milliseconde du paquet d'origine et si le paquet se déplace dans la même direction. Pour qu'un paquet soit dédupliqué, aucun autre paquet ne peut être reçu entre les deux paquets dupliqués. En outre, les paquets doivent avoir la même longueur et le même champ d'identification d'adresse IP, et les paquets TCP doivent également avoir la même somme de contrôle TCP.

Par défaut, les flux entre les VLAN sont activés, et comme la déduplication L3 fonctionne sur une base par flux, la déduplication L3 supprime le même paquet traversant différents VLAN. La déduplication L3 est souvent le résultat de la mise en miroir du même trafic sur plusieurs interfaces du même routeur, et ce trafic peut apparaître sous forme de retransmissions TCP superflues dans le système ExtraHop.

Détection des menaces

Le système ExtraHop offre à la fois un apprentissage automatique et des fonctionnalités basées sur des règles détections qui identifient les menaces actives ou potentielles, les faiblesses du réseau vulnérables aux exploits et les configurations sous-optimales susceptibles de dégrader les performances du réseau.

En outre, graphiques, visualisations, et cartes d'activité des équipements permettre une chasse proactive aux menaces.

Réglage de la détection

Réduisez le bruit et faites uniquement apparaître les détections critiques en ajoutant des informations sur votre réseau qui permettent d'identifier les paramètres connus tels que les domaines fiables et les scanners de vulnérabilités.

En outre, vous pouvez créer des règles d'exceptions qui masquent des détections ou des participants spécifiques et réduisent davantage les bruits indésirables.

Localité du réseau

Par défaut, tout équipement doté d'une adresse IP RFC1918 (incluse dans un bloc CIDR 10/8, 172.16/12 ou 192.168/16) est classé sur le système en tant que périphérique interne.

Cependant, étant donné que certains environnements réseau incluent des adresses IP non conformes à la RFC1918 dans leur réseau interne, vous pouvez modifier la classification interne ou externe des adresses IP depuis la page Localités du réseau.

Renseignements sur les menaces

Le système ExtraHop comprend des renseignements sur les menaces flux d'ExtraHop et Crowdstrike Falçon qui sont mis à jour via le cloud à mesure que de nouvelles menaces sont découvertes. Vous pouvez également ajouter des collections de menaces auprès d'un tiers.

Exposés sur les menaces

Exposés sur les menaces fournir des informations sur les menaces imminentes qui ciblent les réseaux. Les détections mises à jour, les requêtes ciblées sur les enregistrements et les paquets, ainsi que les appareils

concernés sont présentés comme point de départ de votre investigation, accessibles depuis le Aperçu de la sécurité page.

Intégrations
RevealX 360 propose plusieurs intégrations tierces qui peuvent améliorer la gestion de la détection et des réponses et fournir une meilleure visibilité sur le trafic réseau.

Cortex XSOAR

Exportez les détections ExtraHop, exécutez des playbooks de réponse et interrogez les détails de l'équipement dans Cortex XSOAR.

Crowd Strike

Consultez les détails sur les appareils CrowdStrike et conservez ces appareils depuis le système ExtraHop.

Microsoft 365

Importez les détections et les événements Microsoft 365, surveillez les mesures Microsoft 365 dans des tableaux de bord intégrés et affichez les détails des événements à risque dans les enregistrements.

Décryptage du protocole Microsoft

Déchiffrez le trafic via les protocoles Microsoft tels que LDAP, RPC, SMB et WSMan pour améliorer la détection des attaques de sécurité dans votre environnement Microsoft Windows.

QRadar

Exportez et visualisez les détections ExtraHop dans votre QRadar SIEM.

Solution SIEM de sécurité d'entreprise Splunk

Exportez et visualisez les détections ExtraHop dans votre Splunk SIEM.

Splunk SOAR

Exportez et visualisez les détections, les métriques et les paquets ExtraHop dans votre solution Splunk SOAR.

Naviguer dans le système ExtraHop

Le système ExtraHop permet d'accéder aux données d'activité du réseau et aux détails de détection via une interface utilisateur dynamique et hautement personnalisable.

Ce guide fournit une vue d'ensemble de la navigation globale ainsi que des commandes, des champs et des options disponibles dans l'ensemble du système. Voir Présentation du système ExtraHop pour savoir comment le système ExtraHop collecte et analyse vos données.

Vidéos: Consultez la formation associée : Parcours d'apprentissage complet des fondamentaux de l'interface utilisateur

Navigateurs pris en charge

Les navigateurs suivants sont compatibles avec tous les systèmes ExtraHop. Appliquez les fonctionnalités d'accessibilité et de compatibilité fournies par votre navigateur pour accéder au contenu par le biais d'outils technologiques d'assistance.

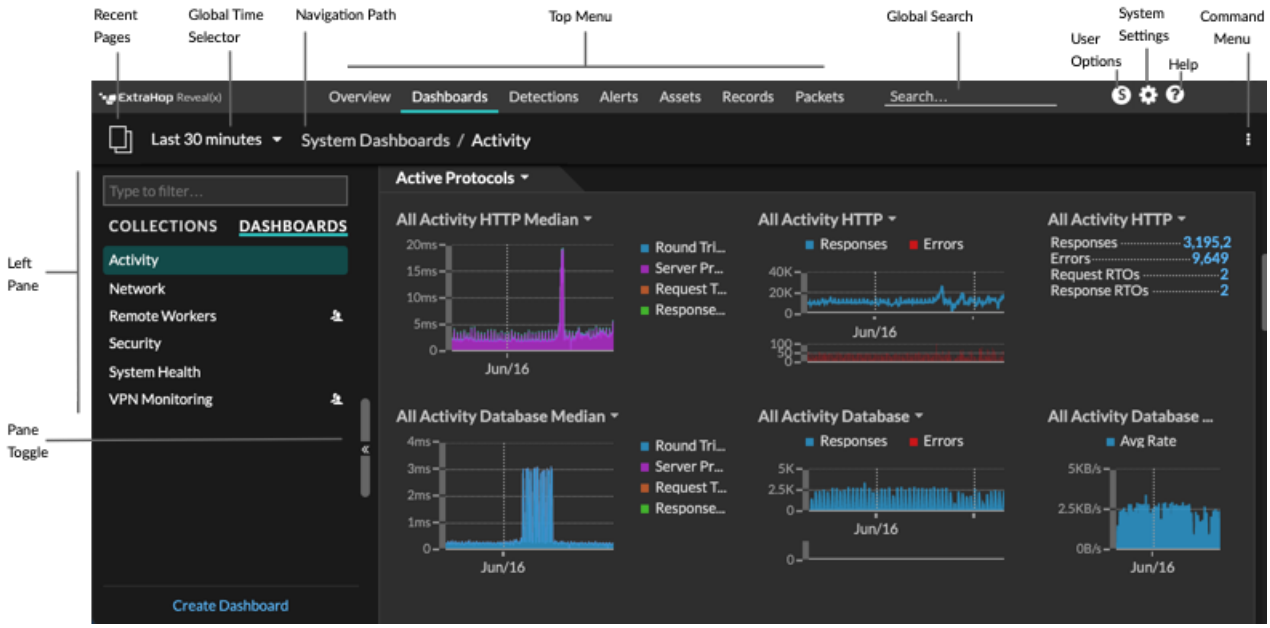
- Firefox
- Google Chrome
- Microsoft Edge
- Safari

Important: Internet Explorer 11 n'est plus pris en charge. Nous vous recommandons d' installer la dernière version de tout navigateur compatible.

Disposition et menus

Les éléments de navigation globale sont situés en haut de la page et contiennent des liens vers les principales sections du système. Dans chaque section, le volet de gauche contient des liens vers des pages ou des données spécifiques.

La figure suivante montre à la fois les éléments de navigation globaux et du volet gauche.



Voici les définitions de chaque élément de navigation global :

Pages de présentation

Les pages de présentation vous permettent d'évaluer rapidement l'étendue des activités suspectes sur votre réseau, d'en savoir plus sur l'activité du protocole et les connexions des équipements, et d'étudier le trafic entrant et sortant sur votre réseau.

- Consultez le Aperçu de la sécurité pour obtenir des informations sur les détections de sécurité sur votre réseau.
- Consultez le Vue d'ensemble du réseau pour obtenir des informations sur les appareils actifs de votre réseau.
- Consultez le Vue d'ensemble du périmètre pour obtenir des informations sur le trafic entrant et sortant de votre réseau.

Tableaux de bord

Cliquez **Tableaux de bord** pour afficher, créer ou partager des tableaux de bord afin de surveiller tous les aspects de votre réseau ou de vos applications. Tableaux de bord du système vous offrent un aperçu instantané de l'activité et des menaces de sécurité potentielles sur votre réseau.

Alertes

Cliquez **Alertes** pour afficher les informations relatives à chaque alerte générée pendant l'intervalle de temps.

Détections

Si votre paquet ou flux sonde est connecté au service d'apprentissage automatique ExtraHop, la navigation de niveau supérieur affiche **Détections** menu. Cliquez **Détections** pour consulter les détections identifiées à partir de vos données Wire Data. Vous pouvez accéder aux détections enregistrées même si sonde est déconnecté du service d'apprentissage automatique.

Note: Les détections par apprentissage automatique nécessitent connexion aux services cloud ExtraHop.

Actifs

Cliquez **Actifs** pour trouver n'importe quelle application, réseau ou équipement découvert par le système ExtraHop. Vous pouvez consulter les mesures de protocole relatives à vos actifs, à vos utilisateurs actifs ou à l'activité réseau par protocole.

Disques

Si votre système ExtraHop est configuré avec espace de stockage des enregistrements, la navigation de niveau supérieur affiche le menu Enregistrements. Cliquez **Disques** pour rechercher tous les enregistrements stockés pour l' intervalle de temps actuel. Les enregistrements sont des informations structurées sur les transactions, les messages et les flux réseau.

Paquets

Si votre système ExtraHop est configuré avec stockage des paquets, la navigation de niveau supérieur affiche le menu Paquets. Cliquez **Paquets** pour rechercher tous les paquets stockés pour l' intervalle de temps actuel.

champ de recherche global

Tapez le nom de n'importe quel équipement, nom d'hôte ou adresse IP, application ou réseau pour trouver une correspondance sur votre sonde ou console. Si vous avez un espace de stockage des enregistrements connecté, vous pouvez rechercher des enregistrements enregistrés. Si vous avez un système de stockage des paquets connecté, vous pouvez rechercher des paquets.

Icône d'aide

Consultez les informations d'aide relatives à la page que vous êtes en train de consulter. Pour accéder à la documentation ExtraHop la plus récente et la plus complète, visitez le Site de documentation ExtraHop.

Icône des paramètres système

Accédez aux options de configuration du système, telles que les déclencheurs, les alertes, les rapports planifiés et les appareils personnalisés, puis cliquez pour afficher le système ExtraHop et sa version. Cliquez **Avis relatifs au système** pour afficher la liste des fonctionnalités de la version la plus récente et de toutes notifications relatives au système telles que les licences expirant ou les mises à niveau du microprogramme disponibles.

Icône d'option utilisateur

Connectez-vous et déconnectez-vous de votre sonde ou console, modifiez votre mot de passe, sélectionnez le thème d'affichage, définir une langue, et accédez aux options de l'API.

Basculement du volet

Réduisez ou agrandissez le volet de gauche.

sélecteur de temps global

Modifier l'intervalle de temps pour afficher l'activité des applications et du réseau observée par le système ExtraHop pendant une période donnée. L'intervalle de temps global est appliqué à toutes les mesures du système et ne change pas lorsque vous naviguez sur différentes pages.

Pages récentes

Consultez la liste des dernières pages que vous avez visitées dans un menu déroulant et faites une sélection pour revenir à la page précédente. Les pages répétées sont dédupliquées et condensées pour économiser de l'espace.

Trajectoire de navigation

Affichez où vous vous trouvez dans le système et cliquez sur le nom d'une page dans le chemin pour revenir à cette page.

Menu déroulant des commandes

Cliquez pour accéder à des actions spécifiques pour la page que vous consultez. Par exemple, lorsque vous cliquez **Tableaux de bord** en haut de la page, le menu de commandes ⋮ propose des actions permettant de modifier les propriétés du tableau de bord ou de créer un nouveau tableau de bord.

Commencez à analyser les données

Commencez votre parcours d'analyse de données avec le système ExtraHop en suivant les flux de travail de base répertoriés ci-dessous. Au fur et à mesure que vous vous familiariserez avec le système ExtraHop, vous pourrez effectuer des tâches plus avancées, telles que l'installation de bundles et la création de déclencheurs.

Voici quelques méthodes de base pour naviguer et utiliser le système ExtraHop pour analyser l' activité du réseau.

Surveillez les métriques et étudiez les données intéressantes

Les bons points de départ sont tableau de bord de l'activité réseau et tableau de bord des performances du réseau, qui vous présentent des résumés des indicateurs importants relatifs aux performances des applications sur votre réseau. Lorsque vous constatez un pic de trafic, des erreurs ou le temps de traitement du serveur, vous pouvez interagir avec les données du tableau de bord pour approfondissez et identifiez quels clients, serveurs, méthodes ou autres facteurs ont contribué à cette activité inhabituelle.

Vous pouvez ensuite poursuivre le suivi des performances ou le dépannage en création d'un tableau de bord personnalisé pour suivre un ensemble de mesures et d' appareils intéressants.

Consultez ce qui suit procédures pas à pas pour en savoir plus sur la surveillance des données dans les tableaux de bord :

- Surveillez les performances du site Web dans un tableau de bord
- Surveiller les erreurs DNS dans un tableau de bord

- Surveiller l'état de la base de données dans un tableau de bord

Recherchez un équipement spécifique et étudiez les métriques et les transactions associées

Si vous souhaitez étudier un serveur lent, vous pouvez recherchez le serveur dans le système ExtraHop par nom d'équipement ou adresse IP puis examinez l'activité du serveur sur une page de protocole. Y a-t-il eu une augmentation du nombre d'erreurs de réponse ou de demandes ? Le temps de traitement du serveur était-il trop long ou la latence du réseau a-t-elle affecté le taux de transfert de données ? Cliquez sur différents protocoles sur la page Appareils pour étudier d'autres données métriques collectées par le système ExtraHop. Exploration par adresses IP homologues pour voir à quels clients ou applications le serveur a communiqué.

Si votre système ExtraHop est connecté à un espace de stockage des enregistrements, vous pouvez examiner l'intégralité des transactions auxquelles le serveur a participé en création d'une requête d'enregistrement.

Consultez ce qui suit procédures pas à pas pour en savoir plus sur l'exploration des indicateurs et des enregistrements :

- Explorez les métriques du système ExtraHop pour étudier les défaillances du DNS
- Interrogez les enregistrements pour trouver les ressources Web manquantes

Obtenez de la visibilité sur les modifications apportées à votre réseau en recherchant l'activité du protocole

Vous pouvez obtenir une vue de haut en bas de votre réseau en consultant les groupes de protocoles intégrés. Un groupe de protocoles est un ensemble d'appareils automatiquement regroupés par le système ExtraHop en fonction du trafic de protocole observé sur le fil. Par exemple, vous pouvez trouver des serveurs nouveaux ou mis hors service qui communiquent activement via un protocole en création d'une carte d'activités.

Si vous trouvez un ensemble d'appareils que vous souhaitez continuer à surveiller, vous pouvez ajouter une étiquette d'équipement ou nom de l'équipement personnalisé pour que ces appareils soient plus faciles à trouver dans le système ExtraHop. Vous pouvez également créer un groupe d'équipements personnalisé ou un tableau de bord personnalisé pour surveiller l'activité d'un groupe déquipements.

Flux de travail avancés pour personnaliser votre système ExtraHop

Une fois familiarisé avec les flux de travail de base, vous pouvez personnaliser votre système ExtraHop en configurant des notifications d'alerte, en créant des métriques personnalisées ou en installant des offres groupées.

Configurer des alertes

Alertes suivez les mesures spécifiées pour vous informer des écarts de trafic susceptibles d'indiquer un problème avec un équipement réseau. Configuration d'une alerte de seuil pour vous avertir lorsqu'une métrique surveillée dépasse une valeur définie. Configuration d'une alerte de tendance pour vous avertir lorsqu'une métrique surveillée s'écarte des tendances normales observées par le système.

Créez un déclencheur pour créer des mesures et des applications personnalisées

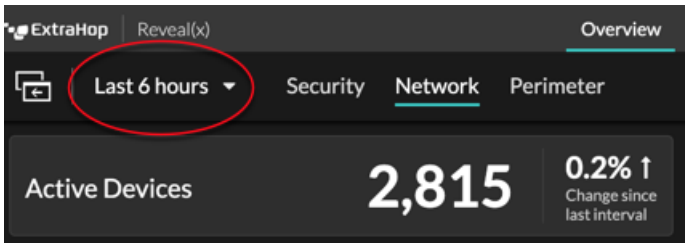
éléments déclencheurs sont des scripts personnalisés qui exécutent une action lors d'un événement prédéfini. Les déclencheurs nécessitent une planification pour s'assurer qu'ils n'ont pas d'impact négatif sur les performances du système.

Consultez ce qui suit procédures pas à pas pour en savoir plus sur l'exploration des métriques et des enregistrements :

- Créez un déclencheur pour collecter des métriques personnalisées pour les erreurs HTTP 404
- Créez un déclencheur pour surveiller les réponses aux requêtes NTP monlist

Intervalles de temps

Le sélecteur de temps est affiché dans le coin supérieur gauche de la barre de navigation et contrôle l'intervalle de temps global pour les métriques et les détections affichées dans le système ExtraHop.



Voici quelques considérations relatives aux intervalles de temps :

- Le sélecteur de temps vous permet de sélectionner un intervalle de temps global relatif, tel que le dernier jour, ou de définir une plage horaire personnalisée.
- Le sélecteur de temps vous permet de modifiez manuellement le fuseau horaire affiché.
- L'intervalle de temps sélectionné reste le même, qu'il s'agisse de consulter des statistiques dans un tableau de bord ou d' enquêter sur des détections, jusqu'à ce que vous modifiiez l'intervalle ou que vous accédiez à une page avec un intervalle de temps prédéfini, tel que les détails de détection ou les informations sur les menaces.
- Si un intervalle de temps relatif est sélectionné lorsque vous vous déconnectez, le système ExtraHop utilise par défaut cet intervalle de temps relatif lorsque vous vous reconnectez.
- Si une plage de temps personnalisée est sélectionnée lorsque vous vous déconnectez, le système ExtraHop utilise par défaut le dernier intervalle de temps relatif que vous avez consulté lors de la session de connexion précédente.
- Vous pouvez accéder aux cinq intervalles de temps uniques les plus récents à partir du **L'histoire** onglet du sélecteur de temps.
- L'intervalle de temps est inclus à la fin de l'URL dans votre navigateur. Pour partager un lien avec d'autres personnes respectant un intervalle de temps spécifique, copiez l'URL complète. Pour maintenir un intervalle de temps spécifique après la déconnexion du système ExtraHop, ajoutez l'URL à vos favoris.

Modifier l'intervalle de temps

Cette procédure explique comment définir l'intervalle de temps global. Vous pouvez également appliquer un intervalle de temps par tableau de bord ou par région.

1. Cliquez sur l'intervalle de temps dans le coin supérieur gauche de la page (par exemple **Les 30 dernières minutes**).
2. Sélectionnez l'une des options d'intervalle suivantes :
   - Un intervalle de temps prédéfini (tel que **Les 30 dernières minutes**, **Les 6 dernières heures**, **Dernier jour**, ou **La semaine dernière**).
   - Une unité de temps personnalisée.
   - Une plage horaire personnalisée. Cliquez sur un jour pour spécifier la date de début de la plage. Un seul clic permet de spécifier un seul jour. Cliquez sur un autre jour pour spécifier la date de fin de la plage.
   - Comparez les deltas métriques à partir de deux intervalles de temps différents.
3. Cliquez **Enregistrer**.

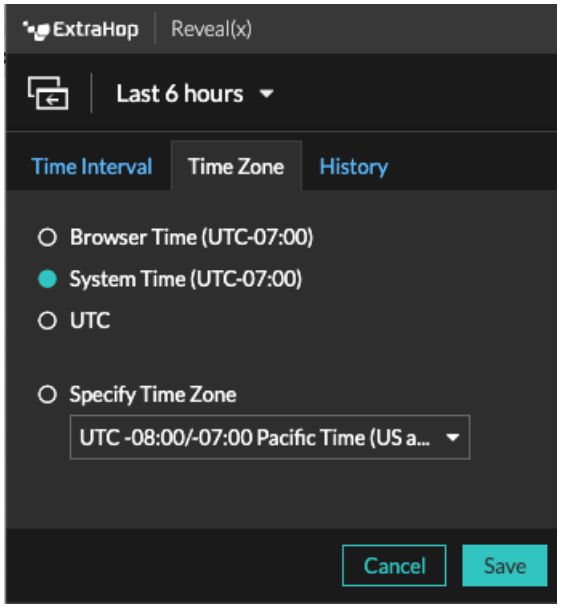
Conseil Vous pouvez également définir l'intervalle de temps à partir du **L'histoire** onglet en sélectionnant un maximum de cinq intervalles de temps récents définis lors d'une session de connexion précédente.

Modifier le fuseau horaire affiché

Le sélecteur de temps vous permet de modifier le fuseau horaire affiché dans le système ExtraHop, offrant ainsi une plus grande flexibilité lors de l'affichage de données temporelles telles que les métriques, les détections et les enregistrements dans des environnements couvrant plusieurs fuseaux horaires.

Voici quelques considérations concernant l'affichage des paramètres horaires dans RevealX 360 :

- La modification du fuseau horaire affiché affecte les horodatages que vous voyez dans le système ExtraHop, mais ne s'applique pas aux rapports planifiés ni aux tableaux de bord exportés.
- La modification de votre fuseau horaire remplace l'heure d'affichage par défaut configurée dans les paramètres d'administration. Voir Heure du système (pour ExtraHop Performance et RevealX Enterprise) ou Configurer l'heure du système (pour RevealX 360) pour plus d'informations.

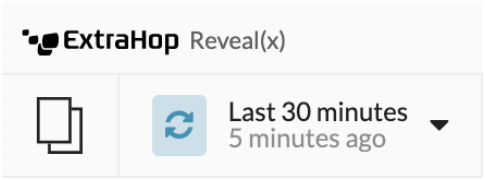


1. <extrahop-hostname-or-IP-address>Connectez-vous au système ExtraHop via https ://.
2. Cliquez sur le sélecteur de temps dans le coin supérieur gauche de la page.
3. Cliquez **Fuseau horaire**.
4. Sélectionnez l'une des options suivantes :
   - **Heure du navigateur**
   - **Heure du système**
   - **UTC**
   - **Spécifier le fuseau horaire** puis sélectionnez un fuseau horaire dans la liste déroulante.
5. Cliquez **Enregistrer**.

Afficher les dernières données pour un intervalle de temps

Les pages qui affichent les données métriques surveillées, telles que les tableaux de bord et les pages de protocole, sont continuellement mises à jour pour afficher les données les plus récentes pour l'intervalle de temps sélectionné.

Les pages de mesures détaillées, les détections, les enregistrements, les paquets et les alertes sont rechargées sur demande en cliquant sur l'icône d'actualisation des données dans le coin supérieur gauche de la page.



Modifier la granularité des données du graphique

Le système ExtraHop stocke les métriques par tranches de 30 secondes. Les données métriques sont ensuite agrégées ou regroupées dans des tranches supplémentaires de cinq minutes et d'une heure. L'agrégation des données permet de limiter le nombre de points de données affichés sur un graphique chronologique afin de faciliter l'interprétation de la granularité des données. L'intervalle de temps que vous sélectionnez détermine la meilleure agrégation, ou agrégation, des données à afficher dans un graphique pour la période que vous consultez.

Par exemple, si vous sélectionnez un intervalle de temps important, par exemple une semaine, les données métriques sont agrégées sous forme de cumuls d'une heure. Sur l'axe X d'un graphique en courbes, vous voyez un point de données pour chaque heure au lieu d'un point de données pour toutes les 30 secondes. Si vous souhaitez augmenter le niveau de granularité, vous pouvez zoomer sur un graphique ou modifier l'intervalle de temps.

Le système ExtraHop inclut des métriques intégrées de haute précision avec des cumuls d'une seconde, à savoir les métriques Network Bytes et Network Packets. Ces métriques sont associées à un équipement ou à une source de capture réseau. Pour plus d'informations sur la façon d'afficher ces statistiques dans un graphique, voir Afficher le taux maximum dans un graphique.

Le système ExtraHop inclut également des métriques intégrées permettant d'identifier la milliseconde de trafic la plus chargée en une seconde. Ces mesures, qui sont le nombre maximal d'octets réseau par milliseconde et le nombre maximal de paquets par milliseconde, sont associées à une source de capture réseau et vous aident à détecter les microrafales. Les microrafales sont des rafales de trafic rapides qui se produisent en quelques millisecondes.

Le tableau suivant fournit des informations sur la manière dont les données sont agrégées en fonction de l'intervalle de temps.

Intervalle de temps	Roll Up d'agrégation (si disponible)	Remarques

Moins de six minutes	1 seconde	Un récapitulatif d'une seconde n'est disponible que pour les métriques personnalisées et pour les métriques intégrées suivantes :
		• Source du réseau :
		  • Octets réseau (débit total)
		  • Paquets réseau (nombre total de paquets)
		  • Nombre maximal d'octets réseau par milliseconde

Intervalle de temps	Roll Up d'agrégation (si disponible)	Remarques

		• Nombre maximal de paquets réseau par milliseconde
		• Source de l'appareil :
		  • Octets réseau (débit entrant et sortant combiné par équipement)
		  • Nombre d'octets réseau entrants (débit entrant par équipement)
		  • Nombre d'octets réseau en sortie (débit sortant par équipement)
		  • Paquets réseau (paquets entrants et sortants combinés par équipement)
		  • Paquets réseau entrants (paquets entrants par équipement)
		  • Paquets réseau sortants (paquets sortants par équipement)

120 minutes ou moins	30 secondes	Si aucun roll up de 30 secondes n'est disponible, un roll up de 5 ou 60 minutes s' affiche.
Entre 121 minutes et 24 heures	5 minutes	Si le roll up de 5 minutes n'est pas disponible, un roll up de 60 minutes s'affiche.
Plus de 24 heures	60 minutes	—

Note: Si vous disposez d'une banque de données étendue configurée pour des métriques de 24 heures, un intervalle de temps spécifié de 30 jours ou plus affiche un cumul d'agrégation de 24 heures.

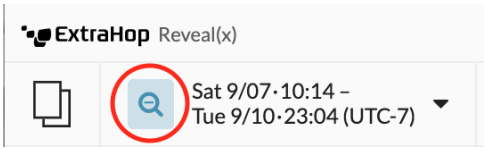
Zoomez sur une plage de temps personnalisée

Vous pouvez cliquer et faire glisser le pointeur sur un graphique pour zoomer sur une activité métrique intéressante. Cette plage de temps personnalisée est ensuite appliquée à l'ensemble du système ExtraHop, ce qui est utile pour étudier d'autres activités métriques survenues en même temps.

Le zoom sur une plage de temps n'est disponible que dans les graphiques dotés d'axes X et Y, tels que les graphiques linéaires, surfaciques, en chandeliers et en histogrammes.

1. Cliquez et faites glisser votre souris sur le graphique pour sélectionner une plage de temps. Si la plage de temps est inférieure à une minute, elle apparaît en rouge. Faites glisser la souris jusqu'à ce que la plage de temps apparaisse en vert.
2. Relâchez le bouton de la souris. Le graphique est redessiné selon la plage de temps personnalisée et l'intervalle de temps dans le coin supérieur droit de la barre de navigation est mis à jour.

3. Pour revenir de l'intervalle de temps personnalisé à l'intervalle de temps d'origine, cliquez sur l'icône d'annulation (une loupe avec un signe moins) qui s'affiche à côté de l'intervalle de temps dans le coin supérieur droit de la barre de navigation.

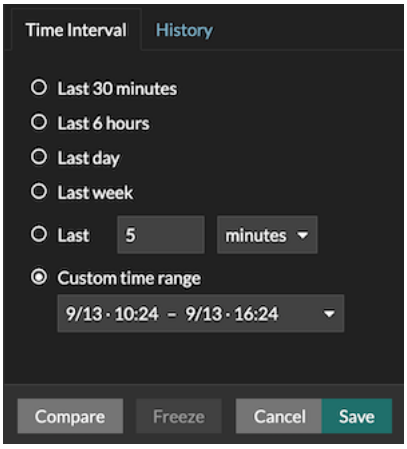


Conseil Sur une page de tableau de bord, vous pouvez limiter la plage de temps personnalisée du zoom avant à une région spécifique. Cliquez sur l'en-tête de la région, sélectionnez **Utiliser le sélecteur de temps par région**, puis zoomez sur un graphique. Chaque graphique ou widget de cette région est mis à jour selon la plage de temps personnalisée.

Gelez l'intervalle de temps pour créer une plage de temps personnalisée

Si vous voyez des données intéressantes sur une carte dactivités, un tableau de bord ou une page de protocole, vous pouvez figer l'intervalle de temps pour créer instantanément une plage de temps personnalisée. Le gel de l'intervalle de temps est utile pour créer des liens que vous pouvez partager avec d'autres personnes et pour étudier les activités métriques connexes survenues simultanément.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur le sélecteur d'heure dans le coin supérieur gauche de la page.
3. Sélectionnez un intervalle de temps prédéfini.
4. Cliquez **Congeler**.
   La plage horaire personnalisée est automatiquement mise à jour comme indiqué dans la figure ci-dessous. La plage commence à l'heure la plus proche de l'intervalle de temps précédent et se termine à l'heure à laquelle vous avez cliqué **Congeler**.



5. Cliquez **Enregistrer**.
   La nouvelle plage horaire personnalisée ne changera pas lorsque vous naviguerez dans le système ExtraHop. Vous pouvez partager ou ajouter l'URL à vos favoris dans votre navigateur.

   Note: L'intervalle de temps est inclus à la fin de l'URL dans votre navigateur. Pour partager un lien avec d'autres personnes respectant un intervalle de temps spécifique, copiez l'URL complète. La création d'un signet pour l'URL permet de conserver la plage de temps personnalisée même après votre déconnexion du système ExtraHop.
6. Pour supprimer la plage horaire personnalisée, modifier l'intervalle de temps.

Pages d'aperçu

Les pages de présentation vous permettent d'évaluer rapidement l'étendue des activités suspectes sur votre réseau, d'en savoir plus sur l'activité des protocoles et les connexions aux équipements, et d'étudier le trafic entrant et sortant sur votre réseau.

- Consultez le Aperçu de la sécurité pour obtenir des informations sur les détections de sécurité sur votre réseau.
- Consultez le Vue d'ensemble du réseau pour obtenir des informations sur les appareils actifs de votre réseau.
- Consultez le Vue d'ensemble du périmètre pour obtenir des informations sur le trafic entrant et sortant de votre réseau.

Aperçu de la sécurité

L'aperçu de la sécurité affiche plusieurs graphiques qui mettent en évidence les données sous différents angles concernant les détections. Ces graphiques peuvent vous aider à évaluer l'étendue des risques de sécurité, à lancer des enquêtes sur des activités inhabituelles et à atténuer les menaces de sécurité. Les détections sont analysées toutes les 30 secondes ou toutes les heures, selon la métrique.

Vidéos: Consultez la formation associée : Présentation de la sécurité, du réseau et du périmètre

Recommandé pour le triage

Ce graphique présente une liste des détections recommandées par ExtraHop sur la base d'une analyse contextuelle de votre environnement, également connue sous le nom de Smart Triage. Cliquez sur une détection pour afficher carte de détection dans Vue de triage sur la page Détections.

Enquêtes

Ce graphique fournit un décompte des enquêtes créées au cours de l' intervalle de temps sélectionné. Le décompte inclut les enquêtes recommandées par ExtraHop ou créées par les utilisateurs. Cliquez sur le graphique pour afficher tableau des enquêtes sur la page Détections.

Détections par catégorie d'attaque

Ce graphique fournit un moyen rapide de voir les types d'attaques susceptibles de menacer votre réseau et affiche le nombre de détections survenues dans chaque catégorie au cours de l'intervalle de temps sélectionné. Les actions relatives aux détections objectives sont répertoriées par type pour vous aider à hiérarchiser les détections les plus graves. Cliquez sur n'importe quel chiffre pour ouvrir une vue filtrée des détections correspondant à la valeur sélectionnée catégorie d'attaque.

Délinquants fréquents

Ce graphique montre les 20 appareils ou terminaux qui ont agi en tant que contrevenants lors d'une ou de plusieurs détections. Le système ExtraHop prend en compte le nombre de catégories d'attaques et de types de détection distincts, ainsi que les scores de risque des détections associés à chaque équipement afin de déterminer quels appareils sont considérés comme des récidivistes.

La taille de l' icône de rôle de l'équipement indique le nombre de types de détection distincts et la position de l'icône indique le nombre de catégories d'attaques distinctes. Cliquez sur l'icône d'un rôle pour afficher plus d'informations sur les catégories d'attaques et les types de détection associés à l'équipement. Cliquez sur le nom de l'équipement pour afficher propriétés de l'équipement.

Pour en savoir plus sur la sécurité du réseau, consultez le Tableau de bord Security Hardening.

Briefings sur les menaces

Les briefings sur les menaces fournissent des conseils actualisés dans le cloud concernant les événements de sécurité à l'échelle du secteur. En savoir plus sur les briefings sur les menaces.

Sélecteur de site et rapport sur les opérations de sécurité

Vous pouvez spécifier les sites dont vous souhaitez consulter les données sur cette page. Les utilisateurs ayant accès au module NDR peuvent générer un rapport sur les opérations de sécurité pour partager les résultats.

Sélecteur de site

Cliquez sur le sélecteur de site en haut de la page pour afficher les données d'un ou de plusieurs sites de votre environnement. Visualisez le trafic combiné sur vos réseaux ou concentrez-vous sur un seul site pour vous aider à trouver rapidement les données des équipements. Le sélecteur de site indique quand tous les sites ou certains sites sont hors ligne. Comme les données ne sont pas disponibles sur les sites hors ligne, les graphiques et les pages d'équipements associés aux sites hors ligne peuvent ne pas afficher de données ou n'afficher que des données limitées. Le sélecteur de site n'est disponible que depuis console.

(module NDR uniquement) Rapport sur les opérations de sécurité

Le rapport sur les opérations de sécurité contient un résumé des principales détections et des principaux risques auxquels votre réseau est exposé. Cliquez **Générer un rapport** pour spécifier le contenu du rapport, l'intervalle de temps et les sites à inclure dans le rapport, puis cliquez sur **Générez** pour créer un fichier PDF. Cliquez **Rapport sur le calendrier** pour créer un rapport sur les opérations de sécurité qui est envoyé par e-mail aux destinataires conformément la fréquence configurée.

Vue d'ensemble du réseau

L'aperçu du réseau affiche une carte des détections sur votre réseau et une liste des délinquants par nombre de détections. La vue d'ensemble du réseau actualise la carte de détection et les données sur les délinquants toutes les minutes.

Vidéos Consultez la formation associée : Présentation de la sécurité, du réseau et du périmètre

Basculer entre les catégories de détection

Vous pouvez basculer entre les vues qui affichent **Toutes les détections d'attaques** ou **Toutes les détections de performances**, en fonction des modules activés et de votre accès aux modules.

Délinquants en cours de détection

Cette liste répertorie les délinquants, triés selon le nombre de détections dans lesquelles l'équipement ou le point de terminaison a agi en tant que contrevenant.

Voici quelques moyens d'interagir avec la liste des délinquants :

- Cliquez sur un équipement ou un point de terminaison dans la liste pour mettre en évidence les détections associées dans la carte de détection et afficher les propriétés de l'équipement et les liens d'accès à recherche de point de terminaison sites, détections, enregistrements ou paquets.
- En fonction de la catégorie de détection sélectionnée et de votre module système, cliquez sur **Afficher toutes les détections d'attaques** ou **Afficher toutes les détections de performances** lien pour accéder au Détections page, filtré par catégorie de détection et groupé par source.
- Sélectionnez le **Afficher les détections sans victimes** case à cocher pour afficher les détections qui n'incluent pas de victime participante. Par exemple, les scans TLS et certaines détections d'avertissement en cas d'activité suspecte ne concernent qu'un délinquant.

Carte de détection

La carte de détection affiche le délinquant et la victime pour toutes les détections sélectionnées lors du basculement entre les catégories de détection.

Les cercles sont surlignés en rouge si l'équipement est apparu en tant que délinquant lors d' au moins une détection pendant l'intervalle de temps sélectionné et sont surlignés en bleu sarcelle si l' équipement est une victime.

Les participants sont connectés par des lignes étiquetées avec le type de détection ou le nombre de détections associés à la connexion, et les rôles des équipements sont représentés par une icône.

Voici quelques manières d'interagir avec la carte de détection :

- Cliquez sur un cercle pour afficher les propriétés de l'équipement et accéder aux liens vers recherche de point de terminaison sites, détections, enregistrements ou paquets.
- Cliquez sur une connexion pour afficher les détections associées.
- Passez la souris sur un cercle pour voir les étiquettes des équipements et surligner les connexions des appareils.

En savoir plus sur Détections.

Sélecteur de site et rapport sur les opérations de sécurité

Vous pouvez spécifier les sites dont vous souhaitez consulter les données sur cette page. Les utilisateurs ayant accès au module NDR peuvent générer un rapport sur les opérations de sécurité pour partager les résultats.

Sélecteur de site

Cliquez sur le sélecteur de site en haut de la page pour afficher les données d'un ou de plusieurs sites de votre environnement. Visualisez le trafic combiné sur vos réseaux ou concentrez-vous sur un seul site pour vous aider à trouver rapidement les données des équipements. Le sélecteur de site indique quand tous les sites ou certains sites sont hors ligne. Comme les données ne sont pas disponibles sur les sites hors ligne, les graphiques et les pages d'équipements associés aux sites hors ligne peuvent ne pas afficher de données ou n'afficher que des données limitées. Le sélecteur de site n'est disponible que depuis console.

(module NDR uniquement) Rapport sur les opérations de sécurité

Le rapport sur les opérations de sécurité contient un résumé des principales détections et des principaux risques auxquels votre réseau est exposé. Cliquez **Générer un rapport** pour spécifier le contenu du rapport, l'intervalle de temps et les sites à inclure dans le rapport, puis cliquez sur **Générez** pour créer un fichier PDF. Cliquez **Rapport sur le calendrier** pour créer un rapport sur les opérations de sécurité qui est envoyé par e-mail aux destinataires conformément la fréquence configurée.

Vue d'ensemble du périmètre

L'aperçu du périmètre affiche des graphiques et des visualisations interactives qui vous aident à surveiller le trafic entrant et sortant de votre réseau via des connexions avec des terminaux externes.

Vidéo: Consultez la formation associée : Présentation de la sécurité, du réseau et du périmètre

Trafic périmétrique

Les graphiques du trafic périmétrique fournissent une vue d'ensemble du trafic des équipements avec des connexions externes.

Trafic entrant

Ce décompte indique le volume total de trafic entrant pendant l' intervalle de temps sélectionné. Cliquez sur le nombre pour afficher la vitesse à laquelle les données sont transférées en provenance de terminaux externes et effectuez une analyse détaillée par site ou par conversation.

Trafic sortant

Ce décompte indique le volume total du trafic sortant pendant l' intervalle de temps sélectionné. Cliquez sur le nombre pour afficher la vitesse à laquelle les données sont transférées vers des terminaux externes et effectuez une analyse détaillée par site ou par conversation.

Appareils acceptant les connexions entrantes

Ce décompte affiche le nombre d'appareils qui ont accepté des connexions entrantes provenant de terminaux externes pendant l'intervalle de temps sélectionné. Cliquez sur le nombre pour ouvrir

une page de présentation des groupes déquipements qui affiche la liste des appareils, les données relatives au trafic et l'activité du protocole.

Connexions entrantes

Ce décompte affiche le nombre de connexions entrantes initiées par des terminaux externes. Cliquez sur le décompte pour accéder à une vue détaillée de ces conversations.

Connexions entrantes suspectes

Ce graphique affiche le nombre de connexions initiées par des terminaux externes suspects. ExtraHop identifie les terminaux suspects via renseignements sur les menaces données. Cliquez sur le graphique pour ouvrir une vue filtrée de ces conversations.

Connexions sortantes suspectes

Ce décompte affiche le nombre de connexions initiées par des terminaux internes avec des terminaux externes suspects. ExtraHop identifie les terminaux suspects via renseignements sur les menaces données. Cliquez sur le graphique pour ouvrir une vue filtrée de ces conversations.

Connexions peu communes

(RevealX 360 uniquement) Ce décompte affiche le nombre de connexions sortantes depuis votre réseau vers des adresses IP qui ne sont pas visitées normalement ou qui n'ont jamais été visitées par le passé. Cliquez sur le graphique pour ouvrir une vue filtrée de ces conversations.

Visualisation de Halo

La visualisation Halo fournit deux vues de vos connexions réseau à des points de terminaison externes : les services cloud et les téléchargements volumineux.

Les extrémités externes apparaissent sur l'anneau extérieur avec des connexions aux extrémités internes et apparaissent sous forme de cercles au milieu de la visualisation. Ces visualisations vous permettent de hiérarchiser vos investigation pour les connexions marquées par des détections à haut risque ou pour les appareils de grande valeur.

Pour aider à identifier les points finaux à fort trafic, la taille des cercles intérieurs et extérieurs augmente à mesure que le volume de trafic augmente. Dans certains cas, la taille des cercles intérieurs et des segments de l'anneau extérieur peut être augmentée pour des raisons de lisibilité. Cliquez sur un point de terminaison pour afficher des informations précises sur le trafic.

Cliquez **Services dans le cloud** pour visualiser les connexions entre les terminaux internes et les fournisseurs de services cloud. Les fournisseurs de services cloud et la quantité de données envoyées ou reçues apparaissent dans le panneau d'informations situé à droite. Vous pouvez basculer entre les vues qui affichent **Octets sortants** aux fournisseurs et **Octets entrants** à votre réseau.

Cliquez **Importations volumineuses** pour visualiser les connexions entre les points de terminaison internes et externes où plus de 1 Mo de données ont été transférés en une seule transmission depuis votre réseau vers un point de terminaison externe. Les points de terminaison externes et la quantité de données téléchargées apparaissent dans le panneau d'informations situé à droite.

Voici quelques manières d'interagir avec ces visualisations de halo :

- Passez la souris sur les points de terminaison ou les connexions pour afficher les noms d'hôte et les adresses IP disponibles.
- Passez la souris sur les points de terminaison ou les connexions pour mettre en surbrillance les éléments de liste correspondants sur la droite. De même, passez la souris sur les éléments de la liste pour mettre en évidence les points de terminaison et les connexions correspondants dans la visualisation du halo.
- Cliquez sur les extrémités ou les connexions dans la visualisation en halo pour maintenir le focus et afficher des informations précises sur le trafic et les liens correspondant à votre sélection sur la droite.
- Cliquez sur un point de terminaison externe dans la visualisation ou la liste du halo pour afficher le volume total de trafic entrant ou sortant associé au point de terminaison et aux points de terminaison internes connectés.

- Cliquez sur un point de terminaison interne dans la liste pour afficher les propriétés de l'équipement et accéder aux liens vers les informations associées, telles que les détections, les enregistrements ou les paquets.
- Cliquez sur la loupe à côté d'un point de terminaison dans la liste pour afficher les enregistrements associés à ce point de terminaison.
- Au bas de la liste des services cloud, basculez entre les vues qui affichent les octets sortants et les octets entrants sur votre réseau.
- Ajustez l'intervalle de temps pour afficher les connexions à des heures spécifiques, telles que les activités inattendues en soirée ou le week-end.

Visualisation de cartes

L'onglet Géolocalisation fournit une carte du monde du trafic entre les points de terminaison internes et les emplacements géographiques, qui sont surlignés dans une couleur contrastante sur la carte. L'intensité de la couleur contrastante représente le volume de trafic à cette géolocalisation. Les géolocalisations représentées sur la carte sont également répertoriées dans le volet droit.

Cliquez sur une géolocalisation surlignée sur la carte ou dans la liste pour afficher le volume total de trafic entrant ou sortant associé aux points de terminaison internes connectés.

Voici quelques moyens d'interagir avec les détails de géolocalisation et la visualisation de la carte :

- Cliquez sur un point de terminaison interne dans la liste pour afficher les propriétés de l'équipement et accéder aux liens vers les informations associées telles que les détections, les enregistrements ou les paquets.
- Cliquez sur la loupe à côté d'un point de terminaison dans la liste pour afficher les enregistrements associés au point de terminaison.
- Au bas de la liste, basculez entre les vues qui indiquent les octets sortants et les octets entrants sur votre réseau.
- Cliquez sur les commandes situées dans le coin inférieur droit de la carte pour zoomer ou dézoomer ou remettre la carte dans sa position initiale, ou vous pouvez faire pivoter la molette de votre souris.
- Cliquez et faites glisser votre souris sur la carte ou appuyez sur les touches fléchées de votre clavier pour repositionner la vue cartographique.
- Ajustez l'intervalle de temps pour visualiser le trafic à des heures précises, par exemple les activités inattendues le soir ou le week-end.

Sélecteur de site et rapport sur les opérations de sécurité

Vous pouvez spécifier les sites dont vous souhaitez consulter les données sur cette page. Les utilisateurs ayant accès au module NDR peuvent générer un rapport sur les opérations de sécurité pour partager les résultats.

Sélecteur de site

Cliquez sur le sélecteur de site en haut de la page pour afficher les données d'un ou de plusieurs sites de votre environnement. Visualisez le trafic combiné sur vos réseaux ou concentrez-vous sur un seul site pour vous aider à trouver rapidement les données des équipements. Le sélecteur de site indique quand tous les sites ou certains sites sont hors ligne. Comme les données ne sont pas disponibles sur les sites hors ligne, les graphiques et les pages d'équipements associés aux sites hors ligne peuvent ne pas afficher de données ou n'afficher que des données limitées. Le sélecteur de site n'est disponible que depuis console.

(module NDR uniquement) Rapport sur les opérations de sécurité

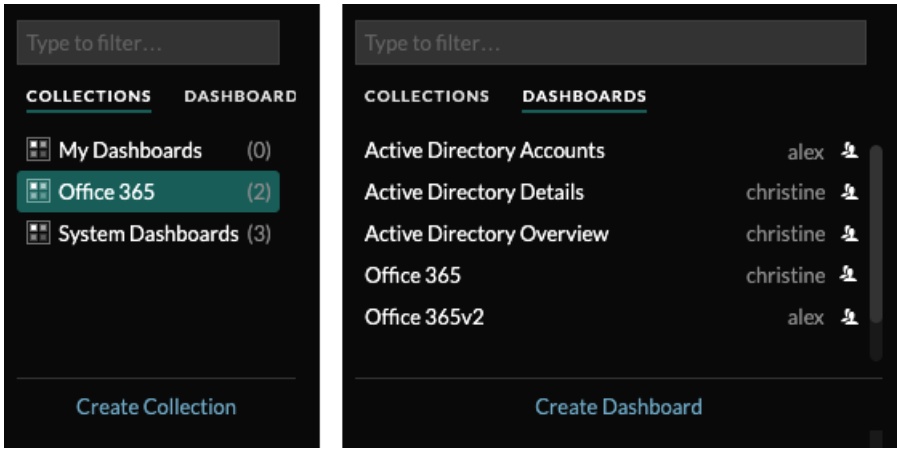
Le rapport sur les opérations de sécurité contient un résumé des principales détections et des principaux risques auxquels votre réseau est exposé. Cliquez **Générer un rapport** pour spécifier le contenu du rapport, l'intervalle de temps et les sites à inclure dans le rapport, puis cliquez sur **Générez** pour créer un fichier PDF. Cliquez **Rapport sur le calendrier** pour créer un rapport sur les opérations de sécurité qui est envoyé par e-mail aux destinataires conformément la fréquence configurée.

Tableaux de bord

Les tableaux de bord constituent un outil efficace pour surveiller le trafic réseau prioritaire ou résoudre les problèmes, car ils regroupent plusieurs graphiques métriques dans un emplacement central où vous pouvez étudier et partager des données. Vous pouvez également ajouter des zones de texte, mises en forme via Markdown, pour fournir du contenu aux parties prenantes.

Vidéo : Consultez la formation associée : Concepts relatifs aux tableaux

Les tableaux de bord et les collections se trouvent dans le dock du tableau de bord.



Cliquez **Collections** pour afficher toutes les collections de tableaux de bord que vous possédez ou qui ont été partagées avec vous. Le nombre de tableaux de bord de chaque collection est affiché. Cliquez sur le nom de la collection pour afficher le propriétaire, les personnes avec lesquelles la collection est partagée et la liste des tableaux de bord de la collection.

Seul le propriétaire de la collection peut modifier ou supprimer une collection. Toutefois, comme les tableaux de bord peuvent être ajoutés à plusieurs collections, vous pouvez créer une collection et partagez-le avec d'autres utilisateurs et groupes.

Cliquez **Tableaux de bord** pour afficher une liste alphabétique de tous les tableaux de bord que vous possédez ou qui ont été partagés avec vous, y compris les tableaux de bord partagés via une collection. Le propriétaire de chaque tableau de bord est affiché. Une icône à côté du nom du propriétaire indique que le tableau de bord a été partagé avec vous.

Création de tableaux de bord

Si vous souhaitez surveiller des mesures spécifiques ou personnalisées, vous pouvez créer un tableau de bord personnalisé. Vous devez disposer de privilèges d'écriture personnels ou supérieurs et d'un accès au module NPM pour créer et modifier des tableaux de bord.

Les tableaux de bord personnalisés sont stockés séparément pour chaque utilisateur qui accède au système ExtraHop. Après avoir créé un tableau de bord personnalisé, vous pouvez le partager avec d'autres utilisateurs d'ExtraHop.

Il existe plusieurs méthodes pour créer votre propre tableau de bord :

- Création d'un tableau de bord personnalisé ou créer un tableau de bord avec des sources dynamiques à partir de zéro
- Copier un tableau de bord existant, puis personnalisez-le
- Copier un graphique existant, puis enregistrez-le dans un nouveau tableau de bord

Les nouveaux tableaux de bord sont ouverts en mode Modifier la mise en page, ce qui vous permet d'ajouter, d'organiser et de supprimer des composants dans le tableau de bord. Après avoir créé un tableau de bord, vous pouvez effectuer les tâches suivantes :

- Ajouter ou supprimer des widgets et des régions
- Modifier une région
- Modifier un graphique
- Modifier une zone de texte

Cliquez sur le menu de commande ⋮ dans le coin supérieur droit de la page pour modifier les propriétés du tableau de bord ou supprimer le tableau de bord.

Note: Vous ne pouvez pas récupérer un tableau de bord supprimé. Lors de la suppression de comptes utilisateurs, les administrateurs d'ExtraHop peuvent transférer la propriété du tableau de bord à un autre utilisateur du système. Dans le cas contraire, tous les tableaux de bord personnalisés associés au compte utilisateur sont également supprimés. Pour préserver les tableaux de bord, faire une copie avant que le compte ne soit supprimé.

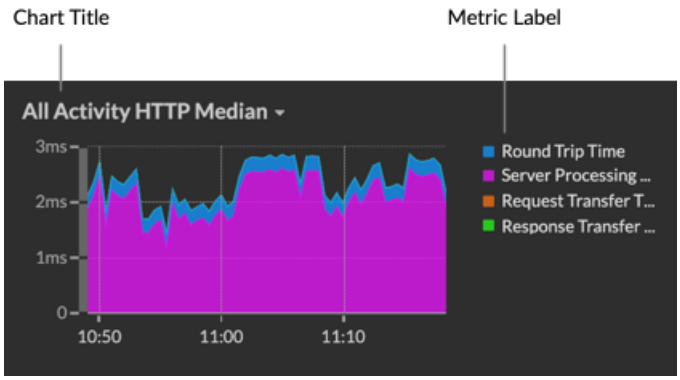
Découvrez comment surveiller votre réseau en réalisation d'une présentation détaillée d'un tableau de bord.

Affichage des tableaux de bord

Les tableaux de bord sont composés de widgets graphiques, de widgets d'alerte et de widgets de zone de texte qui peuvent présenter une vue concise des systèmes critiques ou des systèmes gérés par une équipe particulière.

Cliquez dans un graphique pour interagir avec les données métriques :

- Cliquez sur le titre d'un graphique pour afficher la liste des sources métriques et options de menu.
- Cliquez sur une étiquette métrique pour approfondissez et enquêter par un détail métrique.
- Cliquez sur le libellé d'une métrique, puis sur Maintenir le focus pour afficher uniquement cette métrique dans le graphique.
- Cliquez sur le titre d'un graphique ou sur une étiquette de mesure, puis sur Description pour en savoir plus sur la mesure source.
- Cliquez sur un marqueur de détection pour accéder à la page détaillée de la détection



Modifiez le sélecteur de temps pour observer l'évolution des données au fil du temps :

- Modifier l'intervalle de temps pour l'ensemble du tableau de bord
- Modifier l'intervalle de temps par région
- Zoomez sur un intervalle de temps dans un graphique
- Comparez le delta métrique de deux intervalles de temps dans un graphique

Exporter et partager les données du tableau de bord

Par défaut, tous les tableaux de bord personnalisés sont privés et aucun autre utilisateur d'ExtraHop ne peut consulter ou modifier votre tableau de bord.

Partagez votre tableau de bord pour accorder l'autorisation de consultation ou de modification à d'autres utilisateurs et groupes d'ExtraHop, ou partager une collection pour accorder une autorisation en lecture seule à plusieurs tableaux de bord.

Vous ne pouvez modifier un tableau de bord partagé que si le propriétaire vous a accordé l'autorisation de modification. Cependant, vous pouvez copier et personnaliser un tableau de bord partagé sans autorisation de modification.

Exportez les données par graphique individuel ou par tableau de bord complet :

- Pour exporter les données d'un graphique individuel, cliquez sur le titre du graphique et sélectionnez l'une des options suivantes dans le menu déroulant : Exporter au format CSV ou Exporter vers Excel.
- Pour présenter ou exporter l'intégralité du tableau de bord, cliquez sur le menu de commandes ⋮ dans le coin supérieur droit de la page et sélectionnez l'une des options suivantes : Mode de présentation, Exporter au format PDF ou Rapports planifiés (consoles uniquement).

Tableaux de bord du système

Le système ExtraHop fournit les tableaux de bord intégrés suivants qui affichent l'activité des protocoles courants concernant le comportement général et l'état de votre réseau.

Les tableaux de bord système se trouvent dans la collection de tableaux de bord système par défaut du dock des tableaux de bord et ne peuvent pas être ajoutés à une autre collection partagée avec d'autres utilisateurs.

Les tableaux de bord du système peuvent être consultés par n'importe quel utilisateur, à l'exception de utilisateurs restreints Le tableau de bord d'utilisation du système ne peut être consulté que par les utilisateurs utilisant l'administration du système et des accès privilèges.

tableau de bord de l'activité réseau (accès au module NPM requis)

Trouvez les meilleurs orateurs par protocole d'application (L7) et consultez les alertes récentes. Pour plus d'informations sur les graphiques de ce tableau de bord, voir tableau de bord de l'activité réseau.

tableau de bord des performances réseau (accès au module NPM requis)

Identifiez la latence du trafic et les goulots d'étranglement sur les couches de liaison de données (L2), de réseau (L3) et de transport (L4). Pour plus d'informations sur les graphiques de ce tableau de bord, voir tableau de bord des performances du réseau.

tableau de bord de renforcement de la sécurité (accès au module NDR requis)

Surveillez les informations générales relatives aux menaces de sécurité potentielles sur votre réseau. Pour plus d' informations sur les graphiques de ce tableau de bord, voir tableau de bord sur le renforcement de la sécurité.

Tableau de bord des outils d'IA générative

Vérifiez le trafic OpenAI sur votre réseau et depuis les points de terminaison internes communiquant via OpenAI. Pour plus d'informations sur les graphiques de ce tableau de bord, voir Tableau de bord des outils d'IA générative.

tableau de bord Active Directory

Suivez l'activité du serveur Kerberos pour les comptes d'utilisateurs et d'ordinateurs Active Directory ainsi que pour les services tels que le catalogue global et les politiques de groupe. Pour plus d'informations sur les graphiques de ce tableau de bord, voir tableau de bord Active Directory.

tableau de bord System Health

Assurez-vous que votre système ExtraHop fonctionne comme prévu, résolvez les problèmes et évaluez les domaines qui affectent les performances. Pour plus d'informations sur les graphiques de ce tableau de bord, voir tableau de bord de l'état du système.

tableau de bord de l'utilisation du système (privilèges d'administration du système et des accès requis)

Surveillez la façon dont les utilisateurs interagissent avec les détections, les enquêtes et les tableaux de bord du système ExtraHop. Pour plus d'informations sur les graphiques de ce tableau de bord, voir tableau de bord de l'utilisation du système.

tableau de bord de l'activité réseau

Le tableau de bord de l'activité réseau vous permet de surveiller les informations générales sur l'activité et les performances des applications depuis le transport via les couches d'application (L4 à L7) de votre réseau.

Chaque graphique du tableau de bord de l'activité réseau contient des visualisations des données métriques du réseau et du protocole qui ont été générées au cours du intervalle de temps sélectionné, organisé par région.

Note: Depuis une console, vous pouvez afficher le tableau de bord de l'activité réseau pour chaque site connecté. Le nom du site apparaît dans la barre de navigation ; cliquez sur la flèche vers le bas à côté du nom pour faire pivoter l'affichage vers d'autres sites.

Le tableau de bord Network Activity est un tableau de bord système intégré que vous ne pouvez pas modifier, supprimer ou ajouter à une collection partagée. Cependant, vous pouvez copier un graphique depuis le tableau de bord de l'activité réseau et ajoutez-le à un tableau de bord personnalisé, ou vous pouvez faire une copie du tableau de bord et modifiez-le pour surveiller les indicateurs qui vous concernent.

Les informations suivantes résument chaque région et ses cartes.

Vue d'ensemble du trafic

Vérifiez si les goulots d'étranglement du trafic sont liés à un protocole d'application spécifique ou à la latence du réseau . La région Aperçu du trafic contient les graphiques suivants :

- **Tableau du débit moyen des paquets réseau par protocole L7:** Trouvez le protocole qui a le plus grand volume de transmissions de paquets sur la couche application (L7) pendant l'intervalle de temps sélectionné.
- **Durée aller-retour du réseau All Activity:** La ligne du 95e percentile indique la plage supérieure du temps nécessaire aux paquets pour traverser le réseau. Si cette valeur est supérieure à 250 ms, des problèmes de réseau peuvent ralentir les performances de l'application. Le temps d'aller-retour est une mesure du temps entre le moment où un client ou un serveur a envoyé un paquet et celui où il a reçu un accusé de réception.
- **Alertes:** Consultez jusqu'à 40 des dernières alertes générées, ainsi que leur niveau de gravité. Les alertes sont des conditions configurées par l'utilisateur qui établissent des valeurs de référence pour des mesures de protocole spécifiques.

Protocoles actifs

Observez comment les performances des applications sont affectées par les protocoles qui communiquent activement sur le système ExtraHop. Par exemple, vous pouvez rapidement consulter les graphiques qui indiquent les temps de traitement des serveurs et le rapport entre les erreurs et les réponses par protocole.

Il existe un tableau pour chaque protocole actif. Si vous ne trouvez pas le protocole que vous attendiez, il est possible que les applications ne communiquent pas via ce protocole pour intervalle de temps sélectionné.

Pour plus d'informations sur les protocoles et pour consulter les définitions métriques, consultez le Référence des métriques du protocole ExtraHop.

tableau de bord des performances du réseau

Le tableau de bord des performances du réseau vous permet de surveiller l'efficacité de la transmission des données sur les couches de liaison de données, de réseau et de transport (L2 à L4).

Chaque graphique du tableau de bord des performances du réseau contient des visualisations des données de performance du réseau qui ont été générées au cours du intervalle de temps sélectionné, organisé par région.

Note: Depuis une console, vous pouvez afficher le tableau de bord des performances du réseau pour chaque site connecté. Le nom du site apparaît dans la barre de navigation ; cliquez sur la flèche vers le bas à côté du nom pour faire pivoter l'affichage vers d'autres sites.

Le tableau de bord Network Performance est un tableau de bord système intégré que vous ne pouvez pas modifier, supprimer ou ajouter à une collection partagée. Cependant, vous pouvez copier un graphique depuis le tableau de bord des performances du réseau et ajoutez le graphique à un tableau de bord personnalisé, ou vous pouvez faire une copie du tableau de bord et modifiez le tableau de bord pour suivre les indicateurs qui vous concernent.

Les informations suivantes résument chaque région.

Métriques du réseau L2

Surveillez les débits sur la couche de liaison de données (L2) par bits et par paquets, et surveillez les types de trames transmises. Vous pouvez également déterminer la quantité de données envoyée aux récepteurs par monodiffusion, diffusion ou distribution multicast.

Métriques du réseau L4

Surveillez la latence du transfert de données sur la couche de transport (L4). Visualisez l'activité TCP par le biais de métriques de connexion, de demande et de réponse. Ces données peuvent indiquer l' efficacité avec laquelle les données sont envoyées et reçues à travers la couche de transport de votre réseau.

Performances du réseau

Surveillez l'impact des performances du réseau sur les applications. Visualisez le débit global du réseau en examinant le débit par protocole d'application et l' ampleur des temps d'aller-retour TCP élevés.

Métriques du réseau L3

Visualisez le débit de données au niveau de la couche réseau (L3) et visualisez les paquets et le trafic par protocoles TCP/IP.

DSCP

Consultez la répartition des paquets et du trafic par points de code Differentiated Services, qui fait partie de l'architecture réseau DiffServ. Chaque paquet IP contient un champ pour exprimer la priorité de la manière dont le paquet doit être traité, ce que l' on appelle les services différenciés. Les valeurs des priorités sont appelées points de code.

Groupes de multidiffusion

Visualisez le trafic envoyé à plusieurs récepteurs lors d'une seule transmission, ainsi que les paquets et le trafic par chaque groupe de récepteurs. Le trafic de multidiffusion sur un réseau est organisé en groupes en fonction des adresses de destination.

Tableau de bord Security Hardening

Le tableau de bord Security Hardening vous permet de surveiller les informations générales relatives aux menaces de sécurité potentielles sur votre réseau.

Chaque graphique du tableau de bord Security Hardening contient des visualisations des données de sécurité qui ont été générées via intervalle de temps sélectionné, organisé par région.

Vidéo: Consultez la formation associée : Tableau de bord de sécurité

Note: À partir d'une console, vous pouvez afficher le tableau de bord Security Hardening pour chaque sonde réseau d'analyse de paquets. Cliquez sur la flèche vers le bas à côté du nom de la sonde dans la barre de navigation pour afficher le tableau de bord Security Hardening pour les autres capteurs.

Le tableau de bord Security Hardening est un tableau de bord intégré au système que vous ne pouvez pas modifier, supprimer ou ajouter à une collection partagée. Cependant, vous pouvez copier un graphique depuis le tableau de bord Security Hardening et ajoutez-le à tableau de bord personnalisé, ou vous pouvez faire une copie du tableau de bord et modifiez-le pour suivre les statistiques qui vous concernent.

Les informations suivantes résument chaque région et ses graphiques.

Renseignements sur les menaces

Observez le nombre de connexions et de transactions contenant des noms d'hôte, des adresses IP ou des URI suspects trouvés dans renseignement sur les menaces. Cliquez sur une valeur métrique bleue ou sur le nom d'une métrique dans la légende pour accéder à une métrique suspecte. Une page détaillée apparaît avec une icône de caméra rouge à côté de l'objet suspect. Cliquez sur l'icône rouge représentant une caméra pour en savoir plus sur la source de renseignements sur les menaces.

Note: Les métriques de renseignement sur les menaces affichent une valeur nulle pour l'une ou plusieurs des raisons suivantes :

- Votre abonnement ExtraHop RevealX ne contient pas de renseignements sur les menaces.
- Vous n'avez pas activé les renseignements sur les menaces pour votre système ExtraHop RevealX.
- Vous n'avez pas directement chargé de collections de menaces personnalisées sur votre capteurs. Contactez le support ExtraHop pour obtenir de l'aide lors du téléchargement d'une collecte des menaces personnalisée vers votre site géré par ExtraHop capteurs.
- Aucun objet suspect n'a été trouvé.

TLS - Séances

Observez le nombre de sessions TLS actives avec des suites de chiffrement faibles sur votre réseau. Vous pouvez voir quels clients et serveurs participent à ces sessions ainsi que les suites de chiffrement avec lesquelles ces sessions sont cryptées. Les suites de chiffrement DES, 3DES, MD5, RC4, nulles, anonymes et d'exportation sont considérées comme faibles car elles incluent un algorithme de chiffrement connu pour sa vulnérabilité. Les données chiffrées à l'aide d'une suite de chiffrement faible sont potentiellement dangereuses.

Vous pouvez également observer le nombre de sessions TLS établies avec TLS v1.0 et quels clients participent à ces sessions. Des vulnérabilités connues sont associées à TLS v1.0. Si vous disposez d'un nombre élevé de sessions TLS v1.0, pensez à configurer les serveurs pour qu'ils prennent en charge la dernière version de TLS.

TLS - Certificats

Observez les certificats TLS de votre réseau qui sont auto-signés, comportent un caractère générique, ont expiré ou expirent bientôt. Les certificats auto-signés sont signés par l'entité qui les émet, plutôt que par une autorité de certification fiable. Bien que les certificats auto-signés soient moins chers que les certificats émis par une autorité de certification, ils sont également vulnérables aux attaques de type man-in-the-middle.

Un certificat générique s'applique à tous les sous-domaines de premier niveau d'un nom de domaine donné. Par exemple, le certificat générique *.company.com sécurise www.company.com, docs.company.com et customer.company.com. Bien que les certificats génériques soient moins chers que les certificats individuels, les certificats génériques présentent un risque accru s'ils sont compromis, car ils peuvent s'appliquer à un nombre illimité de domaines.

Scans de vulnérabilité

Observez quels appareils analysent les applications et les systèmes de votre réseau afin de détecter les points faibles et les cibles potentielles, tels que les appareils à valeur élevée. Dans le graphique de gauche, vous pouvez identifier les appareils qui envoient le plus de requêtes de numérisation, à savoir les requêtes HTTP associées à une activité d'analyse connue. Dans le graphique de droite, vous pouvez voir quels agents utilisateurs sont associés aux demandes d'analyse. L'agent utilisateur peut vous aider à déterminer si les demandes de scan sont associées à des scanners de vulnérabilités connus tels que Nessus et Qualys.

DNS

Observez les serveurs DNS les plus actifs sur votre réseau et le nombre total d'échecs de recherche DNS inversée rencontrés par ces serveurs. Un échec de recherche DNS inversée se produit lorsqu'un serveur émet une erreur en réponse à une demande d' enregistrement de pointeur (PTR) d'un client. Les échecs des recherches DNS inversées sont normaux, mais une augmentation soudaine ou régulière du nombre de défaillances sur un hôte spécifique peut indiquer qu'un attaquant analyse votre réseau.

Vous pouvez également observer le nombre de requêtes de mappage d'adresses et d'enregistrement de texte sur votre réseau. Une augmentation importante ou soudaine de ces types de requêtes peut indiquer la présence d'un tunnel DNS potentiel.

Tableau de bord des outils d'IA générative

Le tableau de bord Generative AI vous permet de surveiller le trafic provenant des outils OpenAI sur votre réseau.

Chaque graphique du tableau de bord de Generative AI Tools contient des visualisations du trafic associé au service cloud OpenAI pour des outils tels que ChatGPT. Afficher le trafic généré lors d'une intervalle de temps sélectionné, organisé par région.

Note: Depuis une console, vous pouvez afficher le tableau de bord des outils d'IA générative pour chaque site connecté. Le nom du site apparaît dans la barre de navigation ; cliquez sur la flèche vers le bas à côté du nom pour faire pivoter l'affichage vers d'autres sites.

Le tableau de bord Generative AI Tools est un tableau de bord système intégré, et vous ne pouvez pas modifier, supprimer ou ajouter des tableaux de bord système à une collection. Cependant, vous pouvez copier un graphique depuis le tableau de bord de Generative AI Tools et ajoutez le graphique à un tableau de bord personnalisé, ou vous pouvez faire une copie du tableau de bord et modifiez le tableau de bord pour suivre les indicateurs qui vous concernent.

Les informations suivantes résument chaque région et ses cartes.

Outils d'IA générative

Surveillez le trafic vers les outils basés sur OpenAI observés sur votre réseau. Découvrez à quel moment le trafic s'est produit, combien de données ont été transférées et quels terminaux internes ont participé.

tableau de bord Active Directory

Le tableau de bord Active Directory vous permet de suivre l'activité du serveur Kerberos pour les comptes d'utilisateurs et d'ordinateurs Active Directory, ainsi que pour les services tels que le catalogue global et les politiques de groupe.

Chaque graphique du tableau de bord Active Directory contient des visualisations des données de compte Active Directory qui ont été générées via intervalle de temps sélectionné, organisé par région.

Le tableau de bord Active Directory est un tableau de bord intégré au système que vous ne pouvez pas modifier, supprimer ou ajouter à une collection partagée. Cependant, vous pouvez copier un graphique depuis le tableau de bord Active Directory et ajoutez-le à tableau de bord personnalisé, ou vous pouvez faire une copie du tableau de bord et modifiez-le pour suivre les statistiques qui vous concernent.

Note: Depuis une console, vous pouvez afficher le tableau de bord Active Directory pour chaque site connecté. Le nom du site apparaît dans la barre de navigation ; cliquez sur la flèche vers le bas à côté du nom pour faire pivoter l'affichage vers d'autres sites.

Les informations suivantes résument chaque région et ses graphiques.

Résumé du compte

Observez le nombre de comptes Active Directory dans votre environnement dans les graphiques suivants :

- **Total des comptes:** Nombre total de comptes d'utilisateurs et de comptes d'ordinateurs.
- **Comptes privilégiés:** Nombre total de comptes privilégiés qui se sont connectés avec succès, qui ont reçu une erreur de connexion et qui ont envoyé une demande d'accès au service.

Erreurs d'authentification

Observez le nombre de comptes Active Directory présentant des erreurs d'authentification dans les graphiques suivants :

- **Erreurs liées au compte utilisateur:** Nombre total d'erreurs de connexion au compte utilisateur dues à des mots de passe non valides, à des mots de passe expirés ou à des comptes désactivés. Affiché sous la forme d'un graphique en courbes et d'un graphique en listes.
- **Erreurs liées aux comptes informatiques:** Nombre total d'erreurs de connexion à un compte informatique dues à des mots de passe non valides, à des mots de passe expirés ou à des comptes désactivés. Affiché sous la forme d'un graphique en courbes et d'un graphique en listes.
- **Erreurs de compte:** Nombre total d'erreurs, quel que soit le type de compte, dues à des blocages de comptes et à des erreurs de temps. Affiché sous la forme d'un graphique en courbes et d'un graphique en liste.

Détails de l'erreur d'authentification

Consultez les informations relatives aux comptes Active Directory présentant des erreurs d'authentification dans les tableaux suivants :

- **Comptes d'utilisateurs:** Noms d'utilisateur associés aux comptes utilisateurs qui n'ont pas pu se connecter. Ce graphique indique également le nombre de fois que chaque compte utilisateur a reçu une erreur en raison d'un mot de passe non valide ou d'un compte expiré.
- **Comptes informatiques:** Adresses IP des clients et noms d'hôte associés aux comptes utilisateurs qui n'ont pas pu se connecter. Ce graphique indique également le nombre de fois que chaque compte utilisateur a reçu une erreur en raison d'un mot de passe non valide ou d'un compte expiré.

Service d'attribution de billets

Observez les données de transaction associées au service d'attribution de tickets Kerberos dans les graphiques suivants :

- **Transactions:** Nombre total de demandes de ticket de service et nombre d'erreurs de nom principal de service (SPN) inconnues.
- **Transactions:** Nombre total de demandes de tickets de service.
- **Erreurs SPN inconnues par SPN:** Nombre d'erreurs SPN inconnues répertoriées par le SPN qui a envoyé l' erreur.
- **Erreurs SPN inconnues par client:** Nombre d'erreurs SPN inconnues répertoriées par le client qui a reçu l' erreur.
- **Nombre total d'erreurs SPN inconnues:** Nombre total d'erreurs SPN inconnues.

Stratégie de groupe

Observez les données de transaction des PME associées à la politique de groupe dans les graphiques suivants :

- **Transactions:** Nombre total de réponses de stratégie de groupe et d' erreurs de stratégie de groupe.

- **Transactions:** Nombre total de réponses de stratégie de groupe et d'erreurs de stratégie de groupe, en plus du temps de traitement du serveur nécessaire pour envoyer le premier paquet en réponse après réception du dernier paquet de la demande de stratégie de groupe.

LDAP

Observez les données de transaction LDAP à l'aide des graphiques suivants :

- **Transactions:** Nombre total de réponses et d'erreurs LDAP.
- **Transactions:** Nombre total de réponses et d'erreurs LDAP, en plus du temps de traitement du serveur nécessaire pour envoyer le premier paquet en réponse après réception du dernier paquet de la demande.
- **Informations d'identification LDAP non sécurisées :** Nombre total de demandes de liaison en texte brut. Affiché sous la forme d'un graphique en courbes et d'un graphique en listes.

Catalogue mondial

Observez les données de transaction associées au catalogue global dans les graphiques suivants :

- **Transactions:** Nombre total de réponses et d'erreurs dans le catalogue global.
- **Transactions:** Nombre total de réponses et d'erreurs du catalogue global, en plus du temps de traitement par le serveur nécessaire pour envoyer le premier paquet en réponse à la réception du dernier paquet de la demande de catalogue global.

Enregistrements de service DNS

Observez les données de transaction relatives à l'enregistrement des services DNS dans les graphiques suivants :

- **Transactions:** Nombre total de réponses et d'erreurs liées à l'enregistrement de service.
- **Transactions:** Nombre total de réponses et d'erreurs d'enregistrement de service, en plus du temps de traitement du serveur nécessaire pour envoyer le premier paquet en réponse après réception du dernier paquet de la demande.

tableau de bord de l'état du système

Le tableau de bord de l'état du système fournit une grande collection de graphiques qui vous permettent de vous assurer que votre système ExtraHop fonctionne comme prévu, de résoudre les problèmes et d' évaluer les domaines qui affectent les performances. Par exemple, vous pouvez surveiller le nombre de paquets traités par le système ExtraHop pour vous assurer que les paquets sont capturés en permanence.

Chaque graphique du tableau de bord des performances du réseau contient des visualisations des données de performance du système qui ont été générées sur intervalle de temps sélectionné, organisé par région.

Le tableau de bord System Health est un tableau de bord système intégré que vous ne pouvez pas modifier, supprimer ou ajouter à une collection partagée. Cependant, vous pouvez copier un graphique depuis le tableau de bord de l'état du système et ajoutez-le à un tableau de bord personnalisé, ou vous pouvez faire une copie du tableau de bord et modifiez-le pour suivre les statistiques qui vous concernent.

Note: La page des paramètres d'administration fournit également informations d'état et outils de diagnostic pour tous les systèmes ExtraHop.

Naviguez dans le tableau de bord de l'état du système

Accédez à la page État du système en cliquant sur l'icône Paramètres du système ou en cliquant **Tableaux de bord** depuis le haut de la page. Le tableau de bord de l'état du système affiche automatiquement des informations sur le système ExtraHop auquel vous êtes connecté. Si vous consultez le tableau de bord de l'état du système depuis une console, vous pouvez cliquer sur le sélecteur de site en haut de la page pour afficher les données d'un site spécifique ou de tous les sites de votre environnement.

Les graphiques du tableau de bord de l'état du système sont répartis dans les sections suivantes :

Découverte d'appareils

Consultez le nombre total d'appareils sur votre réseau. Découvrez quels appareils ont été découverts et combien d'entre eux sont actuellement actifs.

Flux de données

Évaluez l'efficacité du processus de collecte de données Wire Data à l'aide de graphiques relatifs au débit, au débit de paquets, aux désynchronisations et aux pertes de capture.

Enregistrements

Afficher le nombre total d'enregistrements envoyés vers un espace de stockage des enregistrements joint.

DÉCLENCHEURS

Surveillez l'impact des déclencheurs sur votre système ExtraHop. Découvrez à quelle fréquence les déclencheurs sont exécutés, à quelle fréquence ils échouent et quels déclencheurs sollicitent le plus votre processeur.

Flux de données ouvert et magasin d'enregistrements

Suivez l'activité des transmissions de flux de données ouvertes (ODS) à destination et en provenance de votre système. Consultez le nombre total de connexions distantes, le débit des messages et les informations relatives à des cibles distantes spécifiques.

Certificats TLS

Consultez les informations d'état de tous les certificats TLS de votre système ExtraHop.

Capture de paquets à distance (RPCAP)

Afficher le nombre de paquets et de trames envoyés et reçus par les homologues RPCAP.

Indicateurs de santé avancés

Suivez l'allocation des tas liée à la capture des données, à la banque de données du système, aux déclencheurs et aux transmissions à distance. Surveillez le débit d'écriture, la taille de l'ensemble de travail et l'activité des déclencheurs sur la banque de données système.

Découverte d'appareils

Le Découverte d'appareils La section du tableau de bord de l'état du système fournit une vue du nombre total d'appareils sur votre réseau. Découvrez quels types d'appareils sont connectés et combien d'entre eux sont actuellement actifs.

Le Découverte d'appareils La section fournit les graphiques suivants :

- Appareils actifs

Appareils actifs

Un graphique en aires qui affiche le nombre de périphériques L2, L3, de passerelle et personnalisés qui ont communiqué activement sur le réseau pendant l'intervalle de temps sélectionné. À côté du graphique en aires, un diagramme de valeurs affiche le nombre de périphériques L2, L3, de passerelle et personnalisés actifs au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider

Surveillez ce graphique après avoir apporté des modifications à la configuration du SPAN pour vous assurer qu'il n'y ait aucune conséquence imprévue susceptible de mettre le système ExtraHop en mauvais état. Par exemple, l'inclusion accidentelle d'un réseau peut mettre à rude épreuve les capacités du système ExtraHop en consommant davantage de ressources et en nécessitant une plus grande gestion des paquets, ce qui entraîne de mauvaises performances. Vérifiez que le système ExtraHop surveille le nombre attendu d'appareils actifs.

Flux de données

Le Flux de données Une section du tableau de bord de l'état du système vous permet d' observer l'efficacité du processus de collecte de données Wire Data à l'aide de graphiques relatifs au débit, au débit de paquets, aux désynchronisations et aux pertes de capture.

Le Flux de données La section fournit les graphiques suivants :

- Débit
- Débit par interface
- Débit de paquets
- Débit de paquets par interface
- Erreurs de paquets par interface
- Flux analysés
- Désynchronisations
- Taux de perte de capture
- Métriques écrites sur le disque (Log Scale)
- Estimations rétrospectives des données métriques

Débit
Un graphique en aires illustrant le débit des paquets entrants sur l' intervalle de temps sélectionné, exprimé en octets par seconde. Le graphique affiche les informations de débit pour les paquets analysés et filtrés, ainsi que pour les doublons L2 et L3.

Comment ces informations peuvent vous aider

Le dépassement des seuils du produit peut entraîner une perte de données. Par exemple, un débit élevé peut entraîner la suppression de paquets au niveau de la source de span ou d'un agrégateur d'span. De même, un grand nombre de doublons L2 ou L3 peut également indiquer un problème au niveau de la source ou de l' agrégateur d'intervalles et peut entraîner des mesures asymétriques ou incorrectes.

Le taux acceptable d'octets par seconde dépend de votre produit. Reportez-vous au Fiche technique des capteurs ExtraHop pour découvrir quelles sont les limites de votre système ExtraHop et déterminer si le taux d'octets par seconde est trop élevé.

Débit par interface
Un graphique en courbes illustrant le débit des paquets entrants, répertorié par chaque interface configurée sur la sonde. Le débit est exprimé en octets par seconde pendant l'intervalle de temps sélectionné. Le graphique affiche les informations de débit pour les paquets analysés et filtrés, ainsi que pour les doublons L2 et L3.

Lorsque vous visualisez plusieurs capteurs depuis une console ExtraHop, le graphique représente le taux de transfert moyen agrégé à partir d'interfaces partageant le même nombre.

Comment ces informations peuvent vous aider

Le dépassement des seuils de produit peut entraîner une perte de données. Par exemple, un débit élevé peut entraîner la perte de paquets à la source de span ou à un agrégateur de span. De même, de grandes quantités de doublons L2 ou L3 peuvent également indiquer un problème au niveau de la source ou de l'agrégateur de span et peuvent entraîner des mesures biaisées ou incorrectes.

Le débit acceptable de paquets par seconde dépend de votre produit. Reportez-vous à la Fiche technique des capteurs ExtraHop pour découvrir quelles sont les limites de votre système ExtraHop et déterminer si le débit de paquets par seconde est trop élevé.

Surveillez ce graphique pour résoudre les problèmes de débit des paquets à un niveau granulaire et ajuster la configuration de l'interface si nécessaire.

Débit de paquets
Un graphique en aires qui affiche le taux de paquets entrants, exprimé en paquets par seconde. Le graphique affiche les informations relatives au débit des paquets analysés et filtrés, ainsi que les doublons L2 et L3.

Comment ces informations peuvent vous aider
Le dépassement des seuils du produit peut entraîner une perte de données. Par exemple, un débit de paquets élevé peut entraîner la suppression de paquets au niveau de la source de span ou d'un agrégateur de span. De même, de grandes quantités de doublons L2 ou L3 peuvent également indiquer un problème au niveau de la source ou de l'agrégateur d'intervalles et peuvent entraîner des mesures asymétriques ou incorrectes.

Le débit acceptable de paquets par seconde dépend de votre produit. Reportez-vous au Fiche technique des capteurs ExtraHop pour découvrir quelles sont les limites de votre système ExtraHop et déterminer si le taux de paquets par seconde est trop élevé.

Débit de paquets par interface
Un graphique en courbes qui affiche le taux de paquets entrants et un graphique à colonnes qui affiche le nombre de paquets abandonnés, répertoriés par chaque interface configurée sur la sonde. Le débit de paquets est exprimé en paquets reçus par seconde pendant l'intervalle de temps sélectionné. Le graphique affiche les informations relatives au débit des paquets analysés et filtrés, ainsi que des doublons L2 et L3.

Lorsque vous visualisez plusieurs capteurs depuis une console ExtraHop, le graphique représente le débit de paquets agrégé et le nombre de paquets abandonnés par les interfaces partageant le même nombre.

Comment ces informations peuvent vous aider

Le dépassement des seuils de produit peut entraîner une perte de données. Par exemple, un débit de paquets élevé peut entraîner la suppression de paquets à la source de span ou à un agrégateur de span. De même, de grandes quantités de doublons L2 ou L3 peuvent également indiquer un problème au niveau de la source ou de l'agrégateur de span et peuvent entraîner des mesures biaisées ou incorrectes.

Le débit acceptable de paquets par seconde dépend de votre produit. Reportez-vous à Fiche technique des capteurs ExtraHop pour découvrir quelles sont les limites de votre système ExtraHop et déterminer si le débit de paquets par seconde est trop élevé.

Surveillez ce graphique pour résoudre les problèmes de débit de paquets à un niveau granulaire et ajuster la configuration de l'interface si nécessaire.

Erreurs de paquets par interface
Un graphique en courbes qui affiche le nombre d'erreurs de paquets reçues pendant l'intervalle de temps sélectionné, répertoriées par chaque interface configurée sur la sonde. Le graphique affiche les informations relatives aux erreurs de paquets pour les paquets analysés et filtrés, ainsi que pour les doublons L2 et L3 .

Lorsque vous visualisez plusieurs capteurs à partir d'une console ExtraHop, le graphique représente le nombre agrégé d'erreurs de paquets survenues sur des interfaces partageant le même nombre.

Comment ces informations peuvent vous aider

Surveillez ce graphique pour résoudre les erreurs de paquets à un niveau granulaire. L'augmentation du nombre d'erreurs de paquets peut entraîner une perte de données. Assurez-vous que les paquets sont envoyés comme prévu et modifiez la configuration de l'interface si nécessaire.

Flux analysés
Un graphique en courbes qui affiche le nombre de flux analysés par le système ExtraHop au cours de l'intervalle de temps sélectionné. Le graphique indique également le nombre de flux unidirectionnels survenus au cours de la même période. À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total de flux analysés et unidirectionnels survenus au cours de l'intervalle de temps sélectionné. Un flux est un ensemble de paquets qui font partie d'une transaction entre deux points de terminaison via un protocole tel que TCP, UDP ou ICMP.

Comment ces informations peuvent vous aider
Le dépassement des seuils du produit peut entraîner une perte de données. Par exemple, un nombre élevé de flux analysés peut entraîner la suppression de paquets au niveau de la source de span ou d'un agrégateur de span.

Désynchronisations
Un graphique en courbes qui affiche les occurrences de désynchronisations à l'échelle du système sur le système ExtraHop au cours de l'intervalle de temps sélectionné. À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total de désynchronisations survenues au cours de l'intervalle de temps sélectionné. Une désynchronisation se produit lorsque le flux de données ExtraHop supprime un paquet TCP et, par conséquent, n'est plus synchronisé avec une connexion TCP.

Comment ces informations peuvent vous aider
Un grand nombre de désynchronisations peut indiquer la perte de paquets sur l'interface de surveillance, le SPAN ou le réseau.

Si les ajustements apportés à votre SPAN ne réduisent pas le nombre important de désynchronisations, contactez Assistance ExtraHop.

Paquets tronqués
Un graphique en courbes qui affiche les occurrences de paquets tronqués sur le système ExtraHop au cours de l'intervalle de temps sélectionné. À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total de paquets tronqués survenus au cours de l'intervalle de temps sélectionné. Un paquet tronqué se produit lorsque la longueur totale réelle du paquet est inférieure à la longueur totale indiquée dans l'en-tête IP.

Comment ces informations peuvent vous aider
Les paquets tronqués peuvent indiquer un découpage en tranches. Une sonde rejette tous les paquets tronqués qu'elle reçoit, ce qui peut provoquer désynchronise à se produire.
Taux de perte de capture
Un graphique en courbes qui affiche le pourcentage de paquets déposés sur l' interface de la carte réseau sur un système ExtraHop sur l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Les pertes de paquets se produisent souvent lorsque les seuils des sondes sont dépassés. Reportez-vous au Fiche technique des capteurs ExtraHop pour découvrir quelles sont les limites de votre système ExtraHop.
Charge de capture
Un graphique en courbes qui affiche le pourcentage de cycles du système ExtraHop consommés par les threads de capture actifs sur l'intervalle de temps sélectionné, en fonction de la durée totale du thread de capture. Cliquez sur le lien associé Charge de capture moyenne graphique permettant d' effectuer une analyse détaillée par thread et de déterminer quels threads consomment le plus de ressources.

Comment ces informations peuvent vous aider
Surveillez les pics ou l'augmentation de la charge de capture pour vérifier si vous vous approchez des limites de la sonde. Reportez-vous au Fiche technique des capteurs ExtraHop pour découvrir les limites de votre système ExtraHop.
Métriques écrites sur le disque (Log Scale)
Un graphique en courbes qui affiche la quantité d'espace consommée par les métriques écrites sur le disque au cours de l'intervalle de temps sélectionné, exprimée en octets par seconde. Comme il existe une large plage entre les points de données, l'utilisation du disque est affichée sur une échelle logarithmique.

Comment ces informations peuvent vous aider
Il est important de connaître la quantité d'espace consommée par les métriques dans votre banque de données. La quantité d'espace disponible dans votre banque de données aura une incidence sur la quantité de lookback disponible. Si certaines mesures consomment trop d' espace, vous pouvez examiner les déclencheurs associés pour voir si vous pouvez modifier le déclencheur pour le rendre plus efficace.
Estimations rétrospectives des données métriques
Affiche les statistiques estimées de la banque de données sur le système ExtraHop. Les métriques Lookback sont disponibles par intervalles de 24 heures, 1 heure, 5 minutes et 30 secondes en fonction du débit d'écriture, exprimé en octets par seconde.

Comment ces informations peuvent vous aider

Reportez-vous à ce tableau pour déterminer jusqu'où vous pouvez rechercher des données historiques pour des intervalles de temps donnés. Par exemple, vous pourriez être en mesure de consulter des intervalles d'une heure de données remontant à 9 jours.

Enregistrements

Le Enregistrements la section du tableau de bord System Health vous permet d'observer l'efficacité du processus de collecte de données filaires à l'aide de graphiques relatifs au nombre d' enregistrements et au débit.

Le Flux de données La section fournit les graphiques suivants :

- Nombre d'enregistrements
- Débit record

Nombre d'enregistrements

Un graphique en courbes qui affiche le nombre d'enregistrements envoyés à un espace de stockage des enregistrements au cours de l'intervalle de temps sélectionné. À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total d' enregistrements envoyés au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider

Un nombre extrêmement élevé d'enregistrements envoyés à un espace de stockage des enregistrements peut entraîner de longues files d'attente de messages et la suppression de messages dans l'espace de stockage des enregistrements. Consultez les graphiques dans le Flux de données ouvert et magasin d'enregistrements section du tableau de bord System Health pour plus d'informations sur les transmissions dans l'espace de stockage des enregistrements.

Débit record

Un graphique en courbes qui affiche le nombre d'enregistrements en octets envoyés à un espace de stockage des enregistrements. À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total d'enregistrements envoyés en octets sur l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider

Ce graphique ne reflète pas les ajustements de taille basés sur la compression ou la déduplication et ne doit pas être référencé pour estimer les coûts de l'espace de stockage des enregistrements. Un débit d'enregistrement extrêmement élevé peut entraîner de longues files d'attente de messages et la suppression de messages dans l'espace de stockage des enregistrements. Consultez les graphiques dans le Flux de données ouvert et magasin d'enregistrements section du tableau de bord System Health pour plus d'informations sur les transmissions dans l'espace de stockage des enregistrements.

DÉCLENCHEURS

Le DÉCLENCHEURS la section du tableau de bord de l'état du système vous permet de surveiller l'impact des déclencheurs sur votre système. Découvrez à quelle fréquence les déclencheurs sont exécutés, à quelle fréquence ils échouent et quels déclencheurs sollicitent le plus votre processeur.

Le DÉCLENCHEURS La section fournit les graphiques suivants :

- Charge du déclencheur
- Retard de déclenchement
- Le déclencheur s'exécute et s'arrête
- Détails du déclencheur
- Déclencheur, charge par gâchette
- Le déclencheur s'exécute par déclencheur
- Déclenchez des exceptions par déclencheur
- Cycles de déclenchement par fil

Charge du déclencheur
Un graphique en courbes qui affiche le pourcentage de cycles de processeur alloués aux processus de déclenchement qui ont été consommés par les déclencheurs pendant l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Surveillez les pics ou la croissance de la charge du déclencheur, en particulier après avoir créé un nouveau déclencheur ou modifié un déclencheur existant. Si vous remarquez l'une ou l'autre de ces conditions, consultez le Déclencheur, charge par gâchette graphique pour voir quels déclencheurs consomment le plus de ressources.
Retard de déclenchement
Un graphique à colonnes qui affiche les délais de déclenchement maximaux survenus au cours de l'intervalle de temps sélectionné en millisecondes. À côté du graphique à colonnes, un diagramme de valeurs affiche le délai de déclenchement le plus long enregistré au cours de l'intervalle de temps sélectionné. Un délai de déclenchement est le délai entre le moment où un événement déclencheur est capturé et le moment où un thread de déclenchement est créé pour cet événement.

Comment ces informations peuvent vous aider

Les longs délais de déclenchement peuvent indiquer des problèmes de traitement, consultez le Déclenchez des exceptions par déclencheuret Déclencheur, charge par gâchette des graphiques pour voir quel déclencheur commet le plus d'exceptions non gérées et lesquels consomment le plus de ressources.

Le déclencheur s'exécute et s'arrête
Un graphique en courbes et à colonnes dans lequel le graphique en courbes indique le nombre de fois que les déclencheurs ont été exécutés, et le graphique à colonnes qui l'accompagne indique le nombre de fois où les déclencheurs ont été supprimés, sur l'intervalle de temps sélectionné. À côté du graphique linéaire et à colonnes, un diagramme de valeurs affiche le nombre total d'exécutions et de baisses de déclencheurs survenues au cours de l'intervalle de temps sélectionné. Ces graphiques fournissent un aperçu global de tous les déclencheurs actuellement en cours d'exécution sur le système ExtraHop.

Comment ces informations peuvent vous aider
Recherchez les pics dans le graphique linéaire et à colonnes et examinez les facteurs déclencheurs qui ont entraîné ces pics. Par exemple, vous remarquerez peut-être une augmentation de l'activité si un déclencheur a été modifié ou si un nouveau déclencheur a été activé. Consultez le Le déclencheur s'exécute par déclencheur graphique pour voir quels déclencheurs s'exécutent le plus fréquemment.
Détails du déclencheur
Un graphique en listes qui affiche les déclencheurs individuels ainsi que le nombre de cycles, d'exécutions et d' exceptions attribués à chacun sur l'intervalle de temps sélectionné. Par défaut, la liste des déclencheurs est triée par ordre décroissant par cycle de déclencheur.

Comment ces informations peuvent vous aider
Identifiez les déclencheurs qui consomment le plus de cycles. Les déclencheurs qui s'exécutent trop fréquemment ou qui consomment plus de cycles qu' ils ne le devraient peuvent être affectés à un plus grand nombre de sources que nécessaire. Assurez-vous que tout déclencheur hyperactif est uniquement attribué à la source spécifique à partir de laquelle vous devez collecter des données.
Déclencheur, charge par gâchette
Un graphique en courbes qui affiche le pourcentage de cycles de processeur alloués aux processus de déclenchement qui ont été consommés par les déclencheurs pendant l'intervalle de temps sélectionné, listés par nom de déclencheur.

Comment ces informations peuvent vous aider
Identifiez les déclencheurs qui consomment le plus de cycles. Les déclencheurs qui consomment plus de cycles qu'ils ne le devraient peuvent être affectés à un plus grand nombre de sources que nécessaire. Assurez-vous que tout déclencheur hyperactif est uniquement attribué à la source spécifique à partir de laquelle vous devez collecter des données.

Le déclencheur s'exécute par déclencheur
Un graphique en courbes qui affiche le nombre de fois que chaque déclencheur actif s'est exécuté sur l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Recherchez les déclencheurs qui s'exécutent plus fréquemment que prévu, ce qui peut indiquer que le déclencheur est attribué de manière trop large. Un déclencheur attribué à toutes les applications ou à tous les appareils peut avoir un coût élevé en termes de performances. Un déclencheur attribué à un groupe déquipements qui a été étendu peut collecter des métriques que vous ne souhaitez pas. Pour minimiser l'impact sur les performances, un déclencheur doit être attribué uniquement aux sources spécifiques auprès desquelles vous devez collecter des données.

Une activité élevée peut également indiquer qu' un déclencheur fonctionne plus que nécessaire. Par exemple, un déclencheur peut s'exécuter sur plusieurs événements pour lesquels il serait plus efficace de créer des déclencheurs distincts, ou un script de déclenchement peut ne pas respecter les directives de script recommandées, telles que décrites dans le Guide des meilleures pratiques en matière de déclencheurs.

Déclenchez des exceptions par déclencheur
Un graphique en courbes qui affiche le nombre d'exceptions non gérées, triées par déclencheur, survenues sur le système ExtraHop au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Les exceptions aux déclencheurs sont la principale cause des problèmes de performances des déclencheurs. Si ce graphique indique qu'une exception de déclencheur s'est produite , vous devez immédiatement examiner le déclencheur.
Cycles de déclenchement par fil
Un graphique en courbes qui affiche le nombre de cycles de déclenchement consommés par les déclencheurs pour un thread.

Comment ces informations peuvent vous aider
Des baisses de déclenchement peuvent se produire si la consommation d'un thread est considérablement supérieure à celle des autres, même si le pourcentage de consommation des threads est faible. Recherchez une consommation de cycle uniforme entre les threads.

Flux de données ouvert et magasin d'enregistrements
La section Open Data Stream (ODS) and Recordstore du tableau de bord System Health vous permet de suivre l'activité des transmissions ODS et de l'espace de stockage des enregistrements vers et depuis votre système. Vous pouvez également afficher le nombre total de connexions à distance, le débit des messages et les détails relatifs à des cibles distantes spécifiques.

Le Open Data Stream (ODS) et Recordstore La section fournit les graphiques suivants :

- Débit des messages
- Messages envoyés
- Messages supprimés par type de télécommande
- Erreurs d'envoi de message
- Connexions
- Longueur de la file d'attente de messages Exremote par cible
- Longueur de la file d'attente de messages Excap par type de télécommande
- Détails de la cible

Débit des messages
Un graphique en courbes qui affiche le débit des données des messages distants, exprimé en octets. À côté du graphique en courbes, un diagramme de valeurs affiche le débit moyen des données des messages distants sur l'intervalle de temps sélectionné. Les messages distants sont des transmissions envoyées à un

espace de stockage des enregistrements ou à des systèmes tiers depuis le système ExtraHop via un flux de données ouvert (ODS).

Comment ces informations peuvent vous aider
Surveillez ce graphique pour vous assurer que les octets sont transférés comme prévu. Si vous constatez un faible débit, cela peut être dû à un problème de configuration d'un ODS ou d'un espace de stockage des enregistrements rattaché. Des baisses de débit importantes peuvent indiquer des problèmes liés à vos flux de données.

Messages envoyés
Un graphique en courbes qui affiche le taux moyen d'envoi de messages distants depuis le système ExtraHop vers un espace de stockage des enregistrements ou une cible de flux de données ouvert (ODS). À côté du graphique en courbes, un diagramme de valeurs affiche le nombre total de messages envoyés au cours de l' intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Surveillez ce graphique pour vous assurer que les paquets sont envoyés comme prévu. Si aucun paquet n'est envoyé, il se peut qu'il y ait un problème de configuration d'un ODS ou d'un espace de stockage des enregistrements attaché.

Messages supprimés par type de télécommande
Un graphique en courbes qui affiche le taux moyen de messages distants abandonnés avant d'atteindre un espace de stockage des enregistrements ou une cible ODS.

Comment ces informations peuvent vous aider
Les messages supprimés indiquent des problèmes de connectivité avec la cible distante. Un nombre élevé de pertes peut également indiquer que le débit des messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible.

Erreurs d'envoi de message
Un graphique en courbes qui affiche le nombre d'erreurs survenues lors de l'envoi d'un message distant à un espace de stockage des enregistrements ou à une cible ODS. Surveillez ce graphique pour vous assurer que les paquets sont envoyés comme prévu. Les erreurs de transmission peuvent avoir les conséquences suivantes :

Erreurs du serveur cible

Nombre d'erreurs renvoyées au système ExtraHop par les magasins de disques ou les cibles ODS. Ces erreurs se sont produites sur le serveur cible et n'indiquent aucun problème avec le système ExtraHop.

Messages supprimés dans la file d'attente complète

Nombre de messages envoyés aux magasins de disques et aux cibles ODS qui ont été supprimés parce que la file d'attente de messages sur le serveur cible était pleine. Un nombre élevé de messages supprimés peut indiquer que le débit de messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible. Regardez le Longueur de la file d'attente de messages Exremote par cible et le Détails de la cible des graphiques pour voir si vos erreurs de transmission peuvent être liées à une longue file d'attente de messages.

Messages supprimés qui ne correspondent pas à la cible

Nombre de messages distants supprimés parce que le système distant spécifié dans le script déclencheur Open Data Stream (ODS) ne correspond pas au nom configuré sur la page Open Data Streams dans les paramètres d'administration. Assurez-vous que les noms des systèmes distants sont cohérents dans les scripts de déclencheur et les paramètres d' administration.

Erreurs de décodage Messages supprimés

Nombre de messages supprimés en raison de problèmes d'encodage interne entre ExtraHop Capture (excap) et ExtraHop Remote (exremote).

Connexions
Un graphique en courbes et en colonnes dans lequel le graphique en courbes indique le nombre de tentatives effectuées par le système pour se connecter à un serveur cible distant et le graphique à colonnes

qui l'accompagne indique le nombre d'erreurs survenues à la suite de ces tentatives. À côté du graphique à lignes et à colonnes, un diagramme de valeurs affiche le nombre total de tentatives de connexion et d'erreurs de connexion survenues au cours de l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Identifiez les serveurs cibles qui nécessitent un nombre inhabituel de tentatives de connexion ou qui génèrent un nombre disproportionné d'erreurs de connexion. Un pic de tentatives de connexion peut indiquer que le serveur cible n'est pas disponible.

Longueur de la file d'attente de messages Exremote par cible
Un graphique en courbes qui affiche le nombre de messages dans la file d'attente ExtraHop Remote (exremote) en attente de traitement par le système ExtraHop.

Comment ces informations peuvent vous aider

Un nombre élevé de messages dans la file d'attente peut indiquer que le débit de messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible. Reportez-vous à la valeur Exremote Full Queue Dropped Messages dans le Erreurs d'envoi de message tableau pour déterminer si des messages ont été envoyés.

Longueur de la file d'attente de messages Excap par type de télécommande
Un graphique en courbes qui affiche le nombre de messages cibles distants dans la file d'attente ExtraHop Capture (excap) en attente de traitement par le système ExtraHop.

Comment ces informations peuvent vous aider
Un nombre élevé de messages dans la file d'attente peut indiquer que le débit de messages est trop élevé pour être traité par le système ExtraHop ou le serveur cible.

Reportez-vous au Messages supprimés par type de télécommande tableau pour déterminer si des messages ont été envoyés.

Détails de la cible
Un graphique en listes qui affiche les mesures suivantes relatives à l'espace de stockage des enregistrements ou aux cibles distantes ODS sur l'intervalle de temps sélectionné : nom de la cible, octets de message cible envoyés, erreurs du serveur cible, messages supprimés dans la file d'attente complète, erreurs de décodage, messages supprimés, tentatives de connexion au serveur cible et erreurs de connexion au serveur cible.

Comment ces informations peuvent vous aider
Si des erreurs de message sont signalées dans le Messages envoyés graphique, les détails de ce graphique peuvent vous aider à déterminer la cause première des erreurs de message à distance.

Certificats TLS
La section Certificats TLS du tableau de bord de l'état du système vous permet de consulter les informations d' état de tous les certificats TLS de votre système.

Le Certificats TLS la section fournit le tableau suivant :

- Détails du certificat

Détails du certificat
Un graphique en listes qui affiche les informations suivantes pour chaque certificat :

Sessions déchiffrées
Le nombre de sessions qui ont été déchiffrées avec succès.

Sessions non prises en charge
Le nombre de sessions qui n'ont pas pu être déchiffrées à l'aide d'une analyse passive, telle que l'échange de clés DHE.

Sessions isolées

Le nombre de sessions qui n'ont pas été déchiffrées ou qui n'ont été que partiellement déchiffrées en raison de désynchronisations.

Sessions directes

Le nombre de sessions qui n'ont pas été déchiffrées en raison d'erreurs matérielles, telles que celles causées par un dépassement des spécifications du matériel d'accélération TLS.

Sessions déchiffrées avec un secret partagé

Le nombre de sessions qui ont été déchiffrées à l'aide d'une clé secrète partagée.

Comment ces informations peuvent vous aider

Surveillez ce graphique pour vous assurer que les certificats TLS appropriés sont installés sur le système ExtraHop et qu'ils effectuent le déchiffrement comme prévu.

Capture de paquets à distance (RPCAP)

La section Remote Packet Capture (RPCAP) du tableau de bord System Health vous permet de visualiser le nombre de paquets et de trames envoyés par des homologues RPCAP et reçus par le système ExtraHop.

Le Capture de paquets à distance (RPCAP) La section fournit les graphiques suivants :

- Transmis par Peer
- Reçu par le système ExtraHop

Transmis par Peer

Un graphique en listes qui affiche les informations suivantes concernant les paquets et les trames transférés par un homologue RPCAP :

Paquets transférés

Le nombre de paquets qu'un pair RPCAP a tenté de transférer vers un système ExtraHop .

Paquets d'interface du redirecteur

Nombre total de paquets consultés par le redirecteur. Les redirecteurs des appareils RPCAP se coordonneront entre eux pour empêcher plusieurs appareils d'envoyer le même paquet . Il s'agit du nombre de paquets qui ont été visualisés avant que les trames ne soient supprimées pour réduire le trafic transféré, et avant que les trames ne soient supprimées par des filtres définis par l'utilisateur.

Forwarder Kernel Frame Drops

Nombre d'images supprimées parce que le noyau de l'homologue RPCAP était surchargé par le flux de trames non filtrées. Les trames non filtrées n'ont pas été filtrées par le noyau pour supprimer les paquets dupliqués ou les paquets qui ne devraient pas être transférés en raison de règles définies par l'utilisateur.

Abandon de l'interface du redirecteur

Nombre de paquets supprimés parce que le redirecteur RPCAP était surchargé par le flux de trames non filtrées. Les trames non filtrées n'ont pas été filtrées pour supprimer les paquets dupliqués ou les paquets qui ne devraient pas être transférés en raison de règles définies par l'utilisateur .

Comment ces informations peuvent vous aider

Chaque fois que vous voyez des paquets abandonnés par l'homologue RPCAP, cela indique qu'il y a un problème avec le logiciel RPCAP.

Reçu par le système ExtraHop

Un graphique en listes qui affiche les informations suivantes concernant les paquets et les trames reçus par un système ExtraHop depuis un homologue RPCAP (Remote Packet Capture) :

Octets encapsulés

Taille totale de tous les paquets liés au flux UDP entre l'équipement RPCAP et le système ExtraHop, en octets. Ces informations vous indiquent le volume de trafic que le redirecteur RPCAP ajoute à votre réseau.

Paquets encapsulés

Le nombre de paquets liés au flux UDP entre l'équipement RPCAP et le système ExtraHop.

Octets de tunnel

Taille totale des paquets, sans compter les en-têtes d'encapsulation, que le système ExtraHop a reçus d'un équipement RPCAP, en octets.

Paquets de tunnels

Le nombre de paquets que le système ExtraHop a reçus d'un homologue RPCAP. Ce nombre doit être très proche du nombre de paquets transférés dans le tableau des paquets envoyés par un périphérique distant. S'il y a un écart important entre ces deux nombres, des paquets tombent entre l'équipement RPCAP et le système ExtraHop.

Comment ces informations peuvent vous aider

Le suivi des paquets et des octets encapsulés est un bon moyen de s'assurer que les redirecteurs RPCAP n'imposent pas de charge inutile à votre réseau. Vous pouvez surveiller les paquets et les octets du tunnel pour vous assurer que le système ExtraHop reçoit tout ce que l' équipement RPCAP envoie.

Indicateurs de santé avancés

La section Advanced Health Metrics du tableau de bord de l'état du système vous permet de suivre l'allocation de tas liée à la capture de données, à la banque de données du système, aux déclencheurs et aux transmissions à distance. Surveillez le débit d'écriture, la taille de l'ensemble de travail et l'activité du déclencheur sur la banque de données du système.

Le Indicateurs de santé avancés La section fournit les graphiques suivants :

- Capture et allocation de tas de données
- Déclencheur et allocation de tas à distance
- Stocker le débit d'écriture
- Taille de l'ensemble de travail
- Chargement déclencheur de la banque de données
- Le déclencheur de la banque de données s'exécute et s'arrête
- Exceptions de déclenchement de la banque de données par déclencheur

Capture et allocation de tas de données

Un graphique en courbes qui affiche la quantité de mémoire que le système ExtraHop consacre à la capture de paquets réseau et à la banque de données.

Comment ces informations peuvent vous aider

Les données de ce tableau sont destinées à des fins internes et peuvent être demandées par Assistance ExtraHop pour vous aider à diagnostiquer un problème.

Déclencheur et allocation de tas à distance

Un graphique en courbes qui affiche la quantité de mémoire, exprimée en octets, que le système ExtraHop consacre au traitement des déclencheurs de capture et aux flux de données ouverts (ODS).

Comment ces informations peuvent vous aider

Les données de ce tableau sont destinées à des fins internes et peuvent être demandées par Assistance ExtraHop pour vous aider à diagnostiquer un problème.

Stocker le débit d'écriture

Un graphique en aires qui affiche le débit d'écriture de la banque de données, exprimé en octets, sur le système ExtraHop. Le graphique affiche les données pour l'intervalle de temps sélectionné et pour des intervalles de 24 heures, 1 heure, 5 minutes et 30 secondes.

Comment ces informations peuvent vous aider

Les données de ce tableau sont destinées à des fins internes et peuvent être demandées par Assistance ExtraHop pour vous aider à diagnostiquer un problème.

Taille de l'ensemble de travail
Un graphique en aires qui affiche la taille définie de travail du cache d'écriture pour les métriques sur le système ExtraHop. La taille de l'ensemble de travail indique le nombre de mesures pouvant être écrites dans le cache pour l'intervalle de temps sélectionné et pour des intervalles de 24 heures, 1 heure, 5 minutes et 30 secondes.

Comment ces informations peuvent vous aider
Les données de ce graphique peuvent augmenter après la création ou la modification du déclencheur si le script de déclenchement ne collecte pas les métriques de manière efficace.
Chargement déclencheur de la banque de données
Un graphique en courbes qui affiche le pourcentage de cycles consommés par les déclencheurs spécifiques à une banque de données sur le système ExtraHop, en fonction de la durée totale du thread de capture.

Comment ces informations peuvent vous aider
Recherchez des pics ou une augmentation de la charge du déclencheur de banque de données, en particulier après avoir créé un nouveau déclencheur de banque de données ou modifié un déclencheur de banque de données existant. Si vous remarquez l'un ou l'autre, cliquez sur **Charge du déclencheur** étiquette métrique permettant d'effectuer une analyse détaillée et de déterminer quels déclencheurs de banque de données consomment le plus de ressources.
Le déclencheur de la banque de données s'exécute et s'arrête
Un graphique à lignes et à colonnes dans lequel le graphique en courbes indique le nombre de fois que des déclencheurs spécifiques à une banque de données ont été exécutés sur le système ExtraHop pendant l'intervalle de temps sélectionné, et le graphique à colonnes correspondant affiche le nombre de déclencheurs spécifiques à la banque de données supprimés de la file de déclencheurs en attente d'exécution sur le système ExtraHop pendant l'intervalle de temps sélectionné.

Comment ces informations peuvent vous aider
Un seul déclencheur de banque de données qui s'exécute souvent peut indiquer que le déclencheur a été attribué à toutes les sources, telles que les applications ou les appareils. Pour minimiser l'impact sur les performances, un déclencheur doit être attribué uniquement aux sources spécifiques auprès desquelles vous devez collecter des données.

À partir du Chargement déclencheur de la banque de données graphique, cliquez sur **Charge du déclencheur** étiquette métrique pour effectuer une analyse détaillée et voir quels déclencheurs de banque de données s'exécutent le plus fréquemment.

Toutes les données de dépôt affichées sur le histogramme indiquent que des abandons déclencheurs de la banque de données se produisent et que les files d'attente des déclencheurs sont sauvegardées.

Le système met en file d'attente les opérations de déclenchement si un thread de déclenchement est surchargé. Si la file d'attente des déclencheurs de la banque de données devient trop longue, le système arrête d'ajouter des opérations de déclenchement à la file d'attente et supprime les déclencheurs. Les déclencheurs en cours d'exécution ne sont pas affectés.

La principale cause des longues files d'attente, et des abandons de déclencheurs qui en découlent, est un déclencheur de longue durée dans une banque de données.

Exceptions de déclenchement de la banque de données par déclencheur
Un graphique en listes qui affiche le nombre d'exceptions non gérées causées par des déclencheurs spécifiques à une banque de données sur le système ExtraHop.

Comment ces informations peuvent vous aider
Les exceptions aux déclencheurs de la banque de données sont la principale cause des problèmes de performances des déclencheurs. Si ce graphique indique qu'une exception de déclencheur s'est produite, le déclencheur de la banque de données doit être corrigé immédiatement.

Outils d'état et de diagnostic dans les paramètres d'administration
Les paramètres d'administration constituent une autre source d'informations et de diagnostics sur le système.

Pour plus de statistiques sur l'état général du système ExtraHop et pour les outils de diagnostic qui permettent Assistance ExtraHop pour résoudre les erreurs du système, consultez le État et diagnostics section des paramètres d'administration.

tableau de bord de l'utilisation du système

Le tableau de bord d'utilisation du système vous permet de surveiller la manière dont les utilisateurs interagissent avec le système ExtraHop.

Chaque graphique du tableau de bord d'utilisation du système contient des visualisations des interactions des utilisateurs avec le système ExtraHop et des détections générées via intervalle de temps sélectionné, organisé par région.

Note: Le tableau de bord d'utilisation du système est un tableau de bord système intégré que vous ne pouvez pas modifier, supprimer ou ajouter à une collection partagée. Vous ne pouvez pas copier le tableau de bord d'utilisation du système ni copier des graphiques dans des tableaux de bord personnalisés.

Avant de commencer
Le tableau de bord de l'utilisation du système ne peut être consulté depuis une console que par les utilisateurs disposant de l'administration du système et des accès privilèges.

Les informations suivantes résument chaque région et ses graphiques.

Utilisateurs d'ExtraHop

Observez l'activité de connexion des utilisateurs et le nombre actuel d'utilisateurs actifs sur le système ExtraHop.

- **Utilisateurs actifs et connexions:** Le nombre de fois que les utilisateurs se sont connectés au système ExtraHop et les instantanés actuels des utilisateurs actifs. Le graphique en courbes affiche les utilisateurs actifs actuels et le graphique à colonnes affiche le nombre de connexions d'utilisateurs au fil du temps. Une connexion est comptabilisée chaque fois qu'un utilisateur se connecte au système, y compris les connexions multiples par un seul utilisateur.
- **Connexions des utilisateurs les plus populaires:** Utilisateurs ayant enregistré le plus grand nombre de connexions sur le système ExtraHop au cours de l'intervalle de temps sélectionné.
- **Utilisateurs actifs et connexions:** Le nombre d'utilisateurs actuellement actifs sur le système ExtraHop et le nombre total de connexions utilisateur au cours de l'intervalle de temps sélectionné.

Tableaux de bord

Observez la fréquence à laquelle les utilisateurs consultent tableaux de bord et quels tableaux de bord sont les plus consultés.

- **Vues du tableau de bord:** Nombre total de vues du tableau de bord au fil du temps. Une vue de tableau de bord est prise en compte lorsqu'un tableau de bord apparaît après la connexion d'un utilisateur, un clic ou une navigation directe via une URL partagée.
- **Tableaux de bord les plus consultés:** Tableaux de bord affichant le plus grand nombre de vues.
- **Total des vues du tableau de bord:** Le nombre total de vues du tableau de bord sur l' intervalle de temps sélectionné.

Détections

Observez les informations sur détections qui sont générés par le système ExtraHop et la façon dont les utilisateurs visualisent et suivi détections.

- **Vues de détection:** Deux valeurs sont affichées dans ce graphique en courbes : Detection List Views compte le nombre de clics sur la liste de détection lorsque groupés par type de détection, et Detection Detail Views compte le nombre de fois que page détaillée de détection apparaît après la

connexion d'un utilisateur, un clic ou une navigation directe via une URL partagée. Cliquez sur le nom de l'une des métriques dans la légende pour effectuer une recherche par type de détection.

• **Détections les plus consultées:** Les types de détection les plus consultés au cours de l' intervalle de temps sélectionné.

• **Nombre total de vues de détection:** Les valeurs totales pour les vues de liste de détection et les vues détaillées de détection sur l'intervalle de temps sélectionné.

• **Suivi des détections (graphique en courbes):** Le nombre de détections qui ont été clôturées avec ou sans action, et le nombre de détections qui ont été confirmées au fil du temps.

• **Suivi des détections (graphique en listes):** Le nombre total de détections clôturées avec ou sans action entreprise, le nombre d'enquêtes créées et le nombre total de détections dont le statut Reconnu a été défini sur l'intervalle de temps sélectionné. La liste inclut également le nombre de détections actuellement définies sur le statut En cours.

• **Total des détections fermées:** Le nombre total de détections clôturées avec et sans action entreprise au cours de l'intervalle de temps sélectionné. Les valeurs du total des détections fermées incluent les détections qui ont été masquées après la définition de l'état de détection.

• **Détections recommandées:** Le nombre de détections recommandées pour le triage, également appelé triage intelligent, pendant l'intervalle de temps sélectionné.

• **Détections les plus recommandées:** Les types de détection les plus recommandés pour le triage au cours de l'intervalle de temps sélectionné.

• **Total des détections fermées recommandées:** Le nombre total de détections recommandées qui ont été clôturées avec et sans action entreprise pendant l'intervalle de temps sélectionné.

Types de détection

Observez quels types de détection ont été le plus générés par le système ExtraHop et comment les utilisateurs interagissent avec ces détections.

• **Types de détection les plus consultés:** Le nombre de vues de la liste de détection et de vues détaillées des détections pour les types de détection qui se sont produits au cours de l' intervalle de temps sélectionné.

Enquêtes

Observez les informations relatives aux enquêtes créées par les utilisateurs, aux enquêtes recommandées par le système ExtraHop et à la manière dont les utilisateurs consultent et interagissent avec les enquêtes.

• **Vues de l'enquête:** Le nombre de vues d'investigation créées et recommandées par les utilisateurs au fil du temps. Une vue d'investigation est prise en compte lorsqu'une enquête est affichée suite à la connexion d'un utilisateur, à un clic ou à une navigation directe via une URL partagée.

• **Enquêtes les plus consultées:** Les types d'enquêtes créées et recommandées par les utilisateurs qui ont été les plus consultées au cours de l'intervalle de temps sélectionné.

• **Nombre total de vues de l'enquête:** Le nombre total de vues d'investigation créées et recommandées par l'utilisateur pendant l'intervalle de temps sélectionné.

• **Enquêtes créées:** Le nombre d'enquêtes créées au fil du temps, répertorié par enquêtes créées par les utilisateurs et par enquêtes recommandées par le système ExtraHop.

• **Enquêtes les plus recommandées:** Les types d'investigation les plus recommandés par le système ExtraHop pendant l'intervalle de temps sélectionné.

• **Nombre total d'enquêtes créées:** Le nombre total d'enquêtes créées par les utilisateurs et le nombre total d'enquêtes recommandées par le système ExtraHop pendant l'intervalle de temps sélectionné.

Exposés sur les menaces

Consultez les informations relatives aux briefings sur les menaces qui fournissent des conseils sur les menaces potentielles qui pèsent sur votre réseau et sur la manière dont les utilisateurs les perçoivent.

• **Vues d'information sur les menaces:** Le nombre de vues d'informations sur les menaces au fil du temps. Une vue d'information sur les menaces est prise en compte lorsqu'une page détaillée d'information sur les menaces s'affiche à la suite d'un clic de l'utilisateur ou d'une navigation directe via une URL partagée.

• **Exposés sur les menaces les plus consultés:** Les exposés sur les menaces qui ont été les plus consultés au cours de l'intervalle de temps sélectionné .

• **Nombre total de vues des exposés sur les menaces:** Le nombre total de séances d'information sur les menaces qui ont été visionnées pendant l'intervalle de temps sélectionné.

Création d'un tableau de bord

Les tableaux de bord fournissent un emplacement unique pour les indicateurs importants qui vous intéressent. Lorsque vous créez un tableau de bord personnalisé, une mise en page de tableau de bord s'ouvre contenant une seule région avec un widget graphique vide et un widget de zone de texte vide. Modifiez un graphique pour intégrer des indicateurs en temps réel dans votre tableau de bord, et modifiez une zone de texte pour fournir des informations. Enfin, ajustez la mise en page et ajoutez d'autres widgets pour compléter votre tableau de bord et commencer à surveiller votre réseau.

Avant de commencer
Déterminez les indicateurs que vous souhaitez surveiller sur votre tableau de bord. Posez-vous les questions suivantes :

- Dois-je savoir si mon serveur est hors ligne ou indisponible ? Ajoutez des indicateurs de disponibilité tels que les demandes et les réponses aux graphiques de votre tableau de bord.
- Mon serveur fonctionne-t-il correctement ? Ajoutez des indicateurs de fiabilité tels que les erreurs aux graphiques de votre tableau de bord.
- Les ressources de mon serveur sont-elles suffisantes ? Ajoutez des indicateurs de performance tels que le temps de traitement du serveur aux graphiques de votre tableau de bord.

Création de la mise en page du tableau de bord

Les étapes suivantes vous montrent comment créer le cadre de votre tableau de bord, qui inclut deux types de widgets vides : un graphique et une zone de texte. Votre nouveau tableau de bord s'ouvre en mode Modifier la mise en page (qui s'affiche dans le coin supérieur droit). Le mode Modifier la mise en page vous permet de modifier rapidement votre graphique et votre zone de texte, et d'organiser le placement des widgets et des régions sur un tableau de bord.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Sur la page Tableaux de bord, effectuez l'une des étapes suivantes :
   - Cliquez **Tableaux de bord** dans le dock du tableau de bord, puis cliquez sur **Créer un tableau de bord** au bas du quai.
   - Cliquez sur le menu de commande ⋮ dans le coin supérieur droit de la page et sélectionnez **Nouveau tableau de bord**.
4. Dans la fenêtre Propriétés du tableau de bord, saisissez le nom de votre tableau de bord.
5. Entrez toutes les autres métadonnées pour votre tableau de bord, telles que le nom de l'auteur ou une description. Notez que le lien permanent fournit une URL directe vers votre tableau de bord pour tous les utilisateurs qui ont privilèges de partage pour votre tableau de bord.
6. Cliquez **Créez**.

Modifier un graphique de base

Les étapes suivantes montrent le flux général de modification d'un widget graphique dans l'outil Metric Explorer. Commencez par spécifier les sources et les indicateurs pour ajouter des données à votre graphique. Par exemple, vous pouvez désormais ajouter à votre tableau de bord les indicateurs de disponibilité, de fiabilité ou de performance que vous avez pris en compte au début de cette procédure. Choisissez ensuite un type de graphique pour visualiser les données.

1. Cliquez sur le graphique pour lancer le explorateur de métriques.
2. Cliquez **Ajouter une source**.
3. Dans le champ de recherche de source, tapez le nom d'une source, puis sélectionnez source à partir des résultats de recherche.
4. Dans le champ de recherche métrique, tapez le protocole et le nom de la métrique, puis sélectionnez la métrique que vous souhaitez ajouter au graphique dans les résultats de recherche. Par exemple, pour contrôler la fiabilité des transactions sur le Web, tapez `Erreurs HTTP` puis sélectionnez **Erreurs HTTP** à partir des résultats de recherche.
5. Sélectionnez un type de graphique en bas de l'explorateur de métriques.

   Certains graphiques peuvent ne pas être compatibles avec les statistiques que vous avez sélectionnées. Par exemple, le graphique de carte thermique peut uniquement afficher jeu de données des données métriques, telles que le temps de traitement du serveur. Pour plus d' informations sur les graphiques et les mesures compatibles, voir Types de graphiques.
6. Optionnel : Sélectionnez une touche d'exploration vers le bas pour afficher les statistiques détaillées. Cliquez **Extraire vers le bas par <None>**, où *<None>* est le nom de la clé métrique détaillée actuellement affichée dans votre graphique. Vous pouvez afficher jusqu'à 20 valeurs clés les plus importantes dans un graphique pour un intervalle de temps spécifique.
7. Cliquez **Enregistrer**.

Prochaines étapes

- Pour en savoir plus sur les graphiques, consultez le FAQ sur les graphiques.
- Entraînez-vous à créer des diagrammes en effectuant les procédures pas à pas suivantes :
  - Surveiller les erreurs DNS dans un tableau de bord
  - Surveiller l'état de la base de données dans un tableau de bord
  - Surveillez les performances Web dans un tableau de bord

Modifier un widget de zone de texte de base

Les étapes suivantes vous montrent comment afficher du texte personnalisé dans une région de tableau de bord. Il s'agit d'un outil utile pour ajouter des notes sur un graphique ou des données dans un tableau de bord. Le widget de zone de texte prend en charge la syntaxe Markdown. Un nouveau widget de zone de texte contient un exemple de texte déjà formaté dans Markdown pour vous fournir des exemples de base.

1. Cliquez sur la zone de texte.
2. Tapez et modifiez le texte dans la partie gauche Rédacteur volet. Le texte de sortie HTML s'affiche dynamiquement dans le volet d'aperçu droit. Pour d'autres exemples de mise en forme, voir Formater le texte dans Markdown.
3. Cliquez **Enregistrer**.

Ajoutez d'autres widgets et régions à votre tableau de bord

Ajoutez et organisez le placement des régions et des widgets sur vos tableaux de bord.

1. Cliquez et faites glisser les composants du tableau de bord, tels qu'une région ou des widgets, depuis le bas de la page vers l'espace de travail.
2. Pour organiser les composants du tableau de bord, cliquez et faites glisser le bord d'une région ou d'un widget pour les redimensionner. Si les composants du tableau de bord se chevauchent, ils seront

surlignés en rouge. Vous devez cliquer et faire glisser les côtés des widgets et des régions pour libérer de l'espace.

3. Optionnel : Cliquez **Supprimer de l'espace supplémentaire** pour supprimer l'espace blanc vertical vide autour des widgets. Les espaces blancs verticaux vides seront supprimés de chaque région du tableau de bord.
4. Après avoir apporté vos modifications, cliquez sur **Quitter le mode Layout**.

> **Note:** Si un message d'erreur apparaît, cela signifie qu'un autre utilisateur est peut-être en train d'apporter des modifications. Il est préférable que chaque utilisateur d'ExtraHop ait un compte individuel.

Prochaines étapes

Maintenant que votre tableau de bord est terminé, vous pouvez effectuer les étapes suivantes :

- Partagez votre tableau de bord
- Mettez à jour votre tableau de bord :
  - Modifier la mise en page d'un tableau de bord
  - Modifier les propriétés du tableau de bord
  - Modifier une région de tableau de bord
  - Modifier un graphique à l'aide de l'explorateur de métriques

Conseils pour l'édition de graphiques

Les conseils suivants vous aident à rechercher et à sélectionner des indicateurs lors de la création d'un graphique.

- Filtrez les résultats de recherche en fonction d'un type de source ou d'un protocole spécifique en cliquant sur **N'importe quel type** ou **N'importe quel protocole** sous les champs de recherche.
- Vous ne pouvez sélectionner que le même type de source que celui qui figure actuellement dans votre ensemble métrique. Un ensemble de mesures contient un type de source et des métriques. Par exemple, si vous sélectionnez l' application All Activity comme source, vous ne pouvez ajouter que d'autres applications à cet ensemble métrique.
- Créez un groupe ad hoc de plusieurs sources dans votre graphique en sélectionnant **Combiner les sources**. Par exemple, vous pouvez combiner deux applications, puis afficher une seule valeur métrique dans le graphique pour ces deux applications.
- Si vous sélectionnez un groupe déquipements comme source, vous pouvez **Exploration par membre du groupe** pour afficher des statistiques individuelles pour un maximum de 20 appareils du groupe.

Création d'un tableau de bord avec des sources dynamiques

Vous pouvez créer un tableau de bord avec des sources dynamiques pour permettre aux utilisateurs de modifier la source du tableau de bord à tout moment. Si vous avez créé un grand nombre de tableaux de bord qui ont tous les mêmes indicateurs, mais des sources différentes, vous pouvez envisager de remplacer ces tableaux de bord par un tableau de bord unique à source dynamique.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Dans le dock du tableau de bord, sélectionnez le tableau de bord que vous souhaitez modifier.
4. Définissez la source de chaque graphique sur une variable de type source.
   a) Cliquez sur le nom d'un graphique, puis sur **Modifier**.
   b) Dans le **Les sources** champ, type $.
   Le Variables de type de source la liste apparaît.
   c) À partir du Variables de type de source dans la liste, sélectionnez le type de source que vous remplacez. Par exemple, si vous remplacez une source d'équipement, sélectionnez `$device`.

5. Cliquez **Enregistrer**.
   En haut du tableau de bord, le Afficher la source un menu déroulant apparaît.
6. À partir du Afficher la source dans le menu déroulant, sélectionnez la source pour laquelle vous souhaitez consulter les statistiques.
   Si aucune donnée n'est affichée dans les graphiques du tableau de bord, essayez d'actualiser la page.

Conseil: Si vous souhaitez masquer le menu source dynamique de votre tableau de bord, ajoutez le paramètre suivant à la fin de l'URL de la page du tableau de bord : `&hideTemplatePanel=true`.

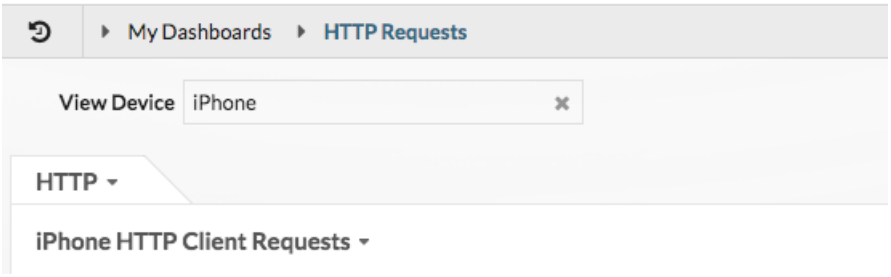


Figure 3: Avant

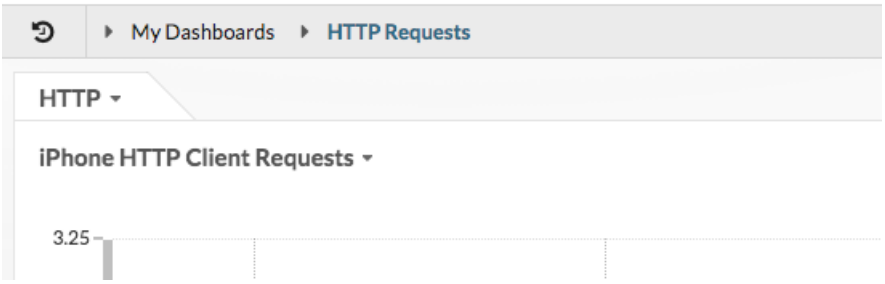


Figure 4: Après

Par exemple :

```
https://eda/extrahop/#/Dashboard/XYFwM/?
$device=16&from=30&interval_type=MIN&until=0&hideTemplatePanel=true
```

Prochaines étapes

- Copier un tableau de bord

Copier un tableau de bord

Si vous souhaitez dupliquer un tableau de bord utile, vous pouvez copier un tableau de bord, puis remplacer ou modifier les sources pour afficher différentes données d'application, d'équipement ou de réseau. Vous ne pouvez copier qu'un seul tableau de bord à la fois.

Note: Si vous souhaitez uniquement copier un tableau de bord afin de pouvoir modifier la source sur l' ensemble du tableau de bord, vous pouvez envisager création d'un tableau de bord avec des sources dynamiques au lieu de créer plusieurs copies d'un seul tableau de bord.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Dans le dock du tableau de bord, sélectionnez le tableau de bord que vous souhaitez copier.
4. Cliquez sur le menu de commandes ⋮ dans le coin supérieur droit de la page du tableau de bord.
5. Cliquez **Copier** et effectuez l'une des étapes suivantes :

- Cliquez **Conservez les sources** pour conserver les configurations de données d'origine dans le nouveau tableau de bord.

  Note: Lorsque vous copiez un tableau de bord avec des sources dynamiques, les configurations de données d'origine sont automatiquement conservées.

- Cliquez **Modifier les sources**, qui vous permet de mettre immédiatement à jour chaque région, graphique et widget du tableau de bord copié avec une autre source, puis de suivre les étapes suivantes :

  1. Dans le volet droit de Modifier les sources fenêtre, cliquez sur le nom d'une source. Un champ de recherche s'ouvre.
  2. Tapez le nom d'une nouvelle source, puis sélectionnez-la dans la liste déroulante. Répétez cette étape si le tableau de bord contient plusieurs sources que vous souhaitez remplacer.
  3. Cliquez **Créer un tableau de bord**.

Un tableau de bord copié avec une version modifiée du titre d'origine est créé.

6. Pour renommer le tableau de bord copié, procédez comme suit :
   a) Cliquez sur le menu de commandes ⋮ dans le coin supérieur droit et sur la page.
   b) Sélectionnez **Propriétés du tableau de bord**.
   c) Dans le champ Titre, saisissez un nouveau nom.
   d) Cliquez **Enregistrer**.

Prochaines étapes

- Modifier une région de tableau de bord
- Modifier un graphique à l'aide de l'explorateur de métriques
- Modifier la disposition du tableau de bord

Modifier la mise en page d'un tableau de bord

Placez votre tableau de bord en mode Modifier la mise en page pour ajouter, supprimer ou réorganiser les widgets et les régions de la mise en page de votre tableau de bord. Vous ne pouvez ajouter ou supprimer des widgets ou des régions que lorsque le tableau de bord est en mode Modifier la mise en page.

Lorsque vous créez un nouveau tableau de bord, celui-ci est automatiquement placé en mode Modifier la mise en page. Pour modifier la mise en page d'un tableau de bord existant, procédez comme suit :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Dans le dock du tableau de bord, sélectionnez le tableau de bord que vous souhaitez modifier.
4. Cliquez sur le menu de commande ⋮ dans le coin supérieur droit de la page, puis sélectionnez **Modifier la mise en page**.
5. En mode Modifier le modèle, sélectionnez l'une des options suivantes :

   Ajouter des widgets et des régions

   Cliquez et faites glisser un widget ou une région depuis le bas de la page et placez-le sur le tableau de bord.

   Les widgets sont des composants de tableau de bord configurables qui fournissent les fonctions suivantes :

   - **Graphique** : ajoutez des métriques et sélectionnez des types de graphiques pour visualiser les données
   - **Zone de texte** : ajoutez des explications, des liens et des images à votre tableau de bord
   - **Alertes** : analyse jusqu'à 40 alertes récentes, triées par gravité

• **Groupe d'activités:** surveille les appareils qui sont regroupés automatiquement en fonction de l'activité du protocole dans le système ExtraHop

Les régions contiennent des widgets et les regroupent de manière logique. Cliquez et faites glisser des widgets dans une région. La largeur d'une région peut inclure un maximum de six widgets. La longueur d'une région et d'un tableau de bord est illimitée.

Supprimer des widgets et des régions

Pour supprimer une région, cliquez sur **Supprimer** dans l'en-tête de la région. Pour supprimer un widget, cliquez sur le titre puis sélectionnez **Supprimer** depuis le menu déroulant.

Organiser le placement des widgets et des régions

Cliquez sur l'en-tête d'une région ou d'un widget pour les faire glisser vers un autre emplacement. Cliquez et faites glisser le bord d'une région ou d'un widget pour les redimensionner.

Si les composants du tableau de bord se chevauchent, ils seront surlignés en rouge. Vous devez cliquer et faire glisser les côtés des widgets et des régions pour libérer de l' espace.

Graphiques dupliqués

Cliquez **Dupliquer** pour créer une copie d'un graphique ou d'une zone de texte dans la même région.

6. Optionnel : Cliquez **Supprimer de l'espace supplémentaire** pour supprimer l'espace blanc vertical vide autour des widgets. Les espaces blancs verticaux vides seront supprimés de chaque région du tableau de bord.
7. Cliquez **Quitter le mode Layout** dans le coin supérieur droit de la page pour enregistrer vos modifications.

Note: Si un message d'erreur apparaît, cela signifie qu'un autre utilisateur est peut-être en train d'apporter des modifications. Il est préférable que chaque utilisateur d'ExtraHop ait un compte individuel.

Prochaines étapes

- Modifier une région
- Modifier un graphique à l'aide de l'explorateur de métriques
- Modifier une zone de texte

Modifier un graphique à l'aide de l'explorateur de métriques

L'explorateur de métriques est un outil de création et de modification de graphiques qui vous permet de créer des visualisations dynamiques du comportement des équipements et des réseaux.

Vous devez avoir une écriture personnelle privilèges ou supérieur et accès au module NPM pour créer et modifier des graphiques dans un tableau de bord.

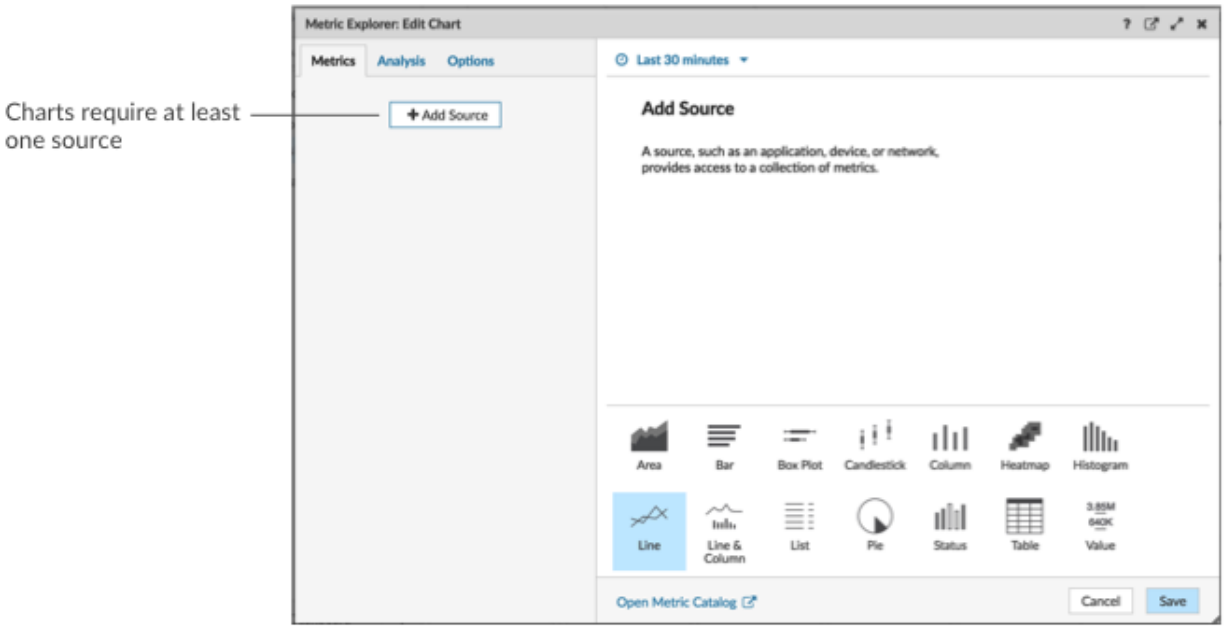
Vidéos: Consultez la formation associée : Choix d'une métrique

Création et modification d'un graphique de base

Avec l'explorateur de mesures, vous pouvez modifier les composants du graphique, tels que les sources , les mesures et les calculs de données, puis prévisualiser la façon dont les données métriques apparaissent dans différents types de graphiques. Lorsque vous êtes satisfait de vos sélections, enregistrez votre graphique dans un tableau de bord.

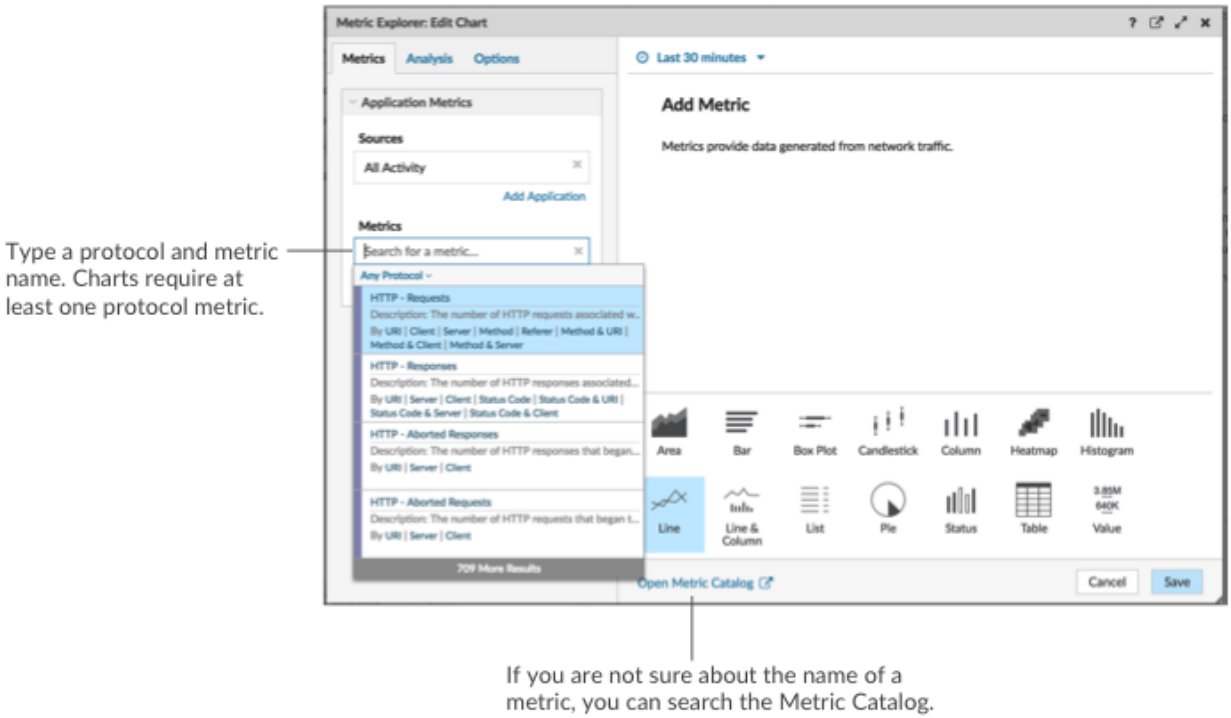
Les étapes suivantes présentent le flux de travail de base et les exigences minimales pour compléter un nouveau graphique.

1. Cliquez **Ajouter une source** puis sélectionnez une source.

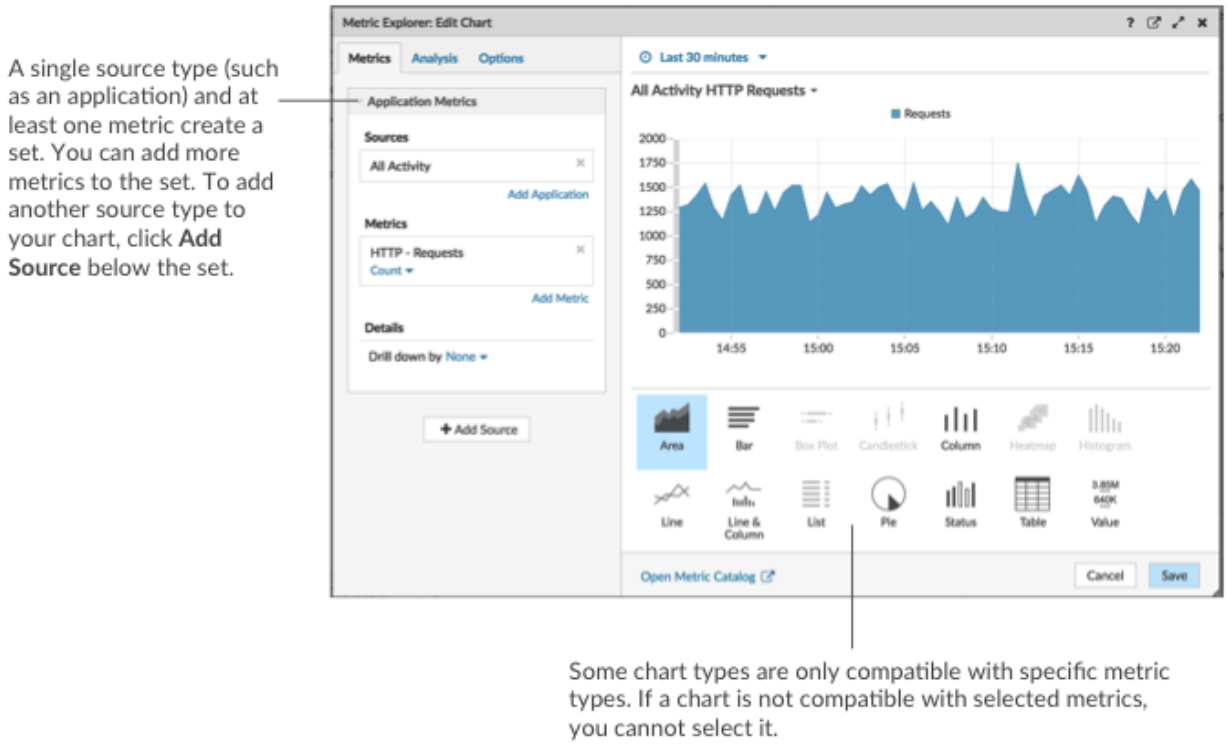


- Vous pouvez sélectionner une source statique pour le graphique en saisissant le nom d'une application, d'un équipement ou d'un réseau.
- Vous pouvez également sélectionner une source dynamique qui peut être modifiée dynamiquement par les utilisateurs du tableau de bord en tapant $ et en sélectionnant une variable dans Variable de type de source liste. Pour plus d'informations sur les variables de type source et les modèles de tableau de bord, voir Création d'un tableau de bord avec des sources dynamiques.

2. Sélectionnez la source dans la liste des résultats.
3. Dans le champ Metrics, saisissez un protocole et un nom de métrique. Sélectionnez ensuite la métrique dans la liste des résultats, comme illustré dans la figure suivante.



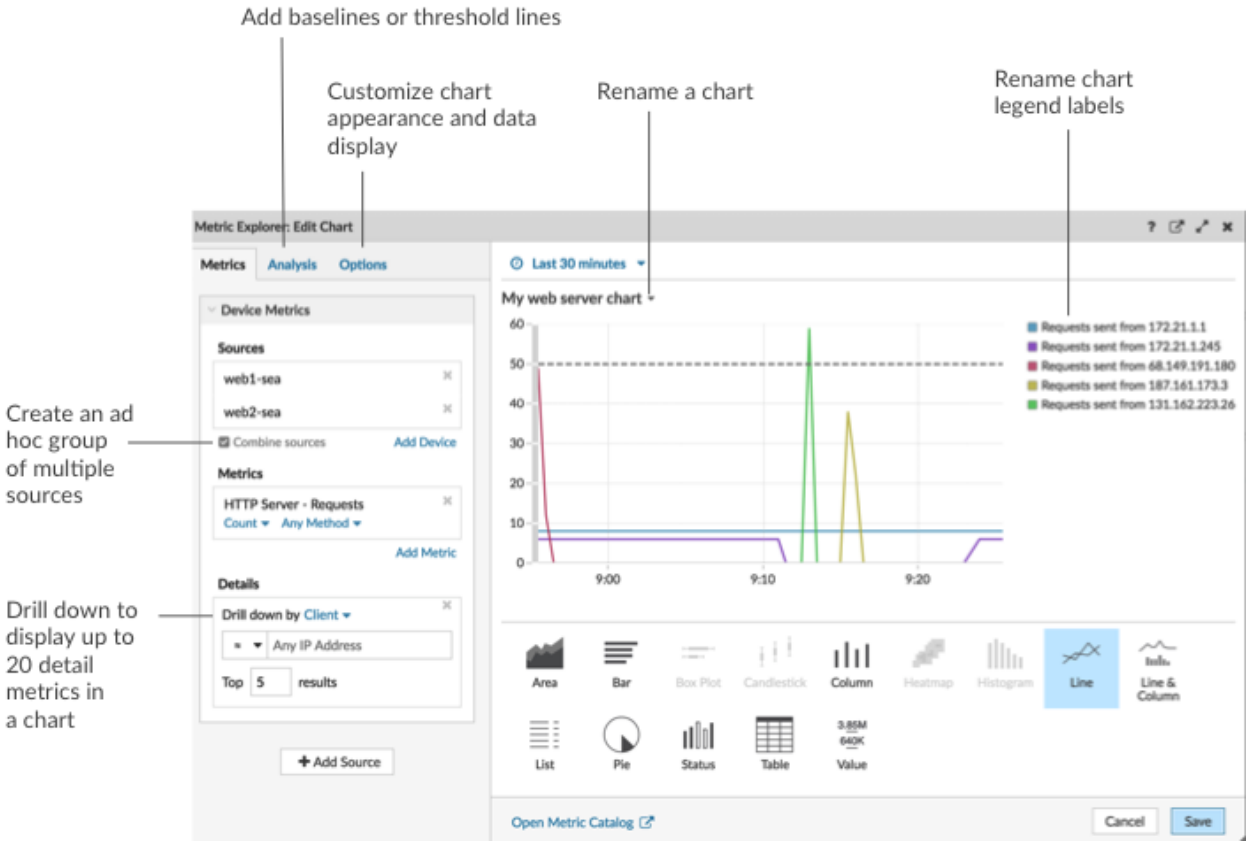
4. Sélectionnez un graphique en bas de l'explorateur de métriques, comme illustré dans la figure suivante.



5. Optionnel : Cliquez sur le lien déroulant situé sous le nom de la métrique pour afficher un décompte ou un taux ou percentile.
6. Effectuez l'une des étapes suivantes :
   - Cliquez **Enregistrer** lors de la création ou de la modification d'un graphique à partir d'un tableau de bord. Votre tableau de bord est mis à jour avec votre graphique de base.
   - Cliquez **Ajouter au tableau de bord** lors de la création ou de la modification d'un graphique à partir d'une page de protocole. Sélectionnez ensuite un tableau de bord existant dans la liste, ou sélectionnez **Créer un tableau de bord**.

Configuration des options avancées pour l'analyse des données et la personnalisation des graphiques

En fonction des mesures et du type de graphique que vous sélectionnez, vous pouvez configurer des options avancées pour créer des visualisations sophistiquées à l'aide de l'explorateur de métriques, comme illustré dans la figure suivante.



Explorez les données métriques et les sources pour afficher les détails
Dans la section Détails de l'onglet Mesures, vous pouvez effectuer une exploration vers le bas pour afficher les mesures détaillées ou effectuer une exploration vers le bas d'un groupe diciéquipements pour afficher les appareils individuels dans le graphique. Vous pouvez également filtrer les statistiques détaillées pour obtenir des correspondances exactes, ou créer un filtre regex .

Ajoutez une ligne de référence ou une ligne de seuil depuis l'onglet Analyse
Vous ajouter une ligne de base dynamique ou ligne de seuil statique à votre graphique. Les lignes de référence sont calculées une fois le graphique enregistré. Pour voir une ligne représentant un seuil, telle qu'une valeur d' accord de niveau de service (SLA), ajoutez une ligne de seuil statique à votre graphique.

Renommer les libellés des légendes et le titre du graphique
Pour les graphiques qui affichent une légende, vous pouvez modifier le nom d'une métrique dans la légende du graphique avec étiquette personnalisée. Dans l'explorateur de métriques, cliquez sur l'étiquette dans le volet d'aperçu, puis sélectionnez **Renommer**. Pour renommer un graphique, cliquez sur le titre du graphique et sélectionnez **Renommer**.

Personnalisez votre graphique depuis l'onglet Options
Vous pouvez accéder aux options suivantes pour personnaliser les propriétés du graphique et l'affichage des données métriques dans votre graphique :

- Convertir les données métriques d'octets en bits
- Convertir les données métriques de la base 2 (Ki=1024) en base 10 (K = 1000)
- Modifier l'axe Y d'un graphique chronologique en passant d'une échelle linéaire à une échelle logarithmique
- Abréger des valeurs métriques dans un graphique (par exemple, abréger 16 130 542 octets en 16,1 Mo)

- Triez les données métriques par ordre croissant ou décroissant dans un graphique à barres, une liste ou un graphique de valeurs
- Modifier la précision du percentile dans un graphique en camembert
- Masquer ou afficher la légende d'un graphique
- Masquer les mesures inactives avec une valeur nulle afin que ces mesures ne soient pas visibles dans le graphique, y compris la légende et l'étiquette
- Inclure Sparkline dans une liste ou un diagramme de valeurs
- Afficher l'état d'alerte pour les données affichées dans des listes ou des graphiques de valeurs (pour plus d'informations, voir Alertes)
- Passez l'affichage couleur des données métriques en niveaux de gris (à l'exception des graphiques qui affichent l'état d'une alerte)
- Pour les étiquettes d'adresse IP, affichez le nom d'hôte (s'il est détecté à partir du trafic DNS dans les données filaires) ou l'adresse IP d'origine (si un proxy est détecté à partir de données filaires)
- Afficher l'heure relative d'une date d'expiration, telle que le nombre de jours avant l'expiration d'un certificat TLS.

Note: Certaines options ne sont disponibles que pour des types de graphiques spécifiques. Par exemple, l' option permettant d'inclure un sparkline n'apparaît que dans l'onglet Options pour les graphiques de liste et de valeurs .

Créez un groupe ad hoc pour combiner des données provenant de plusieurs sources
Dans l'onglet Métrique, vous pouvez créer un groupe ad hoc de plusieurs sources au sein d'un ensemble en sélectionnant **Combiner les sources**. Par exemple, vous pouvez combiner deux applications, puis afficher une seule valeur métrique dans le graphique pour ces deux applications.

Prochaines étapes
Entraînez-vous à créer des graphiques en suivant les procédures pas à pas suivantes :

- Surveillez les erreurs DNS dans un tableau de bord
- Surveillez l'état de santé de la base de données dans un tableau de bord
- Surveillez les performances Web dans un tableau de bord

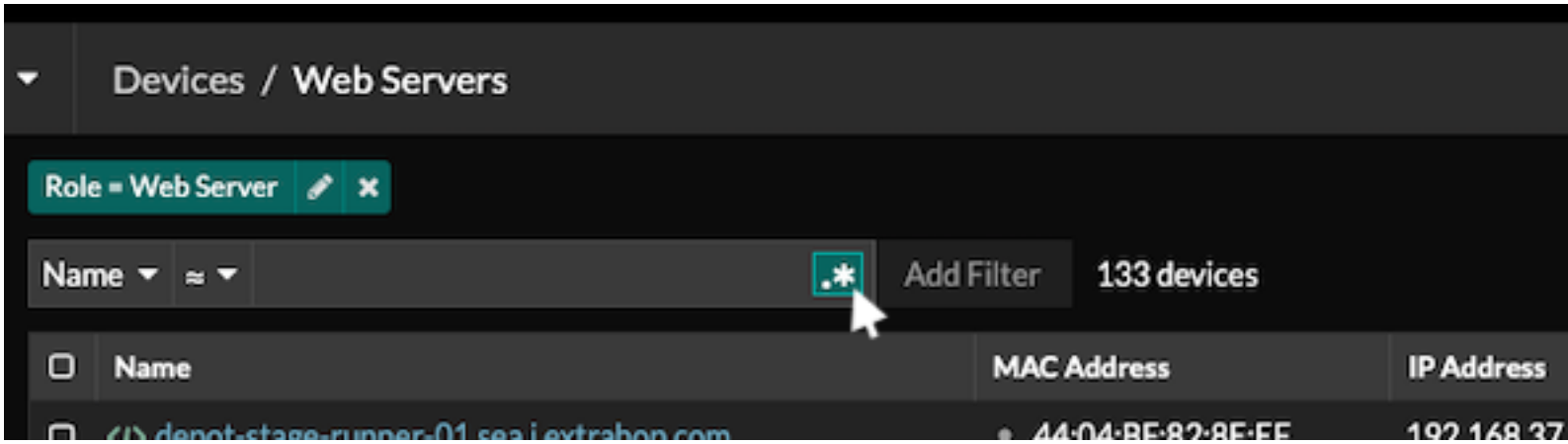
Filtres d'expressions régulières

Filtrez les résultats de votre recherche en écrivant des chaînes d'expressions régulières (regex) dans certains champs de recherche du système ExtraHop. Par exemple, vous pouvez filtrer les paramètres d' une clé métrique détaillée, comme un numéro dans une adresse IP. Vous pouvez également filtrer en excluant des clés spécifiques ou une combinaison de touches des graphiques.

Les champs de recherche compatibles Regex comportent des indicateurs visuels dans tout le système et acceptent la syntaxe standard.

Champs de recherche marqués d'un astérisque

Cliquez sur l'astérisque pour activer les chaînes regex.

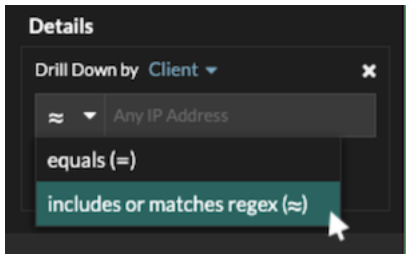


Ce type de champ est disponible sur les pages système suivantes :

- Filtrer un tableau d'appareils
- Création de critères de filtre pour un groupe dequipments dynamique

Certains champs de recherche avec un opérateur à trois champs

Cliquez sur la liste déroulante de l'opérateur pour sélectionner l'option regex.

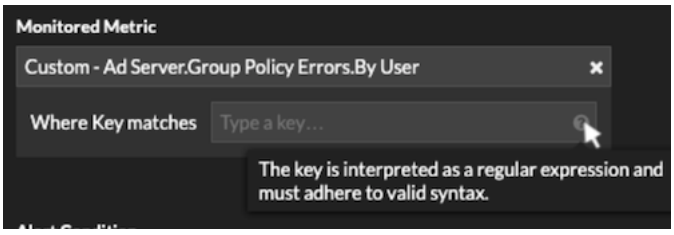


Ce type de champ est disponible sur la page système suivante :

- Modifier un graphique dans l'explorateur de métriques

Certains champs de recherche avec une info-bulle

Passez la souris sur l'info-bulle dans le champ pour voir quand l'expression régulière est requise.



Ce type de champ est disponible sur la page système suivante :

- Ajouter des relations d'enregistrement à une métrique personnalisée

Le tableau suivant inclut des exemples de syntaxe regex standard.

Scénario graphique	Filtre Regex	Comment ça marche
Comparez les codes d'état HTTP `200` à `404`.	`(200 et 404)`	Le symbole de la barre verticale (|) est l'opérateur OR. Ce filtre correspond `200`, ou `404`, ou les deux codes d'état.

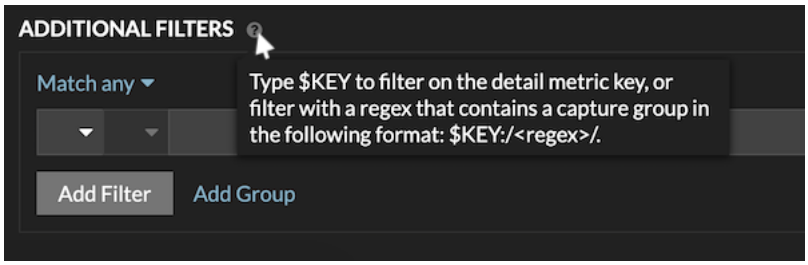
Scénario graphique	Filtre Regex	Comment ça marche
Afficher tout code dD'état HTTP contenant un 4.	`[41]`	Les crochets ([et]) désignent une plage de caractères. Le filtre recherche tous les caractères entre crochets, quel que soit leur ordre. Ce filtre correspond à toute valeur contenant un 4 ou un 1. Par exemple, ce filtre peut renvoyer `204`, `400`, `101`, ou `201` codes d'état.
Afficher tout `500`codes d'état HTTP de niveau.	`^ [5]`	Le signe du curseur (^) placé entre crochets ([et]) signifie « commence par ». Ce filtre correspond à toute valeur commençant par 5. Par exemple, ce filtre peut renvoyer `500` et `502` codes d'état.
Afficher tout `400` et `500`codes d'état HTTP de niveau.	`^ [45]`	Les valeurs multiples entre crochets ([et]) sont recherchées individuellement, même si elles sont précédées du signe caret (^). Ce filtre ne recherche pas les valeurs commençant par 45, mais correspond à toutes les valeurs commençant par un 4 ou 5. Par exemple, ce filtre peut renvoyer `400`, `403`, et `500` codes d'état.
Afficher tous les codes d'état HTTP sauf `200`codes d' état de niveau.	`^ (? ! 2)`	Un point d'interrogation (?) et point d'exclamation (!) entre parenthèses spécifient une valeur à exclure. Ce filtre correspond à toutes les valeurs sauf celles commençant par un 2. Par exemple, ce filtre peut renvoyer `400`, `500`, et `302` codes d'état.
Afficher n'importe quelle adresse IP avec `187.`	`187.`	Allumettes 1, 8, et 7 caractères de l'adresse IP. Ce filtre ne renverra pas les adresses IP se terminant par 187, car la fin de la période indique que quelque chose doit se trouver après les valeurs. Si vous souhaitez rechercher la période en tant que valeur littérale, vous devez la faire précéder d'une barre oblique inverse (\).
Vérifiez toutes les adresses IP contenant `187.18.`	`187 \ ,18.`	Allumettes `187.18` et tout ce qui va suivre. La première période est traitée littéralement car elle est précédée d'une barre oblique inverse (\). La deuxième période est traitée comme un joker. Par exemple, ce

Scénario graphique	Filtre Regex	Comment ça marche
		filtre renvoie les résultats pour `187.18.0.0`, `180.187.0.0`, ou `187.180.0.0/16`. Ce filtre ne renvoie pas d' adresse se terminant par `187.18`, car le caractère générique exige que les caractères suivent les valeurs spécifiées.
Afficher n'importe quelle adresse IP sauf `187.18.197.150`.	`^ (? ! 187 \ ,18 \ .197 \ .150)`	Correspond à tout sauf `187.18.197.150`, où `^(?!)` spécifie la valeur à exclure.
Excluez une liste d'adresses IP spécifiques.	`^(?! 187\.18\.197\.15[012])`	Correspond à tout sauf `187.18.197.150`, `187.18.197.151`, et `187.18.197.152`, où `^(?!)` spécifie la valeur à exclure et les crochets ([et]) indiquent plusieurs valeurs.

Filtres supplémentaires

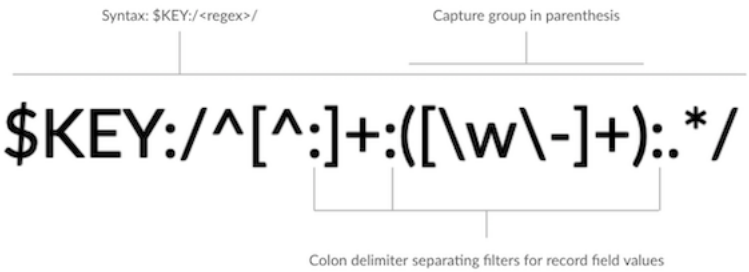
Quand tu créer une métrique détaillée personnalisée depuis le catalogue de métriques, vous pouvez ajouter une syntaxe regex avancée au champ de recherche Filtres supplémentaires de la section Record Relationships.

L'info-bulle apparaît une fois que vous avez sélectionné **Métrique détaillée** et n'est pas disponible lorsque **Métrique de base** est sélectionné.



La syntaxe regex de ce champ doit répondre aux exigences suivantes :

- Si votre clé contient plusieurs valeurs, votre syntaxe regex doit inclure un seul groupe de capture. Un groupe de capture est désigné par des parenthèses. Votre groupe de capture détermine la valeur du filtre.



- Si vous souhaitez renvoyer une valeur spécifique à partir d'une clé de métrique détaillée contenant plusieurs valeurs de champs d'enregistrement, l'expression régulière doit suivre la syntaxe suivante :

  `CLÉ $ :/ <regex> /`

  Par exemple, si votre clé métrique détaillée est ipaddr:host:cipher et que vous souhaitez uniquement renvoyer la valeur de l'adresse IP, vous devez taper ce qui suit :

  `$CLÉ : /^ ([^ :] +) : . +/`
- Si votre clé contient plusieurs valeurs de champ d'enregistrement, celles-ci sont séparées par un délimiteur spécifié dans le déclencheur qui génère la clé. L'emplacement des délimiteurs dans votre syntaxe regex doit correspondre à celui de la clé de détail. Par exemple, si vous avez une clé avec trois valeurs séparées par un séparateur composé de deux points, les trois valeurs de la clé dans votre syntaxe régulière doivent être séparées par deux points.

Conseil: Si vous souhaitez renvoyer toutes les valeurs des champs d'enregistrement dans une clé métrique détaillée, tapez `CLÉ $`. Par exemple, si votre clé métrique détaillée est ipaddr:host:cipher, tapez `CLÉ $` dans le champ de recherche pour renvoyer les trois valeurs d'enregistrement de ces champs (adresse IP, nom d'hôte et suite de chiffrement TLS).

Modifier un widget de zone de texte

Si vous souhaitez inclure un texte explicatif à côté des graphiques de votre tableau de bord ou afficher le logo d'une entreprise dans votre tableau de bord, vous pouvez modifier un widget de zone de texte. Le widget de zone de texte vous permet d'afficher du texte, des liens, des images ou des exemples de mesures dans votre tableau de bord.

Vidéo: Consultez la formation associée : Fournir du contexte à l'aide de widgets de zone de texte

Le widget de zone de texte prend en charge Markdown, une syntaxe de mise en forme simple qui convertit le texte brut en HTML avec des caractères non alphabétiques, tels que « # » ou « * ». Les nouveaux widgets de zone de texte contiennent des exemples Markdown. Un widget de zone de texte est automatiquement fourni chaque fois que vous créer un tableau de bord. Vous pouvez également ajouter un widget de zone de texte à la mise en page de votre tableau de bord.

Pour modifier un widget de zone de texte existant, procédez comme suit :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Dans le dock du tableau de bord, sélectionnez un tableau de bord contenant la zone de texte que vous souhaitez modifier.
4. Cliquez sur le menu de commandes ⋮ dans le coin supérieur droit et sélectionnez **Modifier la mise en page**.
5. Cliquez sur la zone de texte.
6. Tapez et modifiez le texte dans la partie gauche Rédacteur volet.

   Le texte de sortie HTML s'affiche dynamiquement sur la droite Aperçu volet. Avec Markdown, vous pouvez mettre en forme les types de contenu suivants :

   - Formater le texte
   - Ajouter des images
   - Ajouter des exemples métriques
7. Cliquez **Enregistrer** pour fermer l'explorateur de métriques.

Formater le texte dans Markdown

Le tableau suivant présente les formats Markdown courants pris en charge dans le widget de zone de texte.

Note: D'autres exemples de formats Markdown sont fournis dans le Guides GitHub : Maîtriser Markdown et dans le Spécification CommonMark.

Formater	Descriptif	Exemple
Rubriques	Placez un signe numérique (#) et un espace devant votre texte pour mettre en forme les titres. Le niveau du titre est déterminé par le nombre de signes numériques.	`#### Example H4 heading`
Listes non ordonnées	Placez un astérisque (*) avant votre texte. Si possible, placez chaque élément de la liste sur une ligne distincte.	`* First example` `* Second example`
Listes ordonnées	Placez le chiffre 1 et le point (1.) avant votre texte pour chaque élément de ligne ; Markdown incrémentera automatiquement le numéro de liste. Si possible, placez chaque élément de la liste sur une ligne distincte.	`1. First example` `1. Second example`
AUDACIEUX	Placez un double astérisque avant et après votre texte.	`**bold text**`
Italiques	Placez un trait de soulignement avant et après votre texte.	`_italicized text_`
Hyperliens	Placez le texte du lien entre crochets avant l'URL entre parenthèses. Ou saisissez votre URL. Les liens vers des sites Web externes s'ouvrent dans un nouvel onglet du navigateur. Les liens du système ExtraHop, tels que les tableaux de bord, s'ouvrent dans l'onglet actuel du navigateur.	`[Visit our home page](https://www.extrahop.com)` `https://www.extrahop.com`
Citations en blocs	Placez un crochet à angle droit et un espace devant votre texte.	`On the ExtraHop website:` `> Access the live demo and review case studies.`
Fonte Monospace	Placez un backtick (`) avant et après votre texte.	`` `example code block` ``
Emojis	Copiez et collez une image emoji dans la zone de texte. Consultez les Graphique Emoji Unicode site web pour les images. La syntaxe Markdown ne prend pas en charge les shortcodes emoji.	

Ajouter des images dans Markdown

Vous pouvez ajouter des images au widget de zone de texte en créant un lien vers celles-ci. Assurez-vous que votre image est hébergée sur un réseau accessible au système ExtraHop.

Les liens vers les images doivent être spécifiés au format suivant :

```
![<alt_text>](<file_path>)
```

Où *<alt_text>* est le texte alternatif pour le nom de l'image et *<file_path>* est le chemin de l'image. Par exemple :

```
![Graph](/images/graph_1.jpg)
```

Note: Vous pouvez également ajouter des images en les encodant en Base64. Pour plus d'informations, consultez le post suivant sur le forum ExtraHop, »Encoder une image pour l'inclure dans une zone de texte».

Ajouter des exemples métriques dans Markdown

Vous pouvez écrire une requête métrique pour inclure une valeur métrique en ligne avec le texte du widget de zone de texte. Par exemple, pour indiquer le nombre de serveurs Web ayant renvoyé une erreur 404, vous pouvez ajouter une requête métrique à une phrase et la valeur est mise à jour dans le texte.

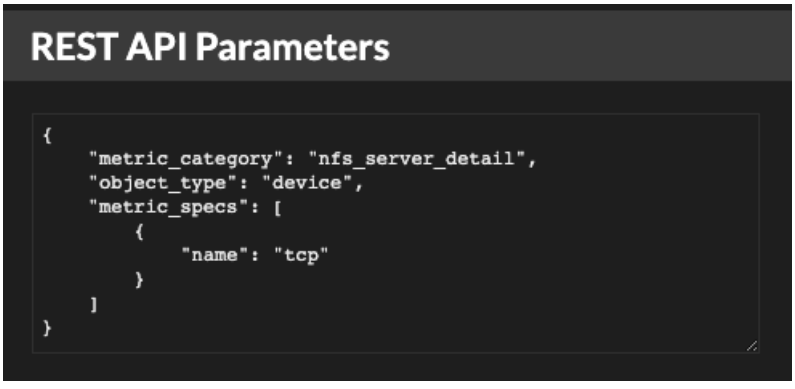
L'exemple suivant montre le format de base pour écrire des requêtes métriques :

```
%%metric:{
    "metric_category": "<metric_category>",
    "object_type": "<object_type>",
    "object_ids": [object_id],
    "metric_specs": [
        {
            "name": "<metric_spec>"
        }
    ]
}%%
```

Pour localiser le `object_type`, `metric_spec`, et `metric_category` pour les valeurs d'une métrique, procédez comme suit :

1. Cliquez **Réglages**
2. Cliquez **Catalogue métrique**.
3. Entrez le nom de la métrique dans le champ de recherche.
4. Sélectionnez la métrique et notez les valeurs de `metric_category`, `object_type`, et `metric_spec` dans le Paramètres de l'API REST section.

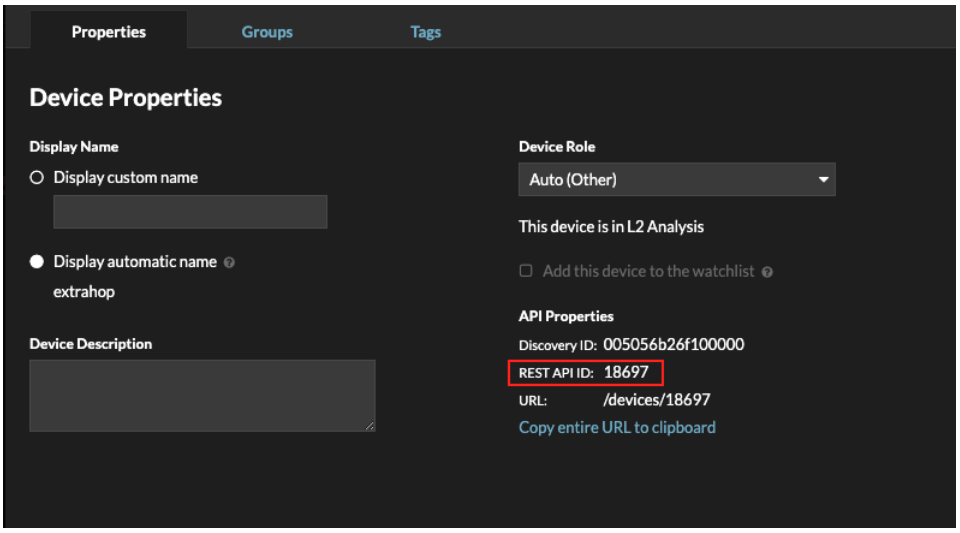
La figure suivante affiche les valeurs pour le serveur NFS - requêtes TCP par client.



Pour localiser le `object_id` pour un équipement, un groupe de dispositifs ou un autre actif , procédez comme suit :

1. Cliquez **Actifs**, puis cliquez sur un type d'actif dans le volet de gauche.
2. Cliquez sur le nom de l'actif souhaité, puis ouvrez la fenêtre des propriétés.
3. Notez la valeur affichée pour l'ID de l'API REST.

La figure suivante affiche les propriétés d'un équipement dont l'ID est 18697.



Après avoir localisé les valeurs de la métrique que vous souhaitez afficher, ajoutez-les à la requête métrique dans l'éditeur de texte. La valeur sera affichée dans le widget de texte.

L'exemple de balisage suivant affiche le nombre de demandes TCP reçues, répertoriées par adresse IP du client, pour un serveur NFS portant l'ID d'objet 18697.

Note: Les requêtes métriques suivantes ne sont pas prises en charge dans le widget de zone de texte :

- Requêtes de séries chronologiques
- Calculs moyens
- Object_ids multiples
- Plusieurs metric_spec
- Percentiles multiples

Exemples de requêtes métriques pour le widget de zone de texte
Les exemples suivants vous montrent comment écrire des requêtes métriques de haut niveau, ou de base, pour des objets d' application, d'équipement et de réseau. Vous pouvez également rédiger une requête pour obtenir des métriques détaillées.

Métriques relatives aux applications

Pour spécifier l'objet All Activity, `object_ids` est `»0»`.

Cet exemple de requête montre comment récupérer des métriques HTTP à partir de l'objet d' application All Activity et affiche le résultat suivant : `»Getting [value] HTTP requests and [value] HTTP responses from All Activity.»`

```
Getting
%%metric:{
"object_type": "application",
"object_ids": [0],
"metric_category": "http",
"metric_specs": [{"name":"req"}]
}%%HTTP requests and
%%metric:{
"object_type": "application",
"object_ids": [0],
"metric_category": "http",
"metric_specs": [{"name":"rsp"}]
}%%
HTTP responses from All Activity.
```

Métriques de l'appareil

Vous devez spécifier soit un client (`»_client»`) ou serveur (`»_server»`) dans le `metric_category`. Pour récupérer les métriques d'un équipement spécifique, spécifiez le numéro d'identification de l'objet de l'équipement dans `object_ids`. Pour récupérer l'identifiant de l'objet de l'équipement (`deviceOid`), recherchez l'objet de l'équipement dans la recherche globale ExtraHop. Sélectionnez l'équipement dans les résultats de recherche. Le `»deviceOid=»` la valeur sera incorporée dans la chaîne de requête URL.

Cet exemple de requête montre comment récupérer des métriques à partir d'un objet client d'équipement et affiche le résultat suivant : `»Getting [value] CLIENT DNS response errors from a specific device.»`

```
Getting
%%metric:{"object_type": "device",
"object_ids": [8],
"metric_category": "dns_client",
"metric_specs": [{"name":"rsp_error"}]
}%%
CLIENT DNS response errors from a specific device.
```

Cet exemple de requête montre comment récupérer des métriques à partir d'un objet de serveur d'équipement et affiche le résultat suivant : `»Getting [value] SERVER DNS response errors from a specific device.»`

```
Getting
%%metric:{
"object_type": "device",
"object_ids": [156],
"metric_category": "dns_server",
"metric_specs": [{"name":"rsp_error"}]
}%%
SERVER DNS response errors from a specific device.
```

Métriques du réseau

Pour spécifier tous les réseaux, `object_type` est »`capture`» et le `object_ids` est »`0`. » Pour spécifier un VLAN spécifique, `object_type` est »`vlan`» et le `object_ids` est le numéro de VLAN.

Cet exemple de requête montre comment récupérer des métriques pour tous les réseaux et affiche le résultat suivant : »`Getting [value] broadcast packets from all networks.`»

```
Getting
%%metric:{
"object_type": "capture",
"object_ids": [0],
"metric_category": "net","metric_specs":
 [{"name":"frame_cast_broadcast_pkts"}]
}%%
broadcast packets from all networks.
```

Cet exemple de requête montre comment récupérer des métriques pour un VLAN spécifique et affiche le résultat suivant : »`Getting [value] broadcast packets from VLAN 3.`»

```
Getting
%%metric:{
"object_type": "vlan",
"object_ids": [3],
"metric_category": "net",
"metric_specs": [{"name":"frame_cast_broadcast_pkts"}]
}%%
broadcast packets from VLAN 3.
```

Métriques du groupe

Pour spécifier un groupe, `object_type` est »`device_group`. » Vous devez spécifier soit un client (»`_client`») ou serveur (»`_server`») dans le `metric_category`. Le `object_ids` pour le groupe spécifique doit être récupéré depuis l' explorateur d'API REST.

Cet exemple de requête montre comment récupérer des métriques pour tous les réseaux et affiche le résultat suivant : »`Getting [value] HTTP responses from the HTTP Client Device Group.`»

```
Getting
%%metric:{
"object_type": "device_group",
"object_ids": [17],
"metric_category": "http_client",
"metric_specs": [{"name":"req"}]
}%%
HTTP responses from the HTTP Client Device Group.
```

Métriques détaillées

Si vous souhaitez récupérer des métriques détaillées, votre requête de métrique doit contenir des paramètres clés supplémentaires, tels que key1 et key2 :

- type_objet
- identifiant_objets
- catégorie_métrique
- metric_spec
  - nom
  - clé1

- clé 2

Les paramètres clés agissent comme un filtre pour afficher les résultats métriques détaillés. Pour les mesures détaillées non personnalisées, vous pouvez récupérer les paramètres de mesure détaillés à partir du catalogue de mesures. Par exemple, tapez `Réponses HTTP par URI`, puis examinez les valeurs des paramètres dans la section Paramètres de l'API REST.

Important: Vous devez fournir le `object_ids` dans votre requête.

Cet exemple montre comment récupérer des requêtes HTTP par URI pour l'application All Activity (`object_ids` est »`0`») :

```
%%metric:{
"object_type": "application",
"object_ids": [0],
"metric_category": "http_uri_detail",
"metric_specs": [{"name":"req"}]
}%%
```

Cet exemple de requête vous montre comment récupérer des requêtes HTTP par des URI contenant une valeur clé pour »`pagead2`» pour l'application All Activity (`object_ids` est »`0`») :

```
%%metric:{
"metric_category": "http_uri_detail",
"object_type": "application",
"object_ids": [0],
"metric_specs": [
{
"name": "req",
"key1": "/pagead2/"
}
]
}%%
```

Cet exemple de requête montre comment récupérer les mesures de comptage pour tous les réseaux et affiche le résultat suivant : »`Getting [value] detail ICA metrics on all networks.`»

```
Getting
%%metric:{
"object_type": "capture",
"object_ids": [0],
"metric_category": "custom_detail",
"metric_specs": [{
"name":"custom_count",
"key1":"network-app-byte-detail-ICA"
}]
}%%
detail ICA metrics on all networks.
```

Cet exemple de requête montre comment récupérer une statistique de jeu de données personnalisée avec des clés topn et des percentiles, et affiche le résultat suivant : »`The fifth percentile is: [value].`»

```
The fifth percentile is:
%%metric:{
"object_type": "vlan",
"object_ids": [1],
"metric_category": "custom_detail",
"metric_specs": [{
"name": "custom_dset",
"key1": "myCustomDatasetDetail",
```

```
"key2": "/10.10.7/",
"calc_type": "percentiles",
"percentiles": [5]
}]
}%%
.
```

Note: Exemples de métriques ne sont pas pris en charge dans le widget de zone de texte. Par exemple, en ajoutant le `"calc_type": "mean"` le paramètre de votre requête de zone de texte n'est pas pris en charge.

Modifier une région de tableau de bord

Les régions du tableau de bord, qui contiennent des graphiques et des widgets, sont hautement personnalisables. Lorsque vous travaillez avec des tableaux de bord, il se peut que vous deviez fréquemment modifier ou copier une région. Vous pouvez uniquement supprimer, redimensionner ou réorganiser une région en modifiant la disposition du tableau de bord.

Pour modifier les propriétés de base d'une région dans un tableau de bord, procédez comme suit :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Dans le dock du tableau de bord, sélectionnez un tableau de bord contenant la région que vous souhaitez modifier.
4. Cliquez sur l'en-tête de la région pour accéder aux options suivantes :

Renommer une région

Ajoutez un nom personnalisé à la région.

Modifier les sources

Remplacez rapidement les sources de données de chaque graphique d'une région par une source différente après copie d'un graphique, région, ou tableaux de bord.

Copier une région

Passez la souris sur **Copier vers...** et effectuez l'une des sélections suivantes :

- Sélectionnez le nom d'un tableau de bord existant dans la liste. La page du tableau de bord s'ouvre et affiche l'emplacement de la région copiée.

  Conseil: La liste des tableaux de bord est ordonnée depuis les derniers tableaux de bord créés (en bas) jusqu'aux tableaux de bord les plus anciens (en haut).
- Sélectionnez **Créer un tableau de bord**. Dans la fenêtre Propriétés du tableau de bord, tapez le nom du nouveau tableau de bord.

Modifier l'intervalle de temps de la région

Appliquer un intervalle de temps à l'ensemble de la région en activant le sélecteur de temps régional.

Plein écran

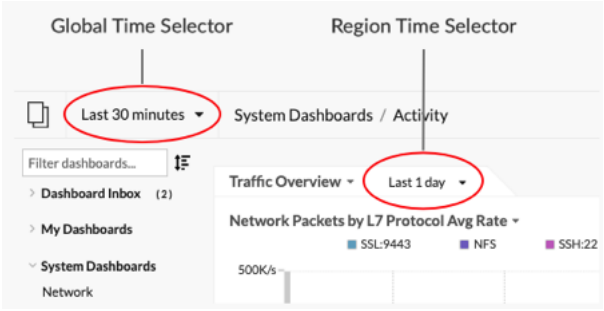
Développez le contenu de la région en mode plein écran.

Prochaines étapes

- Modifier la mise en page d'un tableau de bord
- Modifier un graphique avec l'explorateur de métriques

Modifier l'intervalle de temps pour une région du tableau de bord

Dans un tableau de bord, vous pouvez appliquer un intervalle de temps à l'ensemble d'un tableau de bord à l'aide du sélecteur de temps global, ou appliquer un intervalle de temps différent par région à l'aide du sélecteur de temps de région.



1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Sélectionnez un tableau de bord.
4. Cliquez sur l'en-tête de la région, puis sélectionnez **Utiliser le sélecteur d'heure par région**.
5. Cliquez **Les 30 dernières minutes** et effectuez l'une des étapes suivantes :
   - Dans l'onglet Intervalle de temps, sélectionnez l'une des options suivantes :
     - Sélectionnez un autre intervalle de temps (tel que **Les 30 dernières minutes**, **Les 6 dernières heures**, **Dernier jour**, ou **La semaine dernière**).
     - Spécifiez une unité de temps personnalisée.
     - Sélectionnez une plage horaire personnalisée. Cliquez sur un jour pour spécifier la date de début de la plage. Un seul clic permet de spécifier un seul jour. Cliquez sur un autre jour pour spécifier la date de fin de la plage.
     - Comparez les deltas métriques à partir de deux intervalles de temps différents.
   - Dans l'onglet Historique, sélectionnez un maximum de cinq intervalles de temps récents sélectionnés lors d'une session de connexion précédente.
6. Cliquez **Enregistrer** pour fermer le sélecteur de temps régional.
   Le nouvel intervalle de temps est appliqué à tous les graphiques et widgets de la région.
7. Pour supprimer l'intervalle de temps entre les régions, cliquez sur l'en-tête de la région et sélectionnez **Utiliser le sélecteur de temps global**.
   Lorsque l'intervalle de temps disparaît de l'en-tête de région, l'intervalle de temps global est appliqué à la région.

Modifier les propriétés du tableau de bord

Pour renommer un tableau de bord, modifier le thème ou modifier l'URL, vous devez modifier les propriétés du tableau de bord. Lorsque vous créez un tableau de bord, vous avez la possibilité de définir les propriétés du tableau de bord. Vous pouvez toutefois modifier les propriétés du tableau de bord à tout moment.

Vous ne pouvez modifier les propriétés que d'un seul tableau de bord à la fois. Vous ne pouvez pas sélectionner plusieurs tableaux de bord et modifier une propriété, telle que l'auteur du tableau de bord.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Dans le dock du tableau de bord, sélectionnez le tableau de bord que vous souhaitez modifier.
4. Cliquez sur le menu de commande ⋮ dans le coin supérieur droit de la page, puis sélectionnez **Propriétés du tableau de bord**.
5. Dans le Propriétés du tableau de bord dans cette fenêtre, vous pouvez modifier les champs suivants :

   Titre

   Renommez le tableau de bord.

   Auteur

   Changez le nom de l'auteur.

Description

Modifiez la description du tableau de bord. Notez que la description n'est visible que lors de la modification des propriétés du tableau de bord.

Permalien

Modifiez l'URL du tableau de bord. Par défaut, le permalien, également appelé code court, est un identifiant unique à cinq caractères qui apparaît après `/Dashboard` dans l'URL. Vous pouvez remplacer le permalien par un nom plus convivial.

Note: Le permalien peut comporter jusqu'à 100 caractères combinant des lettres, des chiffres et les symboles suivants : point (.), trait de soulignement (_), tiret (-), signe plus (+), parenthèses () et crochets ([]). Les autres caractères alphanumériques ne sont pas pris en charge. Le permalien ne peut pas contenir d'espaces.

Partage

Pour partager un tableau de bord avec des utilisateurs qui peuvent le consulter et le modifier, cliquez sur le lien. Pour plus d'informations, voir Partager un tableau de bord.

Rédacteurs

Consultez la liste des utilisateurs d'ExtraHop ayant un accès d'édition au tableau de bord. Pour modifier les utilisateurs, cliquez sur **Partage**.

6. Cliquez **Enregistrer**.

Présenter un tableau de bord

Vous pouvez configurer votre tableau de bord pour qu'il s'affiche en mode plein écran pour les présentations ou pour les écrans de votre centre d'exploitation réseau.

Le mode plein écran propose les options d'affichage suivantes :

- Vous pouvez consulter l'ensemble du tableau de bord et interagir avec celui-ci en mode présentation.
- Vous pouvez afficher un cycle continu de chaque graphique dans le tableau de bord dans un diaporama de widgets.
- Vous pouvez consulter un région unique en affichage plein écran .

Pour présenter un tableau de bord complet en plein écran, procédez comme suit :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Dans le dock du tableau de bord, sélectionnez le tableau de bord que vous souhaitez présenter.
4. Dans le coin supérieur droit de la page, cliquez sur le menu de commandes ⋮ et sélectionnez l'une des options suivantes :

Mode de présentation

Le dock du tableau de bord et les menus de navigation supérieurs s'effondrent. Vous pouvez interagir avec l'intervalle de temps et les composants du tableau de bord en mode présentation.

Diaporama de widgets

Un cycle continu de graphiques et de widgets s'affiche en plein écran . Sélectionnez la durée pendant laquelle vous souhaitez que chaque widget s'affiche (par exemple, **20 secondes**, **15 secondes**, etc.). Cliquez sur **x** icône dans le coin supérieur droit de l'écran pour revenir au tableau de bord.

Conseil: Pour ouvrir un tableau de bord en mode présentation, ajoutez `/presentation` à la fin de l'URL, puis ajoutez-la à vos favoris. Par exemple :

```
https://<extrahop_ip>/extrahop/#/Dashboard/437/presentation
```

Partager un tableau de bord

Par défaut, tous les tableaux de bord personnalisés que vous créez sont privés, ce qui signifie qu'aucun utilisateur d' ExtraHop ne peut consulter ou modifier votre tableau de bord. Cependant, vous pouvez partager votre tableau de bord en accordant un accès de consultation ou de modification à d'autres utilisateurs et groupes d'ExtraHop.

Voici quelques points importants à prendre en compte concernant le partage de tableaux de bord :

- La manière dont un utilisateur interagit avec un tableau de bord partagé et les informations qu'il peut consulter dans le système ExtraHop sont déterminées par les privilèges de l'utilisateur. Par exemple, vous pouvez ajouter un utilisateur avec le privilège de lecture seule restreint, qui permet à cet utilisateur de consulter uniquement les tableaux de bord que vous partagez avec lui dans le système ExtraHop. Pour plus d'informations, consultez le Privilèges utilisateur section du guide des administrateurs d'ExtraHop.
- Lorsque vous accordez l'autorisation de modification à un utilisateur, celui-ci peut modifier et partager le tableau de bord avec d'autres utilisateurs, puis l'ajouter à une collection. Toutefois, les autres utilisateurs ne peuvent pas supprimer le tableau de bord. Seul le propriétaire du tableau de bord peut supprimer un tableau de bord.
- Les informations de groupe sont importées dans le système ExtraHop depuis LDAP (tel qu'OpenLDAP ou Active Directory). Les informations utilisateur sont disponibles une fois qu'un utilisateur ExtraHop se connecte à son compte.
- Pour partager un tableau de bord avec un utilisateur qui n'est pas un utilisateur d'ExtraHop, vous pouvez créer un fichier PDF du tableau de bord.
- Tu peux créer un rapport de tableau de bord planifié, qui envoie régulièrement le fichier PDF du tableau de bord à n'importe quel destinataire d'e-mail. (Consoles uniquement.)

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Dans le dock du tableau de bord, sélectionnez le tableau de bord que vous souhaitez partager.

   Vous ne pouvez pas partager les tableaux de bord du système ou les tableaux de bord auxquels vous n'avez pas accès aux modifications.
4. Cliquez sur le menu de commande ⋮ dans le coin supérieur droit de la page du tableau de bord et sélectionnez **Partagez**.
5. Pour accorder l'autorisation de consultation à tous les utilisateurs, sélectionnez **Autoriser tous les utilisateurs à consulter ce tableau de bord**.
6. Pour accorder l'autorisation de consultation ou de modification à certains utilisateurs et groupes, procédez comme suit :
   a) Tapez le nom d'un utilisateur ou d'un groupe, puis sélectionnez-le dans la liste déroulante.
   b) À côté du nom, sélectionnez **Peut voir** ou sélectionnez **Peut modifier**.
7. Cliquez **Enregistrer**.
   Si vous avez partagé votre tableau de bord, une petite icône grise apparaîtra à côté de votre tableau de bord dans le dock.

Supprimer l'accès à un tableau de bord

Vous pouvez supprimer ou modifier l'accès au tableau de bord que vous avez accordé aux utilisateurs et aux groupes.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Dans le dock du tableau de bord, sélectionnez le tableau de bord personnalisé que vous souhaitez modifier.
4. Cliquez sur le menu de commande ⋮ dans le coin supérieur droit de la page et sélectionnez **Partagez**.

5. Supprimez l'accès des utilisateurs ou des groupes en effectuant l'une des étapes suivantes :
   - Supprimer tous les accès d'un utilisateur ou d'un groupe en cliquant sur le bouton rouge Supprimer **(x)** icône à côté du nom de l'utilisateur ou du groupe.
   - Supprimer l'accès aux modifications en sélectionnant **Peut voir** dans la liste déroulante située à côté du nom de l'utilisateur ou du groupe.
6. Cliquez **Enregistrer**.

Création d'une collection de tableaux de bord

Vous pouvez créer une collection pour organiser les tableaux de bord dont vous êtes propriétaire et qui ont été partagés avec vous.

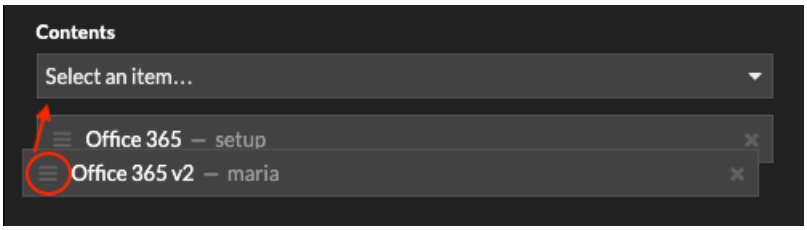
Voici quelques points importants à prendre en compte à propos des collections de tableaux de bord :

- Votre privilèges utilisateur déterminez si vous pouvez créer et partager des collections.
- Vous pouvez ajouter n'importe quel tableau de bord à une collection que vous possédez ou que vous êtes autorisé à consulter ou à modifier.
- Vous pouvez ajouter un tableau de bord à plusieurs collections.
- Vous pouvez partager une collection si vous êtes propriétaire de tous les tableaux de bord de cette collection ou si vous êtes autorisé à les modifier.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Cliquez **Collections** en haut du tableau de bord, puis cliquez sur **Créer une collection** au bas du quai.
4. Dans le **Nom** champ, saisissez un nom unique pour la collection.
5. Optionnel : Dans le **Descriptif** champ, ajoutez des informations sur la collection.
6. Optionnel : Entrez le nom d'un utilisateur ou d'un groupe dans le **Partage** liste déroulante, sélectionnez dans les résultats de recherche, puis cliquez sur **Ajouter**.
7. Entrez le nom d'un tableau de bord dans le **Sommaire** liste déroulante, puis sélectionnez dans les résultats de recherche.

   Le nom du propriétaire est affiché pour chaque tableau de bord ajouté.

   Conseil : Le tableau de bord en haut de la liste s'affiche par défaut lorsque la collection est sélectionnée dans le dock du tableau de bord. Cliquez et faites glisser l'icône à côté du nom d'un tableau de bord pour réorganiser la liste.



8. Cliquez **Enregistrer**.
   La collection est ajoutée au dock du tableau de bord.

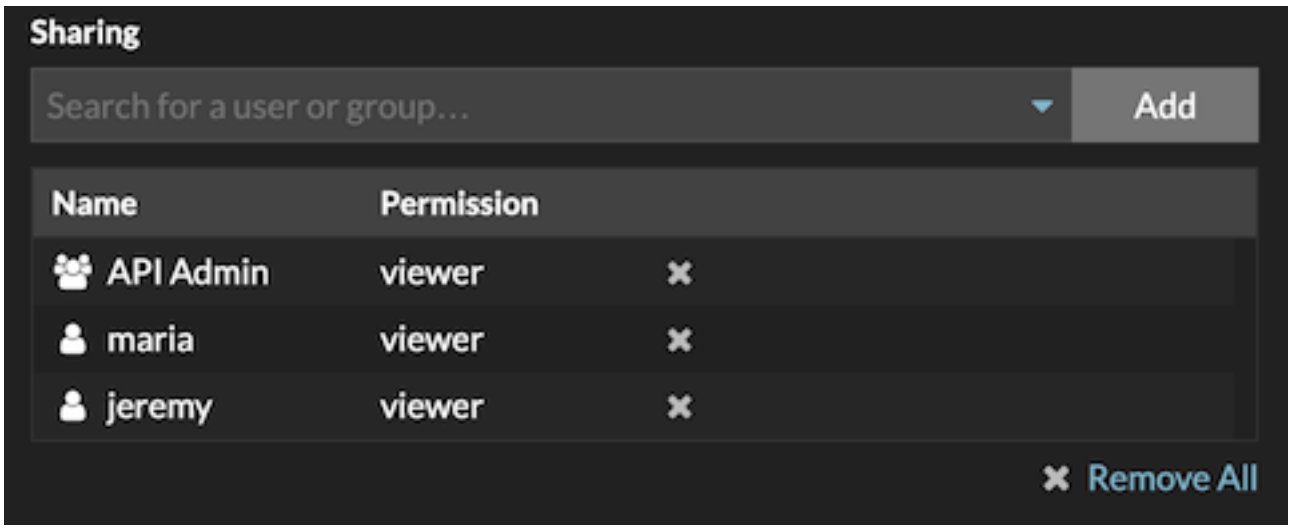
Partager une collection de tableaux de bord

Par défaut, toutes les collections de tableaux de bord sont privées, ce qui signifie qu'aucun autre utilisateur ne peut consulter ou modifier votre collection. Toutefois, vous pouvez partager votre collection avec d'autres utilisateurs et groupes.

Voici quelques points importants à prendre en compte concernant le partage de collections de tableaux de bord :

- Vous ne pouvez partager une collection que si vous êtes propriétaire de tous les tableaux de bord de la collection ou si vous êtes autorisé à les modifier.
- Les utilisateurs peuvent uniquement consulter les tableaux de bord d'une collection partagée ; ils ne peuvent modifier aucune propriété de collection.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Cliquez **Collections** en haut du tableau de bord.
4. Cliquez sur la collection que vous souhaitez partager, puis sur **Modifier**.
5. Entrez le nom d'un utilisateur ou d'un groupe dans le **Partage** liste déroulante, puis sélectionnez dans les résultats de recherche.
6. Cliquez **Ajouter**.
   L'utilisateur ou le groupe est affiché dans une liste d'utilisateurs partagés.



Conseil Supprimez un utilisateur ou un groupe en cliquant sur l'icône de suppression (X) à côté du nom.

7. Cliquez **Enregistrer**.
   La collection apparaît dans le dock du tableau de bord pour chaque utilisateur partagé.

Exporter des données

Vous pouvez exporter les données graphiques du système ExtraHop aux formats CSV et XLSX.

Vous pouvez également créer des PDF de graphiques, de pages et de tableaux de bord ExtraHop.

Exporter des données vers Excel

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Accédez à un tableau de bord ou page de protocole.
3. Cliquez avec le bouton droit sur un graphique, un tableau ou une métrique et sélectionnez **Exporter vers Excel**.

Exporter les données au format CSV

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Accédez à un tableau de bord ou page de protocole.
3. Cliquez avec le bouton droit sur un graphique, un tableau ou une métrique et sélectionnez **Exporter au format CSV**.

Création d'un fichier PDF

Vous pouvez exporter les données d'un tableau de bord, d'une page de protocole ou d'un graphique individuel sous forme de fichier PDF.

1. Recherchez le tableau de bord ou la page de protocole qui contient les données que vous souhaitez exporter et effectuez l'une des étapes suivantes :
   - Pour créer un fichier PDF de la page entière, cliquez sur le menu de commande ⋮ dans le coin supérieur droit de la page et sélectionnez **Imprimer** à partir d'une sonde ou **Exporter au format PDF** depuis une console.
   - Pour créer un fichier PDF contenant un graphique ou un widget individuel, cliquez sur le titre du graphique et sélectionnez **Imprimer** à partir d'une sonde ou sélectionnez **Exporter au format PDF** depuis le menu déroulant d'une console.
2. Une boîte de dialogue d'aperçu du PDF s'ouvre. Effectuez l'une des étapes suivantes :
   - Cliquez **Imprimer la page** puis sélectionnez **PDF** comme destination dans les paramètres d'impression de votre navigateur.
   - À partir d'une sonde, cliquez sur **Widget d'impression** et sélectionnez **PDF** comme destination dans les paramètres d'impression de votre navigateur.
   - À partir d'une console, sélectionnez Personnalisations du format PDF puis cliquez sur **Exporter au format PDF**. Le processus de génération d'un PDF peut prendre plusieurs secondes.

Personnaliser le format d'un fichier PDF

Lorsque vous créez un fichier PDF d'un tableau de bord ou d'une page de protocole à partir d'un console, vous disposez de plusieurs options pour personnaliser l'apparence de votre fichier PDF.

1. Entrez un nom personnalisé pour votre fichier PDF ou acceptez le nom par défaut.
2. Choisissez l'une des options de largeur de page suivantes :

   Étroit

   Affiche du texte volumineux dans les titres et les étiquettes des graphiques, mais laisse moins d' espace pour afficher les données des graphiques. Les longs titres et libellés des graphiques peuvent être tronqués.

   Moyen

   (Recommandé) Affiche une vue des titres, des légendes et des données des graphiques optimisée pour l'orientation des pages en mode portrait.

   Large

   Affiche du texte de petite taille dans les titres et les étiquettes des graphiques, mais offre plus d' espace pour afficher les données des graphiques.
3. Choisissez l'une des options de saut de page suivantes :

   Une seule page

   Affiche l'intégralité du tableau de bord ou de la page de protocole sur une seule page continue. Ce paramètre peut générer un fichier PDF plus grand que le format de page standard de l'imprimante.

   Saut de page par région

   Affiche chaque région du graphique sur une page individuelle.

4. Choisissez l'un des thèmes suivants :

   Lumière
   Fond blanc avec texte foncé.

   Sombre
   Fond noir avec texte blanc.

   Espace
   Fond sombre avec image d'arrière-plan et texte stylisés.

5. Cliquez **Exporter au format PDF**.
   Le processus de génération d'un PDF peut prendre plusieurs secondes.

Prochaines étapes
Le fichier PDF sera téléchargé sur votre ordinateur local. Chaque fichier PDF inclut le titre du tableau de bord et l'intervalle de temps. Cliquez **Voir le rapport sur ExtraHop** pour ouvrir le tableau de bord d'origine défini selon l'intervalle de temps spécifié dans le fichier PDF.

Création d'un rapport planifié

À partir d'un console, vous pouvez planifier l'envoi par e-mail à des destinataires spécifiques de rapports contenant des informations sur l'activité de votre système ExtraHop. Créez un rapport de tableau de bord planifié pour envoyer par e-mail un fichier PDF contenant les informations sélectionnées sur les tableaux de bord, notamment des graphiques et des mesures. Créez un rapport des opérations de sécurité planifié pour envoyer par e-mail un PDF contenant un résumé des principales détections et des principaux risques pour votre réseau.

Création d'un rapport de tableau de bord planifié

Lorsque vous créez un rapport de tableau de bord planifié, vous pouvez spécifier la fréquence à laquelle le rapport est envoyé par e-mail et l'intervalle de temps entre les données du tableau de bord incluses dans le fichier PDF.

Avant de commencer

- La capacité d'écriture de votre compte utilisateur doit être limitée ou supérieure privilèges.
- Votre système ExtraHop doit être configuré pour envoyer des e-mails. (RevealX Enterprise uniquement)
- Vous devez vous connecter à une console du système ExtraHop.
- Vous ne pouvez créer un rapport que pour les tableaux de bord que vous possédez ou auxquels vous avez un accès partagé.
- Si vous créez un rapport pour un tableau de bord qui est ensuite supprimé ou devient inaccessible pour vous, un e-mail est toujours envoyé aux destinataires. Cependant, l'e-mail n' inclut pas le fichier PDF et inclut une note indiquant que le tableau de bord n'est pas disponible pour le propriétaire du rapport.

Procédez comme suit pour créer un rapport de tableau de bord planifié :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Rapports planifiés**.
3. Cliquez **Créez**.
4. Tapez un nom unique pour le rapport dans **Nom du rapport** champ.
5. Optionnel : Dans le **Descriptif** dans ce champ, saisissez les informations relatives au rapport. La description n'apparaît pas dans le rapport final, mais uniquement dans les paramètres du rapport.
6. Dans la section Type de rapport, sélectionnez **Tableau de bord**.
7. À partir du **Contenu du rapport** liste déroulante, sélectionnez un tableau de bord.
   - Si votre environnement comporte plusieurs sites, vous devez en sélectionner un.

- Si le tableau de bord que vous sélectionnez possède une source dynamique, vous devez sélectionner une source.

8. Optionnel : À partir du **Contenu du rapport** dans la liste déroulante, sélectionnez les tableaux de bord supplémentaires que vous souhaitez ajouter au rapport.
9. À partir du Calendrier section, effectuez les étapes suivantes pour configurer un calendrier pour le rapport :
   a) À partir du Intervalle de temps section, sélectionnez la plage temporelle de données que vous souhaitez inclure dans le rapport.

Dernier...	Spécifiez un intervalle de temps par rapport à l'heure à laquelle vous spécifiez le rapport à envoyer par e-mail.
Semaine civile précédente	Sélectionnez cette option pour envoyer les données de la semaine calendaire complète précédant l'heure à laquelle vous avez spécifié le rapport à envoyer par e-mail. Une semaine civile complète commence le dimanche et se termine le samedi. Par exemple, si votre rapport est envoyé par e-mail un mercredi, il contient des données du dimanche au samedi précédent, et non du mercredi au mardi précédent.
Mois civil précédent	Sélectionnez cette option pour envoyer les données du mois civil complet précédant l'heure à laquelle vous avez spécifié le rapport à envoyer par e-mail. Par exemple, si votre rapport est envoyé par e-mail le 15 de chaque mois, il contient des données allant du 1er au dernier jour du mois précédent, par opposition au 15 du mois précédent au 15 du mois en cours.

   b) À partir du Fréquence des rapports section, définissez le calendrier de livraison des e-mails en sélectionnant l'une des options suivantes :

> **Note:** Les options disponibles dépendent de **Intervalle de temps**. Par exemple, si vous avez spécifié des données de la semaine civile précédente, vous ne pouvez pas sélectionner de fréquence quotidienne.
>
> La fréquence des rapports est basée sur heure système par défaut défini par votre administrateur ExtraHop.

Toutes les heures	Envoyez le rapport par e-mail toutes les heures.
Tous les jours	Spécifiez l'heure à laquelle vous souhaitez que le rapport soit envoyé par e-mail. Cliquez **Ajouter un calendrier** pour envoyer le rapport par e-mail plusieurs fois par jour.
Hebdo	Spécifiez un ou plusieurs jours de la semaine et l' heure à laquelle vous souhaitez que le rapport soit envoyé par e-mail. Cliquez **Ajouter un calendrier** pour envoyer des rapports par e-mail plusieurs fois par jour ou à différents moments par semaine.
Mensuel	Spécifiez le jour du mois auquel vous souhaitez que le rapport soit envoyé par e-mail. Cliquez **Ajouter un calendrier** pour envoyer des rapports par e-mail plusieurs fois par mois.

10. À partir du Formater section, effectuez les étapes suivantes pour configurer le format du rapport :
    a) Définissez la mise en page du contenu en sélectionnant l'une des options suivantes dans la première Style liste déroulante :

Étroit	Affiche du texte volumineux dans les titres et les étiquettes des graphiques, mais offre moins d'espace pour l'affichage des données des

	graphiques. Les titres et étiquettes longs des graphiques peuvent être tronqués.
Moyen	(Par défaut) Affiche une vue des titres, des légendes et des données des graphiques optimisée pour l'orientation des pages en mode portrait.
Large	Affiche un petit texte dans les titres et les étiquettes des graphiques, mais offre plus d'espace pour l'affichage des données des graphiques.

b) Définissez le nombre de sauts de page dans le PDF en sélectionnant l'une des options suivantes dans la seconde Style liste déroulante :

Page unique	(Par défaut) Affiche l'intégralité du tableau de bord ou de la page de protocole sur une seule page continue. Ce paramètre peut générer un fichier PDF dont la taille est supérieure à celle des pages d'imprimante standard.
Saut de page par région	Affiche chaque région du graphique sur une page individuelle. Sélectionnez cette option si votre tableau de bord contient un tableau ou une liste qui affiche plus de 20 valeurs métriques détaillées.

c) Définissez le thème d'affichage en sélectionnant l'une des options suivantes Thème options :

Lumière	(Par défaut) Affiche les données du tableau de bord sous forme de texte foncé sur fond clair.
L'espace ou l'obscurité	Affiche les données du tableau de bord sous forme de texte clair sur fond sombre.
Contraste	Affiche les données du tableau de bord avec une palette de couleurs limitée et des couleurs contrastées.

11. À partir du Envoyer un e-mail section, procédez comme suit pour configurer les notifications par e-mail :
    a) Optionnel : (utilisateurs de RevealX Enterprise uniquement) Depuis le Groupes de notifications liste déroulante, sélectionnez un groupe de destinataires.

       Si vous ne trouvez pas le groupe de messagerie que vous recherchez, vous pouvez configurer les groupes de messagerie dans les paramètres d'administration d'ExtraHop ou via l'API REST. Contactez votre administrateur ExtraHop RevealX Enterprise pour ajouter un groupe de notifications par e-mail.
    b) Dans le **Bénéficiaires** dans ce champ, saisissez l'adresse e-mail de chaque destinataire, en la séparant par une virgule.
    c) À partir du Sujet section, cliquez sur **Personnalisé** pour écrire votre propre ligne d'objet pour l' e-mail. La ligne d'objet automatique est le nom du rapport.
    d) Optionnel : Dans le **Message** champ, saisissez les informations que vous souhaitez envoyer dans le corps de l'e-mail du rapport.
12. Pour enregistrer votre rapport, effectuez l'une des étapes suivantes :
    - Cliquez **Envoyer maintenant** pour envoyer un rapport de test par e-mail aux adresses e-mail, puis cliquez sur **Terminé**. Votre rapport est enregistré et programmé.
    - Cliquez **Enregistrer**. Votre rapport est planifié et sera envoyé aux destinataires en fonction de la fréquence de rapport que vous avez spécifiée.

Prochaines étapes

- Pour arrêter l'envoi d'un rapport planifié, désactivez le **Activer le rapport** case à cocher ou supprimez le rapport.

Création d'un rapport sur les opérations de sécurité planifiées

Lorsque vous créez un rapport sur les opérations de sécurité planifié, vous pouvez spécifier la fréquence à laquelle un fichier PDF du rapport est envoyé par courrier électronique et l'intervalle de temps pour les données incluses dans le rapport.

Avant de commencer

- La capacité d'écriture de votre compte utilisateur doit être limitée ou supérieure privilèges.
- Votre système ExtraHop doit inclure le module Network Detection and Response (NDR).
- Vous devez vous connecter à une console du système ExtraHop.
- Votre système ExtraHop doit être configuré pour envoyer des e-mails. (RevealX Enterprise uniquement)

Procédez comme suit pour créer un rapport sur les opérations de sécurité planifié :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Rapports planifiés**.
3. Cliquez **Créez**.
4. Tapez un nom unique pour le rapport dans **Nom du rapport** champ.
5. Optionnel : Dans le **Descriptif** dans ce champ, saisissez les informations relatives au rapport. La description n'apparaît pas dans le rapport final, mais uniquement dans les paramètres du rapport.
6. Dans la section Type de rapport, sélectionnez **Opérations de sécurité**.
7. À partir du **Sites** menu déroulant, sélectionnez les sites que vous souhaitez inclure dans le rapport.
8. À partir du Calendrier section, effectuez les étapes suivantes pour configurer un calendrier pour le rapport :
   a) À partir du Intervalle de temps section, sélectionnez la plage temporelle de données que vous souhaitez inclure dans le rapport.

Les N derniers jours	Sélectionnez cette option pour envoyer des données à partir d'un intervalle de temps relatif à l'heure à laquelle vous avez spécifié le rapport à envoyer par e-mail.
Semaine civile précédente	Sélectionnez cette option pour envoyer les données de la semaine calendaire complète précédant l'heure à laquelle vous avez spécifié le rapport à envoyer par e-mail. Une semaine civile complète commence le dimanche et se termine le samedi. Par exemple, si votre rapport est envoyé par e-mail un mercredi, il contient des données du dimanche au samedi précédent, et non du mercredi au mardi précédent.
Mois civil précédent	Sélectionnez cette option pour envoyer les données du mois civil complet précédant l'heure à laquelle vous avez spécifié le rapport à envoyer par e-mail. Par exemple, si votre rapport est envoyé par e-mail le 15 de chaque mois, il contient des données allant du 1er au dernier jour du mois précédent, par opposition au 15 du mois précédent au 15 du mois en cours.

   b) À partir du Fréquence des rapports section, définissez le calendrier de livraison des e-mails en sélectionnant l'une des options suivantes :

> **Note:** Les options disponibles dépendent de **Intervalle de temps**. Par exemple, si vous avez spécifié des données de la semaine civile précédente, vous ne pouvez pas sélectionner de fréquence quotidienne.
>
> La fréquence des rapports est basée sur heure système par défaut défini par votre administrateur ExtraHop.

Toutes les heures	Envoyez le rapport par e-mail toutes les heures.

Tous les jours	Spécifiez l'heure à laquelle vous souhaitez que le rapport soit envoyé par e-mail. Cliquez **Ajouter un calendrier** pour envoyer le rapport par e-mail plusieurs fois par jour.
Hebdo	Spécifiez un ou plusieurs jours de la semaine et l' heure à laquelle vous souhaitez que le rapport soit envoyé par e-mail. Cliquez **Ajouter un calendrier** pour envoyer des rapports par e-mail plusieurs fois par jour ou à différents moments par semaine.
Mensuel	Spécifiez le jour du mois auquel vous souhaitez que le rapport soit envoyé par e-mail. Cliquez **Ajouter un calendrier** pour envoyer des rapports par e-mail plusieurs fois par mois.

9. À partir du Envoyer un e-mail section, procédez comme suit pour configurer les notifications par e-mail :
   a) Optionnel : (utilisateurs de RevealX Enterprise uniquement) Depuis le Groupes de notifications liste déroulante, sélectionnez un groupe de destinataires.

      Si vous ne trouvez pas le groupe de messagerie que vous recherchez, vous pouvez configurer les groupes de messagerie dans les paramètres d'administration d'ExtraHop ou via l'API REST. Contactez votre administrateur ExtraHop RevealX Enterprise pour ajouter un groupe de notifications par e-mail.
   b) Dans le **Bénéficiaires** dans ce champ, saisissez l'adresse e-mail de chaque destinataire, en la séparant par une virgule.
   c) À partir du Sujet section, cliquez sur **Personnalisé** pour écrire votre propre ligne d'objet pour l' e-mail. La ligne d'objet automatique est le nom du rapport.
   d) Optionnel : Dans le **Message** champ, saisissez les informations que vous souhaitez envoyer dans le corps de l'e-mail du rapport.
10. Pour enregistrer votre rapport, effectuez l'une des étapes suivantes :
    - Cliquez **Envoyer maintenant** pour envoyer un rapport de test par e-mail aux adresses e-mail, puis cliquez sur **Terminé**. Votre rapport est enregistré et programmé.
    - Cliquez **Enregistrer**. Votre rapport est planifié et sera envoyé aux destinataires en fonction de la fréquence de rapport que vous avez spécifiée.

Prochaines étapes

- Pour arrêter l'envoi d'un rapport planifié, désactivez le **Activer le rapport** case à cocher ou supprimez le rapport.

Types de graphiques

Les graphiques du tableau de bord du système ExtraHop offrent plusieurs manières de visualiser les données métriques, ce qui peut vous aider à répondre aux questions concernant le comportement de votre réseau.

Vous sélectionnez un type de graphique lorsque modifier un graphique dans l'explorateur de métriques. Mais comment savoir quel graphique sélectionner ? Cela aide à décider d'abord à quelle question vous souhaitez répondre :

- Pour savoir comment une métrique évolue au fil du temps, sélectionnez un graphique chronologique tel que l'aire, la colonne, la ligne, la ligne et la colonne, ou le graphique dstatus.
- Pour savoir comment une valeur métrique se compare à un ensemble complet de données, sélectionnez un graphique de distribution tel qu'un diagramme à cases, un chandelier, une carte thermique ou un histogramme.
- Pour connaître la valeur métrique exacte pour une période donnée, sélectionnez un graphique de valeurs totales tel qu' une barre, une liste, un secteur, un tableau ou un diagramme de valeurs.
- Pour connaître l'état d'alerte de cette métrique, sélectionnez la liste, le statut ou le diagramme de valeurs.

Trouvez d'autres réponses dans le FAQ sur les graphiques.

Le tableau suivant fournit une liste des types de graphiques et des descriptions. Cliquez sur le type de graphique pour voir plus de détails et d'exemples.

Type de graphique	Descriptif	Type
Carte des zones	Affiche les valeurs métriques sous forme de ligne reliant les points de données au fil du temps, la zone située entre la ligne et l'axe étant colorée.	Séries chronologiques
Diagramme à colonnes	Affiche les données métriques sous forme de colonnes verticales sur un intervalle de temps sélectionné.	Séries chronologiques
Graphique linéaire	Affiche les valeurs métriques sous forme de points de données sur une ligne au fil du temps.	Séries chronologiques
Graphique à lignes et à colonnes	Affiche les valeurs métriques sous forme de ligne, qui connecte une série de points de données au fil du temps, avec la possibilité d'afficher une autre métrique sous forme de graphique à colonnes sous le graphique linéaire.	Séries chronologiques
Tableau de statut	Affiche les valeurs métriques dans un graphique à colonnes ainsi que le statut d'une alerte attribuée à la fois à la source et à la métrique dans le graphique.	Séries chronologiques
Diagramme à boîtes	Affiche la variabilité d'une distribution de données	Diffusion

Type de graphique	Descriptif	Type
	métriques. Chaque ligne horizontale du diagramme à cases comprend trois ou cinq points de données.	
Tableau en chandeliers	Affiche la variabilité d'une distribution des données métriques au fil du temps.	Diffusion
Graphique Heatmap	Affiche une distribution des données métriques dans le temps, où la couleur représente une concentration de données.	Diffusion
Diagramme d'histogramme	Affiche une distribution des données métriques sous forme de barres verticales ou de bacs.	Diffusion
Graphique à barres	Affiche la valeur totale des données métriques sous forme de barres horizontales.	Valeur totale
Tableau de liste	Affiche les données métriques sous forme de liste avec des sparklines facultatifs qui représentent l' évolution des données au fil du temps.	Valeur totale
Diagramme à secteurs	Affiche les données métriques sous forme de portion ou de pourcentage d'un ensemble.	Valeur totale
Tableau graphique	Affiche plusieurs valeurs métriques dans un tableau, qui peut être facilement trié.	Valeur totale
Tableau des valeurs	Affiche la valeur totale d'une ou de plusieurs mesures.	Valeur totale

Carte des zones

Les données métriques sont affichées sous forme de points de données au fil du temps connectés par une ligne, la zone située entre la ligne et l'axe X étant colorée.

Si votre graphique contient plusieurs mesures, les données de chaque métrique sont affichées sous forme de ligne individuelle ou de série. Chaque série est empilée pour illustrer la valeur cumulée des données.

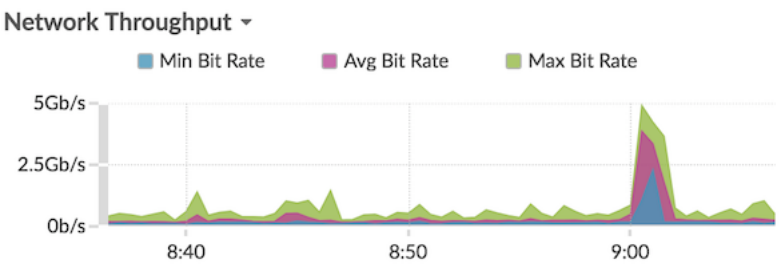
Sélectionnez le graphique en aires pour voir comment l'accumulation de plusieurs points de données métriques au fil du temps contribue à une valeur totale. Par exemple, un graphique en aires peut révéler comment les différents protocoles contribuent à l'activité totale des protocoles.

Pour plus d'informations sur l'affichage des taux dans votre graphique, consultez le Taux d'affichage section.

Note: Ce graphique prend en charge marqueurs de détection, qui indiquent les détections associées aux données cartographiques.

Note: Les détections par apprentissage automatique nécessitent connexion aux services cloud ExtraHop.

La figure suivante montre un exemple de graphique en aires.



Graphique à barres

La valeur totale des données métriques est affichée sous forme de barres horizontales.

Sélectionnez le graphique en barres lorsque vous souhaitez comparer les données de plusieurs mesures pour un intervalle de temps sélectionné.

La figure suivante montre un exemple de graphique en barres.

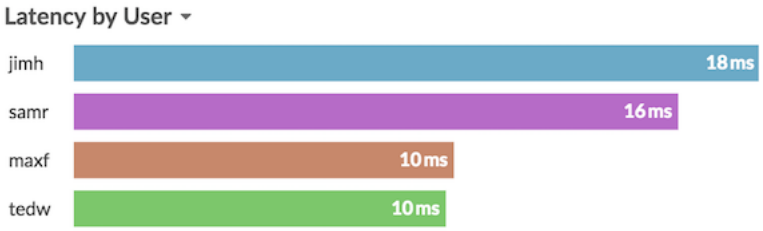


Diagramme à boîtes

Le diagramme à boîtes montre la variabilité d'une distribution de données métriques. Vous ne pouvez afficher que les données issues des métriques du jeu de données, telles que le temps de traitement du serveur, dans ce graphique.

Chaque ligne horizontale du diagramme à cases comprend trois ou cinq points de données. Avec cinq points de données, la ligne contient une barre de corps, un crochet vertical, une ligne d'ombre supérieure et une ligne d'ombre inférieure. Avec trois points de données, la ligne contient une coche verticale, une ombre supérieure et une ombre inférieure. Pour plus d'informations sur l'affichage de valeurs de percentiles spécifiques dans votre graphique, voir Afficher les percentiles.

La figure suivante montre un exemple de diagramme à boîtes.

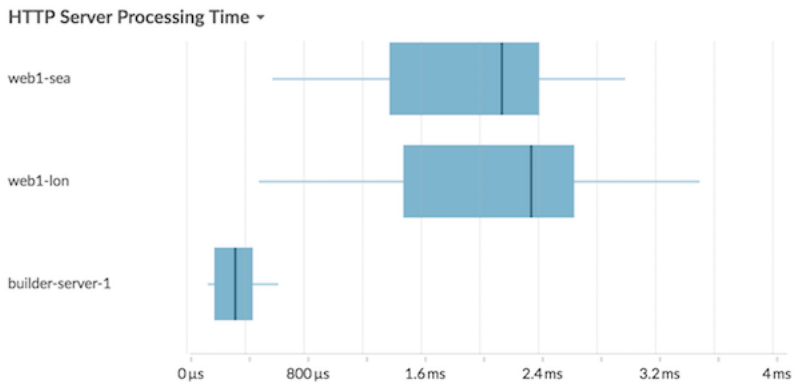


Tableau en chandeliers

Le graphique en chandelier montre la variabilité d'une distribution des données métriques au fil du temps. Vous ne pouvez afficher que les données issues de métriques d'ensembles de données ou de métriques d'octets et de paquets de réseau (L2) de haute précision.

Les lignes verticales à chaque intervalle de temps affichent trois ou cinq points de données. Si la ligne comporte cinq points de données, elle contient un corps, un crochet central, une ligne d'ombre supérieure et une ligne d' ombre inférieure. Si la ligne comporte trois points de données, elle contient un crochet central. Pour plus d' informations sur l'affichage de valeurs de percentiles spécifiques dans votre graphique, voir Afficher les percentiles.

Sélectionnez le graphique en chandelier pour visualiser la variabilité des calculs de données sur une période donnée.

La figure suivante montre un exemple de graphique en chandelier.

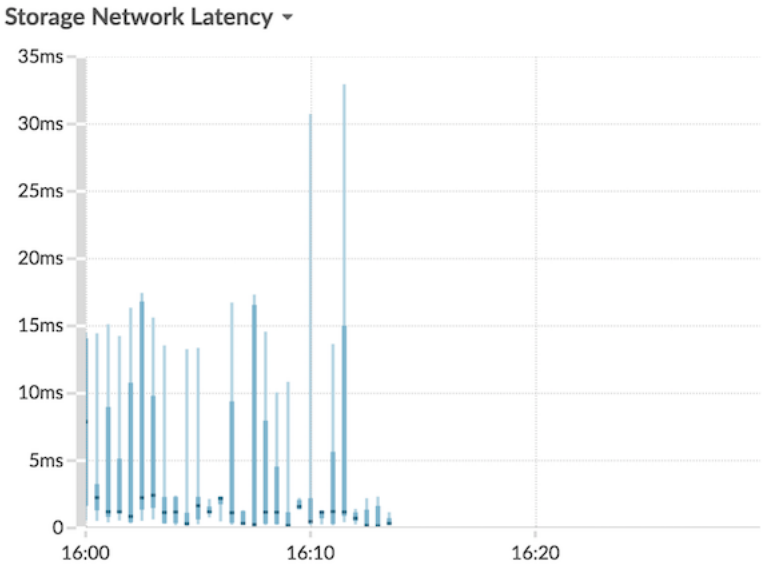


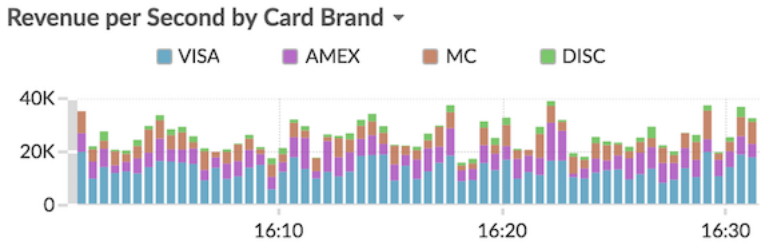
Diagramme à colonnes

Les données métriques sont affichées sous forme de colonnes verticales au fil du temps. Si votre graphique contient plusieurs mesures, les données de chaque métrique sont affichées sous forme de colonne individuelle ou de série. Chaque série est empilée pour illustrer la valeur cumulée des données.

Sélectionnez le graphique à colonnes pour comparer la façon dont l'accumulation de plusieurs points de données métriques à un moment donné contribue à la valeur totale.

Note: Ce graphique prend en charge marqueurs de détection, qui indiquent les détections associées aux données cartographiques.

La figure suivante montre un exemple de graphique à colonnes.



Graphique Heatmap

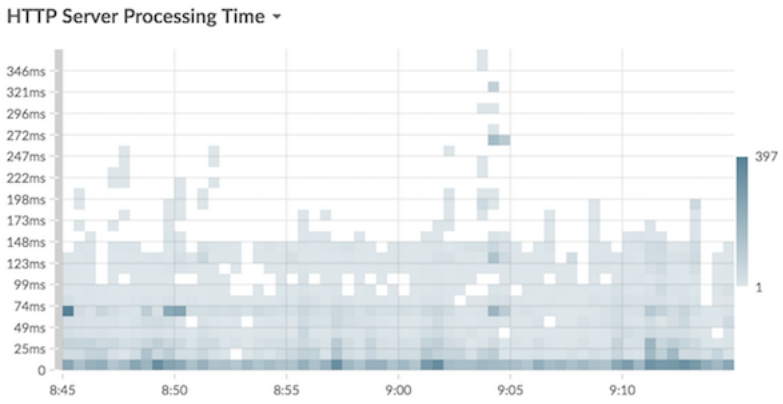
Le graphique de carte thermique affiche une distribution des données métriques dans le temps, la couleur représentant une concentration de données. Vous pouvez uniquement sélectionner une métrique de jeu de données à afficher dans le graphique, telle que le temps de traitement du serveur ou le temps d'aller-retour.

Sélectionnez la carte thermique lorsque vous souhaitez identifier des modèles dans la distribution des données.

Voici quelques points importants à prendre en compte à propos du graphique de carte thermique :

- La légende de la carte thermique affiche le dégradé de couleurs correspondant à la plage de données du graphique. Par exemple, la couleur foncée de la carte thermique indique une concentration plus élevée de points de données.
- La plage de données par défaut se situe entre le 5e et le 95e percentile, ce qui permet de filtrer les valeurs aberrantes de la distribution. Les valeurs aberrantes peuvent fausser l'échelle des données affichées dans votre graphique, ce qui complique l'identification des tendances et des modèles pour la majorité de vos données. Toutefois, vous pouvez choisir d'afficher l'ensemble des données en modifiant le filtre par défaut dans le **Options** onglet. Pour plus d'informations, voir Filtrer les valeurs aberrantes.
- Le thème sélectionné, tel que Clair, Dark ou Space, détermine si une couleur foncée ou claire indique une concentration plus élevée de points de données.

La figure suivante montre un exemple de graphique de carte thermique.



Histogramme

L'histogramme affiche une distribution des données métriques sous forme de barres verticales ou de bacs. Vous ne pouvez sélectionner qu'une métrique de jeu de données à afficher dans ce graphique, telle que le temps de traitement du serveur ou le temps d' aller-retour.

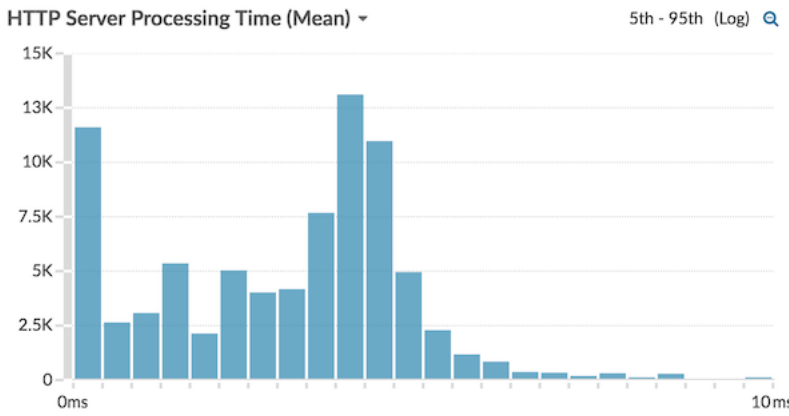
Sélectionnez l'histogramme pour visualiser la forme de distribution des données.

Voici quelques points importants à prendre en compte à propos de l'histogramme :

- La plage de données par défaut est comprise entre le 5e et le 95e percentile (5e au 95e), ce qui permet de filtrer les valeurs aberrantes de la distribution. La vue minimale à maximale (min-max) affiche la plage de données complète. Cliquez sur la loupe dans le coin supérieur droit du graphique pour passer d'une vue à l'autre.
- Les données sont automatiquement réparties dans des groupes sur une échelle linéaire ou logarithmique en fonction de la plage de données. Par exemple, lorsque la plage de données s'étend sur plusieurs ordres de grandeur, les données sont placées dans des groupes sur une échelle logarithmique. Min-Max (log) apparaît dans le coin supérieur droit du graphique.
- Cliquez et faites glisser pour zoomer sur plusieurs bacs ou sur un compartiment spécifique. Cliquez à nouveau sur la loupe dans le coin supérieur droit du graphique pour effectuer un zoom arrière sur la vue d'origine (5e-95e ou Min to Max).

  Note: Le fait de zoomer pour afficher un intervalle de temps personnalisé ne modifie pas l'intervalle de temps global ou régional.
- Votre sélection (entre les vues 5e-95e et min-max) sera conservée pour votre graphique, mais pas pour les utilisateurs avec lesquels vous avez partagé votre tableau de bord et votre graphique. Pour définir une sélection permanente avant de partager un tableau de bord, voir Filtrer les valeurs aberrantes.

La figure suivante montre un exemple d'histogramme.



Note: Ce graphique ne prend pas en charge les lignes de base ou les seuils.

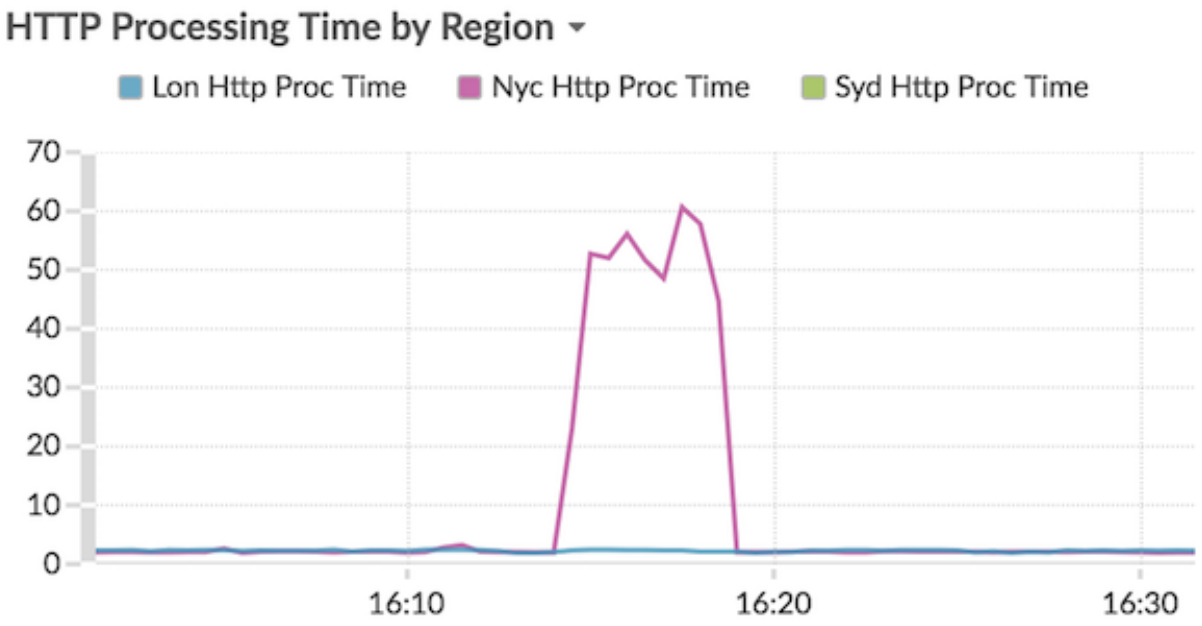
Graphique linéaire

Les données métriques sont affichées sous forme de points de données au fil du temps connectés sur une ligne. Si votre graphique contient plusieurs mesures, les données de chaque métrique sont affichées sous forme de ligne individuelle ou de série. Chaque série se chevauche.

Sélectionnez le graphique en courbes pour comparer les changements au fil du temps.

Note: Ce graphique prend en charge marqueurs de détection, qui indiquent les détections associées aux données cartographiques.

La figure suivante montre un exemple de graphique en courbes.



Graphique à lignes et à colonnes

Les données métriques sont affichées sous forme de points de données au fil du temps connectés par une ligne, avec la possibilité d'afficher un graphique à colonnes sous le graphique en courbes. Par exemple, si votre graphique contient plusieurs mesures (par exemple, les requêtes HTTP et les erreurs HTTP), vous pouvez sélectionner **Afficher sous forme de colonnes** pour afficher l'une des mesures sous forme de graphique à colonnes sous le graphique en courbes.

Les colonnes sont affichées en rouge par défaut. Pour supprimer la couleur rouge, cliquez sur **Options** et désélectionnez **Afficher les colonnes en rouge**.

Sélectionnez le graphique à lignes et à colonnes pour comparer différentes mesures à différentes échelles dans un même graphique. Par exemple, vous pouvez afficher les taux d'erreur et le nombre total de réponses HTTP dans un graphique.

Note: Ce graphique prend en charge marqueurs de détection, qui indiquent les détections associées aux données cartographiques.

La figure suivante montre un exemple de graphique à lignes et à colonnes.

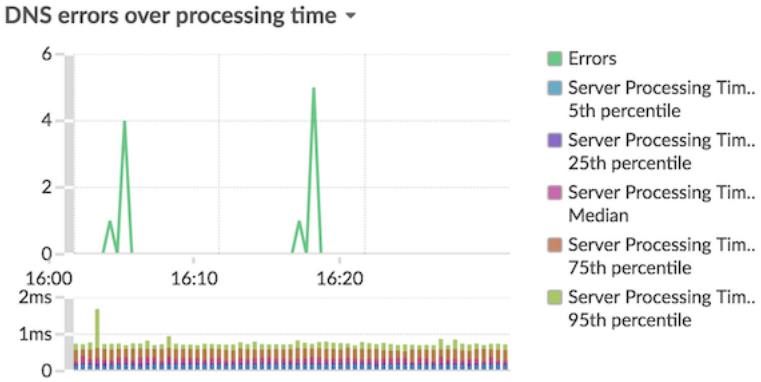


Tableau de liste

Les données métriques sont affichées sous forme de liste. Sélectionnez le graphique en listes pour afficher de longues listes de valeurs métriques, telles que les mesures détaillées.

Ce tableau inclut les options suivantes :

- Ajoutez un sparkline, qui est un simple graphique en aires placé en ligne avec le nom et la valeur de la métrique. Un sparkline montre l'évolution des données au fil du temps. Cliquez sur **Des options** onglet et sélectionnez **Inclure des paillettes**.
- Affichez la valeur métrique dans une couleur d'état d'alerte. Les différentes couleurs indiquent la gravité de l'alerte configurée. Par exemple, si un seuil d'alerte est dépassé pour une métrique affichée dans le graphique en listes, la valeur de cette métrique apparaît en rouge. Cliquez sur le **Des options** onglet et sélectionnez **La couleur indique l' état de l'alerte**.

Note: Ce graphique ne prend pas en charge les lignes de base ou les seuils.

La figure suivante montre un exemple de graphique en listes.

Diagramme à secteurs

Les données métriques sont affichées sous forme de portion ou de pourcentage d'un ensemble. Si votre graphique contient plusieurs mesures, les données de chaque métrique sont représentées sous forme de tranche unique, ou de série, dans le graphique circulaire.

Sélectionnez le graphique en camembert pour comparer les valeurs métriques qui s'excluent mutuellement, telles que les mesures détaillées du code détat pour la métrique de réponse HTTP de niveau supérieur.

Ce tableau inclut les options suivantes :

- Afficher sous forme de graphique en forme de donut. Cliquez sur **Option** appuyez sur l'onglet et sélectionnez **Afficher la valeur totale**.
- Spécifiez la précision décimale, ou le nombre de chiffres, affiché dans votre graphique. La précision au centile est utile pour afficher les ratios de données, en particulier pour les accords de niveau de service (SLA) qui peuvent nécessiter des données précises pour les rapports. Cliquez sur **Des options** onglet, et dans la section Unités, sélectionnez **Afficher les pourcentages au lieu des chiffres**. Sélectionnez ensuite **0,00 %** ou **0,000%** depuis la liste déroulante.

La figure suivante montre un exemple de graphique en camembert.

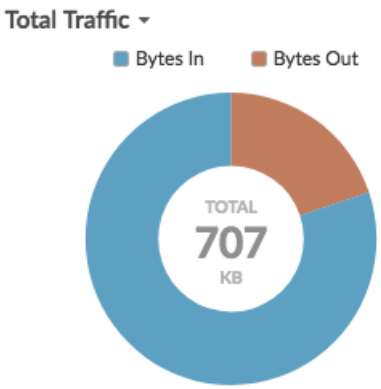


Tableau de statut

Les données métriques sont affichées dans un graphique à colonnes. La couleur de chaque colonne représente l'état d'alerte le plus grave de l'alerte configurée pour la métrique. Vous ne pouvez sélectionner qu'une seule source et une seule métrique à afficher dans ce graphique.

Pour afficher le statut de toutes les alertes associées à la catégorie métrique sélectionnée, cliquez sur **Afficher les alertes associées**. Une liste d'alertes est ensuite affichée sous le graphique à colonnes.

Sélectionnez le graphique dstatus pour voir comment les données et le statut d'alerte de votre métrique évoluent au fil du temps.

Note: Ce graphique ne prend pas en charge les valeurs de référence.

La figure suivante montre un exemple de graphique dstatus.

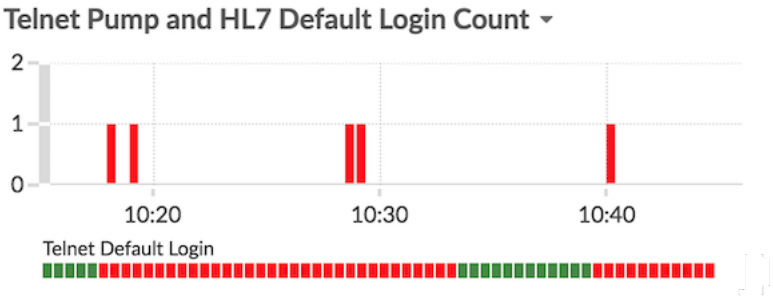


Tableau graphique

Les données métriques sont affichées sur les lignes et les colonnes d'un tableau. Chaque ligne représente une source. Chaque colonne représente une métrique. Vous pouvez ajouter plusieurs sources (du même type) et mesures à un tableau.

Sélectionnez le tableau graphique lorsque vous souhaitez afficher les données métriques dans une grille et trier facilement les valeurs entre plusieurs métriques.

Note: Ce graphique ne prend pas en charge les lignes de base ou les seuils.

La figure suivante montre un exemple de tableau graphique.

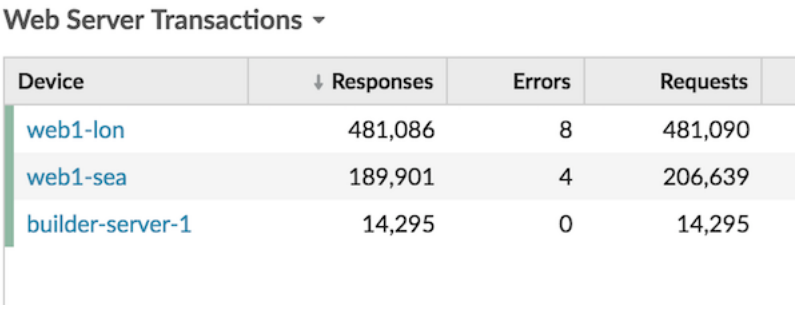


Tableau des valeurs

La valeur totale d'une ou de plusieurs mesures est affichée sous forme de valeur unique. Si vous sélectionnez plusieurs mesures, les valeurs métriques sont affichées côte à côte.

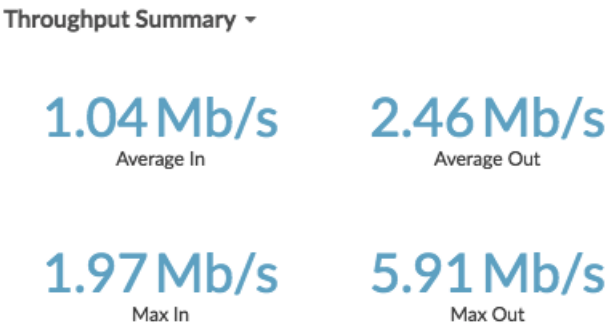
Sélectionnez le diagramme de valeurs pour voir la valeur totale des mesures importantes, telles que le nombre total d'erreurs HTTP survenant sur votre réseau.

Ce tableau inclut les options suivantes :

- Ajoutez des sparklines, un simple graphique en aires placé sous la valeur métrique. Un sparkline montre l'évolution des données au fil du temps. Cliquez sur **Des options** appuyez sur l'onglet et sélectionnez **Inclure des paillettes**.
- Affichez la valeur métrique dans une couleur d'état d'alerte. Les différentes couleurs indiquent la gravité de l'alerte configurée. Par exemple, si un seuil d'alerte est dépassé pour une métrique, la valeur apparaît en rouge. Cliquez sur **Des options** appuyez sur l'onglet et sélectionnez **La couleur indique l'état de l'alerte**.

  Note: Ce graphique ne prend pas en charge les lignes de base ou les seuils.

La figure suivante montre un exemple de diagramme de valeurs.



Création d'un graphique

Les graphiques sont un outil essentiel pour visualiser, analyser et comprendre le comportement du réseau. Vous pouvez créer un graphique personnalisé à partir d'un tableau de bord ou d'une page de protocole pour visualiser les données provenant de plus de 4 000 métriques intégrées ou personnalisées disponibles dans le système ExtraHop. Par exemple, si vous observez une métrique de serveur intéressante lors du dépannage, vous pouvez créer un graphique pour visualiser et analyser plus en détail cette métrique. Les graphiques personnalisés sont ensuite enregistrés dans des tableaux de bord.

Les étapes suivantes vous montrent comment créer rapidement un graphique personnalisé vierge :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Effectuez l'une des étapes suivantes :
   - Cliquez **Tableaux de bord** en haut de page.
   - Cliquez **Actifs** en haut de page. Sélectionnez une source dans le volet de gauche, puis cliquez sur le nom d'une application, d'un équipement, d'un groupe de dispositifs ou d'un réseau dans le volet central. Une page de protocole pour la source s'affiche.
3. Cliquez sur le menu de commande ⋮ dans le coin supérieur droit de la page, puis sélectionnez **Créer un graphique**.
4. Modifiez le graphique dans l'explorateur de métriques.
5. Pour enregistrer votre graphique, cliquez sur **Ajouter au tableau de bord** et effectuez l'une des étapes suivantes :
   - Sélectionnez le nom d'un tableau de bord existant dans la liste. La liste des tableaux de bord est ordonnée depuis les derniers tableaux de bord créés (en bas) jusqu'aux tableaux de bord les plus anciens (en haut).
   - Sélectionnez **Créer un tableau de bord**. Dans le Propriétés du tableau de bord fenêtre, tapez le nom du nouveau tableau de bord, puis cliquez sur **Créez**.

     Conseil: Voici d'autres méthodes pour créer un graphique :
     - Si vous trouvez un graphique qui vous plaît sur une page de protocole ou un tableau de bord, vous pouvez le recréer et l'enregistrer dans votre tableau de bord. Cliquez sur le titre du graphique, puis sélectionnez **Créer un graphique à partir de...**.
     - Tu peux modifier la mise en page d'un tableau de bord et cliquez et faites glisser un nouveau widget graphique sur le tableau de bord.

Prochaines étapes

Après avoir créé un graphique, découvrez comment utiliser les tableaux de bord :

- Modifier la mise en page d'un tableau de bord
- Partager un tableau de bord

Copier un graphique

Vous pouvez copier un graphique depuis un tableau de bord ou une page de protocole, puis enregistrer le graphique copié dans un tableau de bord. Les widgets copiés sont toujours placés dans une nouvelle région du tableau de bord, que vous pouvez modifier ultérieurement.

Conseil: Si vous souhaitez copier un tableau de bord, un graphique ou une zone de texte sans créer de nouvelle région, cliquez sur le menu de commandes ⋮ dans le coin supérieur droit de la page du tableau de bord et cliquez sur **Modifier la mise en page**. Recherchez le graphique que vous souhaitez copier, puis cliquez sur **Dupliquer**.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Sélectionnez un tableau de bord contenant le graphique ou le widget que vous souhaitez copier.
4. Cliquez sur le titre.

   Note: Vous ne pouvez pas cliquer sur le titre d'un widget de zone de texte. Pour copier un widget de texte, vous devez d'abord modifier la disposition du tableau de bord. Cliquez sur le menu de commande ⋮ dans le coin supérieur droit du widget de zone de texte, puis effectuez l'étape 4.
5. Passez la souris sur **Copier vers...** pour développer une liste déroulante, puis effectuer l'une des sélections suivantes :

- Sélectionnez le nom d'un tableau de bord existant dans la liste. La liste des tableaux de bord est ordonnée depuis les derniers tableaux de bord créés (en bas) jusqu'aux tableaux de bord les plus anciens (en haut).
- Sélectionnez **Créer un tableau de bord**. Dans le Propriétés du tableau de bord fenêtre, tapez le nom du nouveau tableau de bord, puis cliquez sur **Créez**.

Prochaines étapes
Le graphique est copié dans une nouvelle région du tableau de bord en mode Modifier la mise en page. Vous pouvez désormais modifier votre tableau de bord ou votre graphique de la manière suivante :

- Modifier une région de tableau de bord
- Modifier la mise en page d'un tableau de bord
- Modifier un graphique à l'aide de l'explorateur de métriques

Percer vers le bas

Une métrique intéressante soulève naturellement des questions sur les facteurs associés à cette valeur métrique. Par exemple, si vous constatez un grand nombre de délais d'expiration des requêtes DNS sur votre réseau, vous vous demandez peut-être quels clients DNS rencontrent ces délais. Dans le système ExtraHop, vous pouvez facilement effectuer une recherche vers le bas à partir d'une métrique de niveau supérieur pour afficher les appareils, les méthodes ou les ressources associés à cette métrique.

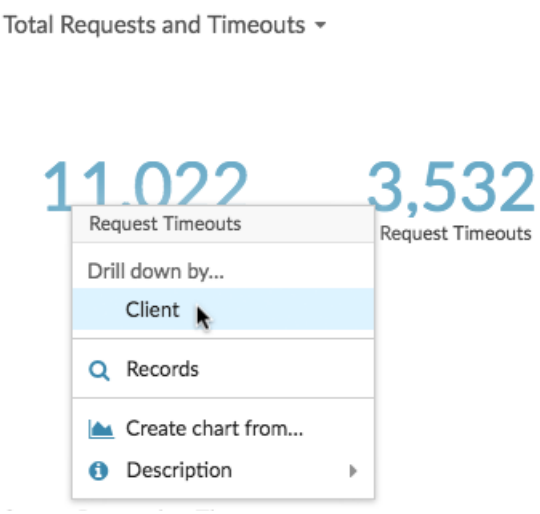
Lorsque vous parcourez une métrique à l'aide d'une clé (telle qu'une adresse IP client, une méthode, un URI ou une ressource), le système ExtraHop calcule un topnset d'un maximum de 1 000 paires clé-valeur. Vous pouvez ensuite étudier ces paires clé-valeur, appelées mesures détaillées, pour savoir quels facteurs sont liés à l'activité intéressante.

Exploration vers le bas à partir d'un tableau de bord ou d'une page de protocole

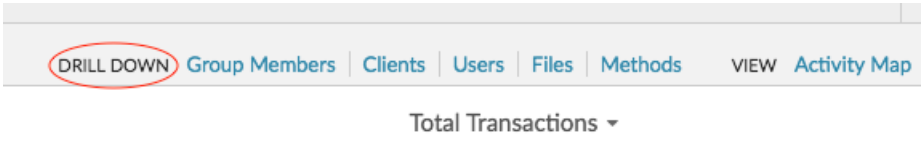
En cliquant sur une métrique dans un graphique ou une légende, vous pouvez voir quelle clé, telle que l' adresse IP du client, l'adresse IP du serveur, la méthode ou la ressource, a contribué à cette valeur.

Les étapes suivantes vous montrent comment localiser une métrique, puis comment effectuer une hiérarchisation vers le bas :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Trouvez une métrique intéressante en effectuant l'une des étapes suivantes :
   - Cliquez **Tableau de bord**, puis sélectionnez un tableau de bord dans le volet de gauche. Un tableau de bord contenant des métriques apparaît.
   - Cliquez **Actifs**, cliquez **Appareil**, **Groupe d'appareils**, ou **Demande** dans le volet de gauche. Sélectionnez ensuite un équipement, un groupe ou une application. Une page de protocole contenant des métriques apparaît.
   - Cliquez **Actifs**, cliquez **Réseaux** dans le volet gauche, puis sélectionnez un réseau de flux. Une page de protocole contenant des métriques apparaît.
3. Cliquez sur une valeur métrique ou sur une étiquette métrique dans la légende du graphique, comme illustré dans la figure suivante. Un menu apparaît.



Conseil: Sur une page de protocole, vous pouvez également cliquer sur un bouton de raccourci déroulant dans le Exploration vers le bas section, située dans le coin supérieur droit de la page. Le type de boutons de raccourci varie en fonction du protocole.



4. Dans le Profilez vers le bas par... section, sélectionnez une clé. Une page de statistiques détaillées avec un topnset des valeurs métriques par clé s'affiche. Vous pouvez consulter jusqu'à 1 000 paires clé-valeur sur cette page.

Conseil: Si disponible, cliquez sur **Afficher plus** lien au bas d'un graphique pour accéder à la métrique affichée dans le graphique.

Prochaines étapes

- Étudiez les indicateurs de détail

Approfondissez la capture du réseau et les métriques VLAN

Cliquez sur une métrique de niveau supérieur intéressante concernant l'activité du réseau sur un Réseau capture ou VLAN page permettant d'identifier les appareils liés à cette activité.

Note: Pour plus d'informations sur la manière d'explorer les métriques à partir d'un réseau de flux ou d'une page d'interface de réseau de flux, consultez le Exploration vers le bas à partir d'un tableau de bord ou d'une page de protocole section.

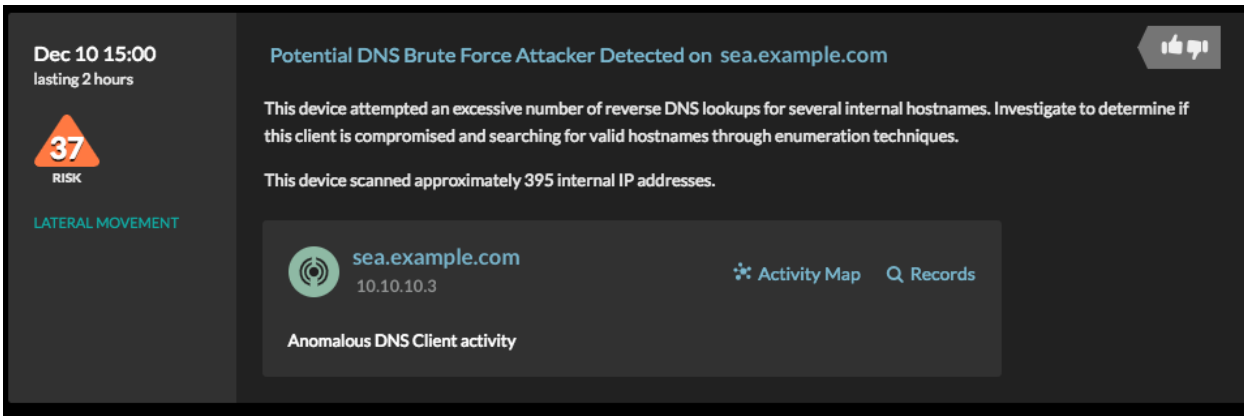
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Actifs**.
3. Cliquez **Réseaux** dans le volet de gauche.
4. Cliquez sur le nom d'une capture réseau ou d'une interface VLAN.
5. Cliquez sur une couche réseau dans le volet de gauche, telle que **L3** ou **Protocoles L7**. Les graphiques qui affichent les valeurs métriques pour l'intervalle de temps sélectionné apparaissent. Pour la plupart des protocoles et mesures, un Appareil le tableau apparaît également au bas de la page.
6. Cliquez sur les données du graphique pour mettre à jour la liste afin d'afficher uniquement les appareils associés aux données.

7. Cliquez sur le nom d'un équipement. UN Appareil une page apparaît, qui affiche le trafic et l'activité du protocole associés à l'équipement sélectionné.

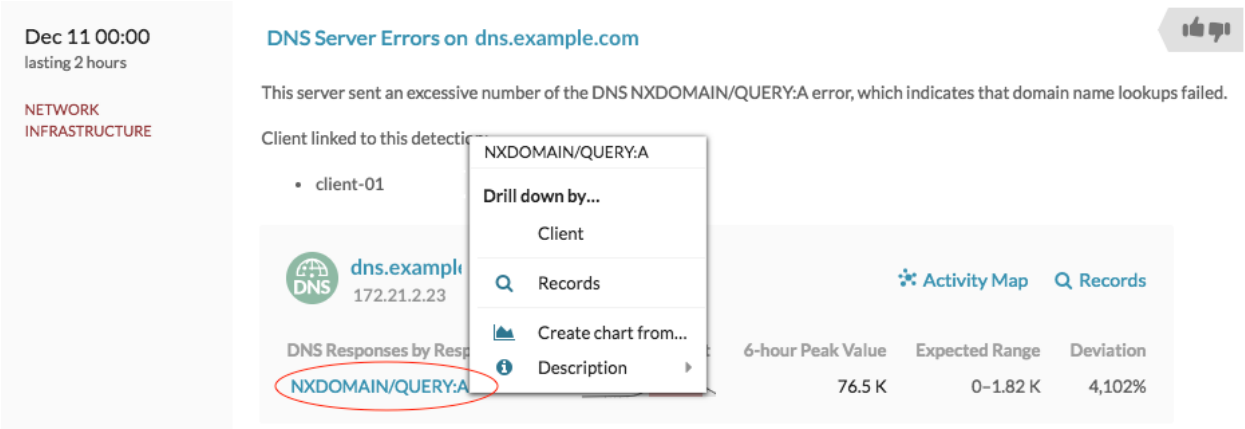
Exploration vers le bas à partir d'une détection

Pour certaines détections, vous pouvez effectuer une analyse détaillée de la métrique ou de la clé à l'origine du comportement inhabituel. Le nom ou la clé métrique apparaît sous forme de lien au bas d'une détection individuelle.

Note: Les détections comportant des mesures ou des clés ne comportant pas de mesures détaillées n'incluent pas d'option d'exploration vers le bas. Les détections qui n'affichent qu'une activité anormale du protocole au lieu d'une métrique n'incluent pas non plus d'option d'exploration des métriques. Par exemple, vous ne pouvez pas effectuer une analyse détaillée d'une détection d'activité anormale d'un client DNS, comme le montre la figure ci-dessous. Cliquez plutôt sur les liens correspondant au nom de l'équipement ou de l'application, **Carte des activités**, ou **Enregistrements** pour en savoir plus sur cette activité anormale.



1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Détections** en haut de page.
3. Trouvez une détection intéressante associée à une métrique et cliquez sur le nom ou la clé de la métrique. Dans la figure suivante, en cliquant sur le code de réponse, nous pouvons afficher tous les clients qui ont reçu des réponses DNS avec NXDOMAIN/QUERY:A.



4. Dans le Profilez vers le bas par... section, cliquez sur une touche telle que **Cliente**.
Une page métrique détaillée apparaît, dans laquelle vous pouvez étudier les métriques répertoriées par clé.

Analyse détaillée à partir d'une alerte

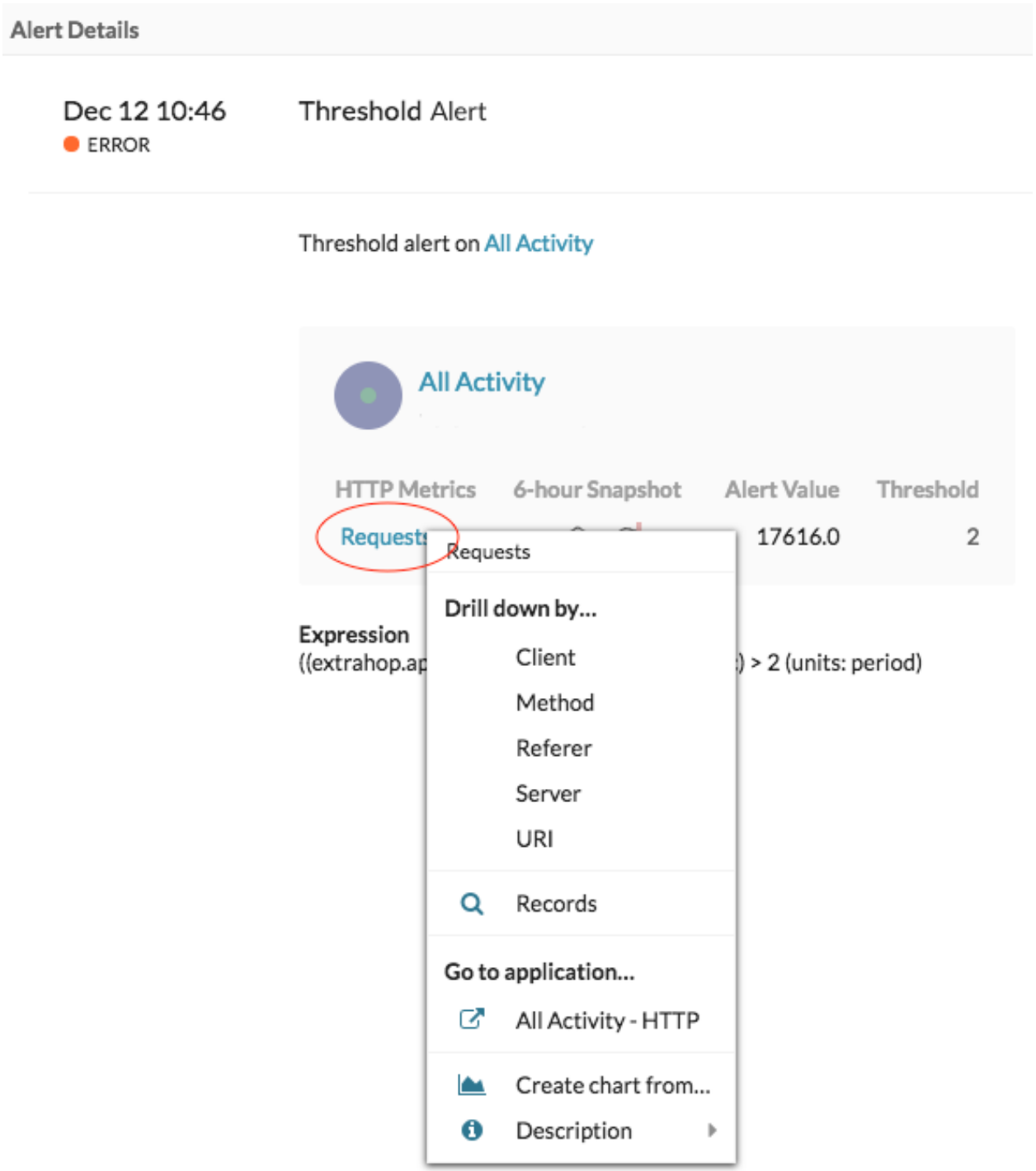
Cliquez sur le nom de la métrique ou sur la clé dans une alerte de seuil pour voir quelle clé, telle que le client, le serveur, la méthode ou la ressource, a contribué à la valeur de la métrique ou à un comportement inhabituel.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Alertes** en haut de page.

   Note: Vous pouvez également accéder aux alertes à partir d'un widget d'alerte sur un tableau de bord ou au bas des pages de protocole suivantes :

   - Page de présentation de l'application
   - Page de présentation des groupes d'appareils
   - Page de présentation du réseau

3. Cliquez sur le nom d'une alerte de seuil.
   Les détails de l'alerte apparaissent.
4. Cliquez sur le nom ou la clé d'une métrique, comme illustré dans la figure suivante.



5. Dans le Profiler vers le bas par section, cliquez sur une touche, telle que **Cliente**, **Méthode**, **Référent**, **serveur**, ou **URI**.
   Une page métrique détaillée apparaît, dans laquelle vous pouvez étudier les métriques répertoriées par clé.

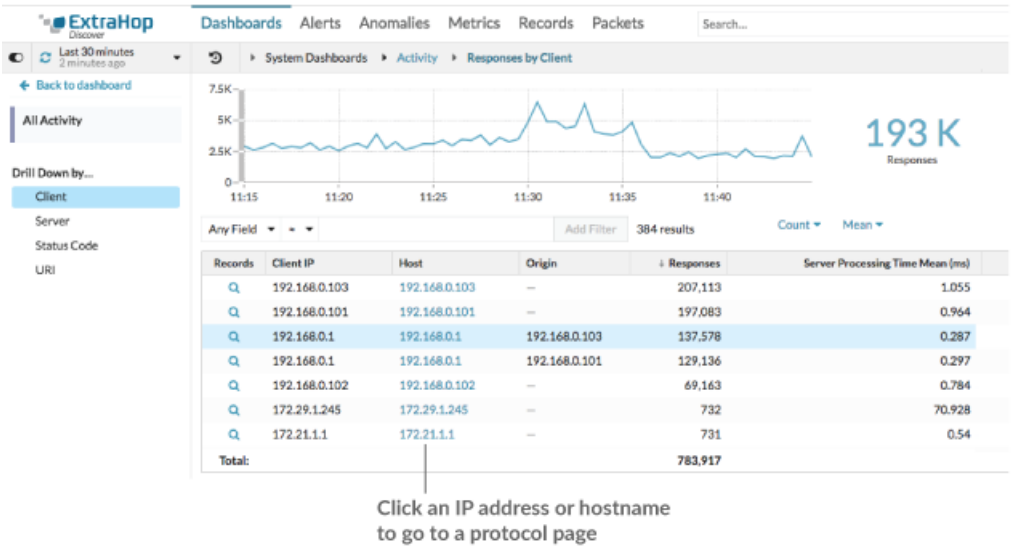
Étudiez les indicateurs de détail

Après avoir exploré une métrique depuis un tableau de bord, une page de protocole, une détection ou une alerte, vous pouvez examiner les valeurs métriques par clé sur une page de métrique détaillée. Filtrez les

données métriques ou sélectionnez différentes clés, telles que des codes d'état ou des URI, pour afficher les données sous différents angles.

La figure suivante montre comment filtrer, faire pivoter, trier ou exporter des données sur une page métrique détaillée.

Si vous avez effectué une recherche approfondie sur une métrique par IP, client ou serveur, les adresses IP et les noms d'hôtes (s'ils sont observés à partir du trafic DNS) apparaissent dans le tableau. Des options supplémentaires s'offrent désormais à vous. Par exemple, vous pouvez accéder directement à la page de protocole d'un client ou d'un serveur, comme illustré dans la figure suivante.



Filtrer les résultats

Une page détaillée peut contenir jusqu'à 1 000 paires clé-valeur. Il existe deux manières de rechercher des résultats spécifiques à partir de données : filtrer les résultats ou cliquez sur une touche du tableau pour créer un autre filtre d'exploration.

Pour filtrer les résultats, cliquez sur **N'importe quel domaine**, puis sélectionnez un champ qui varie en fonction de la touche. Par exemple, vous pouvez sélectionner **Localité du réseau** pour les clés client ou serveur. Sélectionnez ensuite l'un des opérateurs suivants :

- Sélectionnez **=** pour effectuer une correspondance de chaîne exacte.
- Sélectionnez **≈** pour effectuer une correspondance de chaînes approximative. L' opérateur ≈ prend en charge les expressions régulières.

  Note: Pour exclure un résultat, entrez une expression régulière. Pour plus d'informations, voir Création de filtres d'expressions régulières.
- Sélectionnez **#** pour exclure une correspondance de chaîne approximative de vos résultats.
- Sélectionnez **>** ou **≥** pour effectuer une correspondance pour des valeurs supérieures (ou égales à) une valeur spécifiée.
- Sélectionnez **<** ou **≤** pour effectuer une correspondance pour des valeurs inférieures (ou égales) à une valeur spécifiée.
- Cliquez **Ajouter un filtre** pour enregistrer les paramètres du filtre. Vous pouvez enregistrer plusieurs filtres pour une seule requête. Les filtres enregistrés sont effacés si vous sélectionnez une autre clé dans la section Détails du volet de gauche.

Pour terminer le filtre, entrez ou sélectionnez la valeur selon laquelle vous souhaitez filtrer les résultats, puis cliquez sur **Ajouter un filtre**.

Étudier les données relatives aux renseignements sur les menaces (ExtraHop RevealX Premium et Ultra uniquement)

Cliquez sur l'icône rouge de la caméra pour visionner renseignements sur les menaces des informations sur un hôte, une adresse IP ou un URI suspect trouvées dans des données métriques détaillées.

Mettez en surbrillance une valeur métrique dans le graphique supérieur

Sélectionnez une ligne individuelle ou plusieurs lignes pour modifier les données du graphique dans le graphique supérieur de la page des mesures métriques détaillées. Passez la souris sur les points de données du graphique pour afficher plus d'informations sur chaque point de données.

Passez à un plus grand nombre de données par clé

Cliquez sur le nom des touches dans Détails section pour voir des valeurs métriques plus détaillées, ventilées par d'autres clés. Pour l'adresse IP ou les clés d'hôte, cliquez sur le nom d'un équipement dans le tableau pour accéder à Appareil page de protocole, qui affiche le trafic et l'activité protocolaire associés à cet équipement.

Ajustez l'intervalle de temps et comparez les données de deux intervalles de temps

En modifiant l'intervalle de temps, vous pouvez consulter et comparer les données métriques de différentes périodes dans le même tableau. Pour plus d'informations, voir Comparez les intervalles de temps pour trouver le delta métrique.

Note: L'intervalle de temps global situé dans le coin supérieur gauche de la page comprend une icône d'actualisation bleue et un texte gris qui indique la date à laquelle les mesures d'exploration vers le bas ont été interrogées pour la dernière fois. Pour recharger les mesures pour l'intervalle de temps spécifié, cliquez sur l'icône d'actualisation dans l'affichage du sélecteur de temps global. Pour plus d'informations, voir Afficher les dernières données pour un intervalle de temps.

Trier les données métriques en colonnes

Cliquez sur l'en-tête de colonne pour effectuer un tri par métrique afin de voir quelles clés sont associées aux valeurs métriques les plus grandes ou les plus petites. Par exemple, triez en fonction du temps de traitement pour voir quels clients ont connu les temps de chargement de leur site Web les plus longs.

Calcul des données de modification pour les métriques

Modifiez les calculs suivants pour les valeurs métriques affichées dans le tableau :

- Si vous avez une métrique de comptage dans le tableau, cliquez sur **Compter** dans le Options section dans le volet de gauche, puis sélectionnez **Taux moyen**. Pour en savoir plus, consultez le Afficher un taux ou un nombre dans un graphique sujet.
- Si le tableau contient une métrique de jeu de données, cliquez sur **Moyenne** dans le Options section dans le volet de gauche, puis sélectionnez **Résumé**. Lorsque vous sélectionnez **Résumé**, vous pouvez consulter la moyenne et l'écart type.

Exporter des données

Cliquez avec le bouton droit sur une valeur métrique dans le tableau pour télécharger un fichier PDF, CSV ou Excel.

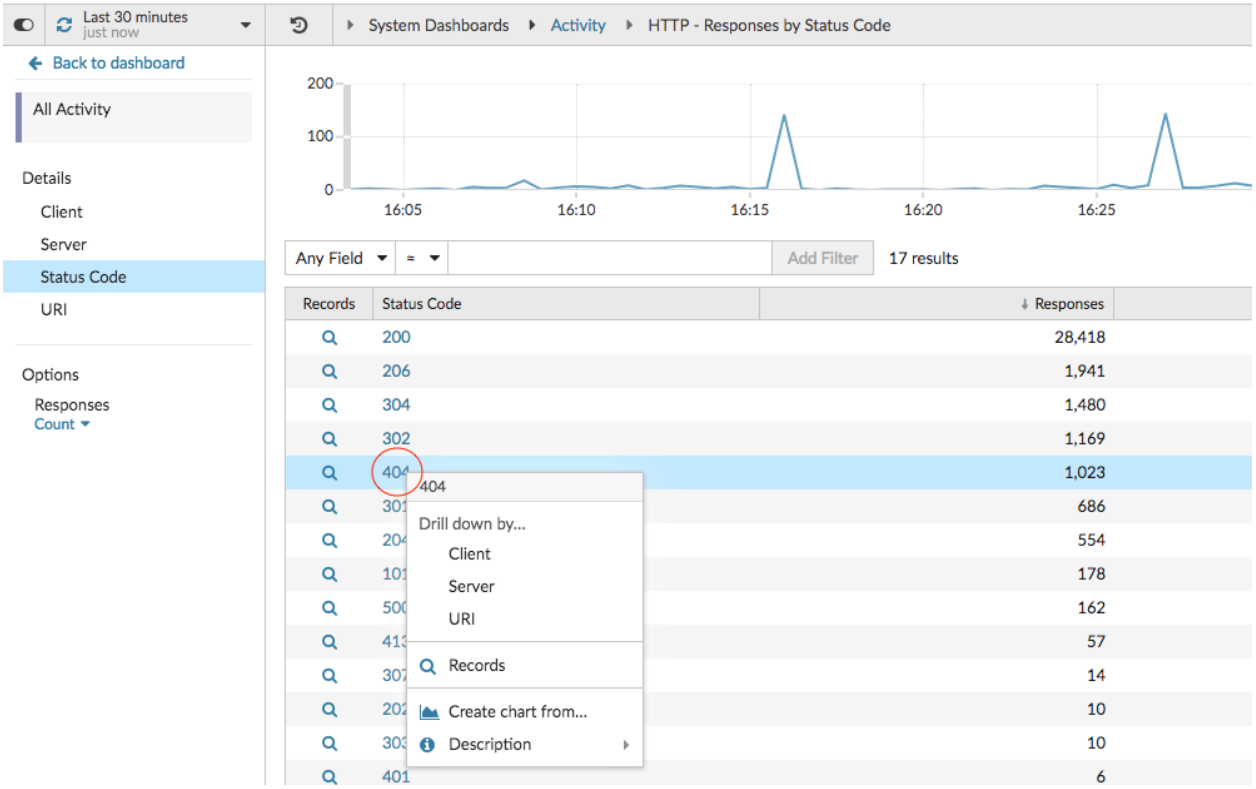
Profilez une seconde fois vers le bas à l'aide d'un filtre clé

Après avoir exploré une métrique de niveau supérieur par touche pour la première fois, une page détaillée apparaît avec un topnset de valeurs métriques ventilées par cette clé. Vous pouvez ensuite créer un filtre pour effectuer une seconde exploration vers le bas à l'aide d'une autre touche. Par exemple, vous pouvez parcourir les réponses HTTP par code d'état, puis effectuer une nouvelle exploration vers le bas en fonction du code d'état 404 pour trouver plus d'informations sur les serveurs, les URI ou les clients associés à ce code d'état.

Note: L'option d'exploration vers le bas une deuxième fois n'est disponible que pour certains topnsets.

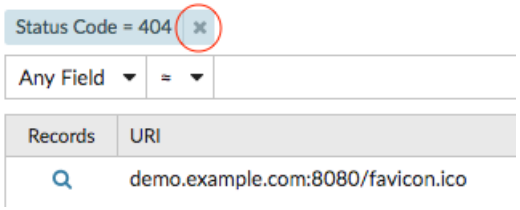
Les étapes suivantes vous montrent comment effectuer une hiérarchisation descendante à partir d'un graphique, puis une nouvelle exploration vers le bas à partir d'une page métrique détaillée :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Accédez à un tableau de bord ou à une page de protocole.
3. Cliquez sur une valeur métrique ou une étiquette.
4. Dans le Profilez vers le bas par... section, sélectionnez une clé.
   Une page détaillée s'affiche.
5. Cliquez sur une clé du tableau, telle qu'un code d'état ou une méthode. (La clé ne doit pas être une adresse IP ou un nom d'hôte.)
6. Dans le Profilez vers le bas par... section, sélectionnez une clé, comme indiqué dans la figure suivante.

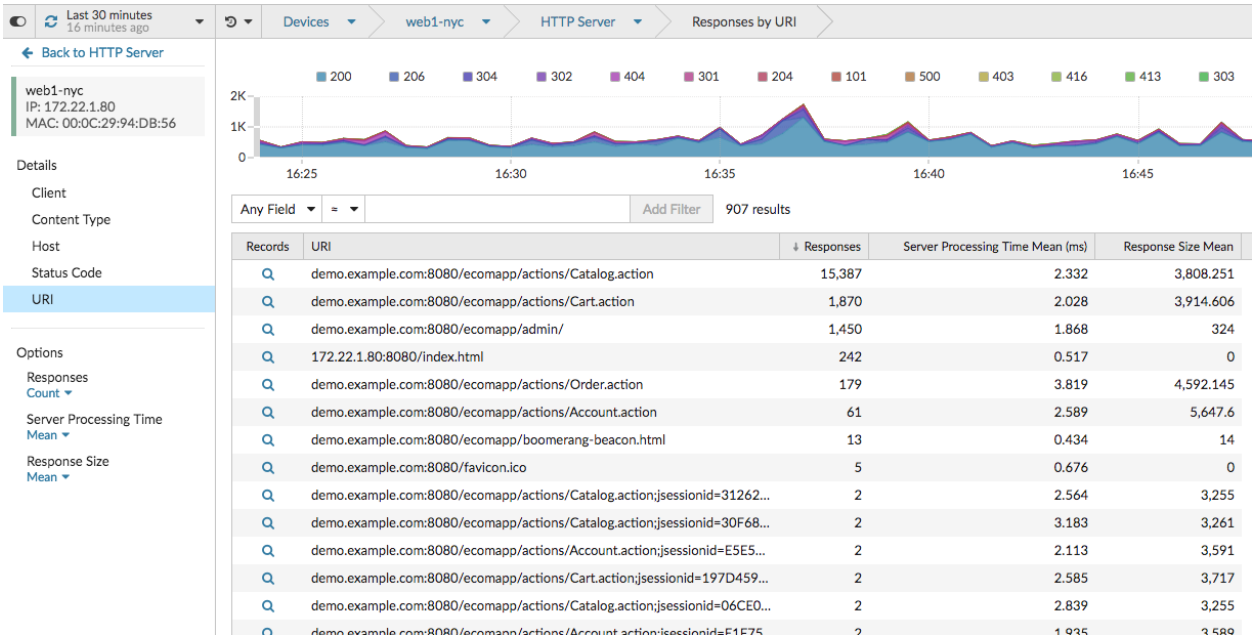


Le filtre principal apparaît au-dessus du tableau. Vous pouvez désormais consulter toutes les mesures détaillées associées à cette clé unique.

7. Pour supprimer ce filtre du tableau, puis l'appliquer au graphique supérieur, cliquez sur le **x** icône, comme illustré dans la figure suivante.



Le filtre du graphique persiste lorsque vous sélectionnez d'autres clés dans la section Détails.



Ajouter des mesures détaillées à un graphique

Si vous souhaitez surveiller rapidement un ensemble de mesures détaillées dans un tableau de bord, sans effectuer à plusieurs reprises les mêmes étapes de hiérarchisation, vous pouvez effectuer une analyse détaillée sur une métrique lorsque vous modifiez un graphique dans explorateur de métriques. La plupart des graphiques peuvent afficher jusqu'à 20 des valeurs métriques les plus détaillées, ventilées par clé. Une clé peut être l'adresse IP d'un client, un nom d'hôte, une méthode, un URI, un référent, etc. Les widgets de tableau et de liste peuvent afficher jusqu' à 200 valeurs métriques détaillées les plus élevées.

Par exemple, un tableau de bord destiné à surveiller le trafic Web peut contenir un graphique affichant le nombre total de requêtes et de réponses HTTP. Vous pouvez modifier ce graphique pour effectuer une analyse détaillée de chaque métrique par adresse IP afin de voir les principaux intervenants.

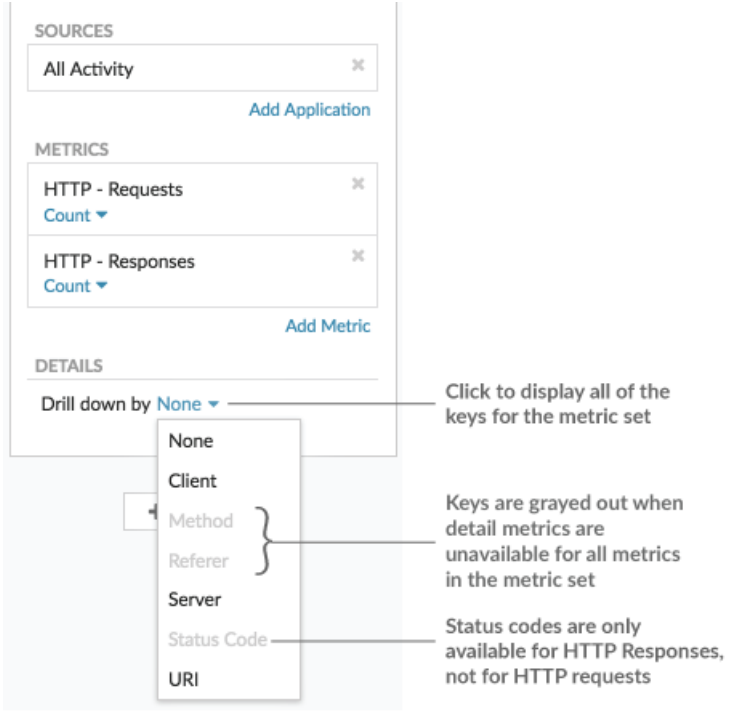
Les étapes suivantes vous montrent comment modifier un graphique existant, puis comment effectuer un défilement vers le bas pour afficher les mesures détaillées :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Accédez à un tableau de bord ou à une page de protocole.
3. Cliquez sur le titre du graphique, puis sélectionnez **Modifier**.
4. Dans le Détails section, cliquez **Profilez vers le bas par *<None>*** , où *<None>* est le nom de la clé métrique détaillée actuellement affichée dans votre graphique.
5. Sélectionnez une clé dans la liste déroulante.

> **Note:** Si vous en avez plusieurs source sélectionnées dans votre ensemble métrique, par exemple deux appareils, les sources sont automatiquement combinées dans un groupe de sources ad hoc au fur et à mesure que vous effectuez une analyse descendante. Vous ne pouvez pas désélectionner le **Combiner les sources** case à cocher. Pour afficher les métriques détaillées pour chaque source, vous devez supprimer une source de l'ensemble de mesures, puis cliquer sur **Ajouter une source** pour créer un nouvel ensemble de mesures.

Si les données métriques détaillées d'une clé commune sont disponibles pour toutes les mesures d'un ensemble de mesures, la clé de la métrique détaillée apparaît automatiquement dans la liste déroulante, comme illustré dans la figure suivante. Si une clé de la liste est grisée, la métrique détaillée associée à cette clé n'est pas disponible pour toutes les métriques de cet ensemble de mesures ci-dessus. Par

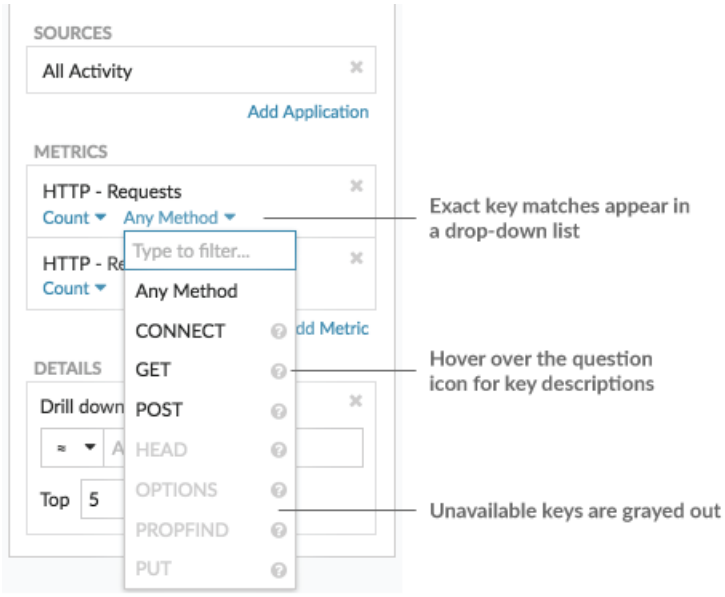
exemple, les données du client, du serveur et de l'URI sont disponibles pour les métriques de requêtes HTTP et de réponses HTTP dans l' ensemble de métriques.



6. Vous pouvez filtrer les clés avec une correspondance approximative, expression régulière (regex), ou une correspondance exacte en suivant l'une des étapes suivantes :
   - Dans le Filtre champ, sélectionnez le **≈** opérateur pour afficher les touches selon une correspondance approximative ou avec une expression régulière. Vous devez omettre les barres obliques avec regex dans le filtre de correspondance approximative.

     Note: Le **#** l'option de filtrage pour exclure les résultats n'est disponible que sur pages de détails. Si vous souhaitez exclure les résultats d'un graphique de tableau de bord, créez un expression régulière (regex).
   - Dans le Filtre champ, sélectionnez le **=** opérateur pour afficher les touches selon une correspondance exacte.
7. Optionnel : Dans le champ des meilleurs résultats, entrez le nombre de clés que vous souhaitez afficher. Ces clés auront les valeurs les plus élevées.
8. Pour supprimer une sélection déroulante, cliquez sur **x** icône.

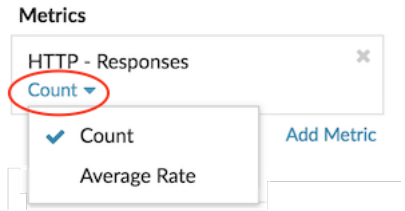
Note: Vous pouvez afficher une correspondance clé exacte par métrique, comme illustré dans la figure suivante. Cliquez sur le nom de la métrique détaillée (tel que **Toutes les méthodes**) pour sélectionner une clé métrique détaillée spécifique (telle que `GET`) dans la liste déroulante. Si une touche apparaît en gris (telle que `PROPFIND`), les données métriques détaillées ne sont pas disponibles pour cette clé spécifique. Vous pouvez également saisir une clé qui ne figure pas dans la liste déroulante.



Afficher un taux ou un nombre dans un graphique

Vous pouvez visualiser les erreurs, les réponses, les demandes et les autres données métriques de comptage dans un graphique sous forme de taux par seconde ou de nombre total d'événements au fil du temps. Pour les métriques de haute précision relatives aux octets réseau et aux paquets réseau, vous disposez d'options supplémentaires pour afficher le débit maximal, minimum et moyen par seconde dans un graphique.

Quand modification d'un graphique dans l'explorateur de métriques, vous pouvez sélectionner un nombre ou un taux en cliquant sur le lien déroulant situé sous le nom de la métrique, comme illustré dans la figure suivante.



En outre, vous pouvez sélectionner l'une des options suivantes pour afficher les taux et les dénombrements. Notez que le type de métrique que vous sélectionnez influe sur le taux ou le nombre automatiquement affiché.

Taux moyen

Calcule la valeur métrique moyenne par seconde pour l'intervalle de temps sélectionné. Pour les métriques liées au réseau, telles que Response L2 Bytes ou NetFlow Bytes, le débit moyen par seconde est automatiquement affiché.

Compter

Affiche le nombre total d'événements pour l'intervalle de temps sélectionné. Pour la majorité des indicateurs de comptage, tels que les erreurs, les demandes et les réponses, le décompte est automatiquement affiché.

Récapitulatif des taux

Calcule les valeurs métriques maximale, minimale et moyenne par seconde. Pour les métriques de haute précision, telles que les octets réseau et les paquets réseau, ces trois débits sont automatiquement affichés dans le graphique sous forme de résumé. Vous pouvez également choisir de n'afficher que le taux maximum, minimum ou moyen dans un graphique. Des mesures de haute précision sont collectées à l'aide d'un Niveau de granularité d'une seconde et ne sont disponibles que lorsque vous configurer votre graphique avec une source de réseau ou d'équipement.

Afficher le taux moyen dans un graphique

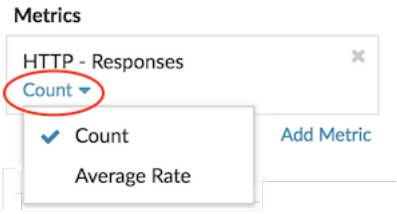
Si vous avez configuré un graphique avec une erreur, une réponse, une demande ou un autre type de métrique de comptage, le nombre total d'événements au fil du temps est automatiquement affiché. Vous pouvez également modifier le graphique pour afficher un taux moyen par seconde pour vos données.

Avant de commencer

Création d'un graphique et sélectionnez une métrique de comptage, telle que les erreurs, les demandes ou les réponses, comme source. Enregistrez votre graphique dans un tableau de bord.

Les étapes suivantes vous montrent comment ajouter un taux moyen à un graphique de tableau de bord existant :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Lancez le explorateur de métriques pour modifier le graphique en suivant les étapes suivantes :
   a) Dans le dock du tableau de bord, sélectionnez un tableau de bord contenant le graphique que vous souhaitez modifier.
   b) Cliquez sur le titre du graphique et sélectionnez **Modifier**.
4. Cliquez **Compter** sous le nom de la métrique.



5. Sélectionnez **Taux moyen** depuis la liste déroulante.
   L'unité « /s » est appliquée aux unités métriques. Vous pouvez revenir au décompte à tout moment.
6. Cliquez **Enregistrer** pour fermer l'explorateur de métriques.

Conseil Lorsque vous sélectionnez plusieurs mesures de dénombrement dans un graphique, évitez d' afficher les taux et les dénombrements ensemble dans le même graphique. Cela peut fausser l' échelle de l'axe Y. L'axe Y inclura un « /s » sur les étiquettes à cocher uniquement si tous les indicateurs affichent des taux.

Afficher le taux maximum dans un graphique

Pour afficher le taux maximal par seconde d'une métrique dans un graphique, vous devez configurer un graphique avec une métrique de haute précision.

Les étapes suivantes vous montrent comment configurer un graphique qui affiche un taux maximal :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Effectuez l'une des étapes suivantes :
   - Pour créer un nouveau graphique, cliquez sur le menu de commandes ⋮ dans le coin supérieur droit de la page, puis sélectionnez **Créer un graphique**.

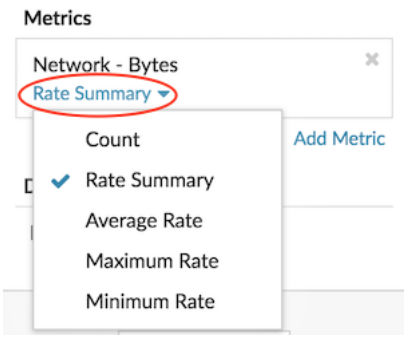
- Pour modifier un graphique existant, cliquez sur **Tableaux de bord** en haut de page. Dans le dock du tableau de bord, sélectionnez un tableau de bord contenant le graphique que vous souhaitez modifier. Cliquez sur le titre du graphique et sélectionnez **Modifier**.

3. Cliquez **Ajouter une source** et sélectionnez l'une des sources suivantes :
   - Une source réseau qui n'est pas un réseau de flux, tel qu'un site.
   - Un équipement, tel qu'un serveur ou un client.
4. Recherchez et sélectionnez l'une des métriques suivantes :

   Pour une source réseau
   - Octets réseau (débit total)
   - Paquets réseau (nombre total de paquets)

   Pour une source d'équipement
   - Octets réseau (débit entrant et sortant combiné par équipement)
   - Nombre d'octets réseau entrants (débit entrant par équipement)
   - Octets de sortie réseau (débit sortant par équipement)
   - Paquets réseau (paquets entrants et sortants combinés par équipement)
   - Paquets réseau entrants (paquets entrants par équipement)
   - Paquets réseau sortants (paquets sortants par équipement)
5. Sélectionnez un type de graphique compatible avec les mesures de comptage (y compris les graphiques en lignes, en valeurs, en colonnes, en barres, en secteurs et en listes).

   L'affichage par défaut d'une métrique de haute précision est un résumé du taux qui affiche automatiquement le taux maximum, moyen et minimum.
6. Cliquez **Récapitulatif des taux** sous le nom de la métrique.



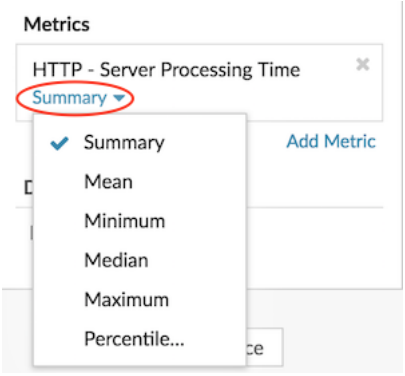
7. Sélectionnez **Taux maximum** depuis le menu déroulant.
8. Cliquez **Enregistrer** pour fermer l'explorateur de métriques.

Afficher des percentiles ou une moyenne dans un graphique

Si vous disposez d'un ensemble de serveurs essentiels à votre réseau, l'affichage du 95e centile du temps de traitement des serveurs dans un graphique peut vous aider à évaluer les difficultés rencontrées par les serveurs. Les percentiles sont des mesures statistiques qui peuvent vous montrer comment un point de données se compare à une distribution totale dans le temps.

Vous ne pouvez afficher les calculs de valeur percentile et de moyenne (moyenne) que dans les graphiques contenant jeu de données ou ensemble d'échantillons métriques. Les métriques du jeu de données sont associées au timing et à la latence, telles que le temps de traitement du serveur et les métriques de temps aller-retour. Les métriques Sampleset fournissent des résumés des métriques temporelles détaillées, telles que le temps de traitement du serveur ventilé par serveur, méthode ou URI.

Quand modification d'un graphique dans l' explorateur de mesures, vous pouvez sélectionner les percentiles ou la moyenne en cliquant sur le lien déroulant situé sous le nom de la métrique du jeu de données ou de l'ensemble d'échantillons, comme illustré dans la figure suivante.



L'explorateur de métriques fournit les calculs suivants pour afficher les percentiles et la moyenne.

Résumé

Pour les métriques du jeu de données, le résumé est une plage qui inclut les valeurs des 95e, 75e, 50e, 25e et 5e percentiles.

Par exemple, chaque ligne d'un graphique en chandelier contient cinq points de données. Si Résumé est sélectionné, le corps principal de la ligne représente la plage comprise entre le 25e percentile et le 75e percentile. Le crochet du milieu représente le 50e percentile (médiane). L'ombre supérieure au-dessus de la ligne du corps représente le 95e percentile. L'ombre inférieure représente le 5e percentile.

Pour les métriques des ensembles d'échantillons, le résumé affiche l'écart type +/-1 et les valeurs moyennes. Dans le graphique en chandelier, le crochet vertical sur la ligne représente la moyenne, tandis que les ombres supérieures et inférieures représentent les valeurs d'écart type.

Méchant

La moyenne calculée des données.

Médiane

La valeur du 50e percentile d'une métrique d'un ensemble de données.

Maximum

La valeur du 100e percentile d'une métrique d'un ensemble de données.

Minimum

La valeur du 0e percentile d'une métrique d'un ensemble de données.

Percentile

Plage personnalisée de trois ou cinq percentiles pour une métrique d'un ensemble de données.

Afficher une plage personnalisée de percentiles

Vous pouvez afficher une plage personnalisée de trois ou cinq percentiles pour les mesures relatives au temps de traitement du serveur ou au temps de trajet aller-retour. Vous ne pouvez pas afficher de percentiles personnalisés dans un diagramme circulaire ou un graphique dstatus.

Les étapes suivantes vous montrent comment ajouter une plage de percentiles personnalisée à un graphique de tableau de bord existant :

Avant de commencer
Création d'un graphique et sélectionnez un jeu de données ou ensemble d'échantillons métrique, et enregistrez-la dans un tableau de bord.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.

3. Lancez le Metric Explorer pour modifier le graphique en suivant les étapes suivantes :
   a) Dans le dock du tableau de bord, sélectionnez un tableau de bord contenant le graphique que vous souhaitez modifier.
   b) Cliquez sur le titre du graphique et sélectionnez **Modifier**.
4. Cliquez **Résumé** sous le nom de la métrique.
5. Sélectionnez **Percentile...** depuis la liste déroulante.
6. Dans le champ Définir les percentiles, tapez un nombre pour chaque valeur de percentile, séparé par une virgule. Par exemple, pour afficher les 10e, 30e et 80e percentiles, tapez `10, 30, 80`.
7. Cliquez **Enregistrer**. Votre plage personnalisée est désormais affichée dans le graphique. Vous pouvez basculer entre votre plage personnalisée et d'autres sélections de percentiles, telles que Résumé ou Maximum, à tout moment.
8. Cliquez **Enregistrer** une nouvelle fois pour fermer l'explorateur de métriques.

Filtrez les valeurs aberrantes dans des histogrammes ou des diagrammes thermiques

Les histogrammes et les cartes thermiques affichent une distribution des données. Cependant, les valeurs aberrantes peuvent fausser l'affichage de la distribution dans votre graphique, ce qui rend difficile l'observation de modèles ou de valeurs moyennes. L'option de filtre par défaut pour ces graphiques exclut les valeurs aberrantes de la plage de données et affiche les 5e au 95e percentiles. Vous pouvez modifier le filtre pour afficher l' ensemble des données (minimales et maximales), y compris les valeurs aberrantes, de votre graphique en suivant la procédure suivante.

1. Cliquez sur le titre du graphique, puis sélectionnez **Modifier** pour lancer le explorateur de métriques.
2. Cliquez sur **Des options** onglet.
3. Dans la liste déroulante Filtre par défaut de la section Filtres, sélectionnez **Min à Max**.
4. Cliquez **Enregistrer** pour fermer l'explorateur de métriques.

Modifier les libellés métriques dans la légende d'un graphique

Vous pouvez remplacer l'étiquette métrique par défaut d'un graphique par une étiquette personnalisée. Par exemple, vous pouvez remplacer l'étiquette par défaut, « Network Bytes », par une étiquette personnalisée telle que « Débit ».

Les libellés personnalisés ne s'appliquent qu'aux graphiques individuels. L'étiquette personnalisée d'une métrique sera conservée si vous copiez le graphique sur un autre tableau de bord, si vous partagez un tableau de bord avec un autre utilisateur ou si vous ajoutez de nouvelles mesures à votre graphique.

Toutefois, si vous apportez des modifications à la métrique d'origine, par exemple en mettant à jour le calcul des données (de la médiane au 95e percentile, par exemple) ou en approfondissant la métrique, l'étiquette personnalisée sera automatiquement effacée. L'étiquette est effacée pour éviter toute erreur d'étiquetage ou toute inexactitude potentielle de l'étiquette personnalisée lorsque les données métriques changent.

Voici quelques points à prendre en compte pour modifier le libellé de la légende d'un graphique :

- Pour métriques détaillées, une étiquette personnalisée est automatiquement ajoutée à toutes les clés affichées dans le graphique. Cependant, vous pouvez modifier l'ordre de la clé dans l'étiquette en incluant la variable, *CLÉ $*:
  - Type `Erreurs $KEY` à afficher **Erreurs 172.21.1.1**
  - Type `[$KEY] erreurs` à afficher **[172.21.1.1] erreurs**
- Vous ne pouvez pas modifier les libellés du diagramme à cases, du chandelier, de la carte thermique, du tableau ou des diagrammes d'état.
- Vous ne pouvez pas renommer les libellés de delta métrique ou de ligne de base dynamique.

Avant de commencer
Création d'un graphique et sélectionnez une métrique.

Les étapes suivantes vous montrent comment modifier les libellés métriques dans un graphique de tableau de bord existant :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Lancez le explorateur de métriques pour modifier le graphique en suivant les étapes suivantes :
   a) Dans le dock du tableau de bord, sélectionnez un tableau de bord contenant le graphique que vous souhaitez modifier.
   b) Cliquez sur le titre du graphique et sélectionnez **Modifier**.
4. Dans le volet d'aperçu de l'explorateur de mesures, cliquez sur le libellé de la métrique.
5. Sélectionnez **Renommer** depuis le menu déroulant.
6. Dans le Afficher une étiquette personnalisée dans ce champ, saisissez une nouvelle étiquette.
   L'étiquette doit être unique par rapport aux autres étiquettes du graphique.
7. Cliquez **Enregistrer**, puis cliquez sur **Enregistrer** une nouvelle fois pour fermer l'explorateur de métriques.
   La nouvelle étiquette apparaît dans votre graphique.

Ajouter une ligne de base dynamique à un graphique

Les lignes de base dynamiques permettent de faire la distinction entre l'activité normale et l'activité anormale dans les données de votre graphique. Les lignes de base ne sont prises en charge que dans les diagrammes en zones, en chandeliers, en colonnes, en lignes et en courbes.

Le système ExtraHop calcule des lignes de base dynamiques sur la base de données historiques. Pour générer un nouveau point de données sur une ligne de base dynamique, le système calcule la valeur médiane pour une période spécifiée.

Avertissement : La suppression ou la modification d'une ligne de base dynamique peut entraîner la suppression des données de référence du système. Si aucune ligne de base dynamique n'est référencée par aucun tableau de bord, les données seront supprimées du système afin de libérer les ressources système inutilisées. Vous ne pouvez pas récupérer une ligne de base dynamique une fois qu'elle a été supprimée.

Sélectionnez le type de référence le mieux adapté à votre environnement. Par exemple, si vous constatez régulièrement des changements spectaculaires d'un jour à l'autre, sélectionnez une base horaire de référence qui compare l'activité observée certains jours de la semaine. Si l'activité HTTP augmente le samedi, la base de référence de l'heure de la semaine peut vous aider à comparer le pic actuel d' activité HTTP avec le niveau observé les autres samedis à la même heure. Le tableau suivant décrit le mode de calcul de chaque type de référence :

Type de ligne de base	Données historiques	Quelles sont les comparaisons entre les données de référence	Nouveaux points de données de référence ajoutés
Heure du jour	10 jours	Valeurs métriques à partir d'une heure donnée de la journée. Par exemple, tous les jours à 14h.	Toutes les heures
Heure de la semaine	5 semaines	Valeurs métriques pour une heure donnée un jour précis de la semaine. Par exemple, tous les mercredis à 14h.	Toutes les heures

Type de ligne de base	Données historiques	Quelles sont les comparaisons entre les données de référence	Nouveaux points de données de référence ajoutés
Tendance à court terme	1 heure	Valeurs métriques pour chaque minute en une heure.	Toutes les 30 secondes

Voici quelques points importants à prendre en compte lors de l'ajout d'une référence à un graphique :

- Les lignes de base dynamiques calculent et stockent les données de référence. Par conséquent, la création d'une ligne de base consomme des ressources système et la configuration d'un trop grand nombre de lignes de base risque de dégrader les performances du système.
- La suppression ou la modification d'une ligne de base dynamique peut supprimer des données de ligne de base dynamique du système.
- Les métriques détaillées, également appelées topnsets, ne sont pas prises en charge. Les mesures relatives à l'ensemble d'échantillons, au taux maximum et au taux minimum ne sont pas non plus prises en charge. Si l'un de ces types de mesures est sélectionné dans votre graphique, vous ne pourrez pas générer de ligne de base dynamique pour ces données.
- Le système ne peut commencer à créer une ligne de base dynamique que si la quantité nécessaire de données historiques est disponible. Par exemple, un **Heure du jour** la base de référence nécessite 10 jours de données historiques. Si le système ne collecte des données que depuis six jours, la base de référence ne commence à être tracée que lorsqu'il dispose de quatre jours supplémentaires de données.
- Le système ne trace pas rétroactivement une ligne de base dynamique pour les données historiques. Le système trace uniquement une ligne de base dynamique pour les nouvelles données.
- Si deux lignes de base dynamiques identiques existent dans des tableaux de bord distincts, les tableaux de bord réutilisent les données de référence ; toutefois, les lignes de base doivent être identiques. Si vous sélectionnez un nouveau type de ligne de base, la nouvelle ligne de base dynamique ne partagera pas de données avec la ligne de base dynamique précédente.

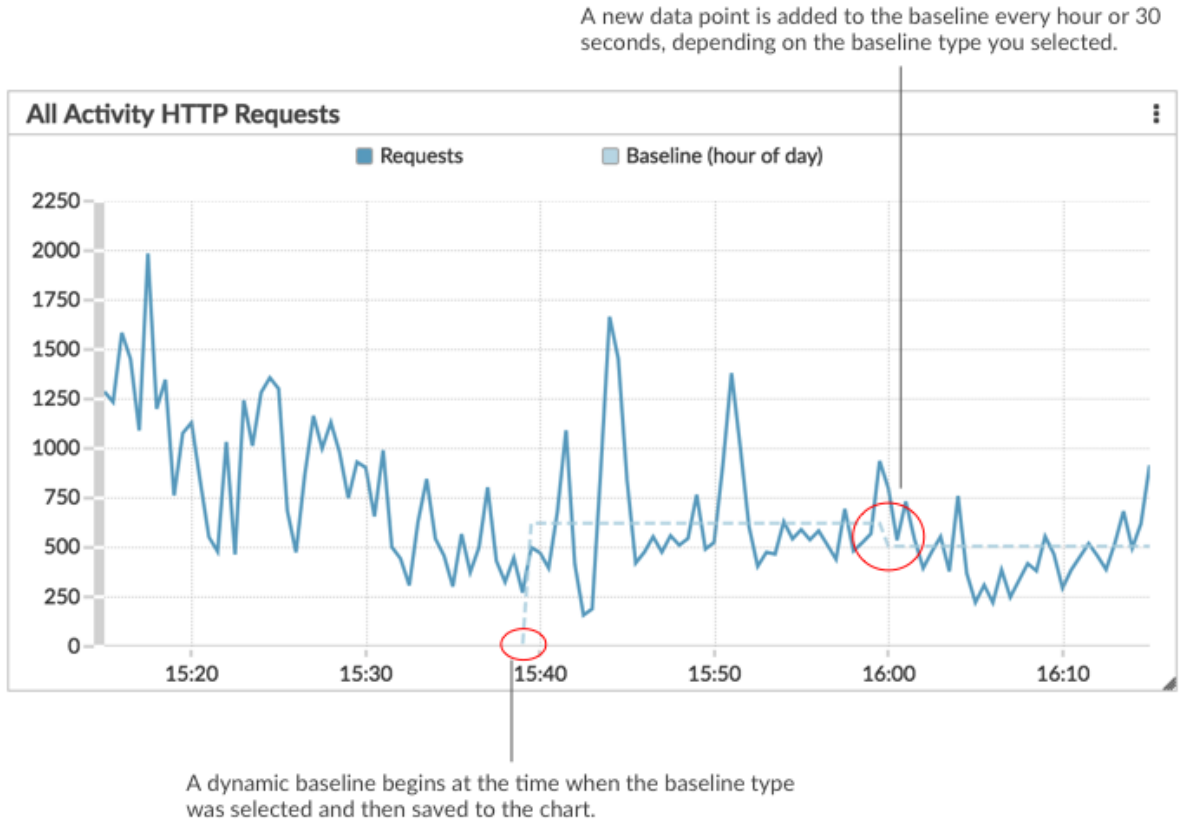
Les étapes suivantes vous montrent comment ajouter une ligne de base dynamique à un graphique de tableau de bord existant :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Lancez le explorateur de métriques pour modifier le graphique en suivant les étapes suivantes :
   a) Dans le dock du tableau de bord, sélectionnez un tableau de bord contenant le graphique que vous souhaitez modifier.
   b) Cliquez sur le titre du graphique, puis sélectionnez **Modifier**.
4. Cliquez sur **Analyse** onglet.
5. Dans le Lignes de base dynamiques section, sélectionnez l'une des options de type de ligne de base dynamique suivantes :

Option	Description
Heure du jour	Affiche la valeur médiane pour une heure donnée de la journée. Cette option est particulièrement utile si l'activité dans votre environnement suit généralement un schéma quotidien constant. Si vous constatez régulièrement des niveaux d'activité radicalement différents selon les jours de la semaine, cette option est moins utile car le niveau de référence ne correspond généralement pas aux valeurs actuelles.

Option	Description
Heure de la semaine	Affiche la valeur médiane pour une heure donnée un jour précis de la semaine. Cette option est particulièrement utile si vous constatez régulièrement des niveaux de trafic très différents chaque jour de la semaine.
Tendance à court terme	Affiche la valeur médiane de la dernière heure. Cette option est utile pour lisser les données du graphique afin de révéler les tendances à court terme.

6. Cliquez **Enregistrer** pour fermer l'explorateur de métriques et revenir au tableau de bord. Le système ExtraHop commencera à calculer la ligne de base dynamique. De nouveaux points de données de référence sont ajoutés toutes les heures ou toutes les 30 secondes, comme le montre la figure suivante.



Ajouter une ligne de seuil statique à un graphique

L'affichage d'une ligne de seuil statique dans un graphique peut vous aider à déterminer quels points de données sont inférieurs ou supérieurs à une valeur significative.

Par exemple, vous pouvez créer un graphique en courbes pour le temps de traitement du serveur afin de vous aider à surveiller les performances d'une base de données importante dans votre environnement

réseau. En ajoutant une ligne de seuil qui définit un accord de niveau de service (SLA) limite de temps de traitement acceptable, vous pouvez voir quand les performances de la base de données ralentissent et résoudre le problème.

Vous pouvez ajouter une ou plusieurs lignes de seuil au fur et à mesure que vous modifier un graphique à l'aide de l'explorateur de métriques. Ces lignes sont locales au graphique et ne sont pas associées à d'autres widgets ou alertes. Les lignes de seuil ne sont disponibles que pour les graphiques de zones, de chandeliers, de colonnes, de lignes, de lignes et de colonnes, ainsi que pour les graphiques d'état.

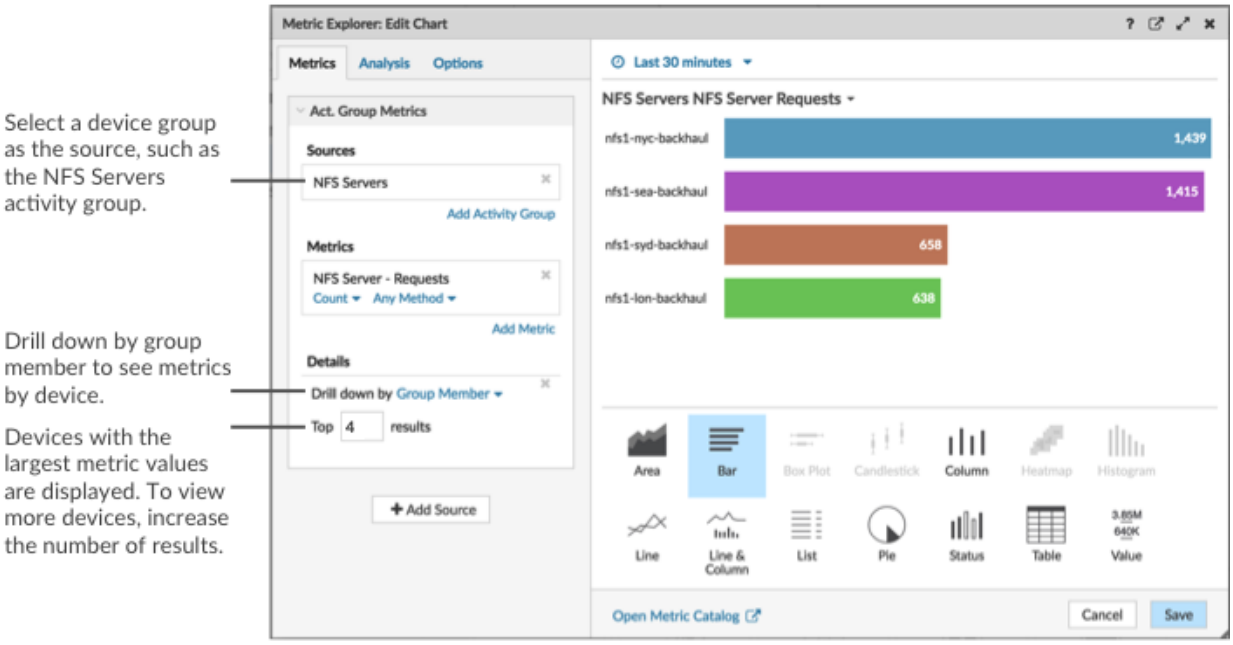
Les étapes suivantes vous montrent comment ajouter une ligne de seuil statique à un graphique de tableau de bord existant :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord**.
3. Lancez le explorateur de métriques pour modifier le graphique en suivant les étapes suivantes :
   a) Dans le dock du tableau de bord, sélectionnez un tableau de bord contenant le graphique que vous souhaitez modifier.
   b) Cliquez sur le titre du graphique, puis sélectionnez **Modifier**.
4. Cliquez sur **Analyse** onglet.
5. Dans le Seuils statiques section, cliquez **Ajouter une ligne de seuil**.
6. Dans le Valeur dans le champ, tapez un chiffre qui indique la valeur de seuil pour la ligne. Cette valeur détermine l'endroit où la ligne apparaît sur l'axe Y de votre graphique.

   Note: Pour les graphiques qui s'affichent uniquement mesures de comptage (tels que les octets, les erreurs et les réponses), la valeur de la ligne de seuil est automatiquement mise à l'échelle en fonction du fait que les données sont affiché sous forme de taux ou de décompte. Lorsque les données ne sont affichées que sous forme de décompte, la valeur de la ligne de seuil est automatiquement adaptée à la période de cumul (30 secondes, 5 minutes, 1 heure ou 1 jour). Le la période de cumul des données est déterminée par l' intervalle de temps vous sélectionnez.
7. Dans le Étiquette champ, saisissez un nom pour votre ligne de seuil.
8. Dans le Couleur dans ce champ, sélectionnez une couleur (gris, rouge, orange ou jaune) pour votre ligne de seuil.
9. Cliquez **Enregistrer** pour fermer l'explorateur de métriques.

Afficher les membres du groupe déquipements dans un graphique

Si vous disposez d'un graphique qui affiche un groupe de dispositifs, vous pouvez consulter les statistiques des principaux appareils du groupe, au lieu de visualiser une seule valeur pour l'ensemble du groupe d'appareils. L'exploration par membre du groupe dans l'explorateur de métriques vous permet de visualiser jusqu'à 20 appareils dans le graphique.



Si le nombre de membres des groupes indiqué dans un graphique est inférieur au nombre de résultats que vous avez indiqué, cela peut être dû au fait que vous avez sélectionné un groupe de groupes intégré comportant un petit nombre d'appareils. Pour les groupes d'équipements intégrés, les appareils sont placés dynamiquement dans un groupe en fonction du type de trafic de protocole auquel ils sont associés ou du rôle qui leur est attribué.

Avant de commencer
Création d'un graphique qui contient un groupe déquipements comme source sélectionnée. Enregistrez le graphique dans un tableau de bord.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Tableaux de bord** .
3. Lancez le Metric Explorer pour modifier le graphique en suivant les étapes suivantes :
   a) Dans le dock du tableau de bord, sélectionnez un tableau de bord contenant le graphique que vous souhaitez modifier.
   b) Cliquez sur le titre du graphique et sélectionnez **Modifier**.
4. Dans le Détails champ, cliquez **Extraire vers le bas par *<None>*** , où *<None>* est le nom de la métrique détaillée actuellement affichée dans votre graphique. Ensuite, sélectionnez **Membre du groupe**.
5. Dans le champ des meilleurs résultats, entrez le nombre de membres du groupe que vous souhaitez afficher. Ces appareils auront les valeurs métriques les plus élevées. Vous pouvez afficher jusqu' à 20 membres du groupe.
6. Cliquez **Enregistrer** pour fermer l'explorateur de métriques.

Note: Si vous effectuez une analyse descendante par membre du groupe, vous ne pouvez pas effectuer d'autres recherches pour voir les mesures détaillées de chaque équipement à l'aide d'une touche. Pour afficher les statistiques détaillées par clé pour un équipement, nous vous recommandons de créer un autre graphique avec des appareils spécifiques sélectionnés comme source.

Filtres d'expressions régulières

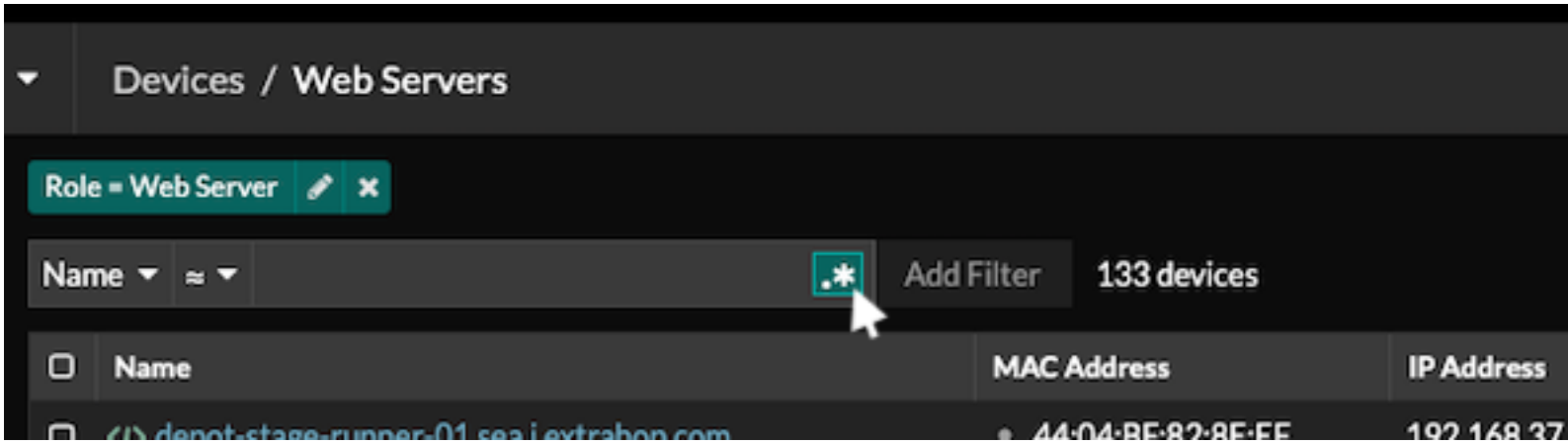
Filtrez les résultats de votre recherche en écrivant des chaînes d'expressions régulières (regex) dans certains champs de recherche du système ExtraHop. Par exemple, vous pouvez filtrer les paramètres d' une clé

métrique détaillée, comme un numéro dans une adresse IP. Vous pouvez également filtrer en excluant des clés spécifiques ou une combinaison de touches des graphiques.

Les champs de recherche compatibles Regex comportent des indicateurs visuels dans tout le système et acceptent la syntaxe standard.

Champs de recherche marqués d'un astérisque

Cliquez sur l'astérisque pour activer les chaînes regex.

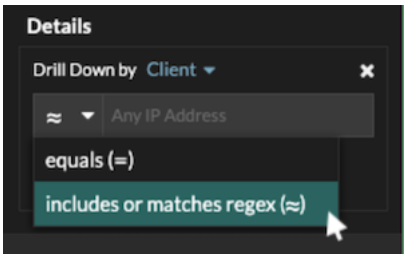


Ce type de champ est disponible sur les pages système suivantes :

- Filtrer un tableau d'appareils
- Création de critères de filtre pour un groupe dequipments dynamique

Certains champs de recherche avec un opérateur à trois champs

Cliquez sur la liste déroulante de l'opérateur pour sélectionner l'option regex.

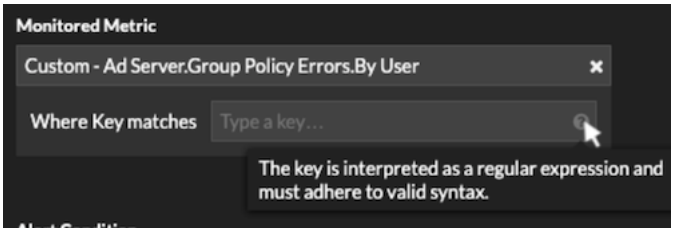


Ce type de champ est disponible sur la page système suivante :

- Modifier un graphique dans l'explorateur de métriques

Certains champs de recherche avec une info-bulle

Passez la souris sur l'info-bulle dans le champ pour voir quand l'expression régulière est requise.



Ce type de champ est disponible sur la page système suivante :

- Ajouter des relations d'enregistrement à une métrique personnalisée

Le tableau suivant inclut des exemples de syntaxe regex standard.

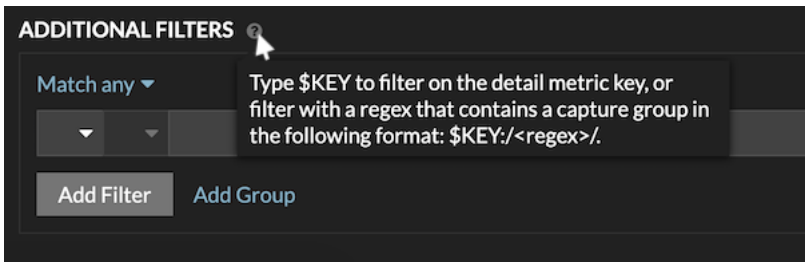
Scénario graphique	Filtre Regex	Comment ça marche
Comparez les codes d'état HTTP `200` à `404`.	`(200 et 404)`	Le symbole de la barre verticale (|) est l'opérateur OR. Ce filtre correspond `200`, ou `404`, ou les deux codes d'état.
Afficher tout code dD'état HTTP contenant un 4.	`[41]`	Les crochets ([et]) désignent une plage de caractères. Le filtre recherche tous les caractères entre crochets, quel que soit leur ordre. Ce filtre correspond à toute valeur contenant un 4 ou un 1. Par exemple, ce filtre peut renvoyer `204`, `400`, `101`, ou `201` codes d'état.
Afficher tout `500`codes d'état HTTP de niveau.	`^ [5]`	Le signe du curseur (^) placé entre crochets ([et]) signifie « commence par ». Ce filtre correspond à toute valeur commençant par 5. Par exemple, ce filtre peut renvoyer `500` et `502` codes d'état.
Afficher tout `400` et `500`codes d'état HTTP de niveau.	`^ [45]`	Les valeurs multiples entre crochets ([et]) sont recherchées individuellement, même si elles sont précédées du signe caret (^). Ce filtre ne recherche pas les valeurs commençant par 45, mais correspond à toutes les valeurs commençant par un 4 ou 5. Par exemple, ce filtre peut renvoyer `400`, `403`, et `500` codes d'état.
Afficher tous les codes d'état HTTP sauf `200`codes d' état de niveau.	`^ (? ! 2)`	Un point d'interrogation (?) et point d'exclamation (!) entre parenthèses spécifient une valeur à exclure. Ce filtre correspond à toutes les valeurs sauf celles commençant par un 2. Par exemple, ce filtre peut renvoyer `400`, `500`, et `302` codes d'état.
Afficher n'importe quelle adresse IP avec `187`.	`187.`	Allumettes 1, 8, et 7 caractères de l'adresse IP. Ce filtre ne renverra pas les adresses IP se terminant par 187, car la fin de la période indique que quelque chose doit se trouver après les valeurs. Si vous souhaitez rechercher la période en tant que valeur littérale, vous devez la faire précéder d'une barre oblique inverse (\).

Scénario graphique	Filtre Regex	Comment ça marche
Vérifiez toutes les adresses IP contenant `187.18.`	`187 \ ,18.`	Allumettes `187.18` et tout ce qui va suivre. La première période est traitée littéralement car elle est précédée d'une barre oblique inverse (\). La deuxième période est traitée comme un joker. Par exemple, ce filtre renvoie les résultats pour `187.18.0.0`, `180.187.0.0`, ou `187.180.0.0/16`. Ce filtre ne renvoie pas d' adresse se terminant par `187.18`, car le caractère générique exige que les caractères suivent les valeurs spécifiées.
Afficher n'importe quelle adresse IP sauf `187.18.197.150`.	`^ (? ! 187 \ ,18 \ .197 \ .150)`	Correspond à tout sauf `187.18.197.150`, où `^(?!)` spécifie la valeur à exclure.
Excluez une liste d'adresses IP spécifiques.	`^(?! 187\.18\.197\.15[012])`	Correspond à tout sauf `187.18.197.150`, `187.18.197.151`, et `187.18.197.152`, où `^(?!)` spécifie la valeur à exclure et les crochets ([et]) indiquent plusieurs valeurs.

Filtres supplémentaires

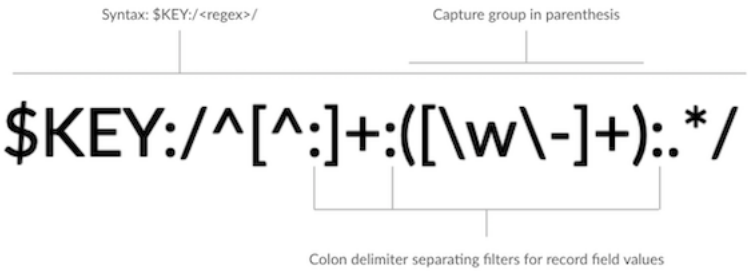
Quand tu créer une métrique détaillée personnalisée depuis le catalogue de métriques, vous pouvez ajouter une syntaxe regex avancée au champ de recherche Filtres supplémentaires de la section Record Relationships.

L'info-bulle apparaît une fois que vous avez sélectionné **Métrique détaillée** et n'est pas disponible lorsque **Métrique de base** est sélectionné.



La syntaxe regex de ce champ doit répondre aux exigences suivantes :

- Si votre clé contient plusieurs valeurs, votre syntaxe regex doit inclure un seul groupe de capture. Un groupe de capture est désigné par des parenthèses. Votre groupe de capture détermine la valeur du filtre.



- Si vous souhaitez renvoyer une valeur spécifique à partir d'une clé de métrique détaillée contenant plusieurs valeurs de champs d'enregistrement, l'expression régulière doit suivre la syntaxe suivante :

  `CLÉ $ :/ <regex> /`

  Par exemple, si votre clé métrique détaillée est ipaddr:host:cipher et que vous souhaitez uniquement renvoyer la valeur de l'adresse IP, vous devez taper ce qui suit :

  `$CLÉ : /^ ([^ :] +) : . +/`
- Si votre clé contient plusieurs valeurs de champ d'enregistrement, celles-ci sont séparées par un délimiteur spécifié dans le déclencheur qui génère la clé. L'emplacement des délimiteurs dans votre syntaxe regex doit correspondre à celui de la clé de détail. Par exemple, si vous avez une clé avec trois valeurs séparées par un séparateur composé de deux points, les trois valeurs de la clé dans votre syntaxe régulière doivent être séparées par deux points.

Conseil: Si vous souhaitez renvoyer toutes les valeurs des champs d'enregistrement dans une clé métrique détaillée, tapez `CLÉ $`. Par exemple, si votre clé métrique détaillée est ipaddr:host:cipher, tapez `CLÉ $` dans le champ de recherche pour renvoyer les trois valeurs d'enregistrement de ces champs (adresse IP, nom d'hôte et suite de chiffrement TLS).

Trouvez tous les appareils qui communiquent avec des adresses IP externes

Les étapes suivantes vous montrent comment trouver toutes les adresses IP externes avec lesquelles vos appareils internes communiquent. Vous pouvez ensuite voir si des appareils établissent ou reçoivent des connexions non autorisées depuis d'autres appareils extérieurs à votre réseau.

Conseil: Par défaut, tout équipement possédant une adresse IP RFC1918 (incluse dans un bloc CIDR 10/8, 172.16/12 ou 192.168/16) que le système ExtraHop découvre automatiquement est classé comme un équipement interne. Étant donné que certains environnements réseau incluent des adresses IP autres que la RFC1918 dans leur réseau interne, vous pouvez spécifier la localité d'une adresse IP sur la page Localités du réseau.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Actifs** en haut de page.
   La page Appareils apparaît. Elle répertorie tous les protocoles ayant un trafic dans l'intervalle de temps sélectionné.
3. À partir de Appareils par activité protocolaire, cliquez sur le nombre de périphériques TCP.
   En haut de la page, le Externe accepté et Connecté à l'extérieur les métriques indiquent le nombre d' adresses IP situées en dehors de votre réseau interne qui sont activement connectées à tous les appareils de votre réseau.
4. Cliquez sur la valeur métrique bleue pour l'une ou l'autre métrique.
5. Dans la section Afficher par..., sélectionnez **Membre du groupe**. Une page métrique détaillée apparaît et affiche tous les noms de vos périphériques réseau ainsi que le nombre de connexions aux adresses IP externes.
6. Cliquez sur le nom de l'équipement que vous souhaitez examiner. Une page de protocole s'affiche pour cet équipement. Elle contient les mesures relatives à l'équipement.

Prochaines étapes

- Trouvez des appareils homologues
- Surveiller un équipement pour détecter les connexions par adresse IP externes

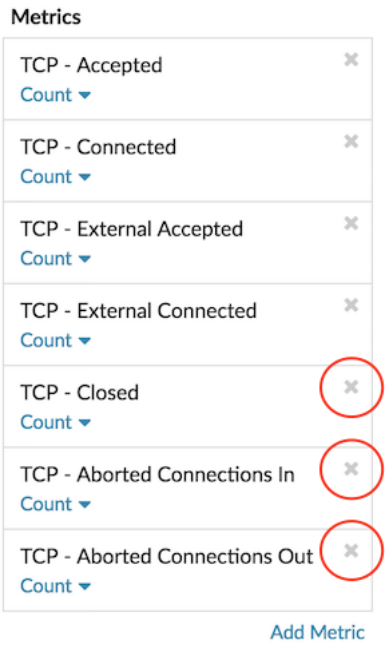
Surveiller un équipement pour détecter les connexions par adresse IP externes

Si vous disposez d'un serveur d'authentification ou d'une base de données qui ne doit pas se connecter à des adresses IP situées en dehors de votre réseau interne, vous pouvez créer un diagramme de valeurs dans un tableau de bord qui suit les métriques externes acceptées et externes connectées. À partir de votre tableau de bord, vous pouvez ensuite surveiller le nombre de connexions externes pour un équipement spécifique.

Conseil Par défaut, tout équipement possédant une adresse IP RFC1918 (incluse dans un bloc CIDR 10/8, 172.16/12 ou 192.168/16) que le système ExtraHop découvre automatiquement est classé comme un équipement interne. Étant donné que certains environnements réseau incluent des adresses IP non conformes à la norme RFC1918 dans leur réseau interne, vous pouvez spécifier la localité d'une adresse IP sur la page Localités du réseau.

Les étapes suivantes vous montrent comment créer un diagramme de valeurs pour ces métriques TCP , puis comment ajouter le graphique à un tableau de bord.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Actifs** en haut de page.
3. Cliquez **Appareils** dans le volet de gauche.
4. Trouvez un équipement puis cliquez sur le nom de l'équipement.
5. Cliquez **TCP** dans le volet de gauche. Dans le graphique du nombre total de connexions situé dans le coin supérieur gauche, les métriques External Accepted et External Connected indiquent le nombre d'adresses IP connectées à l'équipement en dehors de votre réseau interne.
6. Cliquez sur le **Nombre total de connexions** titre du graphique.
7. Dans le menu déroulant, sélectionnez **Créer un graphique à partir de...**. L' explorateur de métriques s'ouvre avec l'équipement et les métriques TCP déjà sélectionnés dans le graphique.
8. Au bas de l'explorateur de métriques, cliquez sur **Valeur** graphique.
9. Dans le volet gauche de la section Métrique, cliquez sur **x** icône pour supprimer chaque métrique TCP que vous ne souhaitez pas afficher dans le graphique, comme illustré dans la figure suivante.



Votre tableau de bord contient désormais des statistiques qui vous aident à suivre le ratio entre toutes les connexions acceptées et les connexions externes acceptées, ainsi que le rapport entre toutes les connexions initiées et les connexions initiées par des connexions externes initiées.

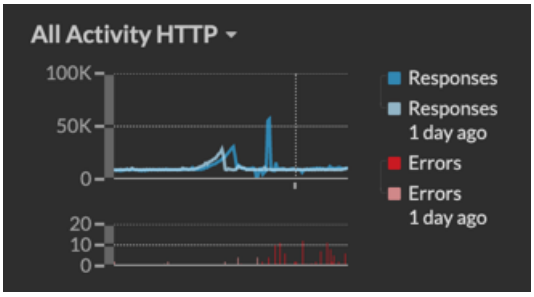
10. Optionnel : Apportez des modifications supplémentaires au graphique à l'aide de l'explorateur de métriques.
11. Cliquez **Ajouter au tableau de bord** et complétez l'une des options suivantes :
    - Sélectionnez le nom d'un tableau de bord existant dans la liste. La liste des tableaux de bord est ordonnée depuis les derniers tableaux de bord créés (en bas) jusqu'aux tableaux de bord les plus anciens (en haut).
    - Sélectionnez **Créer un tableau de bord**. Dans la fenêtre Propriétés du tableau de bord, tapez le nom du nouveau tableau de bord, puis cliquez sur **Créez**.
12. Optionnel : Apportez des modifications supplémentaires à la mise en page du tableau de bord.
13. Cliquez **Quitter le mode Layout**. Votre tableau de bord est terminé.

Prochaines étapes
Partager un tableau de bord

Comparez les intervalles de temps pour trouver le delta métrique

La comparaison des données métriques entre deux intervalles de temps vous permet de voir la différence, ou le delta, entre les données métriques côte à côte dans le même graphique. Si vous créez une comparaison et naviguez vers une autre zone du système ExtraHop, la comparaison est temporairement désactivée. Lorsque vous revenez à votre page d'origine, la comparaison que vous avez enregistrée est de nouveau activée.

1. Trouvez un graphique contenant les indicateurs que vous souhaitez comparer.
2. Dans le coin supérieur gauche de la barre de navigation, cliquez sur l' intervalle de temps.
3. Dans le Intervalle de temps onglet, cliquez **Comparez**.
4. Dans le Intervalle précédent (comparaison) section, sélectionnez l'intervalle de temps à comparer avec l'intervalle de temps actuel.
5. Cliquez **Enregistrer**. Les nouvelles données métriques issues de l' intervalle de temps de comparaison sont placées sur le graphique d'origine.



6. Pour supprimer la comparaison, procédez comme suit :
   a) Cliquez sur l'intervalle de temps.
   b) Cliquez **Supprimer la comparaison**.
   c) Cliquez **Enregistrer**.

   Note: Les lignes de base dynamiques n'apparaissent pas sur un graphique lorsque vous comparez des intervalles de temps.

Actifs

Toutes les activités métriques collectées à partir des données de votre réseau sont regroupées de manière logique en sections sur la page Actifs, où vous pouvez naviguer pour trouver les données dont vous avez besoin.

Vidéo: Consultez la formation associée : Actifs

Appareils

Les appareils, également appelés actifs et points de terminaison, sont des objets de votre réseau dotés d'une adresse MAC ou d'une adresse IP qui ont été automatiquement découverts et classés par le système ExtraHop. Assignez n'importe quel équipement à un graphique, une alerte ou un déclencheur en tant que source métrique. En savoir plus sur les appareils.

Groupes d'appareils

Groupes d'appareils sont des ensembles de périphériques définis par l'utilisateur qui peuvent être assignés collectivement en tant que source métrique à un graphique, une alerte ou un déclencheur. Tu peux créer un groupe dproximatif d'équipements qui ajoute des appareils correspondant à vos critères spécifiés ou vous pouvez créer un groupe dproximatif d'équipements et ajoutez ou supprimez manuellement des appareils. Le système ExtraHop inclut également des groupes d' équipements dynamiques intégrés par rôle et par activité de protocole que vous pouvez attribuer en tant que source métrique. Cliquez sur le lien d'un rôle ou d'un protocole sur la page Appareils pour afficher les mesures relatives à un groupe d'équipements intégré.

Dossiers

Le Page Fichiers affiche un tableau des fichiers hachés à l'aide de l'algorithme de hachage SHA-256 selon les critères de filtre configurés à partir du Paramètres d'analyse de fichiers. Les métadonnées issues de fichiers hachés constituent un outil précieux pour identifier les programmes malveillants et les risques sur votre réseau.

Utilisateurs

La page Utilisateurs affiche la liste de tous les utilisateurs actifs de votre réseau et des appareils auxquels l'utilisateur s'est connecté. Le nom d'utilisateur est extrait du protocole d'authentification , tel que LDAP ou Active Directory. Rechercher les appareils auxquels un utilisateur spécifique a accédé.

Note: Ces utilisateurs ne sont pas associés à des comptes utilisateurs du système ExtraHop.

Demandes

Les applications sont des conteneurs définis par l'utilisateur qui représentent les systèmes distribués de votre réseau. Créez une application pour afficher toutes les activités métriques associées au trafic de votre site Web : transactions Web, requêtes et réponses DNS et transactions de base de données. Consultez les FAQ sur les candidatures.

Les applications de base qui filtrent les métriques intégrées par activité de protocole peuvent être créé via le système ExtraHop. Les applications complexes qui collectent des métriques personnalisées ou des métriques provenant du trafic non L7 doivent être créé à l'aide d'un déclencheur, qui nécessite du code JavaScript. En savoir plus sur déclencheurs de construction.

Réseaux

Les réseaux sont des sites et des réseaux de flux à partir desquels le système ExtraHop collecte et analyse les données. Les sites incluent un paquet capteurs et flux capteurs. Cliquez sur une entrée pour voir les VLAN associés à un site, ou cliquez sur une entrée pour voir les interfaces associées à un réseau de flux.

Appareils

Le système ExtraHop découvre et classe automatiquement les appareils, également appelés points de terminaison, qui communiquent activement sur votre réseau, tels que les clients, les serveurs, les routeurs, les équilibreurs de charge et les passerelles. Chaque équipement bénéficie du plus haut niveau d'analyse disponible, en fonction de la configuration de votre système.

Le système ExtraHop peut découvrir et suivre les appareils par leur adresse MAC (L2 Discovery) ou par leur adresse IP (L3 Discovery). L'activation de L2 Discovery offre l'avantage de suivre les métriques d'un équipement, même si l' adresse IP est modifiée ou réattribuée via une requête DHCP. Si L3 Discovery est activé, il est important de savoir que les appareils peuvent ne pas avoir de corrélation biunivoque avec les périphériques physiques de votre environnement. Par exemple, si un seul équipement physique possède plusieurs interfaces réseau actives, ce périphérique est identifié comme plusieurs appareils par le système ExtraHop.

Une fois qu'un équipement est découvert, le système ExtraHop commence à collecter des métriques en fonction de niveau d'analyse configuré pour cet équipement. Le niveau d'analyse détermine les types de métriques qui sont générés et les fonctionnalités disponibles pour organiser les données métriques.

Appareils de navigation

Cliquez **Actifs** depuis le menu supérieur pour afficher les options de recherche et les graphiques qui fournissent des informations sur les appareils actifs découverts sur votre réseau au cours de l'intervalle de temps sélectionné :

Assistant de recherche AI (nécessite l'accès au module NDR)

Vous permet de rechercher des appareils avec des questions écrit dans un langage naturel et courant. Assistant de recherche IA doit être activé par l'administrateur ExtraHop.

champ de recherche standard

Fournit un filtre pour ajouter des critères rechercher des appareils spécifiques. Cliquez sur le filtre pour modifier les critères de recherche.

Propositions de recherche

Fournit des suggestions de recherches qui tirent parti des filtres de recherche qui ont été créés.

Appareils actifs

Affiche le nombre total d'appareils découverts par le système ExtraHop au cours de l'intervalle de temps sélectionné. Cliquez sur le numéro pour afficher la liste de tous les appareils découverts. À partir de la liste des appareils actifs, vous pouvez rechercher des appareils spécifiques ou cliquez sur le nom d'un appareil pour afficher les détails de l'équipement sur Page de présentation de l'appareil.

Nouveaux appareils

Affiche le nombre d'appareils découverts au cours des cinq derniers jours. Cliquez sur le numéro pour afficher la liste de tous ces appareils.

Appareils par rôle

Affiche chaque rôle d'équipement et le nombre d'appareils affectés à chaque rôle actif pendant l'intervalle de temps spécifié. Cliquez sur un rôle d'équipement pour afficher une page intégrée de présentation du groupe d'appareils qui inclut les données métriques, les adresses IP homologues et l'activité du protocole pour ce groupe d'appareils. Vous pouvez également ajouter des critères de filtre supplémentaires et enregistrer le groupe en tant que nouveau groupe dynamique d'équipements.

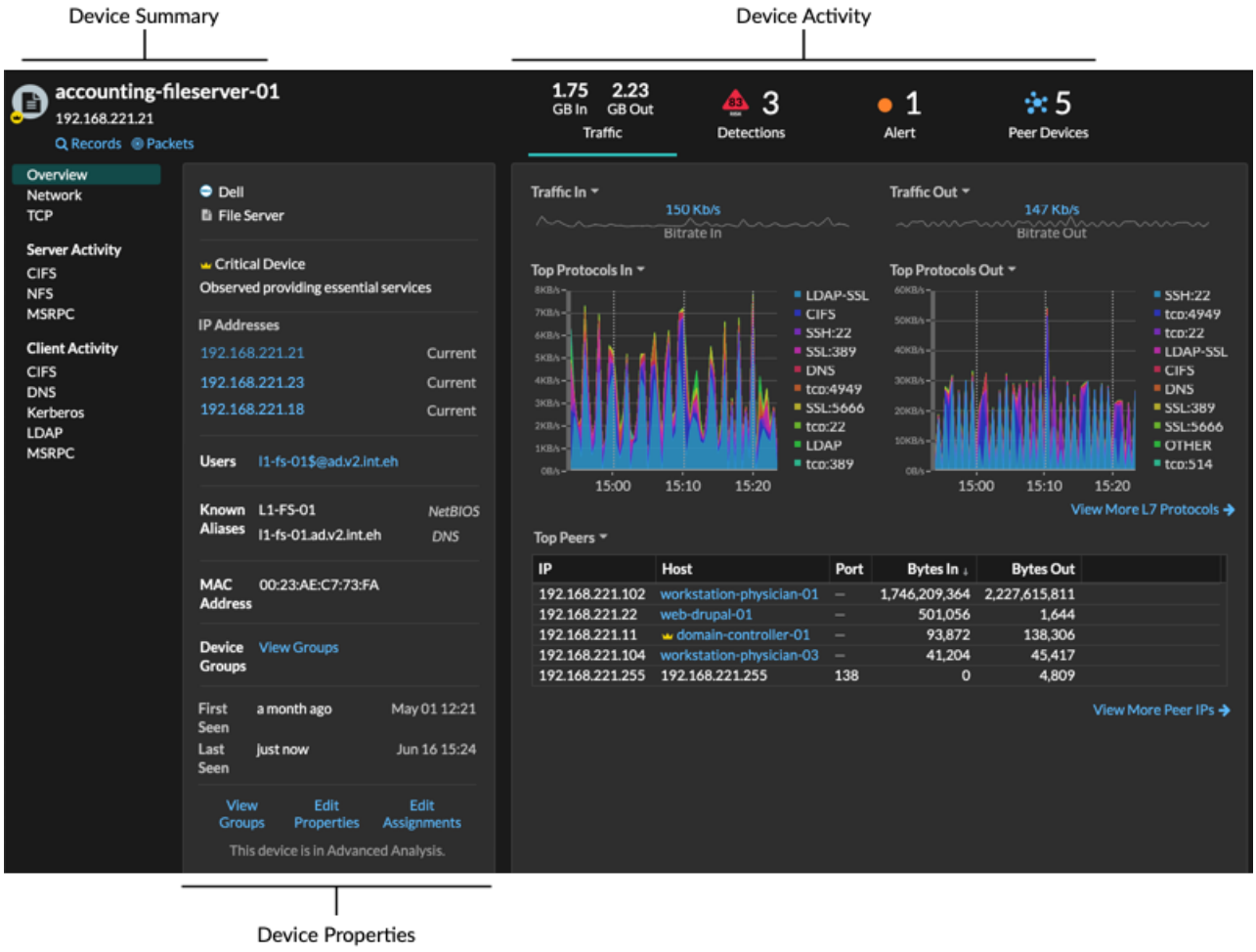
Appareils par activité de protocole

Affiche la liste des activités de protocole détectées sur votre réseau. Cliquez sur le nom d'un protocole ou sur le nombre d'équipements pour afficher une page de présentation des groupes

d'appareils intégrée contenant des graphiques métriques spécifiques concernant cette activité de protocole. Cliquez sur une carte d'activités pour voir toutes les connexions d'appareil à appareil. Vous pouvez également ajouter des critères de filtre supplémentaires et enregistrer le groupe en tant que nouveau groupe dynamique d'équipements.

Page de présentation de l'appareil

En cliquant sur le nom d'un équipement, vous pouvez consulter toutes les informations découvertes à son sujet par le système ExtraHop sur la page Aperçu de l'appareil. La page de présentation de l'appareil est divisée en trois sections : un résumé de niveau supérieur, un panneau des propriétés et un panneau d'activité.



Résumé de l'appareil

Le résumé de l'équipement fournit des informations telles que le nom de l'équipement, l' adresse IP ou l'adresse MAC actuelle et le rôle attribué à l'équipement. Si vous regardez depuis console, le nom du site associé à l'équipement s'affiche également.

- Cliquez **Disques** pour démarrer un requête d'enregistrement qui est filtré par cet équipement.
- Cliquez **Paquets** pour démarrer un requête de paquet qui est filtré par cet équipement.

Propriétés de l'appareil

La section des propriétés de l'équipement fournit les attributs et attributions connus suivants pour l'appareil.

Marque et modèle

La marque (ou le fabricant) de l'équipement et le modèle de l'appareil, le cas échéant.

Le système ExtraHop observe le trafic réseau sur les appareils pour déterminer automatiquement la marque et le modèle, ou vous pouvez attribuer manuellement une nouvelle marque et un nouveau modèle.

Rôle de l'appareil

Le système ExtraHop attribue automatiquement un rôle de l'équipement, comme une passerelle, un serveur de fichiers, une base de données ou un équilibreur de charge, en fonction du type de trafic associé à l'équipement ou à son modèle. Vous pouvez manuellement modifier le rôle d'un équipement.

Appareil de grande valeur

Une icône à valeur élevée apparaît si le système ExtraHop a détecté l'équipement fournissant l'authentification ou les services essentiels ; vous pouvez également spécifier manuellement un équipement comme valeur élevée. Les scores de risque sont augmentés pour les détections sur des appareils à valeur élevée.

Logiciel

Système d'exploitation principal ou logiciel exécuté sur l'équipement.

Conseil : (Intégration à CrowdStrike (sur RevealX 360 uniquement) Vous pouvez cliquer sur des liens depuis des appareils exécutant le logiciel CrowdStrike pour afficher les détails de l'équipement dans CrowdStrike Falçon et initier le confinement des appareils CrowdStrike qui participent à une détection de sécurité.

Adresses IP

Liste des adresses IP observées sur l'équipement à tout moment pendant l'intervalle de temps sélectionné. Si Découverte L2 est activée, la liste peut afficher à la fois les adresses IPv4 et IPv6 qui sont observées simultanément sur l'équipement, ou la liste peut afficher plusieurs adresses IP attribuées via des requêtes DHCP à des moments différents. Un horodateur indique la date à laquelle l'adresse IP a été observée pour la dernière fois sur l'équipement. Cliquez sur une adresse IP pour afficher les autres appareils sur lesquels l'adresse IP a été consultée.

Adresses IP associées

Liste des adresses IP, généralement en dehors du réseau, associées à l'équipement à tout moment pendant l'intervalle de temps sélectionné. Par exemple, un client VPN de votre réseau peut être associé à une adresse IP externe sur l'Internet public. Un horodateur indique la date à laquelle l'adresse IP a été associée pour la dernière fois à l'équipement. Cliquez sur une adresse IP associée pour afficher des détails tels que la localisation géographique et les autres appareils auxquels l'adresse IP a été associée.

Propriétés de l'instance Cloud

Les propriétés d'instance cloud suivantes apparaissent pour l'équipement lorsque vous configurez les propriétés via l'API REST :

- Compte Cloud
- Type d'instance cloud
- Cloud privé virtuel (VPC)
- Sous-réseau
- Nom de l'instance Cloud (apparaît dans la propriété Known Alias)
- Description de l'instance Cloud (les métadonnées de l'instance apparaissent automatiquement pour les appareils dans Flow Analysis)

Voir Ajoutez des propriétés d'instance cloud via l'explorateur d'API ExtraHop pour plus d'informations.

Utilisateurs

Liste des utilisateurs authentifiés connectés à l'équipement. Cliquez sur un nom d'utilisateur pour accéder à la page Utilisateurs et voir à quels autres appareils l'utilisateur est connecté.

Pseudonymes connus

Une liste d'alternatives noms des équipements et le programme ou protocole source.

Note: Plusieurs noms DNS sont pris en charge.

Balises

Le tags attribués à l'équipement. Cliquez sur le nom d'une étiquette pour afficher les autres appareils auxquels la balise est attribuée.

Vu pour la première et la dernière fois

Les horodatages entre la première découverte de l'équipement et la date à laquelle l'activité a été observée pour la dernière fois sur l'appareil. NOUVEAU apparaît si l' équipement a été découvert au cours des cinq derniers jours

Analyse

Le niveau d' analyse que cet équipement reçoit.

Voici quelques moyens d'afficher et de modifier les propriétés de l'équipement :

- Cliquez **Afficher les groupes** pour consulter le groupe d'équipements adhésion à l'équipement.
- Cliquez **Modifier les propriétés** pour afficher ou modifier les propriétés de l'équipement , telles que rôle de l'équipement, des adhésions à des groupes ddevices-équipements, ou étiquettes d'équipement.
- Cliquez **Modifier les devoirs** pour afficher ou modifier lequel alertes et déclencheurs sont attribués à l' équipement.

Activité de l'appareil

La section sur l'activité de l'équipement fournit des informations sur la manière dont l'équipement communique avec d'autres appareils et sur les détections et les alertes associées à l'appareil.

- Cliquez **Trafic** pour afficher les graphiques des protocoles et des données homologues, puis forer vers le bas sur les métriques des graphiques de trafic.

  Note: Les graphiques de trafic ne sont pas disponibles si le niveau d'analyse de l'équipement est en mode découverte. Pour activer les cartes de trafic pour l'appareil, placez l'appareil à Analyse avancée ou Analyse standard.
- Cliquez **Détections** pour afficher la liste des détections, puis cliquez sur le nom d'une détection pour afficher les détails de détection.
- Cliquez **Appareils similaires** pour afficher la liste des appareils présentant un comportement de trafic réseau similaire observé par une analyse d'apprentissage automatique. Des appareils similaires peuvent vous aider à mieux comprendre le comportement normal de l'équipement lors de la recherche de menaces. Cet onglet ne s'affiche que si des appareils similaires sont associés à l'équipement.
- (L'accès au module NPM est requis.) Cliquez **Alertes** pour afficher la liste des alertes, puis cliquez sur le nom d'une alerte pour afficher les détails de l' alerte. Cet onglet ne s'affiche que si des alertes sont associées à l' équipement.
- Cliquez **Appareils homologues** pour consulter une carte dqu`activités, qui est une représentation visuelle de l'activité du protocole L4-L7 entre les appareils de votre réseau. À modifier la carte dqu`activités avec des filtres et des étapes supplémentaires, cliquez sur **Ouvrir la carte des activités**.

Conseil: Vous pouvez ajouter la page Aperçu de l'appareil à un affichage d'activité spécifique à vos favoris en réglant `tab` Paramètre d'URL à l'une des valeurs suivantes :

- `tab=traffic`
- `tab=detections`
- `tab=alerts`

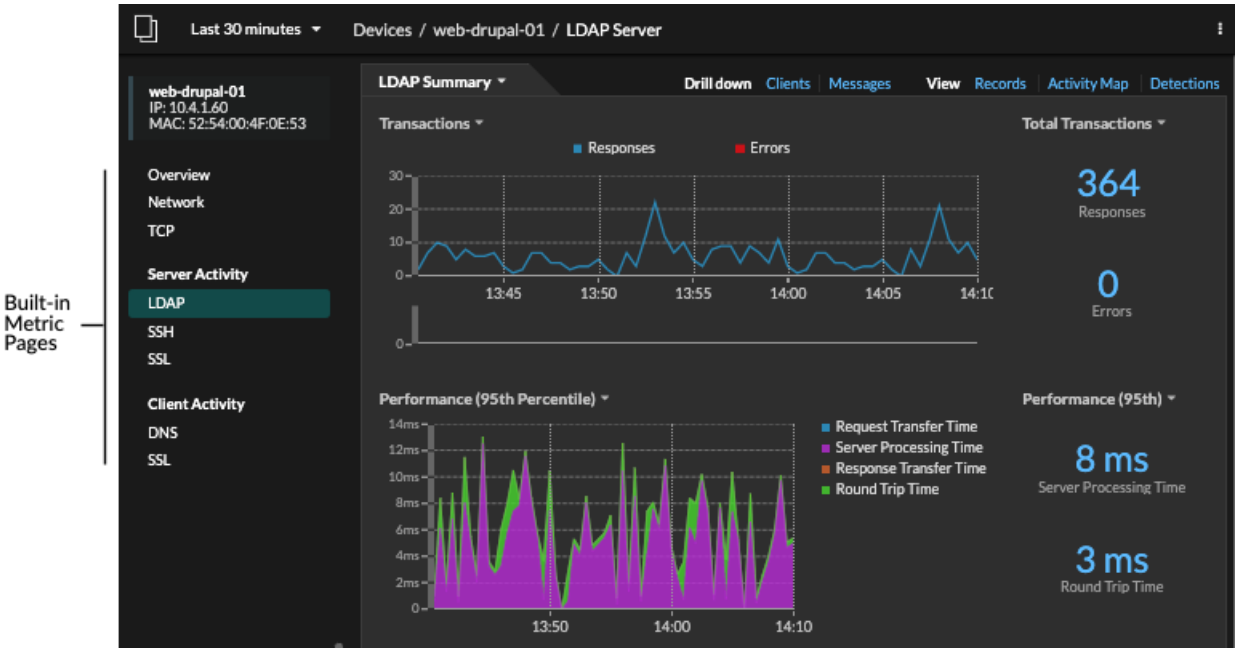
- `tab=peers`

Par exemple, l'URL suivante affiche toujours l'activité de détection pour l'équipement spécifié :

```
https://example-eda/extrahop/#/metrics/devices//0026b94c03810000/
overview/&tab=detections
```

Métriques de l'appareil

Les métriques sont des mesures en temps réel du trafic de votre réseau que le système ExtraHop calcule à partir des données du réseau ou des flux. Les mesures collectées à partir du trafic des équipements peuvent être consultées dans des tableaux et des graphiques intégrés à partir d'une page d'équipement.



Cliquez sur une page métrique intégrée dans le volet de gauche pour afficher le niveau supérieur métriques relatives à l'équipement ou client et serveur métriques par protocole. Cliquez sur un graphique pour Afficher les pages métriques détaillées, qui affichent les valeurs métriques d'une clé spécifique (telle qu'une adresse IP de client ou de serveur).

Outre les pages intégrées au réseau et au protocole TCP, les appareils affichent des pages métriques intégrées pour les services cloud associés si des données sont disponibles. Voir le Référence des métriques du protocole pour plus d'informations sur les données disponibles sur les pages d'équipement intégrées.

Le système ExtraHop fournit des milliers de métriques intégrées. Voici quelques moyens d' obtenir des informations supplémentaires sur vos appareils

- Création d'un graphique pour visualiser des indicateurs spécifiques et enregistrer le graphique dans un tableau de bord.
- Création d'une carte dactivitiés pour afficher les relations entre les équipements homologues sur des protocoles spécifiés.
- Écrire un déclencheur pour créer métriques personnalisées ou créez un application conteneur pour collecter des métriques pour des appareils spécifiques.

Détails de l'adresse IP

Tapez une adresse IP dans le champ de recherche global ou cliquez sur le lien d'une adresse IP depuis une page de présentation des appareils pour afficher les détails d'une adresse IP.

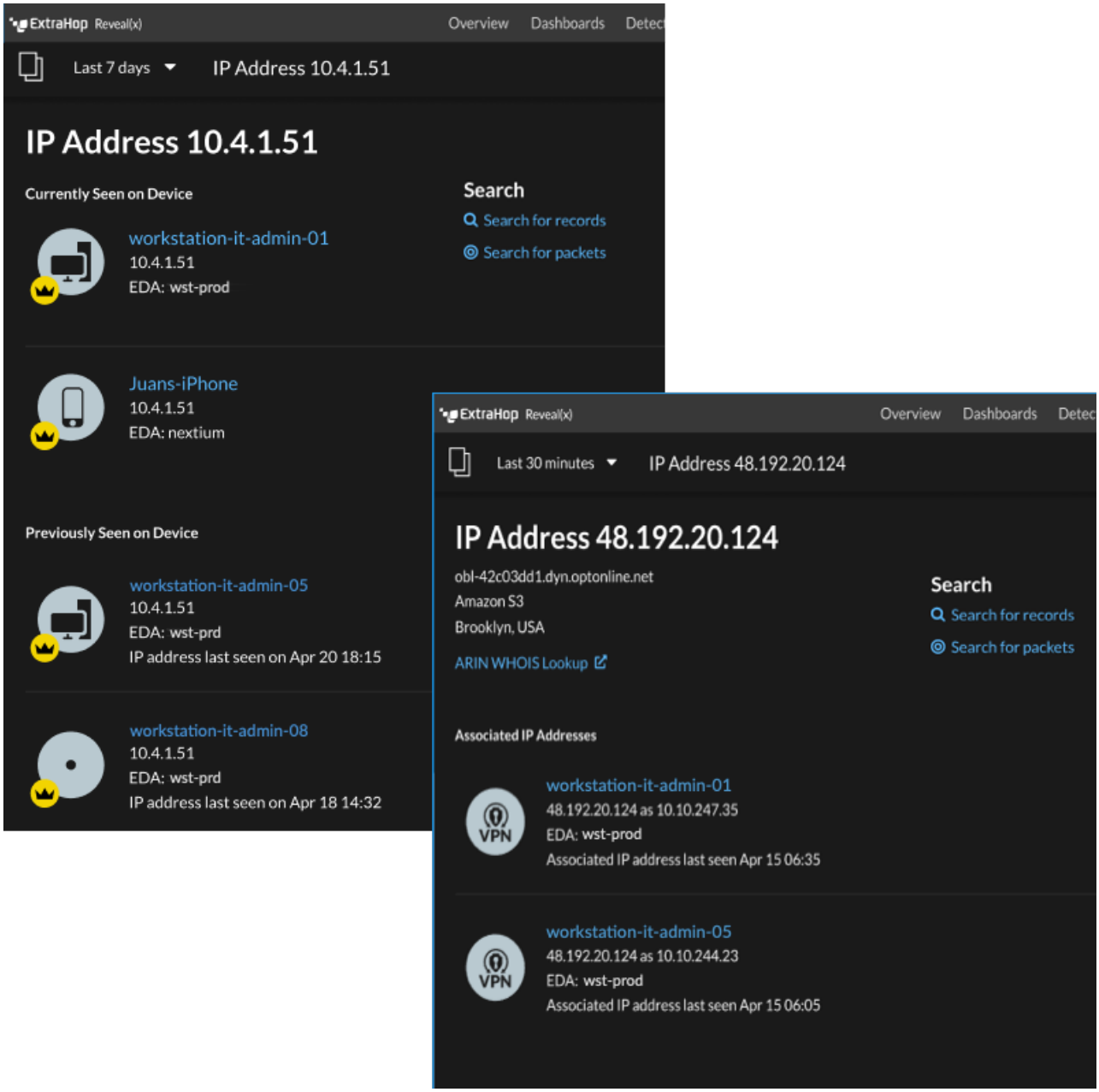
Les informations suivantes s'affichent pour une adresse IP affichée sur un équipement :

- Chaque équipement sur lequel l'adresse IP est actuellement observée, quel que soit l'intervalle de temps sélectionné.
- Chaque équipement sur lequel l'adresse IP a été précédemment observée au cours de l' intervalle de temps sélectionné, y compris l'horodateur depuis la dernière fois que l'adresse IP a été vue sur l'équipement.

Si Découverte L2 est activé, les adresses IPv4 et IPv6 peuvent être observées simultanément sur l'équipement, ou différentes adresses IP peuvent être attribuées à l'équipement par DHCP au fil du temps.

Les informations suivantes s'affichent pour une adresse IP associée à un équipement :

- La géolocalisation de l'adresse IP et des liens vers le site web ARIN Whois.
- Chaque équipement dont l'adresse IP associée a été vue en dehors du réseau à tout moment pendant l'intervalle de temps sélectionné. Par exemple, un client VPN de votre réseau peut être associé à une adresse IP externe sur l'Internet public.
- Tous les services cloud associés à l'adresse IP.
- L'adresse IP de l'équipement telle qu'elle est vue par le système ExtraHop de votre réseau.
- L'horodateur auquel l'adresse IP associée a été vue pour la dernière fois sur l'équipement.



Voici quelques moyens de consulter des informations supplémentaires sur l'adresse IP et l'équipement :

- Passez la souris sur le nom d'un équipement pour afficher ses propriétés.
- Cliquez sur le nom d'un équipement pour afficher la page de présentation de l'appareil.
- Cliquez **Rechercher des enregistrements** pour démarrer un requête d'enregistrement qui est filtré par l'adresse IP .
- Cliquez **Rechercher des paquets** pour démarrer un requête de paquet qui est filtré par cet équipement.

Regroupement d'appareils

Les appareils personnalisés et les groupes d'appareils vous permettent d'agréger les statistiques de vos appareils. Les appareils personnalisés sont des appareils créés par l'utilisateur qui collectent des mesures en fonction de critères spécifiques, tandis que les groupes d'appareils collectent des mesures pour tous les appareils spécifiés d'un groupe. Avec les groupes d'appareils, vous pouvez toujours consulter les statistiques de chaque appareil ou membre du groupe. Les statistiques d'un équipement personnalisé sont collectées et

affichées comme s'il s'agissait d'un seul appareil. Vous ne pouvez pas consulter les mesures individuelles des appareils .

Les groupes d'appareils et les appareils personnalisés peuvent agréger dynamiquement les métriques en fonction des critères que vous avez spécifiés. Nous vous recommandons de sélectionner des critères fiables, tels que l'adresse IP, l'adresse MAC, le VLAN, la balise ou le type de l'équipement. Bien que vous puissiez sélectionner les appareils par leur nom, si le nom DNS n'est pas découvert automatiquement, l'équipement n'est pas ajouté.

	Groupes d'appareils	Appareils personnalisés
Critères	Comprend : • Noms et alias des appareils • adresse IP, adresse MAC, sous-réseau • Port source et port de destination • L'heure de la découverte • Criticité de l'appareil • Rôle de l'appareil • Activité protocolaire • Connexions externes • Fournisseur, modèle, logiciel • Propriétés de l'instance Cloud • VLAN • Étiquettes d'appareils	• adresse IP • Trafic sortant, entrant ou bidirectionnel • adresse IP homologue • Port source • Port de destination • VLAN
Coût de performance	Relativement faible. Étant donné que les groupes d'équipements ne combinent que des métriques déjà calculées, l'effet sur la collecte des métriques est relativement faible. Cependant, le traitement d'un grand nombre de groupes d' appareils comportant un grand nombre d'appareils et des critères complexes prendra plus de temps.	Relativement élevé. Étant donné que les statistiques relatives aux appareils personnalisés sont agrégées en fonction de critères définis par l'utilisateur, un grand nombre d'appareils personnalisés, ou des appareils personnalisés avec des critères extrêmement larges, nécessitent un traitement plus important. Les appareils personnalisés augmentent également le nombre d' objets système pour lesquels les métriques sont validées.
Afficher les statistiques de chaque équipement	Oui	Non
Contrôle d'édition pour les utilisateurs à écriture limitée	Oui Utilisateurs avec privilèges d'écriture limités peut créer et modifier des groupes d'équipements. Cette politique de privilèges globale doit être activée dans les paramètres d'administration.	Non
Meilleures pratiques	Créez pour les appareils locaux sur lesquels vous souhaitez	Créez pour les appareils situés en dehors de votre réseau local

	Groupes d'appareils	Appareils personnalisés
	afficher et comparer les statistiques dans un seul graphique. Les groupes d'appareils peuvent être définis en tant que source métrique.	ou pour les types de trafic que vous souhaitez organiser en tant que source unique. Par exemple, vous souhaiterez peut-être définir toutes les interfaces physiques d'un serveur comme un seul équipement personnalisé afin de mieux visualiser les statistiques de ce serveur dans son ensemble.

Appareils personnalisés

Les appareils personnalisés vous permettent de collecter des statistiques pour les appareils qui se trouvent en dehors de votre réseau local ou lorsque vous disposez d'un groupe d'appareils pour lesquels vous souhaitez regrouper les mesures en tant qu' équipement unique. Ces appareils peuvent même être des interfaces physiques différentes situées sur le même équipement ; l'agrégation des métriques de ces interfaces peut permettre de comprendre plus facilement le niveau de charge de vos ressources physiques dans leur ensemble, plutôt que par interface.

Tu pourrais créer un équipement personnalisé pour suivre des appareils individuels en dehors de votre domaine de diffusion local ou pour collecter des statistiques sur plusieurs adresses IP ou blocs CIDR connus à partir d'un site distant ou d'un service cloud. Tu peux collecter des statistiques de sites distants pour des appareils personnalisés pour découvrir comment les sites distants consomment les services et pour obtenir une visibilité sur le trafic entre les sites distants et un centre de données. Consultez les Référence des métriques du protocole pour obtenir la liste complète des statistiques et des descriptions des sites distants.

Une fois que vous avez créé un équipement personnalisé, toutes les mesures associées aux adresses IP et aux ports sont agrégées dans un seul équipement qui collecte les mesures L2-L7. Un seul équipement personnalisé compte comme un seul appareil dans le cadre de votre capacité sous licence pour Analyse avancée ou analyse standard, qui vous permet de ajouter un équipement personnalisé à la liste de surveillance. Tous les déclencheurs ou alertes sont également attribués à l'équipement personnalisé en tant qu' appareil unique.

Alors que les appareils personnalisés regroupent les métriques en fonction de leurs critères définis, les calculs de métriques ne sont pas traités de la même manière que pour les appareils découverts. Par exemple, un déclencheur peut être attribué à un équipement personnalisé qui valide des enregistrements dans un espace de stockage des enregistrements. Cependant, l'équipement personnalisé n'apparaît ni en tant que client ni en tant que serveur dans aucun enregistrement de transaction. Le système ExtraHop renseigne ces attributs avec l'équipement correspondant à la conversation sur les données filaires.

Les appareils personnalisés peuvent affecter les performances globales du système. Vous devez donc éviter les configurations suivantes :

- Évitez de créer plusieurs appareils personnalisés pour les mêmes adresses IP ou les mêmes ports. Les appareils personnalisés configurés selon des critères qui se chevauchent peuvent dégrader les performances du système.
- Évitez de créer un équipement personnalisé pour un large éventail d'adresses IP ou de ports, car cela pourrait dégrader les performances du système.

Si un grand nombre de périphériques personnalisés affectent les performances de votre système, vous pouvez supprimer ou désactiver un équipement personnalisé. L' ID de découverte unique de l'équipement personnalisé reste toujours dans le système. Voir Créez un équipement personnalisé pour surveiller le trafic des bureaux distants pour vous familiariser avec les appareils personnalisés.

Groupes d'appareils

Un groupe déquipements est un ensemble défini par l'utilisateur qui peut vous aider à suivre les métriques de plusieurs appareils, généralement regroupés selon des attributs partagés tels que l'activité du protocole.

Tu peux créer un groupe dcessaires d'équipements qui vous oblige à ajouter ou à supprimer manuellement un équipement du groupe. Ou, tu peux créer un groupe dcesséquipements dynamique qui inclut des critères qui déterminent quels appareils sont automatiquement inclus dans le groupe. Par exemple, vous pouvez créer un groupe dcessaires dynamique en fonction de l'heure de découverte des équipements qui ajoute des appareils découverts au cours d'un intervalle de temps spécifique.

Par défaut, la page Groupe d'appareils inclut les groupes d'équipements dynamiques suivants que vous pouvez remplacer ou supprimer :

Nouveaux appareils (dernières 24 heures)

Comprend les actifs et les points de terminaison qui ont été vus pour la première fois par le système ExtraHop au cours des dernières 24 heures.

Nouveaux appareils (7 derniers jours)

Comprend les actifs et les points de terminaison qui ont été vus pour la première fois par le système ExtraHop au cours des 7 derniers jours.

Le système ExtraHop inclut également des groupes d'équipements dynamiques intégrés par rôle et par protocole. Vous pouvez attribuer des groupes d'équipements intégrés en tant que source métrique pour des objets tels que des graphiques, des alertes, des déclencheurs et des cartes d'activité. Vous ne pouvez pas remplacer ou supprimer un groupe d'appareils intégré, mais vous pouvez ajouter des critères de filtre et l'enregistrer en tant que nouveau groupe d'appareils.

Sur la page Appareils, cliquez sur le nombre d'équipements correspondant à un rôle ou à un protocole, tel que le contrôleur de domaine ou les clients SMB, pour afficher la page de présentation des groupes d'appareils. En cliquant sur le filtre en haut de la page, vous pouvez ajouter des critères supplémentaires et mettre à jour les données de la page à la demande au lieu de devoir créer un groupe dcessaires d'équipements.

La collecte de métriques auprès de groupes d'équipements n'a aucun impact sur les performances. Nous vous recommandons toutefois de donner la priorité à ces groupes par leur importance pour s'assurer que les bons appareils reçoivent le plus haut niveau d'analyse.

Les groupes d'appareils constituent un bon choix lorsque vous avez des appareils que vous souhaitez appliquer collectivement en tant que source. Par exemple, vous pouvez collecter et afficher des statistiques pour tous vos serveurs Web de production prioritaires dans un tableau de bord.

En créant un groupe d'appareils, vous pouvez gérer tous ces appareils comme une seule source métrique au lieu de les ajouter à vos graphiques en tant que sources individuelles. Notez toutefois que tous les déclencheurs ou alertes attribués sont attribués à chaque membre du groupe (ou à chaque équipement individuel).

Noms et rôles des appareils

Après la découverte d'un équipement, le système ExtraHop suit l'ensemble du trafic associé à l'équipement afin de déterminer le nom et le rôle de l'équipement.

Noms des appareils

Le système ExtraHop découvre les noms des équipements en surveillant passivement les protocoles de dénomination, notamment DNS, DHCP, NETBIOS et Cisco Discovery Protocol (CDP).

Si aucun nom n'est découvert par le biais d'un protocole de dénomination, le nom par défaut est dérivé des attributs de l' équipement, tels que les adresses MAC et IP. Pour certains appareils découverts lors du flux capteurs, le système ExtraHop attribue des noms en fonction du rôle de l'équipement, comme Internet

Gateway ou Amazon DNS Server. Vous pouvez également créer un nom personnalisé ou définir un nom d'instance cloud pour un équipement.

Un équipement peut être identifié par plusieurs noms, qui apparaissent sous la forme d'alias connus sur la page de présentation de l'appareil. Si un équipement porte plusieurs noms, l'ordre de priorité d'affichage est spécifié dans les paramètres d'administration. Vous pouvez effectuer une recherche par n'importe quel nom pour trouver un équipement.

Note: Les noms personnalisés ne sont pas synchronisés entre les systèmes ExtraHop connectés. Par exemple, un nom personnalisé créé sur une sonde n'est pas disponible sur une console connectée.

Si le nom d'un équipement n'inclut pas de nom d'hôte, le système ExtraHop n'a pas encore observé le trafic du protocole de dénomination associé à cet équipement. Le système ExtraHop n' effectue pas de recherches DNS pour les noms d'équipement.

Rôles des appareils

En fonction du type de trafic associé à l'appareil ou à son modèle, le système ExtraHop attribue automatiquement un rôle à l'équipement, tel qu'une passerelle, un serveur de fichiers, une base de données ou un équilibreur de charge. Le rôle Autre est attribué aux appareils qui ne peuvent pas être identifiés.

Un équipement ne peut se voir attribuer qu'un seul rôle à la fois. Vous pouvez manuellement modifier le rôle d'un équipement, ou le système ExtraHop peut réattribuer un rôle différent si le trafic observé et le comportement changent. Par exemple, si un PC a été transformé en serveur Web, vous pouvez modifier le rôle immédiatement, ou le changement peut être observé au fil du temps et le rôle mis à jour par le système.

Le système ExtraHop identifie les rôles suivants :

Icône	Rôle	Descriptif
	Appareil personnalisé	Un équipement créé par l'utilisateur qui collecte des métriques en fonction de critères spécifiques. Le système ExtraHop attribue automatiquement ce rôle lorsque vous créer un équipement personnalisé. Vous ne pouvez pas attribuer manuellement le rôle personnalisé à un équipement.
	Simulateur d'attaque	Un équipement qui exécute un logiciel de simulation de brèches et d'attaques (BAS) pour simuler des attaques sur un réseau.
	Base de données	Un équipement qui héberge principalement une instance de base de données.
	Serveur DHCP	Un équipement qui traite principalement l'activité du serveur DHCP.

Icône	Rôle	Descriptif
	Serveur DNS	Un équipement qui traite principalement l'activité du serveur DNS.
	Contrôleur de domaine	Un équipement qui fait office de contrôleur de domaine pour l'activité des serveurs Kerberos, SMB et MSRPC.
	Serveur de fichiers	Un équipement qui répond aux demandes de lecture et d'écriture de fichiers via les protocoles NFS et SMB.
	Pare-feu	Un équipement qui surveille le trafic réseau entrant et sortant et bloque le trafic conformément aux règles de sécurité. Le système ExtraHop n'attribue pas automatiquement ce rôle aux appareils.
	Passerelle	Un équipement qui fait office de routeur ou de passerelle. Le système ExtraHop recherche les appareils associés à un grand nombre d'adresses IP uniques (au-delà d' un certain seuil) lors de l'identification des passerelles. Les noms des équipements de passerelle incluent le nom du routeur, tel que Cisco B1B500. Contrairement à d'autres Appareils parents L2, vous pouvez ajouter un équipement de passerelle à la liste de surveillance pour une analyse avancée.
	Caméra IP	Un équipement qui envoie des données d'image et de vidéo via le réseau. Le système ExtraHop attribue ce rôle en fonction du modèle d'équipement.
	Équilibreur de charge	Un équipement qui agit comme un proxy inverse pour distribuer le trafic sur plusieurs serveurs.

Icône	Rôle	Descriptif
	Dispositif médical	Un équipement conçu pour les besoins de santé et les environnements médicaux. Le système ExtraHop peut attribuer ce rôle si un équipement est d'une marque et d'un modèle médicaux connus ou s'il traite du trafic DICOM.
	Appareil mobile	Un équipement sur lequel un système d'exploitation mobile est installé, tel qu'iOS ou Android.
	Passerelle NAT	Un équipement qui fait office de passerelle de traduction d'adresses réseau (NAT). Le système ExtraHop peut attribuer ce rôle si un équipement est associé à au moins quatre familles d'empreintes digitales de système d'exploitation ou à au moins quatre marques et modèles de matériel ou de fournisseurs. Une fois ce rôle attribué à un appareil, les propriétés du logiciel, de la marque et du modèle du matériel et des utilisateurs authentifiés n'apparaissent plus pour l'appareil.
	PC	Un équipement tel qu'un ordinateur portable, un ordinateur de bureau, une machine virtuelle Windows ou un appareil macOS qui traite le trafic des clients DNS, HTTP et TLS.
	Imprimante	Un équipement qui permet aux utilisateurs d'imprimer du texte et des graphiques à partir d'autres appareils connectés. Le système ExtraHop attribue ce rôle en fonction du modèle d' équipement ou du trafic observé sur mDNS (DNS multicast).
	Téléphone VoIP	Un équipement qui gère les appels téléphoniques de voix sur IP (VoIP).

Icône	Rôle	Descriptif
	Client VPN	Un équipement interne qui communique avec une adresse IP distante. Si La découverte des clients VPN est activée, le système ExtraHop attribue automatiquement ce rôle aux appareils internes communiquant avec des adresses IP distantes via une passerelle VPN. Vous ne pouvez pas attribuer manuellement le rôle de client VPN à un équipement.
	Passerelle VPN	Un équipement qui connecte deux ou plusieurs appareils ou réseaux VPN ensemble pour relier des connexions distantes. Le système ExtraHop attribue ce rôle aux appareils dotés d'un grand nombre de pairs VPN externes si la classification automatique de ce rôle est activée dans le fichier de configuration en cours d'exécution.
	Scanner de vulnérabilité	Un équipement qui exécute des programmes d'analyse de vulnérabilités.
	Serveur proxy Web	Un équipement qui traite les requêtes HTTP entre un équipement et un autre serveur.
	Serveur Web	Un équipement qui héberge principalement des ressources Web et répond aux requêtes HTTP.
	Point d'accès Wi-Fi	Un équipement qui crée un réseau local sans fil et projette un signal de réseau sans fil vers une zone désignée. Le système ExtraHop attribue ce rôle en fonction du modèle d'équipement.

Trouvez un équipement

Le système ExtraHop détecte automatiquement les appareils tels que les clients, les serveurs, les routeurs, les équilibreurs de charge et les passerelles qui communiquent activement avec d'autres appareils via le fil. Vous pouvez rechercher un équipement spécifique sur le système, puis consulter les mesures relatives au trafic et au protocole sur une page de protocole.

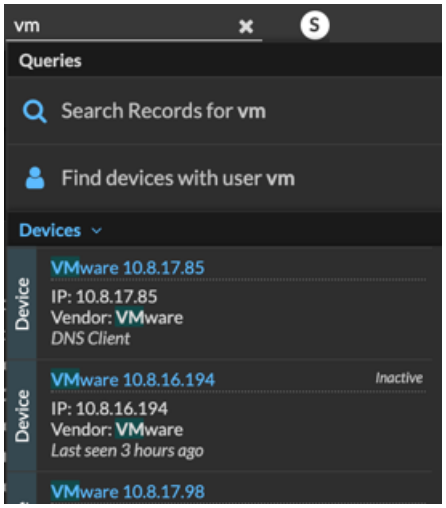
Il existe plusieurs manières de rechercher un équipement :

- Trouvez des appareils à partir d'une recherche globale
- Trouvez des appareils par détails
- Trouvez des appareils avec AI Search Assistant
- Trouvez des appareils grâce aux recherches suggérées
- Trouvez des appareils par activité de détection
- Trouvez des appareils par activité de protocole
- Trouvez les appareils auxquels un utilisateur spécifique a accédé
- Trouvez des appareils homologues

Trouvez des appareils à partir d'une recherche globale

Vous pouvez rechercher des appareils dans le champ de recherche global en haut de la page. La recherche globale compare un terme de recherche à plusieurs propriétés de l'équipement, telles que le nom d'hôte, l' adresse IP, l'alias connu, le fournisseur, le tag, la description et le groupe d'équipements. Par exemple, si vous recherchez le terme `vm`, les résultats de la recherche peuvent afficher des appareils qui incluent `vm` dans le nom de l'appareil, le fournisseur de l'appareil ou l'étiquette de l'appareil.

1. Tapez un terme de recherche dans le champ de recherche global en haut de la page.
2. Cliquez **N'importe quel type** puis sélectionnez **Appareils**.
   Les résultats de la recherche sont affichés dans une liste en dessous du champ de recherche. Cliquez **Plus de résultats** pour faire défiler la liste.



Les appareils correspondants qui n'ont aucune activité pendant l'intervalle de temps spécifié ont une étiquette Inactive.

Conseil Les appareils inactifs pendant plus de 90 jours sont exclus des résultats de recherche globaux. Cependant, vous pouvez immédiatement exclure tous les appareils inactifs depuis moins de 90 jours via les paramètres d'administration.

3. Cliquez sur le nom d'un équipement pour ouvrir le Page de présentation de l'appareil et consultez les propriétés et les statistiques de l'équipement.

Trouvez des appareils par détails

Vous pouvez rechercher des appareils en fonction des informations observées sur le réseau, telles que l'adresse IP, l'adresse MAC, le nom d'hôte ou l'activité du protocole. Vous pouvez également rechercher des appareils à l'aide d'informations personnalisées, telles que les étiquettes des appareils.

Le filtre de recherche à trois champs vous permet d'effectuer une recherche par plusieurs catégories à la fois. Par exemple, vous pouvez ajouter des filtres pour le nom de l'équipement, l'adresse IP et le rôle afin d'afficher les résultats pour les appareils qui répondent à tous les critères spécifiés.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs** puis cliquez sur **Appareils actifs** graphique.
3. Optionnel : Si cela s'affiche, cliquez sur **Recherche standard**.
4. Dans le filtre à trois champs, cliquez sur **Nom** et sélectionnez l'une des catégories suivantes :

Option	Description
Nom	Filtre les appareils en fonction du nom de l'équipement découvert. Par exemple, le nom d'un équipement découvert peut inclure l'adresse IP ou le nom d'hôte.
Adresse MAC	Filtre les appareils en fonction de leur adresse MAC.
Adresse IP	Filtre les appareils par adresse IP au format de bloc IPv4, IPv6 ou CIDR.
Site	Filtre les appareils associés à un site connecté. Console uniquement.
L'heure de la découverte	Filtre les appareils découverts automatiquement par le système ExtraHop dans l'intervalle de temps spécifié. Pour plus d'informations, voir Création d'un groupe dproximatif d'équipements en fonction de l'heure de découverte.
Niveau d'analyse	Filtre les appareils par niveau d'analyse, ce qui détermine quelles données et mesures sont collectées pour un équipement. Vous ne pouvez pas créer de groupe déquipements dynamique pour les appareils filtrés par niveau d'analyse.
modèle	Filtre les appareils par marque, famille ou nom de modèle. La marque représente le fabricant de l'équipement. Une famille représente un groupe tel qu'une gamme de produits. Les conseils suivants peuvent vous aider à trouver le modèle d'équipement que vous souhaitez : • Vous pouvez faire votre choix parmi la liste des marques présentes sur votre système ExtraHop, puis cliquer sur le filtre pour affiner les résultats. • Vous pouvez afficher des info-bulles à côté des marques et des familles pour voir combien d'appareils et de modèles correspondants ont été trouvés.

Option	Description
	• Vous pouvez sélectionner une marque ou une famille pour trouver tous les appareils de ce groupe, quel que soit le modèle.
Activité	Filtre les appareils en fonction de l'activité de protocole associée à l'équipement. Par exemple, la sélection d'un serveur HTTP renvoie les appareils dont les métriques sont associées au serveur HTTP, ainsi que tout autre équipement dont le rôle d' équipement est défini sur Serveur HTTP. Filtre également les appareils qui ont accepté ou initié une connexion externe, ce qui peut vous aider à déterminer si les appareils sont impliqués dans une activité suspecte.
Compte Cloud	Filtre les appareils en fonction du compte de service cloud associé à l'appareil.
ID d'instance cloud	Filtre les appareils en fonction de l'ID d'instance cloud associé à l'équipement.
Type d'instance cloud	Filtre les appareils en fonction du type d'instance cloud associé à l'équipement.
Hachage de fichiers SHA-256	Filtre les appareils sur lesquels des fichiers hachés par l'algorithme de hachage SHA-256 ont été observés. Vous pouvez consulter un tableau des fichiers hachés sur le Page Fichiers.
Valeur élevée	Filtre les appareils considérés comme à valeur élevée parce qu'ils fournissent des services d'authentification, prennent en charge les services essentiels de votre réseau ou sont spécifiés par l'utilisateur comme étant à valeur élevée.
Actuellement actif	Filtre les appareils en fonction de l'activité observée sur un équipement au cours des 30 dernières minutes.
Type de localité du réseau	Filtre les appareils en fonction de toutes les localités du réseau interne ou externe.
Nom de la localité du réseau	Filtre les appareils par nom de localité du réseau.
Rôle	Filtre les appareils en fonction du rôle d'équipement attribué, tel que la passerelle, le pare-feu, l'équilibreur de charge et le serveur DNS.
Logiciel	Filtre les appareils en fonction du logiciel du système d'exploitation détecté sur l'équipement.
Type de logiciel	Filtre les appareils en fonction du type de logiciel observé sur l'équipement, tel qu'un simulateur d'attaque, un accès à distance ou un serveur de bases de données.
Sous-réseau	Filtre les appareils en fonction du sous-réseau associé à l'équipement.

Option	Description
Balise	Filtre les appareils en fonction de balises d'équipement définies par l'utilisateur.
Fournisseur	Filtre les appareils en fonction du nom du fournisseur de l'équipement, tel que déterminé par la recherche de l'identifiant unique organisationnel (OUI).
Cloud privé virtuel	Filtre les appareils en fonction du VPC associé à l'équipement.
VLAN	Filtre les appareils en fonction de la balise VLAN de l'équipement. Les informations VLAN sont extraites des balises VLAN, si le processus de mise en miroir du trafic les conserve sur le port miroir. Disponible uniquement si le `devices_accross_vlans` le réglage est réglé sur `False` dans le fichier de configuration en cours d'exécution.
Nom CDP	Filtre les appareils en fonction du nom CDP attribué à l'équipement.
Nom de l'instance Cloud	Filtre les appareils en fonction du nom d'instance cloud attribué à l'équipement.
Nom personnalisé	Filtre les appareils en fonction du nom personnalisé attribué à l'équipement.
Nom DHCP	Filtre les appareils en fonction du nom DHCP attribué à l'équipement.
Nom DNS	Filtre les appareils selon n'importe quel nom DNS attribué à l'équipement.
Nom NetBIOS	Filtre les appareils en fonction du nom NetBIOS attribué à l'équipement.
Activité de détection	Filtre les appareils ayant une activité de détection où l'équipement était un participant. Active des critères supplémentaires tels que la catégorie, l'indice de risque et la technique MITRE. **Note:** Vous ne pouvez pas créer de groupe dveloppement contenant cette option de critère.

5. Sélectionnez l'un des opérateurs suivants ; les opérateurs disponibles sont déterminés par la catégorie sélectionnée :

Option	Description
=	Filtre les appareils qui correspondent exactement au champ de recherche de la catégorie sélectionnée.
≠	Filtre les appareils qui ne correspondent pas exactement au champ de recherche.

Option	Description
≈	Filtre les appareils qui incluent la valeur du champ de recherche pour la catégorie sélectionnée.
≈/	Filtre les appareils qui excluent la valeur du champ de recherche pour la catégorie sélectionnée.
commence par	Filtre les appareils dont le nom commence par la valeur du champ de recherche de la catégorie sélectionnée.
existe	Filtre les appareils qui ont une valeur pour la catégorie sélectionnée.
n'existe pas	Filtre les appareils qui n'ont pas de valeur pour la catégorie sélectionnée.
correspondre	Filtre les appareils qui incluent la valeur du champ de recherche pour la catégorie sélectionnée.
et	Filtre les appareils qui correspondent aux conditions spécifiées dans au moins deux champs de recherche.
ou	Filtre les appareils qui correspondent à au moins une condition spécifiée dans au moins deux champs de recherche.
pas	Filtre les appareils qui ne correspondent pas aux conditions spécifiées dans un champ de recherche.

6. Dans le champ de recherche, saisissez la chaîne à rechercher ou sélectionnez une valeur dans la liste déroulante. Le type d'entrée est basé sur la catégorie sélectionnée.

   Par exemple, si vous souhaitez rechercher des appareils en fonction de leur nom, saisissez la chaîne à laquelle vous souhaitez faire correspondre dans le champ de recherche. Si vous souhaitez rechercher des appareils en fonction du rôle, sélectionnez-le dans la liste déroulante des rôles.

   Conseil Selon la catégorie sélectionnée, vous pouvez cliquer sur l'icône Regex dans le champ de texte pour activer la correspondance par expression régulière.

7. Cliquez **Ajouter un filtre**.
   La liste des appareils est filtrée selon les critères spécifiés.

Prochaines étapes

- Cliquez sur le nom d'un équipement pour afficher les propriétés et les statistiques de l'appareil sur le Page de présentation de l'appareil.
- Cliquez **Création d'un groupe dynamique** depuis le coin supérieur droit jusqu'à créer un groupe ddevices-équipements dynamique en fonction des critères de filtrage.
- Cliquez sur le menu de commandes ⋮ puis sélectionnez PDF ou CSV pour exporter la liste des équipements dans un fichier.

Trouvez des appareils avec AI Search Assistant

AI Search Assistant vous permet de rechercher des appareils contenant des questions rédigées dans un langage naturel courant afin de créer rapidement des requêtes complexes par rapport à la création d'une requête de recherche standard avec les mêmes critères.

Par exemple, si vous tapez « Quels appareils ont un trafic HTTP avec TLS v1.0 ? » , la requête suivante de l'assistant de recherche AI s'affiche :

```
(Detection Activity where  Device Role = As Participant and  Type =
 Deprecated SSL/TLS Versions )
```

Voici quelques éléments à prendre en compte lors de la recherche d'appareils avec AI Search Assistant :

- Les invites sont mappées de la même manière critères de filtrage des équipements que vous spécifiez lors de la création d'une recherche standard. Le système ExtraHop peut ne pas être en mesure de traiter une requête contenant des demandes d'informations sur l'équipement ne répondant pas aux critères.
- Les instructions peuvent inclure des plages temporelles absolues et relatives, telles que « Lequel de mes appareils a participé à des transferts de données bloqués cette semaine ? ». L' année en cours est appliquée si une année n'est pas incluse dans la date.
- Les instructions doivent être aussi claires et concises que possible et nous vous recommandons d'essayer d' écrire quelques variantes pour optimiser vos résultats.
- Le système ExtraHop peut conserver les instructions des utilisateurs à des fins d'amélioration du produit ; nous vous recommandons de ne pas inclure de données exclusives ou confidentielles dans vos invites.
- Vous pouvez modifier les critères du filtre de requête pour affiner les résultats de recherche.

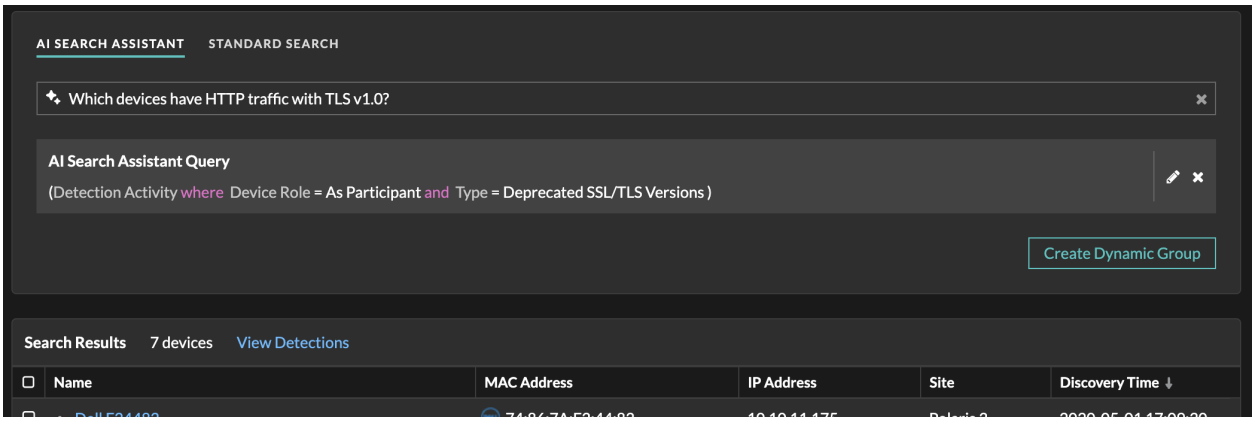
Avant de commencer

- Votre système ExtraHop doit être connecté à ExtraHop Cloud Services.
- L'assistant de recherche AI doit être activé par votre administrateur ExtraHop.

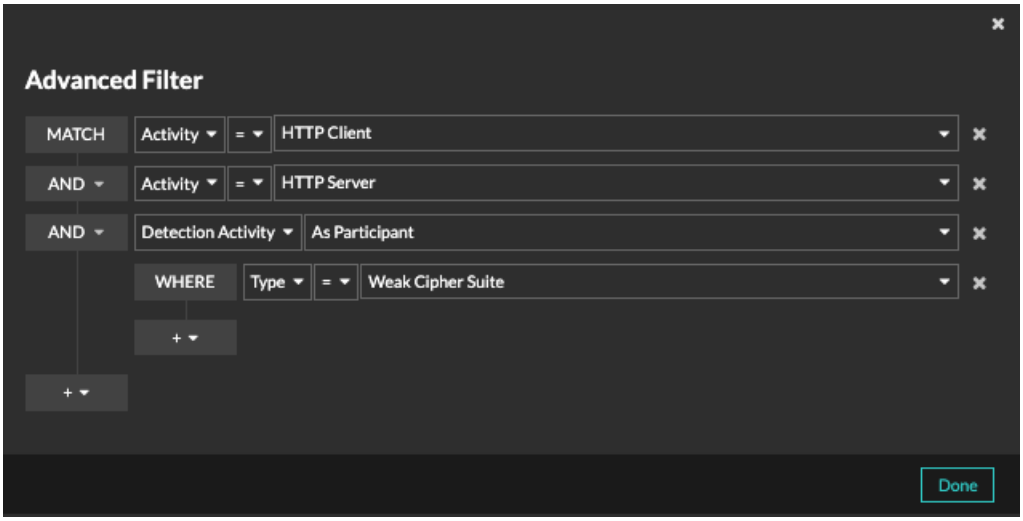
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs**.
3. Écrivez une invite dans le champ AI Search Assistant et appuyez sur ENTER.

   Conseil : Cliquez sur le champ d'invite de recherche pour sélectionner une requête récente ou une recherche suggérée.

   La sortie de requête de l'assistant de recherche AI et la liste des résultats s'affichent.



4. Optionnel : Dans la section Requête de l'assistant de recherche AI, cliquez sur l'icône de modification pour ouvrir la fenêtre Filtre avancé et affiner les critères de votre filtre de requête.



a) Cliquez sur l'icône Ajouter un filtre + et sélectionnez **Ajouter un filtre** ou **Ajouter un groupe de filtres** pour spécifier d'autres critères au niveau supérieur ou secondaire du filtre.

   Un nouveau groupe de filtres ajoute des critères au résultat du filtre d'origine. Par exemple, si vous recherchez des clients et des serveurs HTTP qui ont participé à la détection d'une suite de chiffrement faible, vous pouvez ajouter un groupe de filtres pour exclure les détections dont l'indice de risque est inférieur à 30.

b) Cliquez **Terminé**.

Prochaines étapes

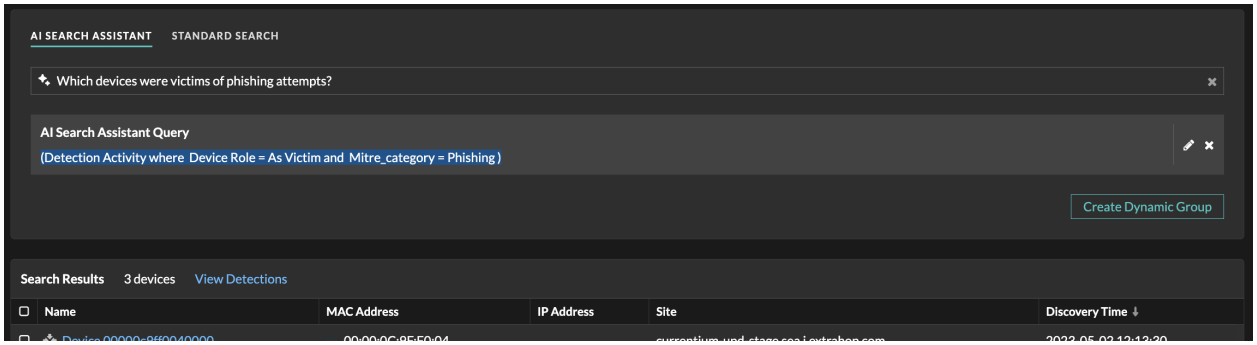
- Cliquez **Afficher les détections** pour accéder à la page Détections ; le filtre d'équipement est appliqué au résumé des détections. Cliquez **Filtre d'appareils avancé** pour afficher et modifier les critères de filtre.
- Cliquez sur le nom d'un équipement pour afficher les propriétés et les statistiques de l'appareil sur le Page de présentation de l'appareil.
- Cliquez sur le menu de commandes ⋮ puis sélectionnez PDF ou CSV pour exporter la liste des équipements dans un fichier.

Trouvez des appareils grâce aux recherches suggérées

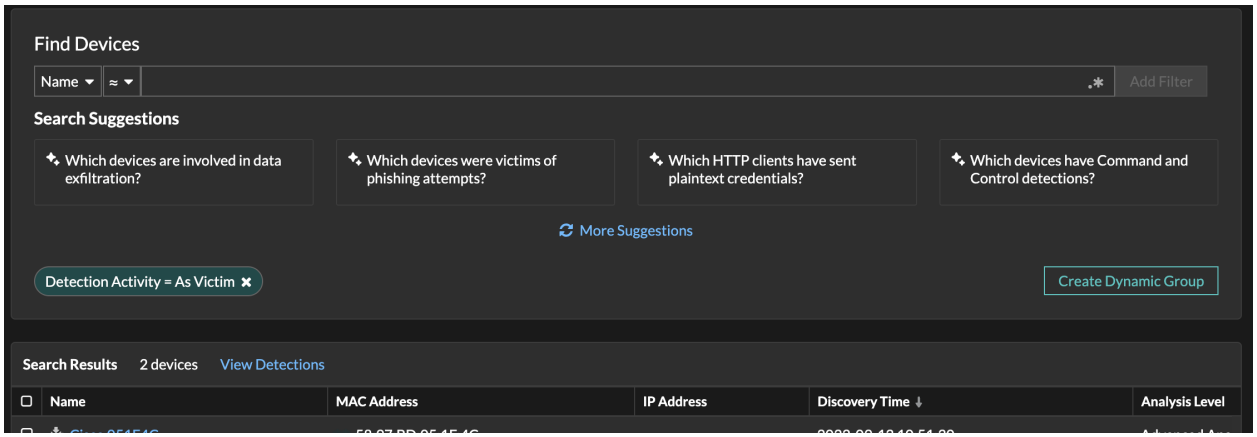
Le système ExtraHop propose plusieurs suggestions de recherches avec des filtres prédéfinis pour vous aider à effectuer plus efficacement les recherches courantes sur les équipements. Après avoir sélectionné une recherche suggérée, vous pouvez modifier les critères de filtre pour affiner vos résultats.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs**.
3. Cliquez sur une invite de recherche suggérée.

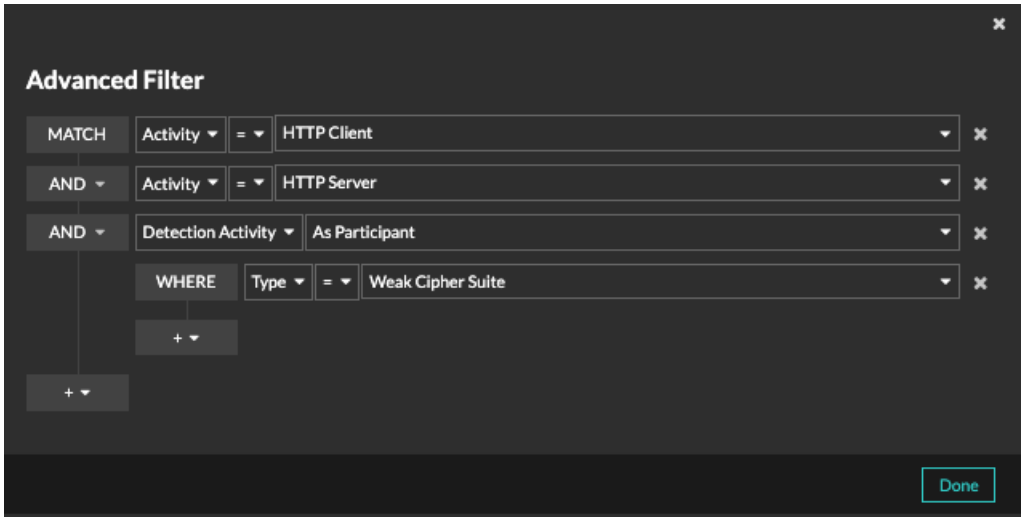
   Si AI Search Assistant est activé, les critères de filtre sont affichés dans le champ Requête de l'assistant AI Search.



Dans le cas contraire, la page affiche le filtre standard.



4. Optionnel : Dans le champ de requête de l'assistant de recherche AI, cliquez sur l'icône de modification ou cliquez sur le filtre standard pour ouvrir la fenêtre Filtre avancé et affiner votre requête.



a) Cliquez sur l'icône Ajouter un filtre + et sélectionnez **Ajouter un filtre** ou **Ajouter un groupe de filtres** pour spécifier d'autres critères au niveau supérieur ou secondaire du filtre.

   Un nouveau groupe de filtres ajoute des critères au résultat du filtre d'origine. Par exemple, si vous recherchez des clients et des serveurs HTTP qui ont participé à la détection d'une suite de chiffrement faible, vous pouvez ajouter un groupe de filtres pour exclure les détections dont l'indice de risque est inférieur à 30.

b) Cliquez **Terminé**.

Prochaines étapes

- Cliquez **Afficher les détections** pour accéder à la page Détections ; le filtre d'équipement est appliqué au résumé des détections. Cliquez **Filtre d'appareils avancé** pour afficher et modifier les critères de filtre.
- Cliquez **Créer un groupe dynamique** depuis le coin supérieur droit jusqu'à créer un groupe dveloppement d'équipements dynamique en fonction des critères de filtrage.
- Cliquez sur le nom d'un équipement pour afficher les propriétés et les statistiques de l'appareil sur le Page de présentation de l'appareil.
- Cliquez sur le menu de commandes ⋮ puis sélectionnez PDF ou CSV pour exporter la liste des équipements dans un fichier.

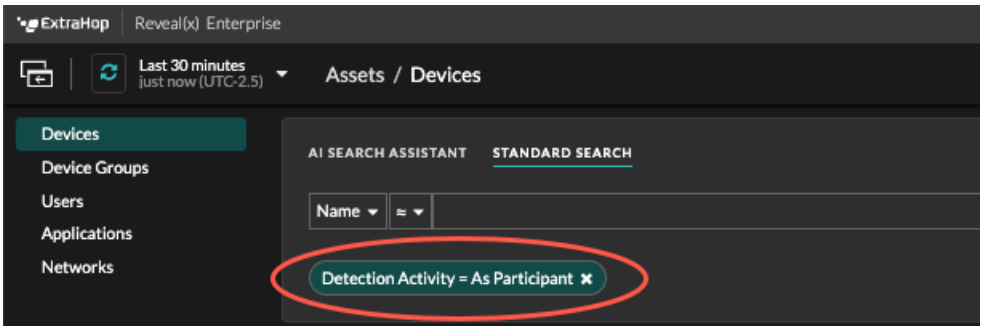
Trouvez des appareils par activité de détection

Vous pouvez rechercher des appareils en fonction des détections associées en ajoutant l'option Critères d' activité de détection à votre filtre de recherche, puis en affinant votre recherche à l'aide de critères tels que les catégories de détection, les scores de risque et les techniques MITRE.

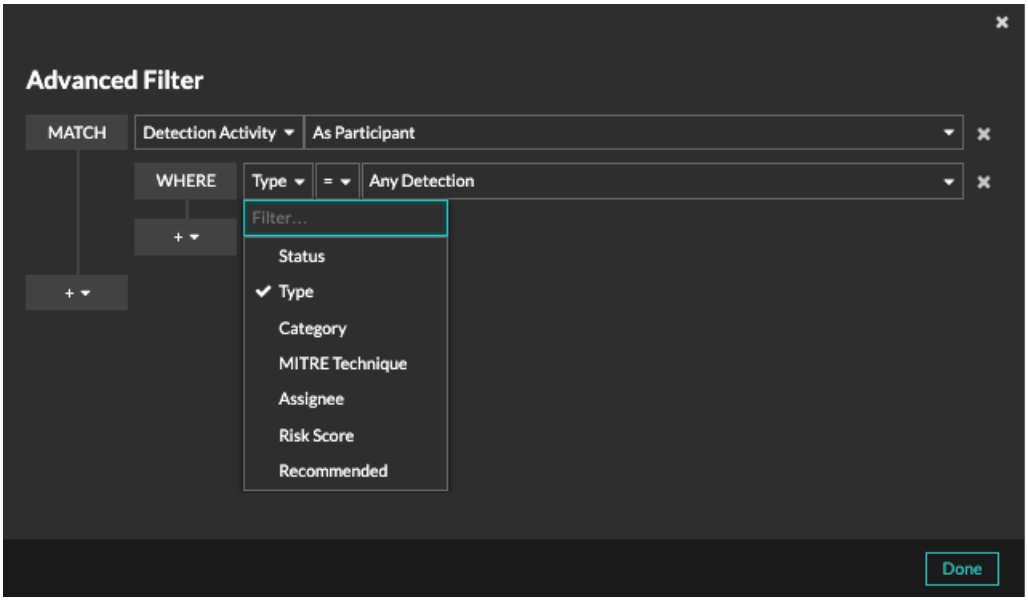
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs** puis cliquez sur **Appareils actifs** graphique.
3. Optionnel : Cliquez **Recherche standard** si l'onglet est affiché.
4. Dans le filtre à trois champs, cliquez sur **Nom** et sélectionnez **Activité de détection**.
5. Cliquez **Sélectionnez un article...** et sélectionnez l'une des options suivantes :

Option	Description
En tant que participant	Filtre les appareils qui ont participé à une détection.
En tant que délinquant	Filtre les appareils qui n'ont participé à une détection qu'en tant que délinquant.
En tant que victime	Filtre les appareils qui n'ont participé à une détection qu'en tant que victime.

6. Cliquez **Ajouter un filtre**.
7. Optionnel : Pour spécifier des critères d'activité de détection supplémentaires, cliquez sur le filtre que vous venez d' ajouter.



Le filtre avancé s'ouvre pour afficher les critères MATCH que vous avez ajoutés. Un opérateur WHERE est automatiquement ajouté au niveau secondaire du filtre pour les critères d'activité de détection.



8. Cliquez **Tapez** et sélectionnez l'un des critères d' activité de détection suivants :

Option	Description
État	Filtre les détections par statut, par exemple si la détection a été confirmée ou fermée
Tapez	Filtre les détections par type, comme l'exfiltration de données ou les certificats de serveur TLS expirés.
Catégorie	Filtre les détections par catégorie, telle que les attaques, les opérations, le renforcement et les intrusions.
Technique MITRE	Filtre les détections par ID de technique MITRE. Le framework MITRE est une base de connaissances largement reconnue sur les attaques
Cessionnaire	Filtre les détections par l'utilisateur désigné.
Score de risque	Filtre les détections par indice de risque.
Recommandé	Filtre les détections recommandées pour le triage, également connu sous le nom de triage intelligent. (module NDR uniquement)

Voir Filtrage des détections pour plus d'informations sur les critères d'activité de détection.

9. Optionnel : Cliquez sur l'icône Ajouter un filtre + et sélectionnez **Ajouter un filtre** ou **Ajouter un groupe de filtres** pour spécifier d'autres critères au niveau supérieur ou secondaire du filtre.

   Un nouveau groupe de filtres ajoute des critères au résultat du filtre d'origine. Par exemple, si vous recherchez des appareils qui ont agi en tant que contrevenant dans des détections de catégories d'exfiltration, vous pouvez ajouter un groupe de filtres pour exclure les détections dont le statut est fermé de ces résultats.

10. Cliquez **Enregistrer**.

Prochaines étapes

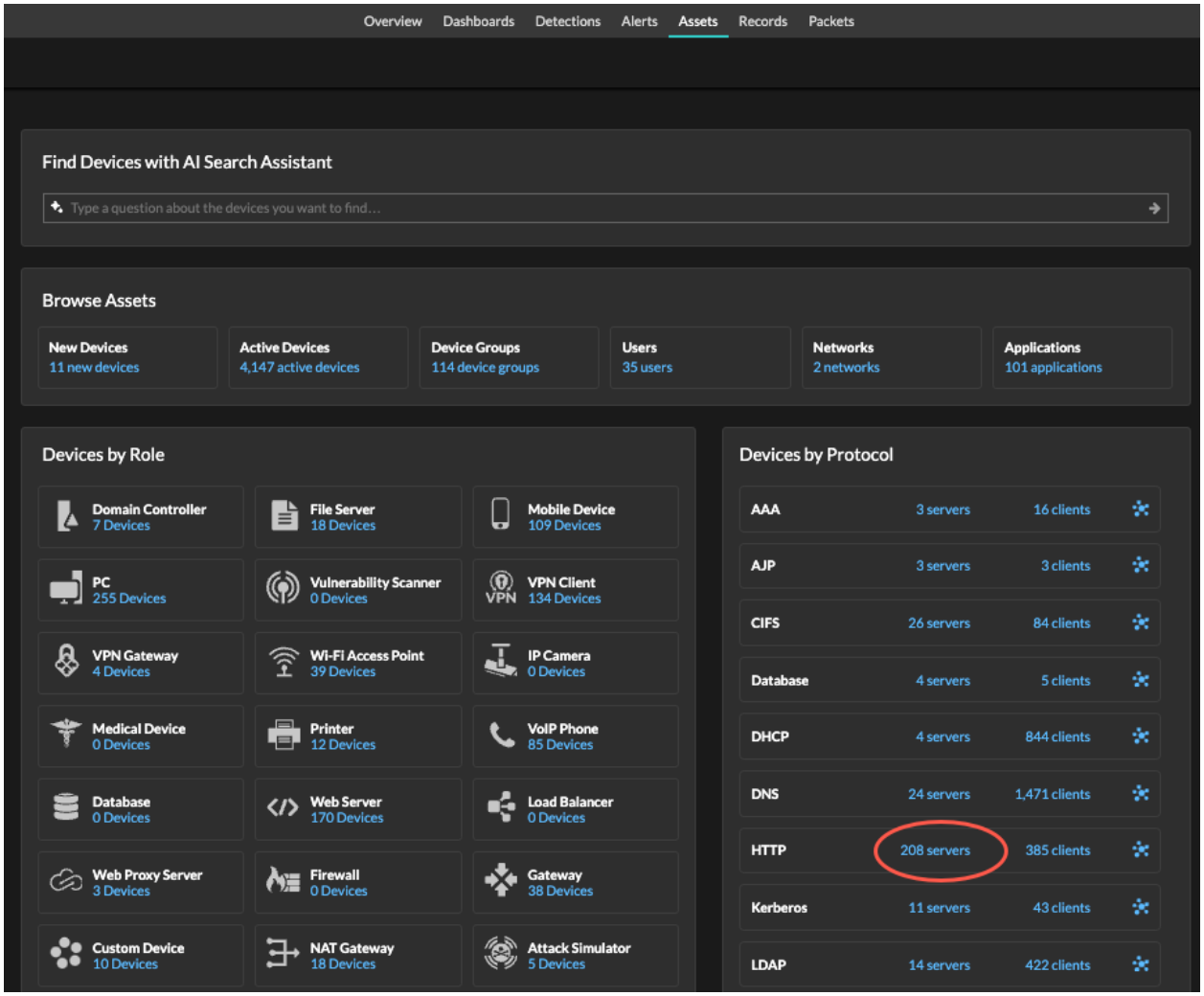
- Cliquez sur le nom d'un équipement pour afficher les propriétés et les statistiques de l'appareil sur le Page de présentation de l'appareil.
- Cliquez sur le menu de commandes ⋮ puis sélectionnez PDF ou CSV pour exporter la liste des équipements dans un fichier.

Trouvez des appareils par activité de protocole

La page Appareils affiche tous les protocoles qui communiquent activement sur le système ExtraHop pendant l'intervalle de temps sélectionné. Vous pouvez rapidement localiser un équipement associé à un protocole ou découvrir un équipement hors service qui communique toujours activement via un protocole.

Dans l'exemple suivant, nous vous montrons comment rechercher un serveur Web dans le groupe de serveurs HTTP.

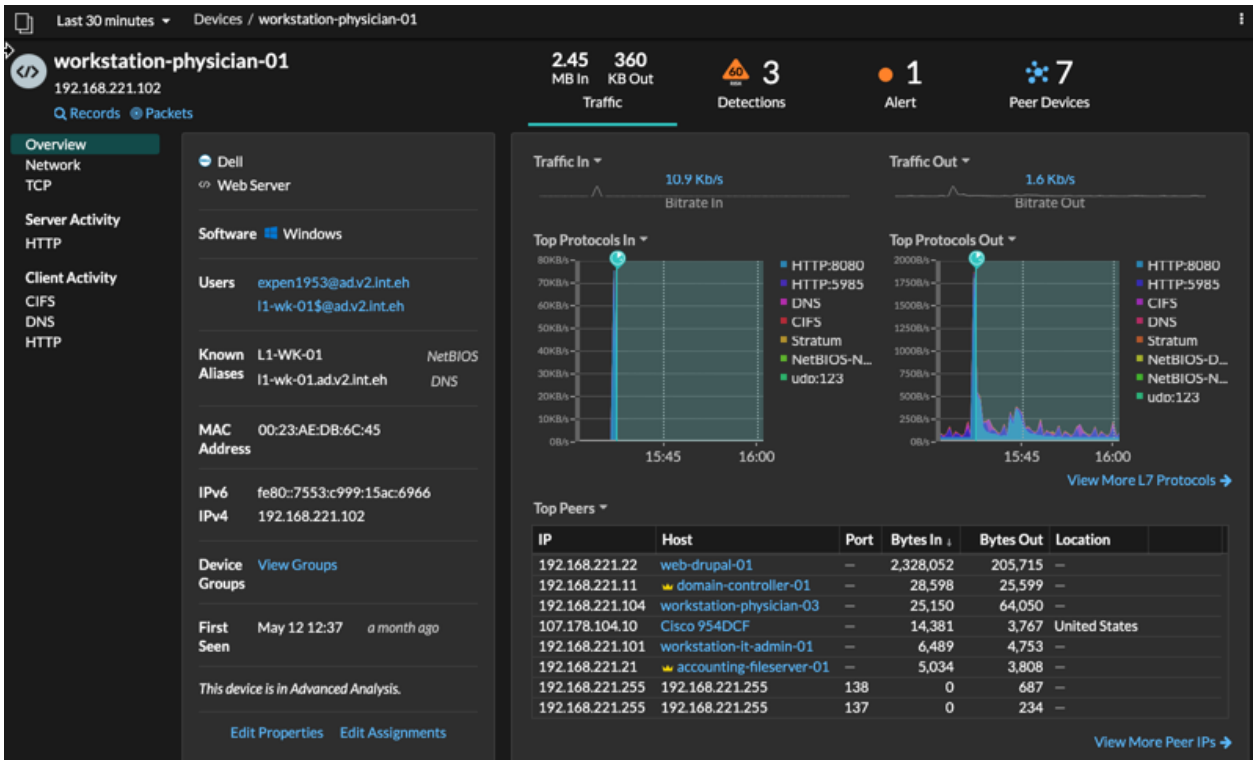
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs**.
3. Dans le graphique d'activité des appareils par protocole, cliquez sur le nombre de serveurs HTTP, comme indiqué dans la figure suivante.



Note: Si vous ne trouvez pas le protocole souhaité, il se peut que le système ExtraHop n'ait pas observé ce type de trafic de protocole sur le fil pendant l'intervalle de temps spécifié, ou que le protocole nécessite une licence de module. Pour plus d'informations, consultez le Je ne vois pas le trafic de protocole auquel je m'attendais ? section de la FAQ sur les licences.

La page affiche les mesures de trafic et de protocole associées au groupe de serveurs HTTP.

4. En haut de la page, cliquez sur **Membres du groupe**.
   La page affiche un tableau contenant tous les périphériques qui ont envoyé des réponses HTTP par câble pendant l'intervalle de temps sélectionné.
5. Dans le tableau, cliquez sur le nom d'un équipement.
   La page affiche les mesures de trafic et de protocole associées à cet équipement, comme dans l'image suivante.



Trouvez les appareils auxquels un utilisateur spécifique a accédé

Sur la page Utilisateurs, vous pouvez voir les utilisateurs actifs et les appareils auxquels ils se sont connectés au système ExtraHop pendant l'intervalle de temps spécifié.

Conseil Vous pouvez également rechercher des utilisateurs à partir du champ de recherche global en haut de la page.

Cette procédure vous montre comment effectuer une recherche à partir de la page Utilisateurs.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs** puis cliquez sur **Utilisateurs** graphique.
3. Dans la barre de recherche, sélectionnez l'une des catégories suivantes dans la liste déroulante :

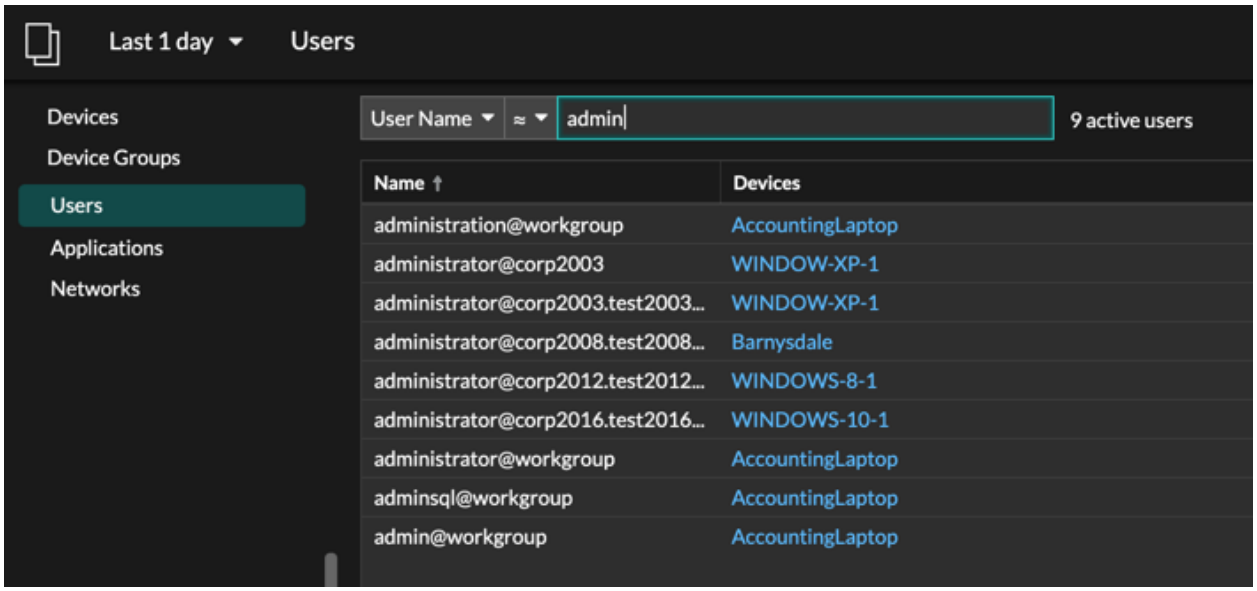
Option	Description
Nom d'utilisateur	Effectuez une recherche par nom d'utilisateur pour savoir à quels appareils l'utilisateur a accédé. Le nom d'utilisateur est extrait du protocole dauthentification, tel que LDAP ou Active Directory.

Option	Description
Protocole	Effectuez une recherche par protocole pour savoir quels utilisateurs ont accédé à des appareils communiquant via ce protocole.
Nom de l'appareil	Effectuez une recherche par nom d'équipement pour savoir quels utilisateurs ont accédé à l' appareil.

4. Sélectionnez l'un des opérateurs suivants dans la liste déroulante :

Option	Description
=	Recherchez un nom ou un équipement correspondant exactement au champ de texte.
≠	Recherchez des noms ou des appareils qui ne correspondent pas exactement au champ de texte.
≈ (par défaut)	Recherchez un nom ou un équipement qui inclut la valeur du champ de texte.
≈/	Recherchez un nom ou un équipement qui exclut la valeur du champ de texte.

5. Dans le champ de texte, saisissez le nom de l'utilisateur ou de l'équipement que vous souhaitez associer ou exclure.
La page Utilisateurs affiche une liste de résultats similaire à la figure suivante :



6. Cliquez sur le nom d'un équipement pour ouvrir le Page de présentation de l'appareil et visualisez tous les utilisateurs qui ont accédé à l'équipement pendant l'intervalle de temps spécifié.

Trouvez des appareils homologues

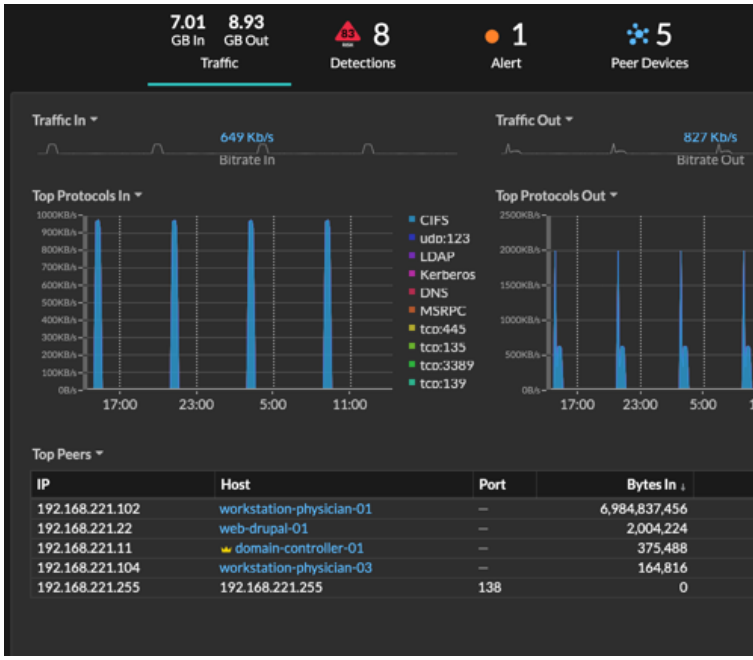
Si vous voulez savoir quels appareils communiquent activement entre eux, vous pouvez effectuer une recherche par IP homologue depuis la page de protocole d'un appareil ou d'un groupe déquipements.

Quand tu explorer vers le bas par adresse IP homologue, vous pouvez consulter une liste de périphériques homologues, consulter les mesures de performance ou de débit associées aux périphériques

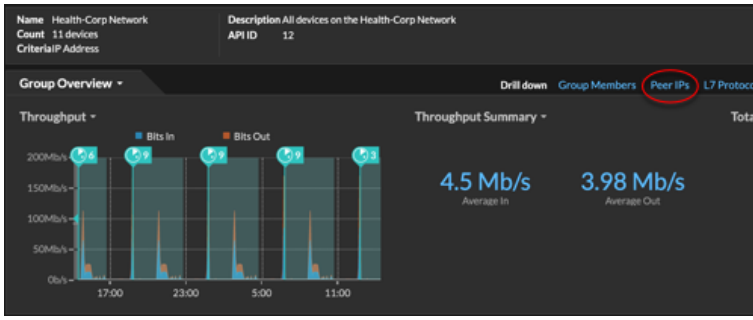
homologues, puis cliquer sur le nom d'un équipement homologue pour afficher des mesures de protocole supplémentaires.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs** puis sélectionnez **Appareil** ou **Groupe d'appareils** dans le volet de gauche.
3. Rechercher un équipement ou un groupe dproximatif d'équipements, puis cliquez sur le nom dans la liste des résultats.
4. Sur la page de présentation de l'équipement ou du groupe dveloppement sélectionné, cliquez sur l'un des liens suivants :

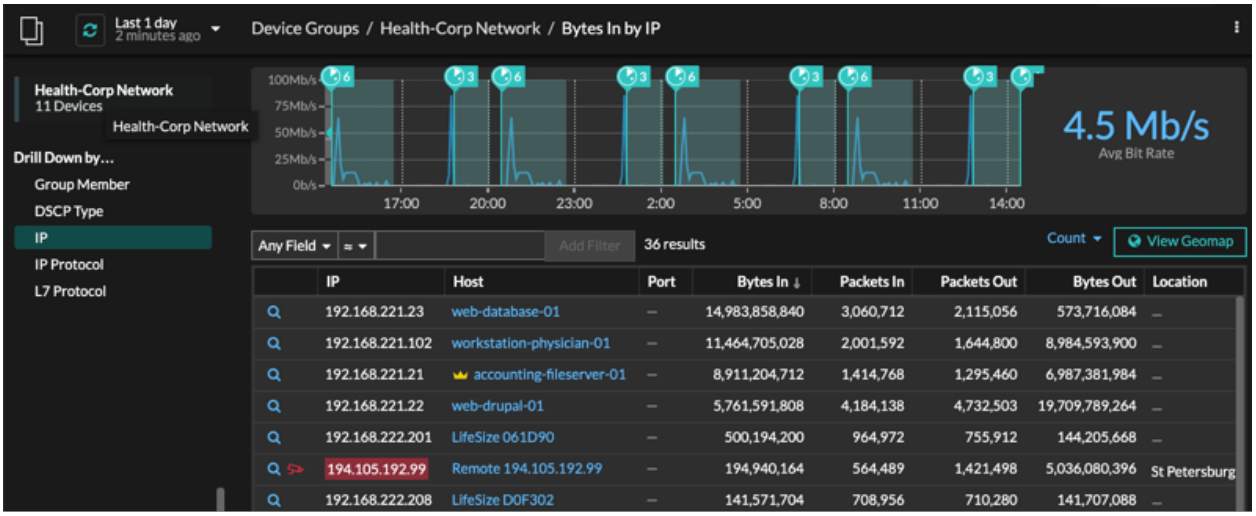
Option	Description
Pour appareils	Cliquez **Afficher plus d'adresses IP homologues**, situé en bas du tableau des meilleurs pairs.



Pour les groupes d'équipements	Cliquez **IP homologues**, situé dans la section Détails dans le coin supérieur droit de la page.



Une liste des appareils homologues s'affiche, ventilés par adresse IP. Vous pouvez examiner les informations relatives aux octets et aux paquets du réseau pour chaque équipement homologue, comme illustré dans la figure suivante.



Modifier le nom d'un équipement

Le système ExtraHop nomme automatiquement les périphériques en surveillant passivement le trafic du protocole de dénomination (DNS, DHCP, NETBIOS, CDP). Si le trafic du protocole de dénomination n'est pas observé pour un équipement, le nom de l'équipement affiche soit l'adresse IP, soit l'adresse MAC. Dans les deux cas, vous pouvez remplacer le nom automatique de l'équipement par un nom personnalisé. Le nom personnalisé apparaîtra dans tout le système ExtraHop.

Voici quelques considérations importantes concernant la modification du nom d'un équipement :

- Les noms personnalisés ne sont pas synchronisés entre les systèmes ExtraHop connectés. Par exemple, un nom personnalisé créé sur une sonde n'est pas disponible depuis un appareil connecté console.
- Le système ExtraHop n'effectue pas de recherches DNS pour les noms d'équipements. Le système ExtraHop dérive le nom DNS d'un équipement en observant le trafic DNS sur des données filaires. Pour plus d'informations, voir Découverte des appareils.
- Si un équipement possède plusieurs noms, l'ordre de priorité d'affichage est spécifié dans les paramètres d'administration.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs** puis cliquez sur **Appareils actifs** graphique.
3. Filtrez la liste des appareils pour trouver l'appareil de votre choix, puis cliquez sur le nom de l'appareil. La page Aperçu de l'appareil apparaît. Elle affiche le trafic et l'activité du protocole pour l'équipement sélectionné.
4. Cliquez **Modifier les propriétés**.
5. Cliquez **Afficher le nom personnalisé**.
6. Tapez un nom personnalisé dans le champ.
7. Cliquez **Enregistrer**.

Modifier le rôle d'un équipement

Le système ExtraHop découvre et classe automatiquement les appareils de votre réseau en fonction de l'activité du protocole ou du modèle d'appareil et attribue un rôle à chaque appareil, tel qu'une passerelle, un serveur de fichiers , une base de données ou un équilibreur de charge. Vous pouvez modifier le rôle attribué à un équipement à tout moment.

Voici quelques considérations importantes concernant la modification du rôle d'un équipement :

- Une fois que vous avez modifié le rôle de l'équipement, l'équipement peut être retiré ou ajouté à groupes d'équipements dynamiques qui incluent un rôle d'équipement comme critère.
- Les changements de rôle des appareils ne sont pas synchronisés entre les systèmes ExtraHop connectés. Par exemple, si vous modifiez le rôle d'un équipement sur un sonde, le rôle n'est pas modifié depuis un rôle connecté console.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs** puis cliquez sur **Appareils actifs** graphique.
3. Filtrez la liste des appareils pour trouver celui que vous souhaitez, puis cliquez sur son nom.
   La page Aperçu de l'appareil apparaît. Elle affiche le trafic et l'activité du protocole pour l'équipement sélectionné.
4. Cliquez **Modifier les propriétés** .
5. Dans le Rôle de l'appareil section, cliquez sur la liste déroulante, puis cliquez sur l'un des rôles suivants :

Rôle	Descriptif
Automatique	Attribuez le rôle que le système ExtraHop a identifié pour l'équipement, qui apparaît entre parenthèses.
Simulateur d'attaque	Attribuez à un équipement qui exécute un logiciel de simulation de brèches et d'attaques (BAS) pour simuler des attaques sur un réseau.
Base de données	Attribuer à un équipement qui héberge une instance de base de données.
Serveur DHCP	Attribuer à un équipement dont la fonction principale est de traiter l'activité du serveur DHCP.
Serveur DNS	Attribuer à un équipement dont la fonction principale est de traiter l'activité du serveur DNS.
Contrôleur de domaine	Attribuez à un équipement qui fait office de contrôleur de domaine pour l'activité des serveurs Kerberos, SMB et MSRPC.
Serveur de fichiers	Attribuez à un équipement qui répond aux demandes de lecture et d'écriture de fichiers via les protocoles NFS et SMB.
Pare-feu	Attribuez à un équipement qui surveille le trafic réseau entrant et sortant et bloque le trafic conformément aux règles de sécurité.
Passerelle	Attribuer à un équipement qui fait office de routeur ou de passerelle.
Caméra IP	Attribuez à un équipement qui envoie des données d'image et de vidéo via le réseau, tel que des caméras de sécurité.

Rôle	Descriptif
Équilibreur de charge	Attribuez à un équipement qui fait office de proxy inverse pour distribuer le trafic sur plusieurs serveurs.
Dispositif médical	Attribuer à un équipement spécialement conçu pour les besoins de santé et les environnements médicaux.
Appareil mobile	Attribuer à un équipement sur lequel un système d'exploitation mobile est installé, tel qu'iOS ou Android.
Passerelle NAT	Attribuer à un équipement qui fait office de passerelle de traduction d'adresses réseau (NAT). Une passerelle NAT est généralement associée à au moins quatre familles d'empreintes digitales de systèmes d'exploitation ou à au moins quatre marques et modèles de matériel ou de fournisseurs. Une fois ce rôle attribué à un appareil, les propriétés du logiciel, de la marque et du modèle du matériel et des utilisateurs authentifiés n' apparaissent plus pour l'appareil.
PC	Attribuer à un équipement tel qu'un ordinateur portable, un ordinateur de bureau, une machine virtuelle Windows ou un appareil macOS.
Imprimante	Attribuer à un équipement qui permet aux utilisateurs d'imprimer du texte et des graphiques à partir d'autres appareils connectés.
Téléphone VoIP	Attribuer à un équipement qui gère les appels téléphoniques de voix sur IP (VoIP).
Passerelle VPN	Attribuez à un équipement qui connecte deux ou plusieurs appareils ou réseaux VPN ensemble pour relier les connexions distantes.
Scanner de vulnérabilité	Attribuer à un équipement qui exécute des programmes d'analyseur de vulnérabilités.
Serveur proxy Web	Attribuer à un équipement qui traite les requêtes HTTP entre un équipement et un autre serveur.
Serveur Web	Attribuez à un équipement qui héberge des ressources Web et répond aux requêtes HTTP.
Point d'accès Wi-Fi	Attribuez à un équipement qui crée un réseau local sans fil et projette un signal de réseau sans fil vers une zone désignée.
Autres	Attribuer à un équipement lorsque l'activité de l'équipement ne permet pas d' identifier clairement un seul rôle.

6. Cliquez **Enregistrer**.

Modifier le modèle d'un équipement

Le système ExtraHop observe le trafic réseau des appareils pour déterminer automatiquement la marque et le modèle, mais vous pouvez modifier manuellement le modèle de l'appareil.

Voici quelques considérations importantes concernant la modification d'un modèle d'équipement :

- Les appareils sont automatiquement ajoutés et supprimés des groupes d'appareils dynamiques selon des critères basés sur les modèles d'appareils.
- Vous pouvez modifier le modèle d'un équipement depuis capteurs et consoles. Lorsque l'équipement est mis à jour sur console, le changement est synchronisé avec connecté capteurs. Cependant, le changement n'est pas synchronisé d'une personne à l'autre capteurs vers le connecté console.

Avant de commencer
Tu dois avoir privilèges d'écriture complets ou supérieur.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs** puis cliquez sur **Appareils actifs** graphique.
3. Filtrez la liste des appareils pour trouver l'appareil de votre choix, puis cliquez sur le nom de l'appareil. Le Présentation de l'appareil une page apparaît, qui affiche le trafic et l'activité du protocole pour l'équipement sélectionné.
4. Cliquez **Modifier les propriétés**.
5. Dans le Modèle d'appareil section, sélectionnez l'une des options suivantes :

Option	Description
Automatique	• Sélectionnez cette option pour permettre au système ExtraHop de déterminer automatiquement la marque et le modèle de l' équipement, qui apparaissent entre parenthèses.
Personnalisé	1. Sélectionnez cette option pour spécifier manuellement la marque et le modèle de l'équipement. 2. Cliquez **Spécifiez la marque d'un équipement...** et saisissez le nom de la marque de votre choix. La liste déroulante affiche les marques correspondantes. 3. Sélectionnez une marque dans la liste déroulante ou saisissez un nom de marque personnalisé. 4. Cliquez **Spécifiez un modèle d'équipement...** et saisissez le nom du modèle que vous souhaitez. Si vous avez sélectionné une marque existante, la liste déroulante affiche les modèles correspondants à cette marque. 5. Sélectionnez un modèle dans la liste déroulante ou saisissez un nom de modèle personnalisé.

6. Cliquez **Enregistrer**.

Identifier manuellement un équipement comme étant à valeur élevée

Alors que le système ExtraHop identifie automatiquement les appareils fournissant une authentification ou des services essentiels comme étant à valeur élevée, vous pouvez également identifier manuellement un appareil comme ayant une valeur élevée ou non.

Voici quelques considérations importantes concernant l'identification d'un équipement comme étant à valeur élevée :

- Les scores de risque sont augmentés pour les détections sur des appareils à valeur élevée.
- Les appareils sont automatiquement ajoutés et supprimés des groupes d'équipements dynamiques selon des critères basés sur une valeur élevée.
- Vous pouvez identifier manuellement les appareils à valeur élevée à partir de capteurs et consoles. Lorsque l' équipement est mis à jour sur console, le changement est synchronisé avec connecté capteurs. Cependant, le changement n'est pas synchronisé d'une personne à l'autre capteurs vers le connecté console.

Avant de commencer
Tu dois avoir privilèges d'écriture complets ou supérieur.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le menu supérieur, cliquez sur **Actifs** puis cliquez sur **Appareils actifs** graphique.
3. Filtrez la liste des appareils pour trouver l'appareil de votre choix, puis cliquez sur le nom de l'appareil. La page Aperçu de l'appareil apparaît. Elle affiche le trafic et l'activité du protocole pour l'équipement sélectionné.
4. Cliquez **Modifier les propriétés**.
5. Dans la section Valeur élevée, sélectionnez l'une des options suivantes :
   - Sélectionnez **Automatique** pour permettre au système ExtraHop de déterminer automatiquement si la valeur de l'équipement est élevée, ce qui apparaît entre parenthèses.
   - Sélectionnez **Oui** pour identifier manuellement l'équipement comme étant à valeur élevée.
   - Sélectionnez **Non** pour identifier manuellement que la valeur de l'équipement n'est pas élevée.
6. Cliquez **Enregistrer**.

Création d'une étiquette d'équipement

Les balises sont des étiquettes définies par l'utilisateur que vous pouvez associer à un équipement. Les balises peuvent aider à différencier les appareils du système ExtraHop qui partagent un attribut ou une caractéristique commune. Vous pouvez ensuite rechercher des appareils ou créer des appareils dynamiques groupes d'équipements en fonction de l'étiquette de l'équipement.

Note: Vous ne pouvez pas renommer une étiquette d'équipement une fois qu'elle a été créée.

Note: Vous pouvez également automatiser cette tâche via l' API REST.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Balises**.
3. Cliquez **Créez**.
4. Dans le **Nom** champ, saisissez un nom unique pour le tag.
5. Optionnel : Pour ajouter immédiatement le nouveau tag à un équipement, procédez comme suit :
   a) Cliquez **Sélectionnez un équipement**.
   b) Entrez un nom d'équipement, une adresse IP, une adresse MAC ou un nom d'hôte.
   c) Sélectionnez l'équipement dans les résultats de recherche.

Le nom de l'équipement apparaît dans la fenêtre, indiquant que le nouveau tag sera ajouté à cet équipement.

6. Cliquez **Enregistrer**.
   La nouvelle balise apparaît dans Gérer les tags fenêtre.
7. Cliquez **Terminé** pour fermer la fenêtre.

Conseil Vous pouvez également ajouter un tag à partir d'une page de présentation de l'appareil. Trouvez un équipement puis cliquez sur le nom de l'équipement. À partir du Page de présentation de l'appareil, cliquez **Modifier les propriétés**, puis cliquez sur **Balises**.

Prochaines étapes

- Rechercher un équipement par tag
- Création d'un groupe d'équipements dynamique par tag

Création d'un groupe dquelconque d'équipements

Vous pouvez créer des groupes d'appareils qui collectent des statistiques pour tous les appareils spécifiés dans un groupe. Avec les groupes d'appareils, vous pouvez toujours consulter les statistiques de chaque appareil ou membre du groupe. Les groupes d'appareils peuvent également être définis en tant que source métrique.

Utilisateurs avec privilèges d'écriture limités peut créer et modifier des groupes d'équipements dynamiques et statiques.

- Création d'un groupe d'équipements dynamique pour ajouter automatiquement au groupe tous les appareils qui correspondent à des critères spécifiques.
- Création d'un groupe d'équipements statiques pour ajouter manuellement chaque équipement.

Voici quelques considérations relatives aux performances à prendre en compte lors de la création d'un groupe diciéquipements :

- Le traitement d'un grand nombre de groupes d'appareils comportant un grand nombre d'appareils prendra plus de temps.
- Les groupes statiques sont traités plus rapidement que les groupes dynamiques et sont recommandés pour un groupe défini d' appareils.
- Les groupes dynamiques avec des critères complexes peuvent avoir un coût de performance plus élevé.

Création d'un groupe dproximatif d'équipements

Vous pouvez créer des groupes d'équipements dynamiques avec des filtres complexes, qui vous permettent de spécifier plusieurs critères et de créer des groupes de critères imbriqués.

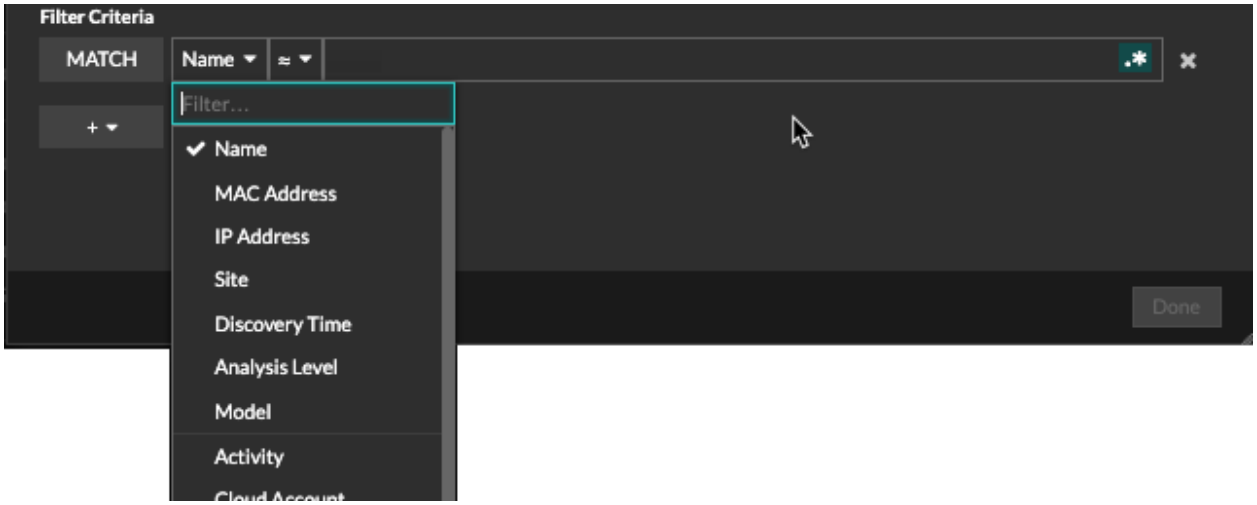
Conseil Vous pouvez créer rapidement un groupe d'appareils dynamique à partir d'une liste filtrée d'appareils sur la page Appareils. Cliquez **Création d'un groupe dynamique** depuis le coin supérieur droit.

Vous pouvez également créer un groupe d'appareils dynamique à partir d'un groupe d'appareils intégré . Sur la page Ressources, cliquez sur un rôle ou un protocole, mettez à jour les critères de filtre, puis cliquez sur Enregistrer icône dans le coin supérieur droit.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le menu supérieur, cliquez sur **Actifs** puis cliquez sur **Groupes d'appareils** graphique.
3. Cliquez **Créer un groupe d'appareils**.
4. Dans le **Nom du groupe** dans le champ, saisissez un nom descriptif pour identifier le groupe
5. Optionnel : À partir du **Rédacteurs** dans la liste déroulante, sélectionnez les utilisateurs disposant de privilèges d'écriture limités qui peuvent modifier ce groupe dcesséquipements. Ce privilège global doit être activé dans les paramètres d'administration.

- La liste affiche uniquement un nombre limité d'utilisateurs en écriture possédant des comptes actifs.
- Seul un utilisateur disposant d'une autorisation de modification pour un groupe d'équipements peut ajouter d'autres utilisateurs à écriture limitée.

6. Optionnel : Dans le **Descriptif** dans ce champ, ajoutez des informations sur ce groupe dproximatif d'équipements.
7. Dans le Type de groupe section, cliquez sur **Dynamique**.
8. Dans le Critères de filtrage rubrique, **Nom** et sélectionnez l'une des catégories suivantes dans la liste déroulante :
9. Cliquez **Nom** et sélectionnez l'une des catégories suivantes dans la liste déroulante :



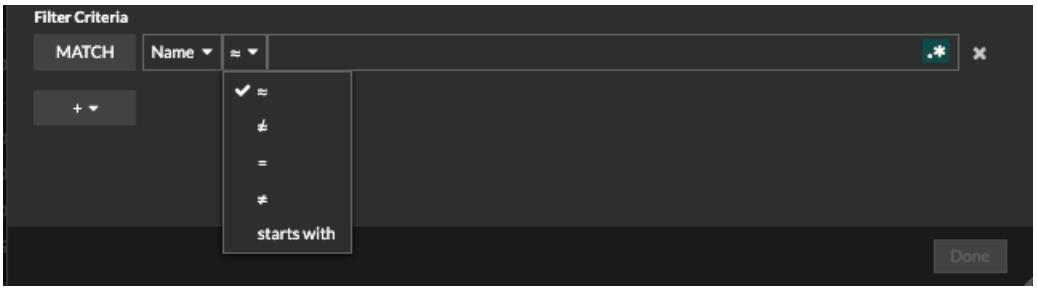
Option	Description
Nom	Filtre les appareils en fonction du nom de l'équipement découvert. Par exemple, le nom d'un équipement découvert peut inclure l'adresse IP ou le nom d'hôte.
Adresse MAC	Filtre les appareils en fonction de leur adresse MAC.
Adresse IP	Filtre les appareils par adresse IP au format de bloc IPv4, IPv6 ou CIDR.
Site	Filtre les appareils associés à un site connecté. Console uniquement.
L'heure de la découverte	Filtre les appareils découverts automatiquement par le système ExtraHop dans l'intervalle de temps spécifié. Pour plus d'informations, voir Création d'un groupe dproximatif d'équipements en fonction de l'heure de découverte.
Niveau d'analyse	Filtre les appareils par niveau d'analyse, ce qui détermine quelles données et mesures sont collectées pour un équipement. Vous ne pouvez pas créer de groupe déquipements dynamique pour les appareils filtrés par niveau d'analyse.

Option	Description
modèle	Filtre les appareils par marque, famille ou nom de modèle. La marque représente le fabricant de l'équipement. Une famille représente un groupe tel qu'une gamme de produits. Les conseils suivants peuvent vous aider à trouver le modèle d'équipement que vous souhaitez : • Vous pouvez faire votre choix parmi la liste des marques présentes sur votre système ExtraHop, puis cliquer sur le filtre pour affiner les résultats. • Vous pouvez afficher des info-bulles à côté des marques et des familles pour voir combien d'appareils et de modèles correspondants ont été trouvés. • Vous pouvez sélectionner une marque ou une famille pour trouver tous les appareils de ce groupe, quel que soit le modèle.
Activité	Filtre les appareils en fonction de l'activité de protocole associée à l'équipement. Par exemple, la sélection d'un serveur HTTP renvoie les appareils dont les métriques sont associées au serveur HTTP, ainsi que tout autre équipement dont le rôle d' équipement est défini sur Serveur HTTP. Filtre également les appareils qui ont accepté ou initié une connexion externe, ce qui peut vous aider à déterminer si les appareils sont impliqués dans une activité suspecte.
Compte Cloud	Filtre les appareils en fonction du compte de service cloud associé à l'appareil.
ID d'instance cloud	Filtre les appareils en fonction de l'ID d'instance cloud associé à l'équipement.
Type d'instance cloud	Filtre les appareils en fonction du type d'instance cloud associé à l'équipement.
Hachage de fichiers SHA-256	Filtre les appareils sur lesquels des fichiers hachés par l'algorithme de hachage SHA-256 ont été observés. Vous pouvez consulter un tableau des fichiers hachés sur le Page Fichiers.
Valeur élevée	Filtre les appareils considérés comme à valeur élevée parce qu'ils fournissent des services d'authentification, prennent en charge les services essentiels de votre réseau ou sont spécifiés par l'utilisateur comme étant à valeur élevée.
Actuellement actif	Filtre les appareils en fonction de l'activité observée sur un équipement au cours des 30 dernières minutes.
Type de localité du réseau	Filtre les appareils en fonction de toutes les localités du réseau interne ou externe.
Nom de la localité du réseau	Filtre les appareils par nom de localité du réseau.

Option	Description
Rôle	Filtre les appareils en fonction du rôle d'équipement attribué, tel que la passerelle, le pare-feu, l'équilibreur de charge et le serveur DNS.
Logiciel	Filtre les appareils en fonction du logiciel du système d'exploitation détecté sur l'équipement.
Type de logiciel	Filtre les appareils en fonction du type de logiciel observé sur l'équipement, tel qu'un simulateur d'attaque, un accès à distance ou un serveur de bases de données.
Sous-réseau	Filtre les appareils en fonction du sous-réseau associé à l'équipement.
Balise	Filtre les appareils en fonction de balises d'équipement définies par l'utilisateur.
Fournisseur	Filtre les appareils en fonction du nom du fournisseur de l'équipement, tel que déterminé par la recherche de l'identifiant unique organisationnel (OUI).
Cloud privé virtuel	Filtre les appareils en fonction du VPC associé à l'équipement.
VLAN	Filtre les appareils en fonction de la balise VLAN de l'équipement. Les informations VLAN sont extraites des balises VLAN, si le processus de mise en miroir du trafic les conserve sur le port miroir. Disponible uniquement si le `devices_accross_vlans` le réglage est réglé sur `False` dans le fichier de configuration en cours d'exécution.
Nom CDP	Filtre les appareils en fonction du nom CDP attribué à l'équipement.
Nom de l'instance Cloud	Filtre les appareils en fonction du nom d'instance cloud attribué à l'équipement.
Nom personnalisé	Filtre les appareils en fonction du nom personnalisé attribué à l'équipement.
Nom DHCP	Filtre les appareils en fonction du nom DHCP attribué à l'équipement.
Nom DNS	Filtre les appareils selon n'importe quel nom DNS attribué à l'équipement.
Nom NetBIOS	Filtre les appareils en fonction du nom NetBIOS attribué à l'équipement.
Activité de détection	Filtre les appareils ayant une activité de détection où l'équipement était un participant. Active des critères supplémentaires tels que la catégorie, l'indice de risque et la technique MITRE.

Option	Description
	Note: Vous ne pouvez pas créer de groupe dveloppement contenant cette option de critère.

10. Sélectionnez l'un des opérateurs suivants dans la liste déroulante ; les opérateurs disponibles dépendent de la catégorie sélectionnée :

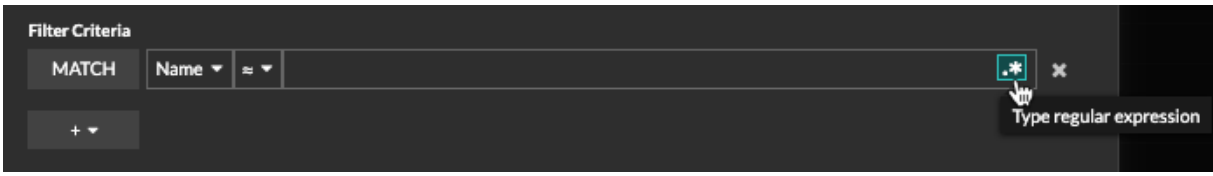


Option	Description
=	Filtre les appareils qui correspondent exactement au champ de recherche de la catégorie sélectionnée.
≠	Filtre les appareils qui ne correspondent pas exactement au champ de recherche.
≈	Filtre les appareils qui incluent la valeur du champ de recherche pour la catégorie sélectionnée.
≈/	Filtre les appareils qui excluent la valeur du champ de recherche pour la catégorie sélectionnée.
commence par	Filtre les appareils dont le nom commence par la valeur du champ de recherche de la catégorie sélectionnée.
existe	Filtre les appareils qui ont une valeur pour la catégorie sélectionnée.
n'existe pas	Filtre les appareils qui n'ont pas de valeur pour la catégorie sélectionnée.
correspondre	Filtre les appareils qui incluent la valeur du champ de recherche pour la catégorie sélectionnée.
et	Filtre les appareils qui correspondent aux conditions spécifiées dans au moins deux champs de recherche.
ou	Filtre les appareils qui correspondent à au moins une condition spécifiée dans au moins deux champs de recherche.
pas	Filtre les appareils qui ne correspondent pas aux conditions spécifiées dans un champ de recherche.

11. Dans le champ de recherche, saisissez la chaîne à rechercher ou sélectionnez une valeur dans la liste déroulante. Le type d'entrée est déterminé par la catégorie sélectionnée.

Par exemple, si vous souhaitez rechercher des appareils en fonction de leur nom, saisissez la chaîne à laquelle vous souhaitez faire correspondre dans le champ de recherche. Si vous souhaitez rechercher des appareils en fonction du rôle, sélectionnez-le dans la liste déroulante des rôles.

Conseil: Selon la catégorie sélectionnée, vous pouvez cliquer sur l'icône Regex dans le champ de texte pour activer la correspondance par expression régulière.



12. Optionnel : Cliquez sur l'icône Ajouter un filtre + et sélectionnez **Ajouter un filtre** ou **Ajouter un groupe de filtres** pour spécifier d'autres critères au niveau supérieur ou secondaire du filtre.

    Par exemple, si vous filtrez les noms d'appareils commençant par « acct », vous pouvez ajouter un nouveau groupe de critères qui filtre un certain rôle ou une étiquette au sein du groupe d'appareils commençant par « acct ».
13. Cliquez **Enregistrer**.

Vous pouvez modifier les critères en cliquant sur le groupe que vous souhaitez modifier sur la page Groupes d'appareils, puis en cliquant sur **Propriétés**.

Création d'un groupe dcessaires d'équipements

Conseil: Sur la page Appareils, vous pouvez cocher la case à côté d'un ou de plusieurs appareils et cliquer sur **Ajouter au groupe** pour créer rapidement un groupe d'appareils statique ou ajouter des appareils à un groupe existant.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le menu supérieur, cliquez sur **Actifs** puis cliquez sur **Groupes d'appareils** graphique.
3. Cliquez **Créer un groupe d'appareils**.
4. Dans le **Nom du groupe** dans ce champ, saisissez le nom du nouveau groupe.
5. Optionnel : À partir du **Rédacteurs** dans la liste déroulante, sélectionnez les utilisateurs disposant de privilèges d'écriture limités qui peuvent modifier ce groupe dcesséquipements. Ce privilège global doit être activé dans les paramètres d'administration.
   - La liste affiche uniquement un nombre limité d'utilisateurs en écriture possédant des comptes actifs.
   - Seul un utilisateur disposant d'une autorisation de modification pour un groupe dproximatifs d'équipements peut ajouter d'autres utilisateurs à écriture limitée.
6. Optionnel : Dans le **Descriptif** champ, ajoutez des informations sur ce groupe d'équipements.
7. Dans le Type de groupe section, sélectionnez **Statique**.
8. Cliquez **Enregistrer**.
   Votre groupe dcesséquipements est maintenant créé.
9. Ajoutez un équipement spécifique à votre groupe.
   a) Cliquez sur le groupe dcesséquipements statiques de votre choix, puis cliquez sur **Appareils** depuis le volet de gauche.
   b) Cliquez sur le champ Rechercher un équipement... en haut du tableau des appareils, saisissez le nom de l'appareil souhaité, puis sélectionnez-le dans la liste.
   c) Cliquez **Ajouter au groupe**.
10. Ajoutez à votre groupe des appareils répondant à des critères spécifiques.
    a) Cliquez **Appareils** dans le volet de gauche.

b) Trouvez un équipement puis cochez la case à côté des appareils que vous souhaitez ajouter à votre groupe.
c) En haut du tableau des équipements, cliquez sur **Ajouter au groupe**.
d) Dans la boîte de dialogue Ajouter au groupe, sélectionnez **Ajouter à un groupe existant**.
e) Sélectionnez un groupe diciels dans Groupe liste déroulante.
f) Cliquez **Ajouter au groupe**.

Prochaines étapes
Supprimez des appareils d'un groupe en cochant la case à côté du nom de l'équipement et en cliquant sur **Supprimer du groupe** dans le coin supérieur droit.

Création d'un équipement personnalisé

Collectez des métriques pour un segment de trafic sur plusieurs adresses IP et ports en créant un équipement personnalisé. Les appareils personnalisés sont utiles pour surveiller le trafic en dehors de votre domaine de diffusion local, comme les succursales, les magasins ou les cliniques.

Voici quelques considérations importantes concernant les appareils personnalisés :

- Les appareils personnalisés n'apparaissent dans le système ExtraHop qu'une fois que le trafic correspondant aux critères que vous avez spécifiés est observé.
- Évitez de créer plusieurs appareils personnalisés pour les mêmes adresses IP ou ports. Les appareils personnalisés configurés selon des critères qui se chevauchent peuvent dégrader les performances du système.
- Évitez de créer un équipement personnalisé pour un large éventail d'adresses IP ou de ports, car cela pourrait dégrader les performances du système.
- Un seul équipement personnalisé compte comme un seul appareil dans le cadre de votre capacité sous licence pour Analyse avancée et Analyse standard.
- Vous pouvez également automatiser cette tâche via l'API REST.

Avant de commencer
Tu dois avoir privilèges d'écriture complets ou supérieur.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Appareils personnalisés**.
3. Cliquez **Créez**.
4. Dans le Nom champ, saisissez un nom unique pour l' équipement personnalisé.
5. Dans le Identifiant Discovery champ, saisissez un identifiant unique.

   Si ce champ est laissé vide, un Discovery ID est généré à partir du nom de l' équipement personnalisé. Le Discovery ID ne peut pas contenir d'espaces et ne peut pas être modifié une fois l'équipement personnalisé enregistré.
6. À partir du **capteur** dans la liste déroulante, sélectionnez la sonde que vous souhaitez associer à l'équipement personnalisé. (Consoles uniquement.)
7. Sélectionnez le **Activer un équipement personnalisé** case à cocher pour activer ou désactiver l'équipement personnalisé.
8. Optionnel : Dans le Descriptif champ, ajoutez des informations sur l' équipement personnalisé.
9. Cliquez **Ajouter des critères** pour spécifier une adresse IP, une plage de ports ou une plage de VLAN comme critères de correspondance pour l'équipement personnalisé.

   Vous pouvez spécifier une seule option, telle qu'une adresse IP, ou définir une combinaison de critères ; il n'est pas nécessaire de remplir chaque champ.

   a) Dans le Adresse IP champ, saisissez une adresse IP ou une notation CIDR. Si vous spécifiez une adresse IP, vous pouvez également spécifier la direction du trafic et une adresse IP homologue.

- (Facultatif) : À partir du **Direction du trafic** liste déroulante, sélectionnez **Envoyé depuis l'adresse IP** ou **Entrant depuis l'adresse IP** comme critère de correspondance. Ces options vous permettent de créer un équipement personnalisé qui collecte des métriques uniquement à partir du trafic envoyé ou envoyé depuis cette adresse IP. La sélection par défaut est Bidirectionnel.
- (Facultatif) : Dans le Adresse IP du pair champ, spécifiez une adresse IP ou une notation CIDR qui communique avec l'adresse spécifiée dans **Adresse IP** champ. Cette option vous permet de créer un équipement personnalisé qui collecte des métriques uniquement à partir du trafic entre des adresses IP source et de destination spécifiques.

Note: Si vous spécifiez une adresse IP homologue, vous ne pouvez pas sélectionner **Bidirectionnel** pour le sens du trafic.

b) Dans le Plage de ports de destination dans les champs, saisissez un numéro de port de destination minimum et maximum. Si aucune plage n'est spécifiée, tous les ports sont considérés comme répondant aux critères.

10. Optionnel : Cliquez **Afficher les options avancées** pour configurer un port source ou une plage de VLAN.
    a) Dans le Plage de ports source dans les champs, saisissez un numéro de port source minimum et maximum. Si aucune plage n'est spécifiée, tous les ports sont considérés comme répondant aux critères.
    b) Dans le Gamme VLAN dans les champs, saisissez un ID de VLAN minimum et maximum.
11. Optionnel : Cliquez **Ajouter des critères** pour configurer des adresses IP, des plages de ports ou des plages de VLAN supplémentaires.
12. Cliquez **Enregistrer**.

Conseil: Cliquez **Enregistrer toutes les modifications** pour enregistrer tous les appareils personnalisés dont les modifications de configuration n'ont pas été enregistrées.

Prochaines étapes

- Configuration de sites distants pour des appareils personnalisés
- Trouvez un équipement
- Ajouter un équipement personnalisé à la liste de surveillance
- Ajouter un tag à un équipement personnalisé
- Supprimer ou désactiver un équipement personnalisé

Supprimer ou désactiver un équipement personnalisé

Les appareils personnalisés sont créés manuellement sur un système ExtraHop pour collecter des métriques relatives au trafic observé sur plusieurs adresses IP et ports. Si un grand nombre de périphériques personnalisés affecte les performances de votre système, vous pouvez supprimer ou désactiver un appareil personnalisé.

Avant de commencer
Des privilèges complets ou supérieurs sont requis pour créer ou supprimez un équipement personnalisé.

- Lorsque vous supprimez ou désactivez un équipement personnalisé, celui-ci devient inactif, ce qui signifie que le système arrête de collecter des métriques pour cet équipement.
- Lorsque vous supprimez ou désactivez un équipement personnalisé, celui-ci continue d'apparaître en tant qu' actif jusqu'à ce que toutes les mesures collectées pour cet équipement soient remplacées dans le fichier local banque de données.
- Lorsque vous supprimez un équipement personnalisé, le Discovery ID unique de ce dernier reste toujours dans le système et ne peut pas être appliqué à un nouvel équipement personnalisé.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Appareils personnalisés**.

3. Optionnel : Dans la zone de texte du filtre, recherchez l'équipement personnalisé.

   La zone de texte du filtre prend en charge la correspondance des sous-chaînes par nom, description, statut de l'équipement personnalisé, sonde, et Discovery ID.
4. Dans le tableau, sélectionnez l'équipement personnalisé de votre choix, puis effectuez l'une des étapes suivantes :

   - Dans les options de configuration, désactivez **Appareil personnalisé activé** case à cocher. L'équipement sélectionné devient inactif et est retiré du décompte complet des équipements d'analyse. Vous pouvez réactiver l' équipement personnalisé à tout moment, et vous pouvez toujours accéder aux métriques personnalisées de l'appareil à partir des intervalles de temps précédents jusqu'à ce qu'elles soient remplacées dans le système local banque de données.
   - En haut de la page, cliquez sur **Supprimer l'appareil**, puis cliquez sur **Supprimer un appareil personnalisé** depuis la fenêtre de confirmation. L'équipement personnalisé sélectionné est définitivement supprimé du système ExtraHop et ne peut pas être restauré.

Configuration de sites distants pour des appareils personnalisés

Les appareils personnalisés sont utiles pour surveiller le trafic en dehors de votre domaine de diffusion local, comme les succursales, les magasins ou les cliniques. Vous pouvez collecter des statistiques sur des sites distants concernant des appareils personnalisés afin de savoir facilement comment les sites distants consomment les services et de gagner en visibilité sur le trafic entre les sites distants et un centre de données.

Par exemple, créez un tableau de bord et ajoutez un équipement personnalisé comme source métrique pour consulter les indicateurs du site distant, tels que le débit entrant et sortant, les délais de retransmission, les temps d'aller-retour et les fenêtres nulles. Voir le Référence des métriques du protocole pour obtenir la liste complète des statistiques et des descriptions des sites distants.

Voici quelques considérations importantes concernant les sites distants pour les appareils personnalisés :

- La configuration du site distant s'applique à tous les appareils personnalisés activés ; vous ne pouvez pas configurer de sites distants pour un équipement personnalisé individuel.
- Les métriques de sites distants ne sont affichées dans le catalogue de métriques et dans l' explorateur de métriques que si la collecte de métriques de sites distants est activée.

Avant de commencer
Tu dois avoir privilèges d'écriture complets ou supérieur.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Appareils personnalisés**.
3. Cliquez **Configuration de sites distants**.
4. Sélectionnez ou désactivez le **Collectez les métriques des sites distants** case à cocher.
5. Cliquez **Enregistrer**.

Spécifier une localité du réseau

Les localisations réseau vous permettent de classer le trafic provenant d'adresses IP et de blocs CIDR comme étant interne ou externe à votre réseau. Vous pouvez également spécifier un nom pour chaque localité, tel que « DMZ » ou « réseau invité », et filtrer en fonction de ce nom dans les appareils et les enregistrements.

Voici quelques considérations importantes concernant ces paramètres :

- La désignation des localités du réseau affecte les détections et les déclencheurs ainsi que les fonctionnalités associées telles que les notifications, les pages de présentation et le rapport sur les opérations de sécurité.

- Si votre déploiement ExtraHop inclut une console, nous vous recommandons gestion des transferts de tous les capteurs connectés à la console.
- Pour ExtraHop RevealX 360, ces paramètres sont synchronisés sur tous les capteurs connectés. Vous ne devez pas configurer ces paramètres sur des capteurs individuels.
- Pour ExtraHop RevealX Enterprise, lorsque vous transférez la gestion vers une console connectée, ces paramètres sont synchronisés sur tous les capteurs. Dans le cas contraire, les paramètres de localisation du réseau doivent être configurés sur tous les capteurs et consoles.
- Vous devez avoir une écriture complète privilèges pour modifier ces paramètres.

Vidéos Consultez la formation associée : Configurer les localités du réseau

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Localités du réseau**.
3. Cliquez **Créez**.
4. Dans le champ Nom de la localité du réseau, saisissez un nom unique.
5. Optionnel : Dans le Descriptif champ, saisissez des informations sur la localité du réseau.
6. Dans la section Type de localité réseau, sélectionnez Interne ou Externe, en fonction de la classification que vous souhaitez appliquer aux adresses IP et aux blocs CIDR.
7. Dans le champ Adresses IP et blocs CIDR, saisissez les adresses IP et les blocs CIDR que vous souhaitez ajouter à la localité. Vous devez saisir une plage unique d' adresses ou de blocs.
8. Cliquez **Enregistrer**.

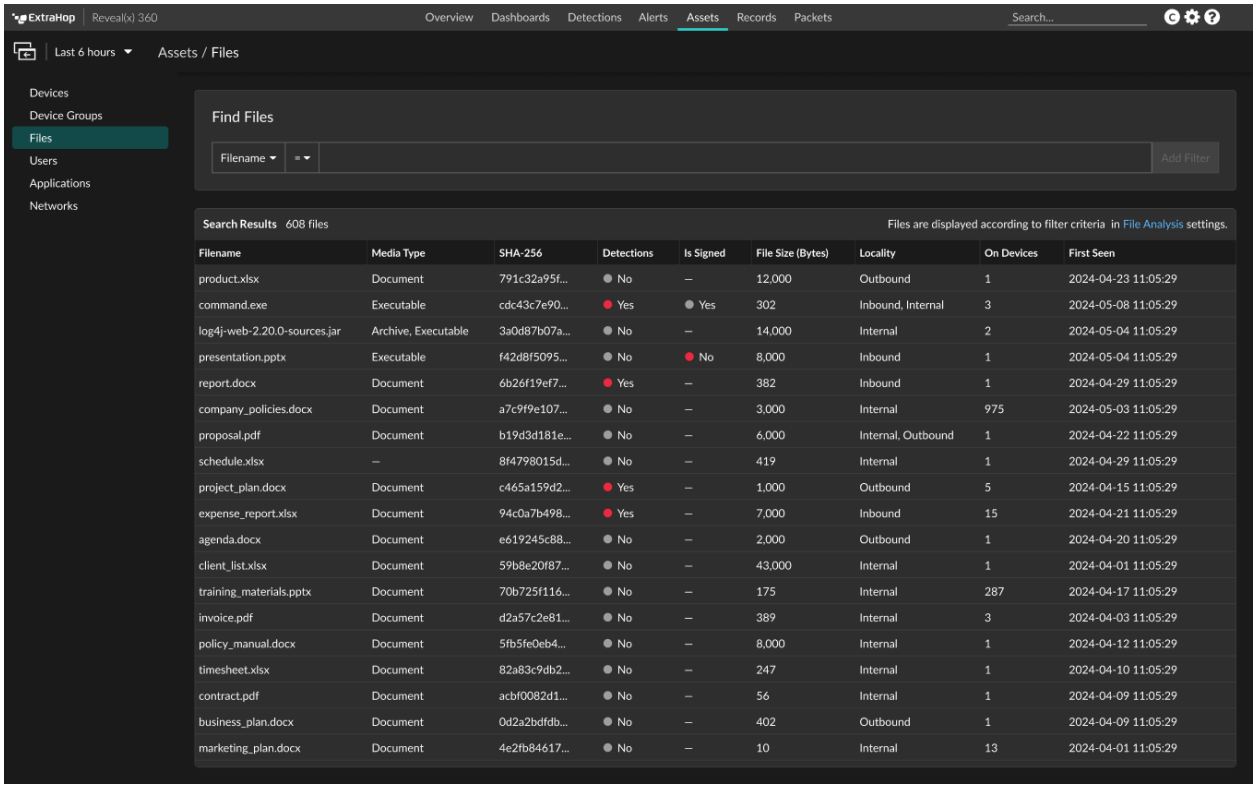
Prochaines étapes

- Depuis la page Actifs, trouver des appareils par localité du réseau.
- Explorez une métrique par client, serveur ou adresse IP et sélectionnez Interne ou Externe comme localité du réseau dans le filtre à trois champs.
- Filtrez les enregistrements en spécifiant l'un des filtres suivants :
  - Nom de la localité du réseau
  - Nom de la localité du réseau client
  - Nom de la localité du réseau du serveur
  - Nom de la localité du réseau de l'expéditeur
  - Nom de la localité du réseau récepteur

Dossiers

Les métadonnées issues de fichiers hachés constituent un outil précieux pour identifier les programmes malveillants et les risques sur votre réseau. Par exemple, les fichiers téléchargés par plusieurs appareils, les fichiers dont l'extension ne correspond pas au type de support, les fichiers non signés ou les transferts de fichiers sortants ou entrants volumineux sont des observations qui méritent d'être étudiées. La page Fichiers affiche un tableau des fichiers hachés et des informations sur les fichiers associés que vous pouvez filtrer et rechercher. Pour afficher la page Fichiers, cliquez sur **Actifs** dans le menu de navigation supérieur, puis cliquez sur **Dossiers** graphique.

Les fichiers sont hachés à l'aide de l'algorithme de hachage SHA-256 et affichés dans le tableau Fichiers selon les critères de filtrage configurés à partir du Paramètres d'analyse de fichiers. Vous pouvez ajouter des filtres dans Rechercher des fichiers section pour affiner les résultats dans le tableau Fichiers.

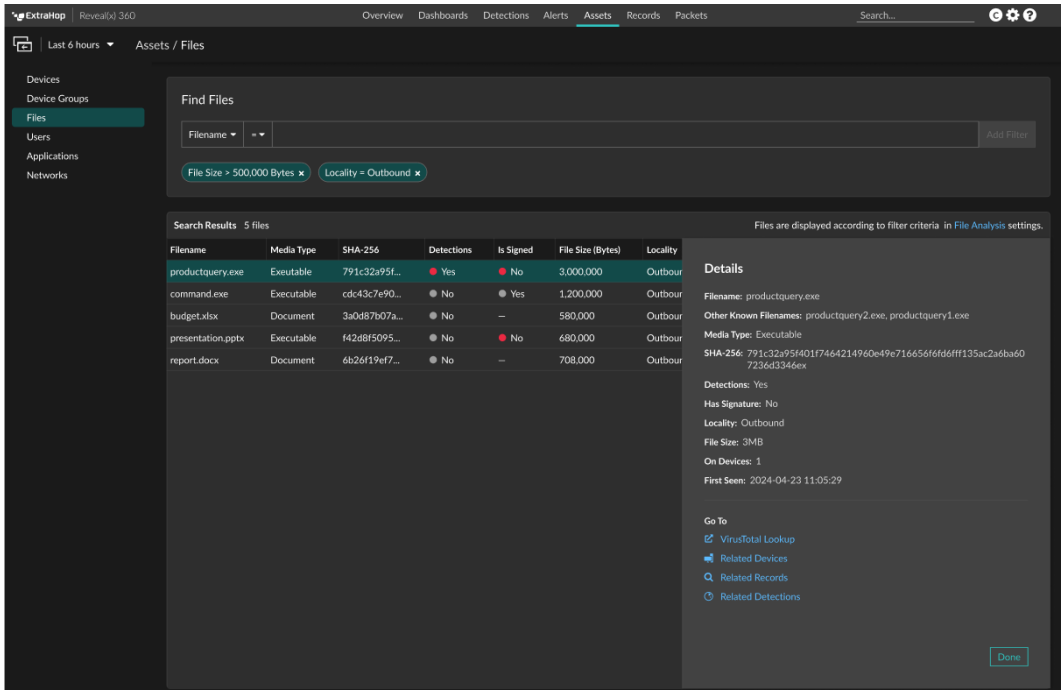


Le tableau Fichiers affiche les informations suivantes pour chaque fichier.

Détail du dossier	Descriptif
Nom de fichier	Le nom du fichier haché. Les autres noms de fichiers renvoyés par le même algorithme de hachage SHA-256 sont affichés dans le volet Détails.
Type de média	Type de support du fichier haché. Les types de fichiers pris en charge sont Document, Archive et Exécutable. Le système ExtraHop détermine le type de support de fichier en analysant les modèles dans l'en-tête et les premiers octets de la charge utile du fichier.

Détail du dossier	Descriptif
SHA-256	Algorithme de hachage de fichier SHA-256 appliqué au fichier. Conseil : vous pouvez trouver des appareils associés à des fichiers hachés spécifiques en ajoutant le filtre SHA-256 à la recherche d'un équipement.
Détections	Indique si le fichier haché a été impliqué dans une détection correspondant à un indicateur d'une collecte des menaces, tel qu'un transfert de fichier malveillant. (Disponible uniquement sur une console connectée à une sonde IDS (Intrusion Detection System) pour les utilisateurs ayant accès au module NDR)
Est signé	Indique si une signature a été observée sur le fichier haché, mais ne vérifie pas si la signature est valide.
Taille du fichier	Taille du fichier haché, en octets.
Localité	Localité, ou direction du flux, du fichier haché. Les localités prises en charge sont les suivantes : entrante, sortante et interne.
Sur les appareils	Le nombre d'appareils sur lesquels le fichier haché a été observé.
Vu pour la première fois	L'horodateur auquel le fichier haché a été observé pour la première fois.

Cliquez sur un fichier dans le tableau pour ouvrir le volet Détails et afficher plusieurs liens qui vous permettent d'étudier le hachage du fichier SHA-256.



- Cliquez **Recherche VirusTotal** pour accéder au site VirusTotal et vérifier que le hachage du fichier ne contient pas de contenu malveillant.
- Cliquez **Appareils associés** pour filtrer les appareils en fonction du hachage du fichier et afficher les résultats sur Appareils page.
- Cliquez **Enregistrements associés** pour filtrer les enregistrements en fonction du hachage du fichier et afficher les résultats sur Disques page.
- Cliquez **Détections associées** pour filtrer les détections en fonction du hachage du fichier et afficher les résultats sur Détections page. (Disponible uniquement sur une console connectée à une sonde IDS (Intrusion Detection System) pour les utilisateurs ayant accès au module NDR.)

Configuration de l'analyse des fichiers

L'analyse de fichiers vous permet de spécifier les fichiers à hacher à l'aide de l'algorithme de hachage SHA-256. Les hachages de fichiers qui correspondent à une collecte des menaces génèrent une détection, et les données de hachage de fichiers peuvent être interrogées dans des enregistrements.

ExtraHop vous recommande de gérer ces paramètres à partir d'une console ExtraHop, qui est la configuration par défaut de RevealX 360. Pour RevealX Enterprise, les capteurs gèrent ces paramètres par défaut. Si vous préférez gérer les paramètres sur une console plutôt que sur une sonde, vous pouvez transférer la gestion vers une console.

Prérequis

- Vous devez disposer de l'administration du système et des accès ou de l'administration du système (RevealX 360 uniquement) privilèges d'utilisateur.

Configurer une limite de taille pour les filtres de fichiers

Vous pouvez spécifier une limite de taille qui s'applique globalement à tous les filtres de fichiers. Tout fichier dépassant cette limite ne sera pas haché.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Analyse de fichiers**.
3. Dans le Limite de taille (Mo) champ, spécifiez une taille de fichier, en Mo.
   La plage est comprise entre 1 et 1 000 000 Mo. La valeur par défaut est de 10 Mo.
4. Cliquez **Enregistrer**.

Création d'un filtre de fichiers

Vous pouvez créer des filtres de fichiers personnalisés qui déterminent quels fichiers sont hachés sur le système ExtraHop. Le filtre ExtraHop par défaut est automatiquement activé et configuré pour hacher les fichiers de type multimédia exécutable et les fichiers observés sur tous les protocoles, localités et extensions de fichiers pris en charge par l'analyse des fichiers. Vous pouvez désactiver le filtre par défaut, mais vous ne pouvez pas modifier la configuration du filtre.

Note: L'activation d'un grand nombre de filtres de fichiers personnalisés peut affecter les performances du système.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Analyse de fichiers**.
3. Dans le Filtres de fichiers section, cliquez sur **Ajouter un filtre**.
4. Dans le Nom champ, entrez un nom unique pour le filtre.
5. À partir du **Protocole** dans la liste déroulante, sélectionnez l'une des options de protocole suivantes :
   - N'importe quel protocole (par défaut)
   - HTTP

- SMP
- FTP

Sélection **N'importe quel protocole** ne permet de hacher que les fichiers observés sur les protocoles HTTP, SMB ou FTP.

6. À partir du **Localité** dans la liste déroulante, sélectionnez l'une des options de direction de flux suivantes :
   - N'importe quelle localité (par défaut)
   - Entrant
   - Interne
   - Sortant
7. Dans le Format de fichier section, sélectionnez le type de fichiers à filtrer :
   - Pour filtrer par type de média, cliquez sur **Type de média**, puis sélectionnez l'une des options multimédia suivantes :
     - Archive
     - Document
     - Exécutable
   - Pour filtrer par extension de fichier, cliquez sur **Extension de fichier**, puis saisissez une ou plusieurs extensions de fichier, en les séparant par une virgule. Vous pouvez saisir des extensions dans l'un des formats suivants : `txt` ou `.txt`.
8. Dans la section Options, sélectionnez **Activer le filtre de fichiers** case à cocher pour activer le filtre et commencer à hacher les fichiers qui correspondent aux critères.
9. Optionnel : Si le filtre de fichiers est activé, vous pouvez sélectionner **Afficher les fichiers hachés dans le tableau Fichiers** case à cocher pour afficher les fichiers hachés et les métadonnées associées dans Tableau des fichiers disponible sur la page Actifs.
10. Cliquez **Enregistrer**.

Gestion du transfert des paramètres d'analyse des fichiers

Pour RevealX 360, les consoles ExtraHop gèrent les paramètres d'analyse des fichiers par défaut. Pour RevealX Enterprise, les capteurs ExtraHop gèrent ces paramètres.

Vous pouvez vous connecter à une console et transférer la gestion des paramètres d'analyse des fichiers vers une sonde, ou vous connecter à une sonde et transférer la gestion vers une console.

Note: Le transfert de la gestion de ces paramètres permet également de transférer la gestion de tous paramètres partagés.

1. Connectez-vous à la console ou à la sonde qui gère actuellement les paramètres d'analyse des fichiers via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Analyse de fichiers**.
3. Transférez la gestion de l'analyse des fichiers vers un autre système.

Option	Description
Transfert de la sonde à la console	1. Cliquez **Gestion des transferts**. 2. À partir du **Console de gestion** liste déroulante, sélectionnez un nom de console.
Transfert de la console à la sonde	1. Cliquez ***N* de *N* capteurs connectés**. La fenêtre Paramètres de gestion affiche la liste des capteurs dont la console gère les paramètres partagés et une liste des capteurs qui gèrent leurs propres paramètres.

Option	Description
	2. Cliquez sur le nom de la sonde dont vous souhaitez gérer ses propres paramètres. 3. Connectez-vous à la sonde. 4. Cliquez **Gestion des transferts**. 5. À partir du **Console de gestion** liste déroulante, sélectionnez **Appareil à capteur - Self**.

Priorités d'analyse

Le système ExtraHop analyse le trafic et collecte les données de tous les appareils découverts sur un seul sonde. Chaque équipement découvert reçoit un niveau d'analyse qui détermine quelles données et mesures sont collectées pour un équipement. Les priorités d'analyse déterminent le niveau d'analyse reçu par un équipement.

Important: Les priorités d'analyse peuvent être géré de manière centralisée depuis une console.

Vidéo: Consultez la formation associée : Priorités d'analyse

Hiérarchisation des appareils et des groupes

Le système ExtraHop peut analyser des centaines de milliers d'appareils et déterminer automatiquement le niveau d'analyse que chaque équipement reçoit, mais vous pouvez contrôler quels appareils sont priorisés pour l'analyse avancée et standard.

La plupart des appareils peuvent être ajoutés à une liste de surveillance pour garantir une analyse avancée ou vous pouvez ajouter des groupes d'équipements à une liste ordonnée afin de les classer par ordre de priorité pour l'analyse avancée et l'analyse standard.

Voici quelques points importants à prendre en compte pour hiérarchiser les appareils dans la liste de surveillance :

- Les appareils restent sur la liste de surveillance même lorsqu'ils sont inactifs, mais aucune statistique n'est collectée pour les appareils inactifs.
- Le nombre d'appareils figurant dans la liste de surveillance ne peut pas dépasser votre capacité d'Analyse avancée.
- Les appareils ne peuvent être ajoutés à la liste de surveillance qu'à partir de la page des propriétés de l'équipement ou de la page de liste des équipements. Vous ne pouvez pas ajouter d'appareils à la liste de surveillance depuis la page des priorités d'analyse.
- Si vous souhaitez ajouter plusieurs appareils à la liste de surveillance, nous vous recommandons créer un groupe d'équipements puis prioriser ce groupe pour l' analyse avancée.
- Les appareils recevant une analyse parent L2 ou une analyse de flux ne peuvent pas être ajoutés à la liste de surveillance.

Voici quelques considérations importantes concernant la hiérarchisation des groupes d'équipements :

- Classez les groupes d'équipements de la priorité la plus élevée à la plus faible dans la liste.
- Cliquez et faites glisser les groupes pour modifier leur ordre dans la liste.
- Assurez-vous que chaque équipement du groupe est actif ; les groupes contenant un grand nombre d' appareils occupent de la capacité et les appareils inactifs ne génèrent pas de mesures.
- Vous ne pouvez pas hiérarchiser plus de 200 groupes d'équipements pour chaque niveau.

Par défaut, le système ExtraHop remplit automatiquement les niveaux d'analyse avancée et standard jusqu'à sa capacité maximale. Voici quelques considérations importantes concernant les niveaux de capacité et l'option de remplissage automatique :

- Les appareils classés par ordre de priorité dans la liste de surveillance ou via un groupe hiérarchisé remplissent d'abord les niveaux d' analyse les plus élevés, puis les appareils découverts le plus tôt.
- Les appareils sont priorisés pour l'Analyse avancée s'ils sont associés à certaines détections, s'ils ont accepté ou initié une connexion externe, ou s'ils exécutent des outils d'attaque courants.
- Les propriétés de l'appareil, telles que le rôle, le matériel et le logiciel, l'activité du protocole, l'historique de détection et la valeur élevée, peuvent également déterminer les niveaux d'analyse.

- L'option Remplissage automatique est activée par défaut. Si cette option est désactivée, tous les appareils qui ne figurent pas dans les groupes prioritaires ou dans la liste de surveillance sont supprimés et le système ExtraHop définit la priorité de chaque équipement.
- Votre abonnement et votre licence ExtraHop déterminent les niveaux de capacité maximaux.

Voir le FAQ sur les priorités d'analyse pour en savoir plus sur les capacités des niveaux d'analyse.

Comparez les niveaux d'analyse

Niveau d'analyse	Fonctionnalités	Comment recevoir ce niveau
mode de découverte	• Détections • Protocoles observés • Adresses IP • Utilisateurs authentifiés • Logiciel • Marque et modèle du matériel	Les appareils reçoivent automatiquement le mode de découverte s'ils ne sont pas en mode Standard, Advanced ou L2 Parent Analysis.
Analyse standard	• Métriques L2-L3 • Cartes d'activités • Détections • Protocoles observés • Adresses IP • Utilisateurs authentifiés • Logiciel • Marque et modèle du matériel	Hiérarchiser les groupes d'équipements pour l'analyse standard.
Analyse avancée	• Métriques L2-L7 • Métriques personnalisées • Cartes d'activités • Détections • Protocoles observés • Adresses IP • Utilisateurs authentifiés • Logiciel • Marque et modèle du matériel	Hiérarchiser les groupes d'équipements pour l'Analyse avancée ou ajouter des appareils individuels à la liste de surveillance.
Analyse des parents L2 (Applicable uniquement si L3 Discovery est activé)	• Métriques L2-L3 • Cartes d'activités	Les appareils parents L2 reçoivent automatiquement une analyse parent L2, à l'exception des passerelles et des routeurs.
Analyse des flux	• Métriques L2-L3 • Cartes d'activités • Protocoles observés • Adresse IP • Propriétés de l'instance cloud • Types de détection limités	Les appareils reçoivent automatiquement une analyse de flux s'ils sont découverts sur un capteur de débit.

Gestion des transferts des priorités d'analyse

Chaque sonde réseau d'analyse de paquets peut gérer ses propres priorités d'analyse, qui déterminent quels appareils reçoivent Analyse avancée ou Analyse standard. Si votre sonde est connectée à une console, vous pouvez transférer la gestion des priorités vers cette console pour une vue centralisée de ces paramètres.

Voici quelques considérations importantes concernant le transfert de la gestion :

- Vous devez disposer de tous les privilèges d'écriture pour modifier les priorités d'analyse.
- Une fois la gestion transférée à un console, toutes les autres modifications que vous apportez à des capteurs individuels sont inactives. Voir quels autres les paramètres sont également transférés.
- Les paramètres des priorités d'analyse ne sont pas disponibles pour les capteurs de flux ; la gestion ne peut pas être transférée.

Les étapes suivantes vous montrent comment transférer la gestion des priorités vers un console:

1. Connectez-vous au système ExtraHop.

   Répétez ces étapes pour chaque sonde de votre environnement.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Priorités d'analyse**.
3. En haut de la page, cliquez sur Console liste déroulante et sélectionnez la console vers laquelle vous souhaitez transférer la gestion.
4. Cliquez **Transfert**.

Conseil Pour éviter toute interruption de l'analyse, vous pouvez enregistrer une ébauche des paramètres des priorités d'analyse pour chaque sonde avant de transférer la gestion sur une console.

Classer les groupes par ordre de priorité pour l'Analyse avancée

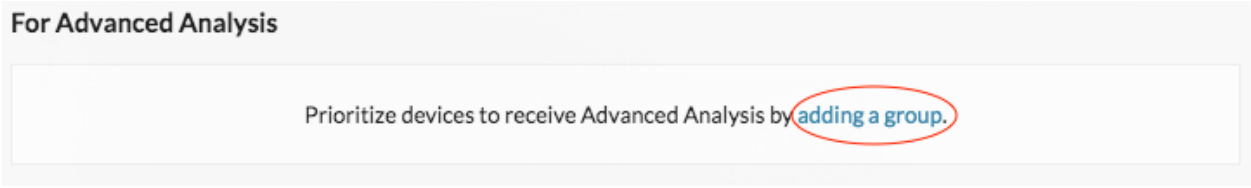
Vous pouvez spécifier des groupes d'équipements pour l'Analyse avancée en fonction de leur importance pour votre réseau. Les groupes sont classés dans une liste ordonnée.

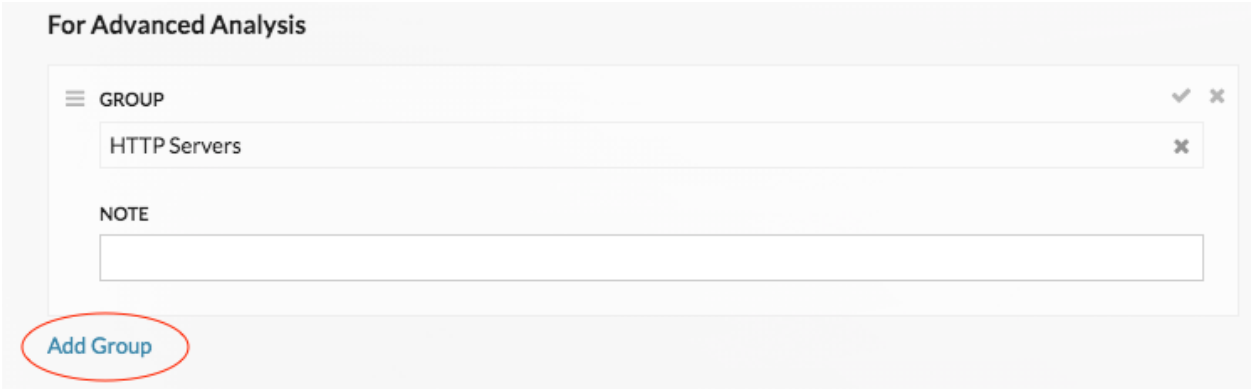
Voici quelques considérations importantes concernant Analyse avancée:

- Appareils sur le liste de surveillance sont garantis par une Analyse avancée et sont priorisés par rapport aux groupes d'équipements.
- Les appareils inactifs d'un groupe de dispositifs n'affectent pas la capacité d'Analyse avancée.
- Les métriques personnalisées ne sont disponibles que pour les appareils dans Analyse avancée. Si vous souhaitez consulter des statistiques personnalisées pour un équipement spécifique, donnez la priorité au groupe contenant l'équipement ou ajoutez l'équipement à la liste de surveillance.
- Vous devez disposer de droits d'écriture complets pour modifier les priorités d'analyse.
- Vous ne pouvez pas hiérarchiser plus de 200 groupes d'équipements pour l'Analyse avancée.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.

   (Ces étapes doivent être effectuées sur le console ou une sonde qui est gestion de ces paramètres partagés.)
2. Accédez aux paramètres des priorités standard.
   - Sur une console, cliquez sur l'icône Paramètres système puis cliquez sur **Priorités d'analyse**. Cliquez ensuite sur **Modifier les priorités** à côté de la sonde que vous souhaitez modifier.
   - Sur une sonde, cliquez sur l'icône des paramètres système puis cliquez sur **Priorités d'analyse**.
3. Priorisez les groupes en suivant les étapes suivantes :
   a) Dans le Pour une analyse avancée section, cliquez **ajout d'un groupe** pour ajouter le groupe initial ou **Ajouter un groupe** pour ajouter des groupes supplémentaires.





b) Dans le **Groupe** dans la liste déroulante, tapez le nom d'un groupe déquipements, puis cliquez sur le nom du groupe dans les résultats de recherche. Par exemple, tapez `Serveurs HTTP` et sélectionnez le **Serveurs HTTP** groupe d'équipements.

c) Optionnel : Dans le **Remarque** champ, saisissez des informations sur le groupe.

4. Dans le Remplissage automatique section, assurez-vous **Sur** est sélectionné.

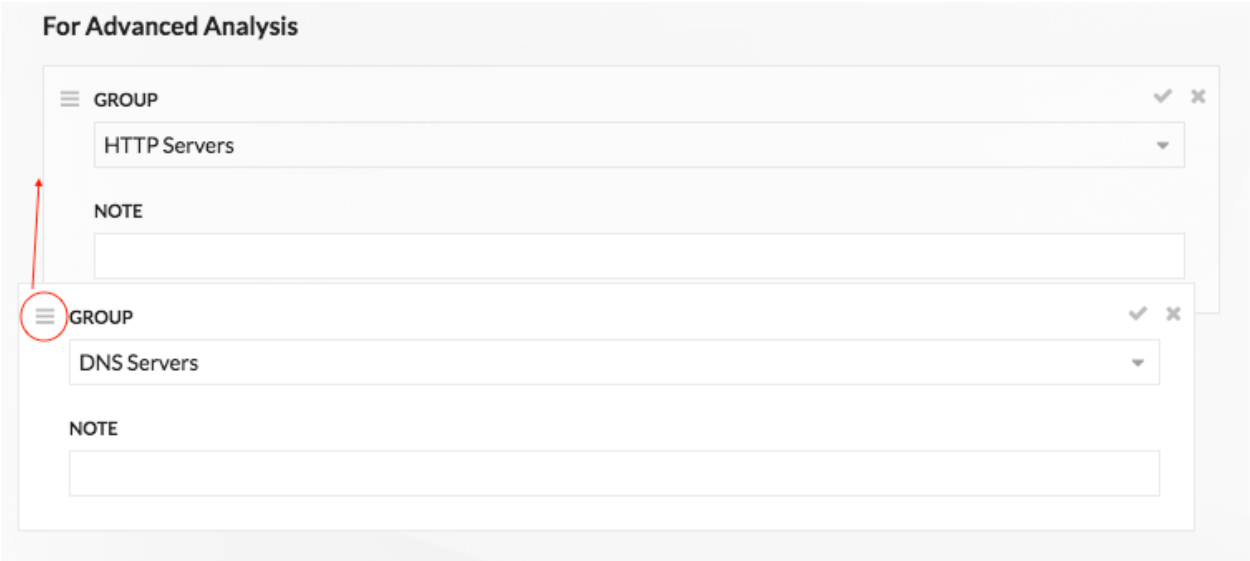
   Note: Si votre système rencontre des problèmes de performances, cliquez sur **Off**. Seuls les appareils appartenant à des groupes prioritaires ou figurant sur la liste de surveillance bénéficieront d'une Analyse avancée.

5. En haut de la page, cliquez sur **Enregistrer**.

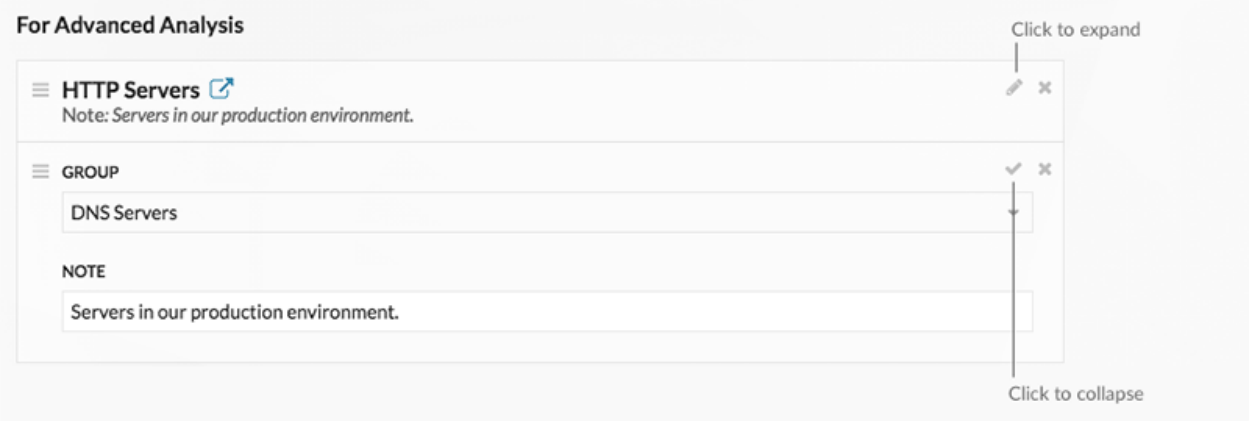
Prochaines étapes

Voici d'autres méthodes pour gérer et affiner les groupes qui reçoivent une analyse avancée :

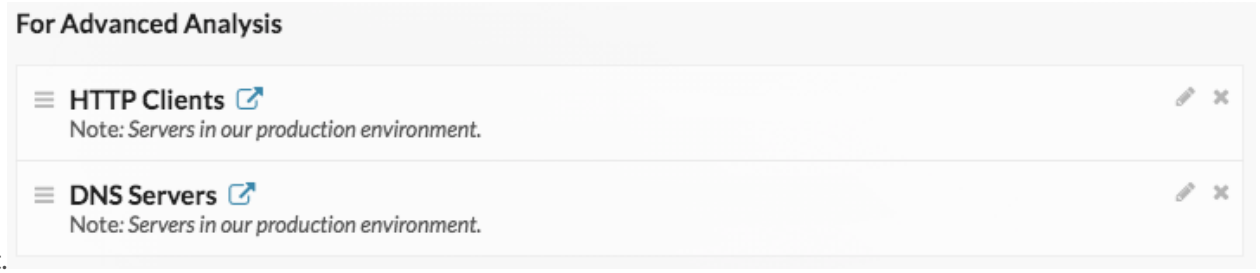
- Si vous ajoutez plusieurs groupes, les groupes sont priorisés de haut en bas. Cliquez sur l'icône en haut à gauche à côté de Groupe, puis faites glisser le groupe vers une autre position dans la liste ordonnée.



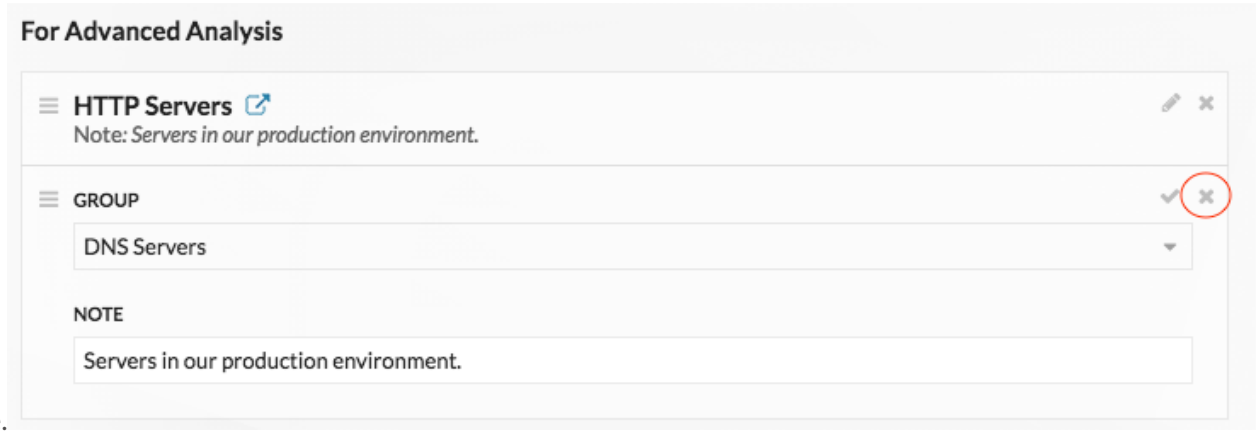
- Cliquez sur le chèque icône pour réduire le groupe. Cliquez sur le crayon icône pour développer à nouveau le groupe, comme indiqué dans la figure suivante.



- Cliquez sur le bouton « Accéder à icône à côté du nom d'un groupe pour accéder à la page du groupe d'équipements. La page des groupes d'appareils indique quels appareils et combien d'appareils font partie du groupe. L'icône n'est disponible que lorsque le groupe est réduit.



- Cliquez sur l'icône X pour supprimer un groupe de la liste, comme illustré dans la figure suivante.



Prioriser les groupes pour l'analyse standard

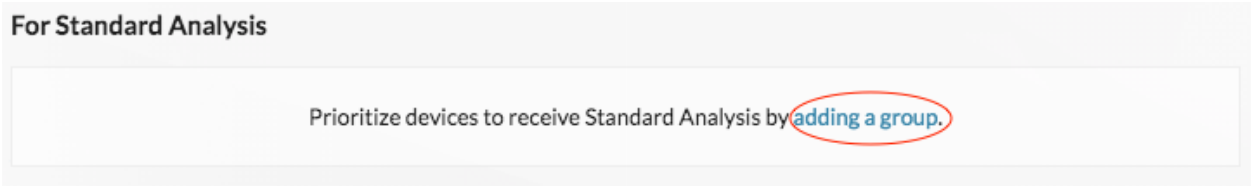
Vous pouvez spécifier des groupes d'équipements pour l'analyse standard en fonction de leur importance pour votre réseau. Les groupes sont classés dans une liste ordonnée.

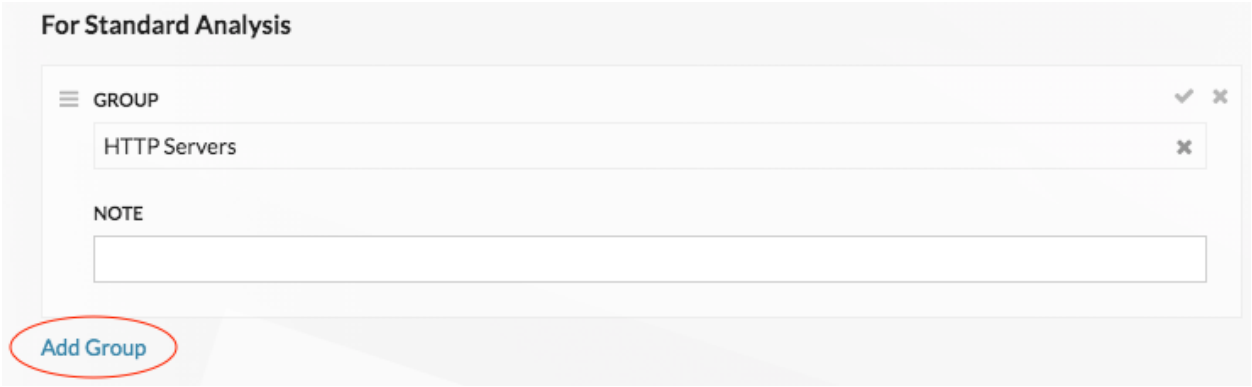
Voici quelques considérations importantes concernant Analyse standard:

- Les appareils priorisés pour la section Analyse standard reçoivent une analyse avancée lorsqu'ils sont en capacité.
- Vous devez disposer de tous les privilèges d'écriture pour modifier les priorités d'analyse.

- Vous ne pouvez pas hiérarchiser plus de 200 groupes d'équipements pour l'analyse standard.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
   (Ces étapes doivent être effectuées sur le console ou une sonde qui est gestion de ces paramètres partagés.)
2. Accédez aux paramètres des priorités standard.
   - Sur une console, cliquez sur l'icône Paramètres système puis cliquez sur **Priorités d'analyse**. Cliquez ensuite sur **Modifier les priorités** à côté de la sonde que vous souhaitez modifier.
   - Sur une sonde, cliquez sur l'icône des paramètres système puis cliquez sur **Priorités d'analyse**.
3. Priorisez les groupes en suivant les étapes suivantes :
   a) Dans le Pour une analyse standard section, cliquez **ajout d'un groupe** pour ajouter le groupe initial ou **Ajouter un groupe** pour ajouter des groupes supplémentaires.





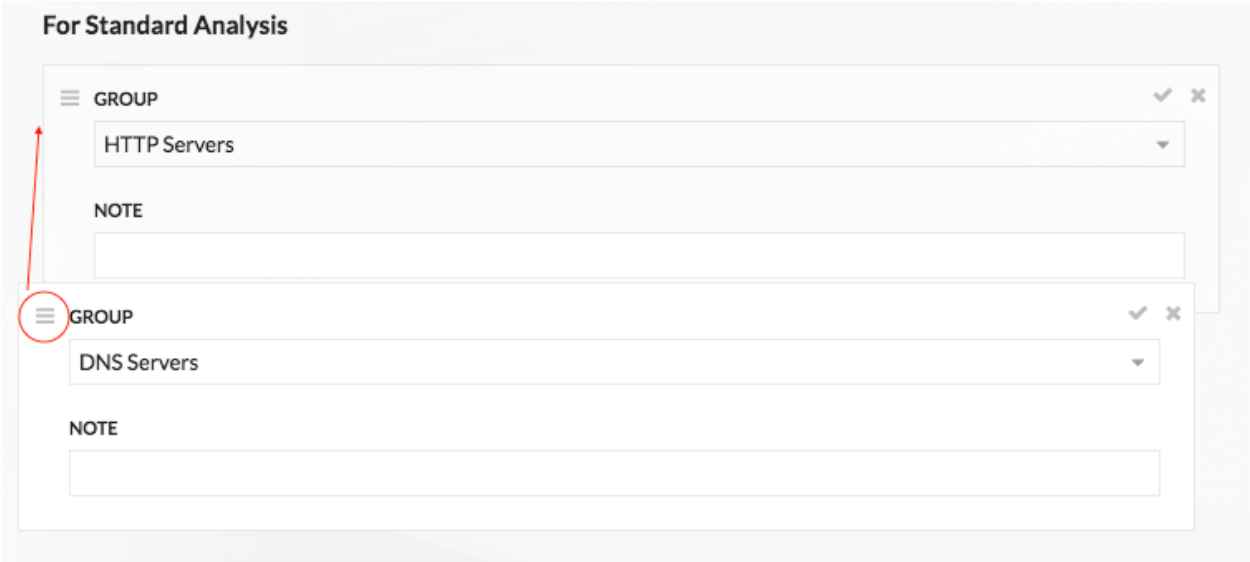
   b) Dans le **Groupe** dans la liste déroulante, tapez le nom d'un groupe déquipements, puis cliquez sur le nom du groupe dans les résultats de recherche. Par exemple, tapez `Serveurs HTTP` et sélectionnez le **Serveurs HTTP** groupe dÈRE d'équipements.
   c) Optionnel : Dans le **Remarque** champ, saisissez des informations sur le groupe.
4. Dans le Remplissage automatique section, assurez-vous **Sur** est sélectionné.

   Note: Si votre système rencontre des problèmes de performances, cliquez sur **Off**. Seuls les appareils appartenant à des groupes prioritaires font l'objet d' une analyse standard.
5. En haut de la page, cliquez sur **Enregistrer**.

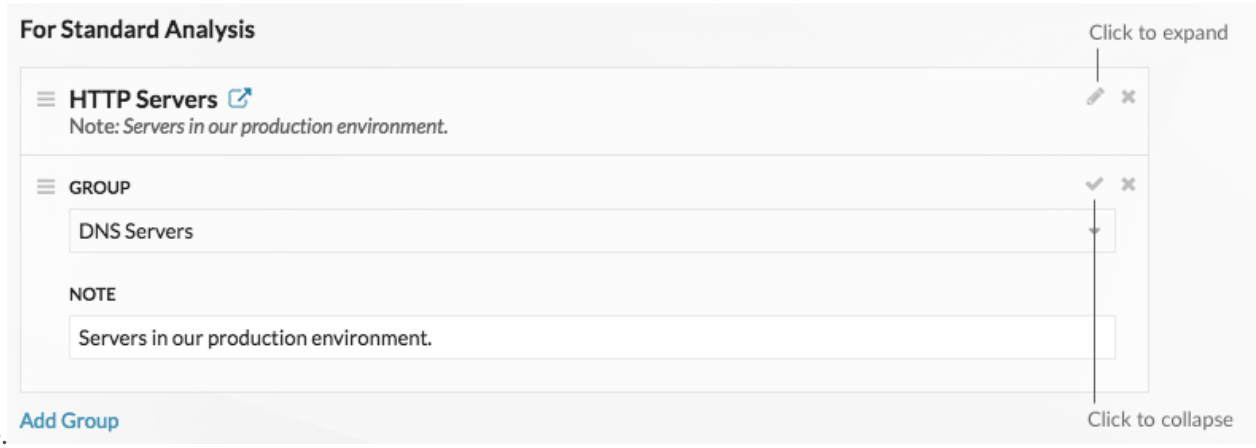
Prochaines étapes

Voici d'autres méthodes pour gérer et affiner les groupes qui reçoivent une analyse standard :

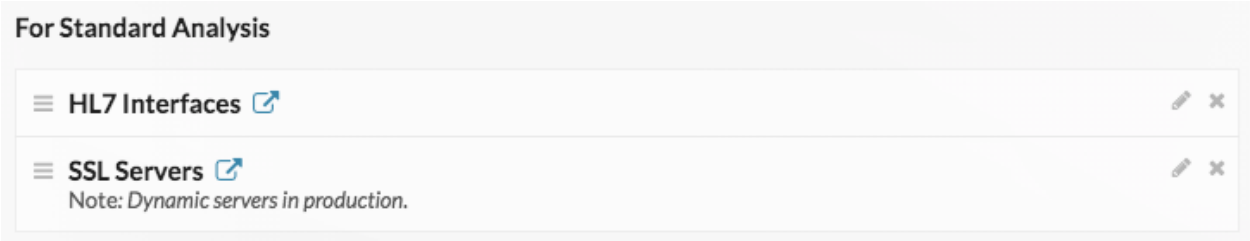
- Si vous ajoutez plusieurs groupes, les groupes sont priorisés de haut en bas. Cliquez sur l'icône en haut à gauche à côté de Groupe, puis faites glisser le groupe vers une autre position dans la liste ordonnée.



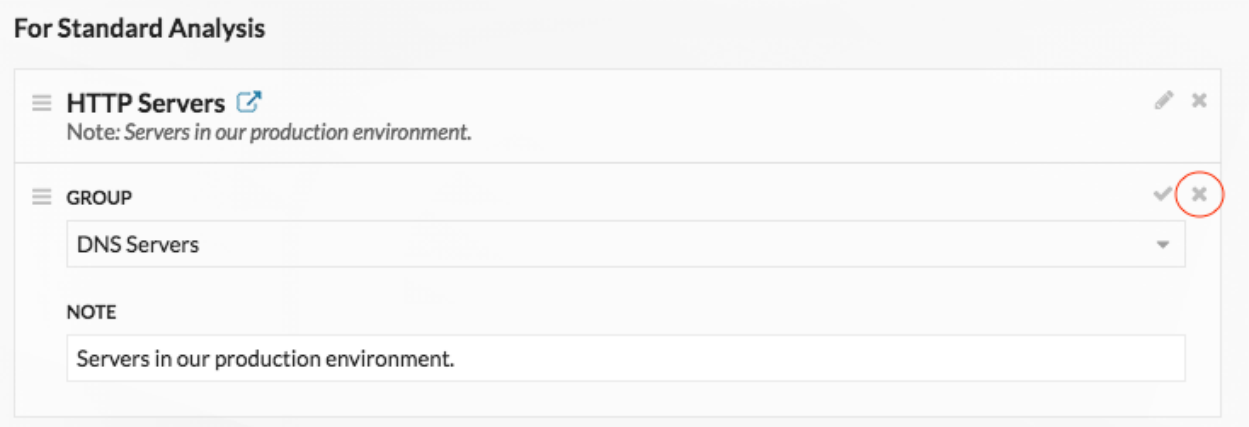
- Cliquez sur le chèque icône pour réduire le groupe. Cliquez sur le crayon icône pour développer à nouveau le groupe, comme indiqué dans la figure suivante.



- Cliquez sur le bouton « Accéder à icône à côté du nom d'un groupe pour accéder à la page du groupe d'équipements. La page des groupes d'appareils indique quels appareils et combien d'appareils font partie du groupe. L'icône n'est disponible que lorsque le groupe est réduit.



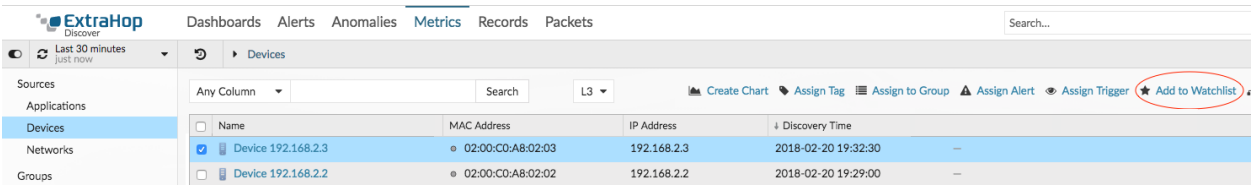
- Cliquez sur l'icône X pour supprimer un groupe de la liste, comme illustré dans la figure suivante.



Ajouter un équipement à la liste de surveillance

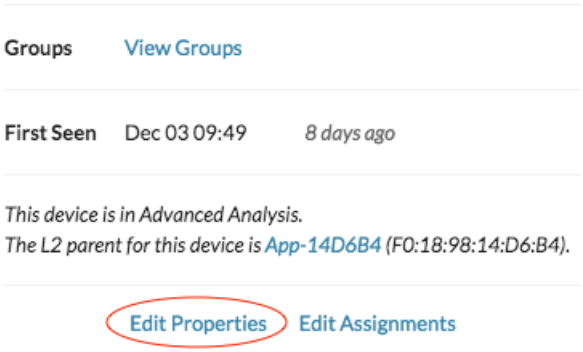
Ajoutez des appareils à la liste de surveillance pour garantir une Analyse avancée. Vous pouvez ajouter un appareil personnalisé à la liste de surveillance, mais vous ne pouvez pas ajouter d'appareil parent L2 à la liste de surveillance, sauf s'il s'agit d'une passerelle ou d'un routeur, et vous ne pouvez pas ajouter d'appareil dans Flow Analysis. Les appareils restent sur la liste de surveillance, qu'ils soient actifs ou inactifs, mais un équipement doit être actif pour que le système ExtraHop collecte des métriques d'Analyse avancée.

Conseil Au lieu d'ajouter plusieurs appareils à la liste de surveillance, créer un groupe dproximatifs d'équipements et puis donner la priorité à ce groupe pour l'Analyse avancée. Vous pouvez également ajouter plusieurs appareils à la liste de surveillance depuis la page de liste des appareils. Cochez la case à côté d'un ou de plusieurs appareils, puis cliquez sur l'icône Ajouter à la liste de suivi ★ dans le coin supérieur droit.



En savoir plus sur Priorités d'analyse.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs** puis cliquez sur **Appareils actifs** graphique.
3. Recherchez l'équipement de votre choix, puis cliquez sur son nom. La page Présentation de l'appareil apparaît. Elle affiche les mesures de trafic et de protocole associées à l'équipement.
4. Cliquez **Modifier les propriétés**.



5. Cliquez **Ajouter cet équipement à la liste de surveillance**.
6. Cliquez **Terminé**.

Votre équipement figure désormais sur la liste de surveillance. Visitez la page de la liste de suivi pour supprimer un équipement de la liste de surveillance .

Supprimer un équipement de la liste de surveillance

Vous pouvez supprimer les appareils figurant sur la liste de surveillance depuis la page des priorités d'analyse.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
   (Ces étapes doivent être effectuées sur le console ou une sonde qui est gestion de ces paramètres partagés .)
2. Accédez aux paramètres des priorités standard.
   - Sur une console, cliquez sur l'icône Paramètres système puis cliquez sur **Priorités d'analyse**. Cliquez ensuite sur **Modifier les priorités** à côté de la sonde que vous souhaitez modifier.
   - Sur une sonde, cliquez sur l'icône des paramètres système puis cliquez sur **Priorités d'analyse**.
3. En haut de page, dans Liste de surveillance pour les analyses avancées section, cliquez **Afficher la liste de surveillance**. Le Liste de surveillance la page apparaît et affiche tous les appareils de la liste de surveillance.
4. Pour supprimer des appareils de la liste de surveillance, procédez comme suit :
   a) Cochez la case à côté du nom de l'équipement.
   b) Cliquez **Supprimer des appareils**.
5. Cliquez **Enregistrer**.

Note: Il est possible d'ajouter des appareils à une liste de blocage, en fonction de leurs adresses MAC uniques, en modifiant le fichier de configuration en cours d'exécution sur le système ExtraHop. Contactez votre administrateur ExtraHop pour ajouter des appareils à une liste de blocage.

Cartes d'activités

Une carte d'activité est une représentation visuelle dynamique de l'activité du protocole L4-L7 entre les appareils de votre réseau. Vous pouvez voir une disposition 2D ou 3D des connexions des appareils en temps réel pour en savoir plus sur le flux de trafic et les relations entre les appareils.

Les cartes d'activité peuvent vous aider dans les cas d'utilisation suivants :

Effectuez une migration vers un centre de données ou vers le cloud

Dans le cadre de votre stratégie de migration, vous devez déterminer quels services peuvent être désactivés et à quel moment. Une carte dproximative des activités vous aide à identifier les appareils encore connectés afin d'éviter toute interruption de service imprévue pendant le processus de migration. Pour plus d'informations, consultez Planifiez et surveillez votre migration à l'aide de cartes d'activité procédure pas à pas.

Identifiez la cause première d'une application lente

Les applications dépendent souvent de plusieurs niveaux de services au sein d'un réseau. Une carte d'activité peut vous aider à identifier la chaîne de distribution du trafic vers votre serveur dproximatif d'applications lent. Cliquez sur un équipement pour étudier les indicateurs associés, ce qui peut permettre de mieux comprendre la cause première du ralentissement.

Suivez les appareils suspects ou les connexions inattendues

Lors d'un événement de sécurité, une carte d'activités peut vous aider à identifier les appareils concernés en suivant le trafic est-ouest en temps réel associé à un équipement suspect. Dans le cadre d'une stratégie de surveillance quotidienne de la sécurité, vous pouvez créer une carte dactivités pour vous assurer que les appareils n'établissent pas de connexions inattendues avec d'autres appareils.

Voici quelques considérations importantes concernant les cartes d'activités :

- Tu peux créer des cartes d'activités pour les appareils en mode Advanced, Standard, L2 Parent Analysis et Flow Analysis. Vous ne pouvez pas créer de carte dactivités pour les appareils en mode découverte. Pour plus d'informations, voir Priorités d'analyse.
- Si vous créez une carte dactivités pour un équipement ou un groupe déquipements qui n'a aucune activité de protocole pendant l'intervalle de temps sélectionné, la carte apparaît sans aucune donnée. Modifiez l'intervalle de temps ou votre sélection d'origine et réessayez.
- Vous pouvez créer une carte dproximative d'activités à partir d'un console pour visualiser les connexions des équipements entre tous vos capteurs.
- Tu peux enregistrer et partager une carte dactivités , accordant l'accès à la consultation ou à la modification à d'autres utilisateurs ou groupes du système. Vous pouvez également charger une carte d'activités sauvegardée pour modifier les propriétés de la carte.

Pour plus d'informations sur les cartes d'activités, consultez le FAQ sur les cartes d'activités.

Parcourez les cartes d'activités

Après création d'une carte d'activités, vous pouvez commencer à étudier les données. Les sections suivantes fournissent des détails sur la manière d'interagir avec une carte dactivitiés et de trouver des informations sur les données que vous consultez.

Disposition

Les appareils sont représentés par des cercles et les connexions par des lignes.

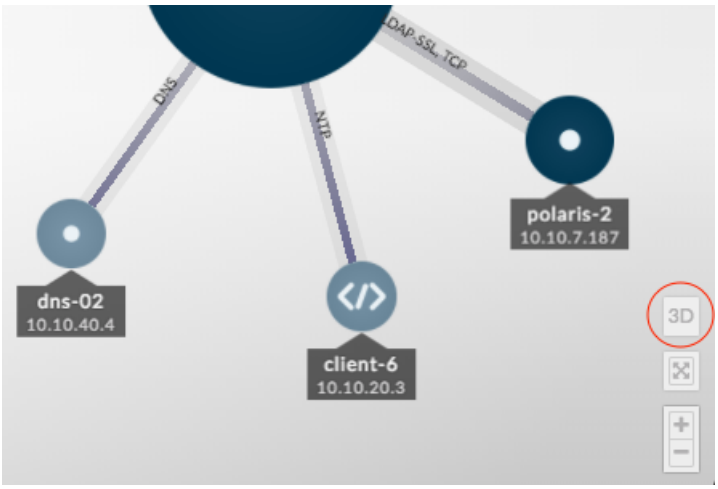
Le placement des appareils est optimisé pour afficher les informations. La mise en page peut changer à mesure que les données relatives à l'activité de l'équipement sont mises à jour en temps réel. Par exemple,

la mise en page est mise à jour à mesure que de nouvelles connexions sont observées ou que les appareils deviennent inactifs.

Note: Lorsque l'intervalle de temps indiqué dans le coin supérieur gauche de la page est défini sur Les 30 dernières minutes, les 6 dernières heures ou le dernier jour, les données de la carte dactivités sont continuellement mises à jour toutes les minutes avec des données en temps réel. Définissez un intervalle de temps personnalisé avec une heure de début et de fin spécifique pour arrêter les mises à jour de mise en page en temps réel.

Disposition 2D ou 3D

Par défaut, les cartes d'activités sont affichées dans une mise en page 2D, mais vous pouvez cliquer sur 3D pour transformer l'affichage en un modèle 3D rotatif. Par exemple, vous souhaiterez peut-être présenter des cartes 3D sur grand écran dans un réseau ou un centre des opérations de sécurité.

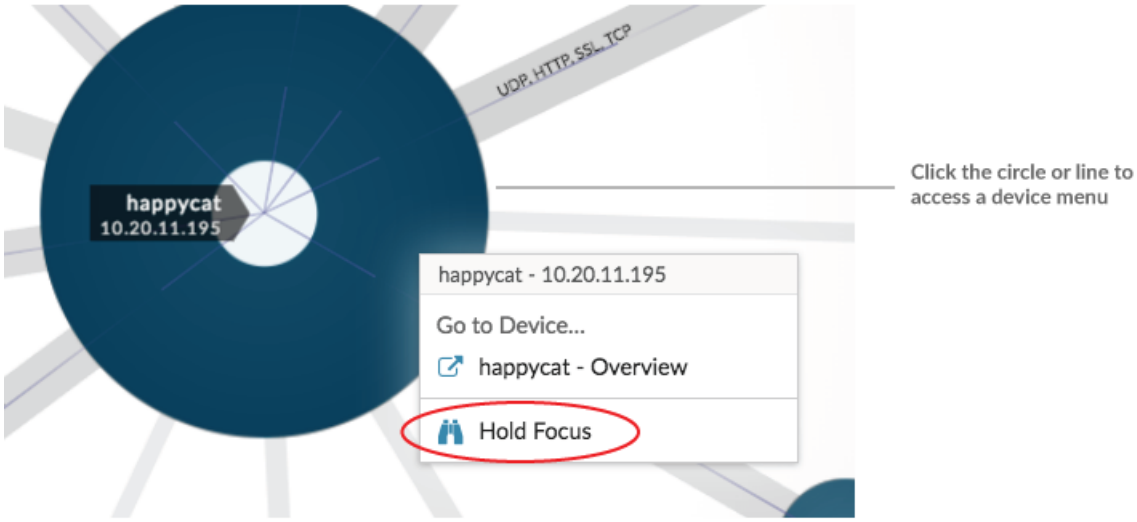


Repositionnement, rotation et zoom

Effectuez un zoom avant ou arrière sur une carte à l'aide des commandes situées dans le coin inférieur droit de la page ou zoomez avec la molette de votre souris. Cliquez et faites glisser votre souris pour repositionner une carte 2D ou faire pivoter une carte 3D.

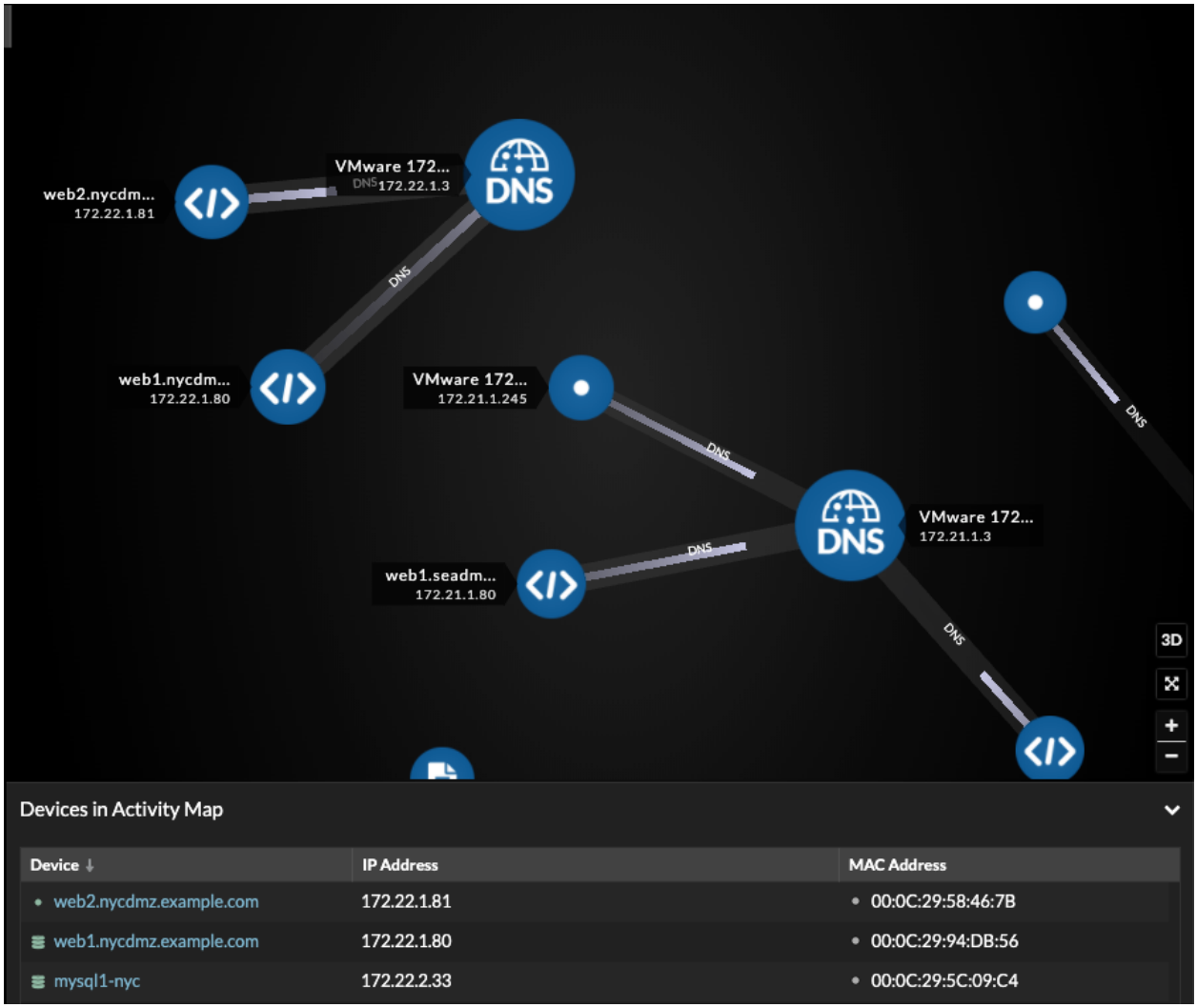
Restez concentré

Cliquez sur n'importe quel équipement et sélectionnez **Maintenez le focus**. Vous pouvez ensuite repositionner ou faire pivoter, en fonction de votre mise en page, et zoomer ou dézoomer sur la carte tout en vous concentrant sur l'équipement sélectionné et ses homologues immédiats.



Afficher la liste des équipements

Cliquez **Appareils dans la carte d'activité** au bas de la page pour afficher la liste de tous les appareils, leurs noms, adresses IP et adresses MAC. Cliquez sur le nom d'un équipement pour accéder à la page de l'équipement.

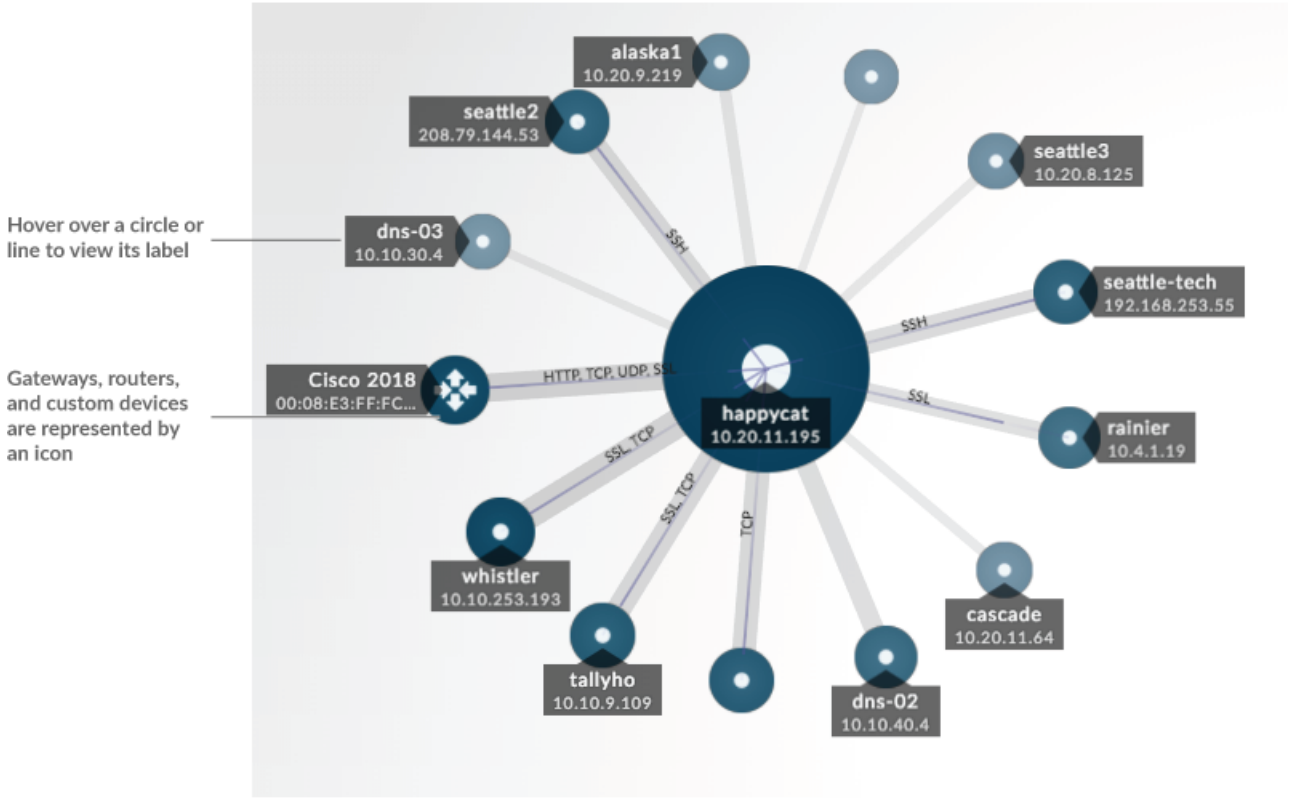


Étiquettes et icônes

Les étiquettes circulaires contiennent des informations telles que le nom d'hôte, l'adresse IP ou l'adresse MAC de l'équipement.

Les étiquettes de ligne contiennent les noms des protocoles associés à la connexion de l'équipement et à la direction du trafic circulant entre les appareils, qui sont affichés sous forme d'impulsions animées. Spécifique rôles de l'équipement sont représentés par une icône.

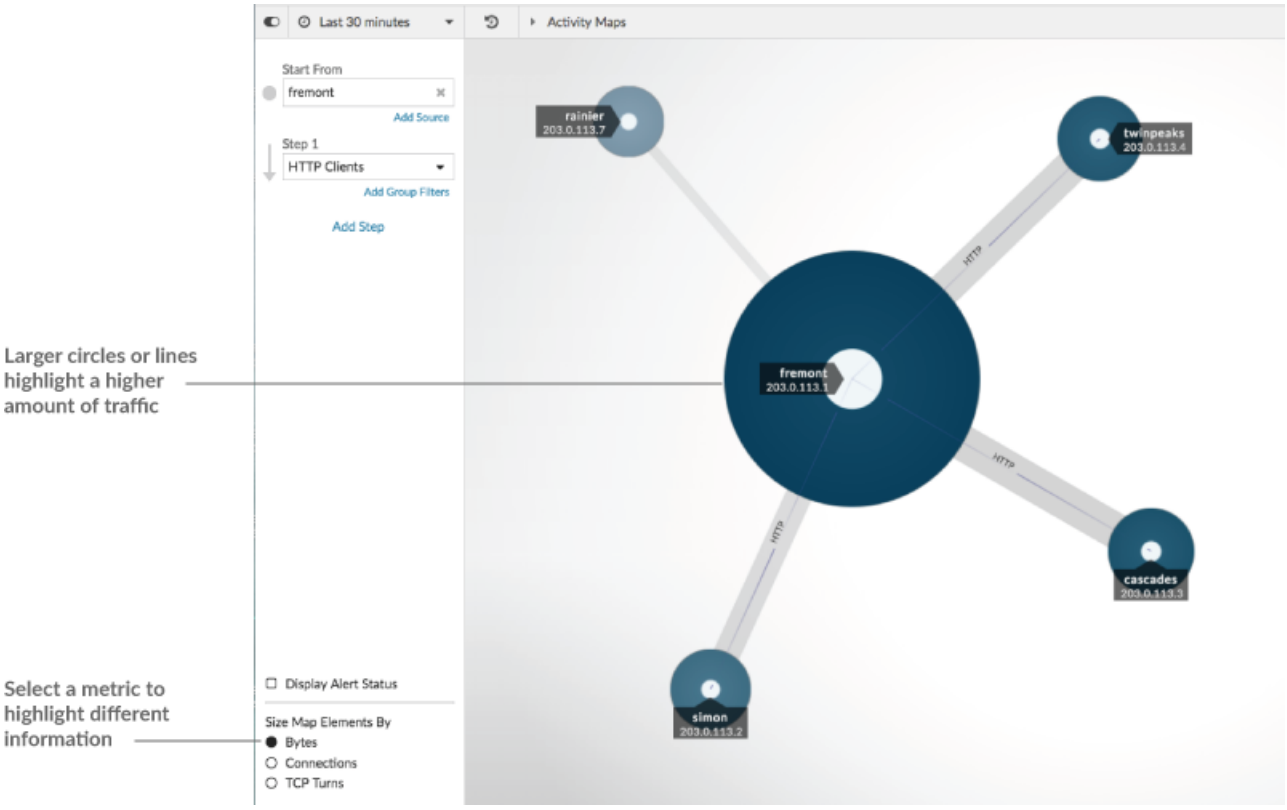
Pour optimiser l'affichage des informations, toutes les étiquettes ne sont pas affichées. Passez le pointeur de la souris sur un cercle ou une ligne pour afficher son étiquette, comme illustré dans la figure suivante.



Note: Les rôles des appareils sont automatiquement attribués à un équipement en fonction du type de trafic observé par le système ExtraHop pour cet équipement. Pour plus d'informations, voir Modifier le rôle d'un équipement.

Taille du cercle et de la ligne

La taille des objets sur la carte correspond à une valeur métrique, qui permet de mettre en évidence les zones d'activité accrue, telles que le nombre d'octets, ou le volume de trafic, associés à la connexion d'un équipement.



Au bas du volet de gauche, vous pouvez sélectionner une autre métrique pour les éléments cartographiques :

• **Octets:** Consultez tous les appareils qui transmettent ou reçoivent des données pendant l'intervalle de temps.

• **Connexions:** Afficher uniquement les appareils qui ont établi une nouvelle connexion au moins une fois pendant l' intervalle de temps.

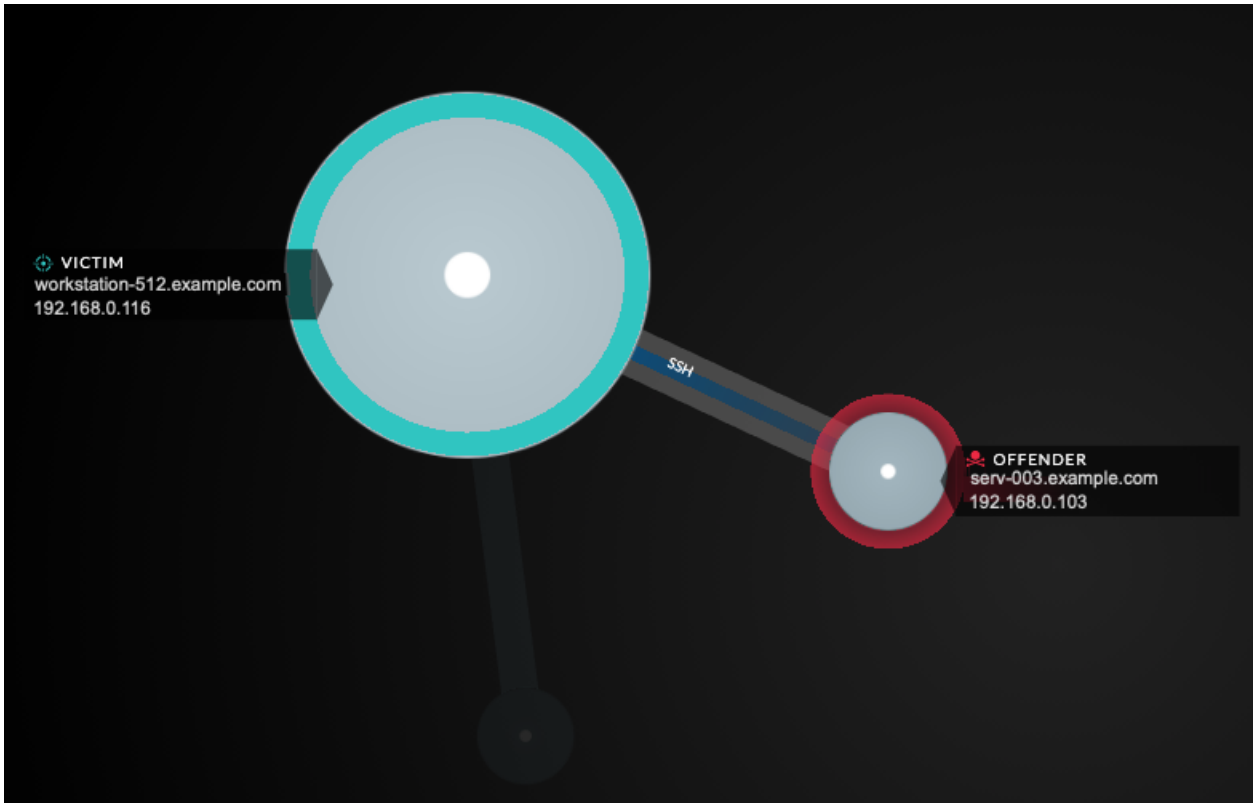
• **TCP tourne:** Consultez uniquement les appareils qui ont basculé entre la transmission et la réception de données au moins une fois pendant l'intervalle de temps.

Couleur

Le bleu et le gris sont les couleurs par défaut des cercles et des lignes. Ces couleurs par défaut sont optimisées pour afficher les informations sur une carte. Toutefois, vous pouvez appliquer différentes couleurs à votre carte pour mettre en évidence le niveau de gravité d'une alerte ou indiquer à quel moment la connexion d'un équipement a été établie.

Détections

Détections associés à un équipement sur la carte apparaissent autour du cercle sous forme d'impulsions animées, appelées marqueurs de détection. La couleur du pouls est rouge si l' équipement est le délinquant et bleu sarcelle si l'équipement est victime de la détection. Le statut du participant apparaît également sur l'étiquette de l'équipement.



Note: Les détections par apprentissage automatique nécessitent connexion aux services cloud ExtraHop.

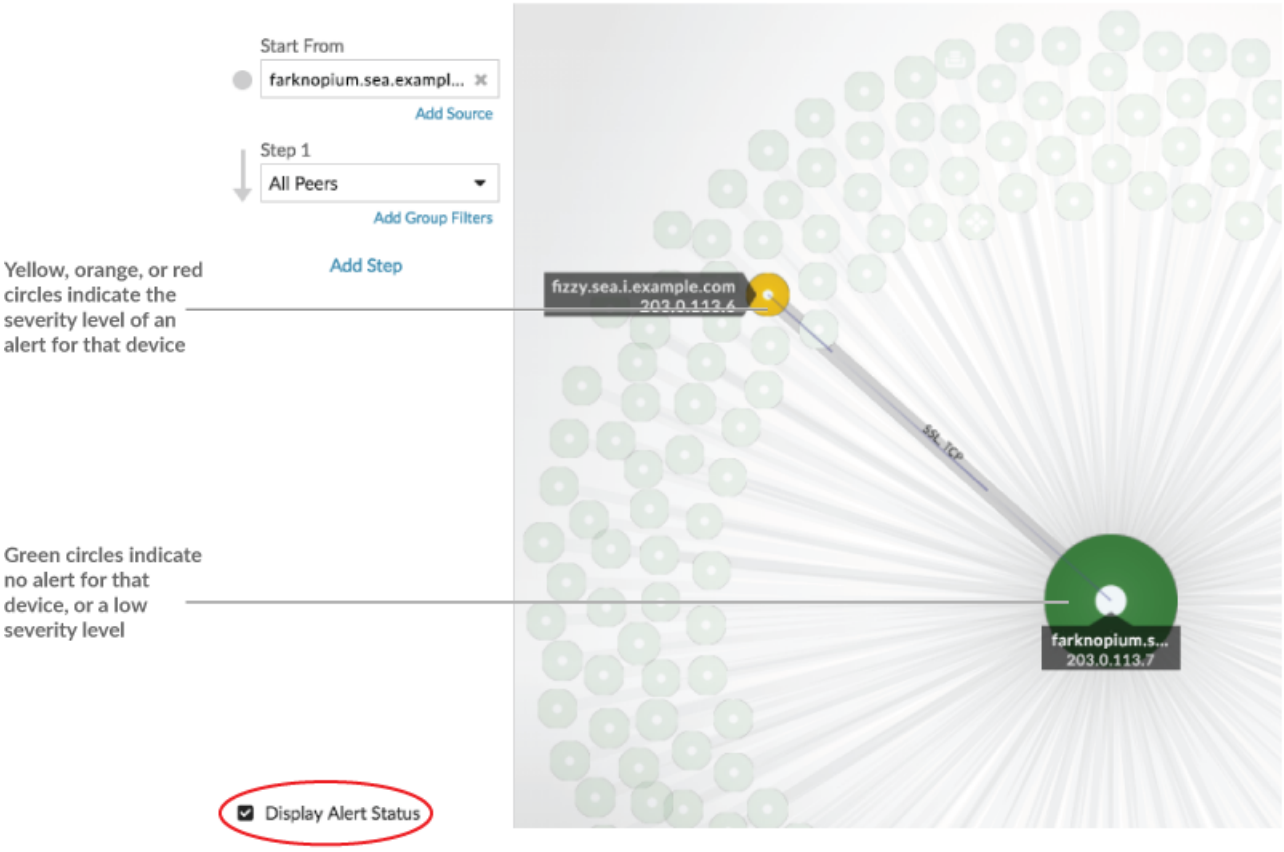
Cliquez sur un cercle avec un marqueur de détection pour afficher et naviguer vers les détections associées ou Page de présentation de l'appareil.

Si les marqueurs de détection n'apparaissent pas sur vos cartes d'activité comme prévu, ils peuvent être désactivés. Tu peux activer ou désactiver les marqueurs de détection à partir du **Utilisateur** menu.

État de l'alerte (accès au module NPM requis)

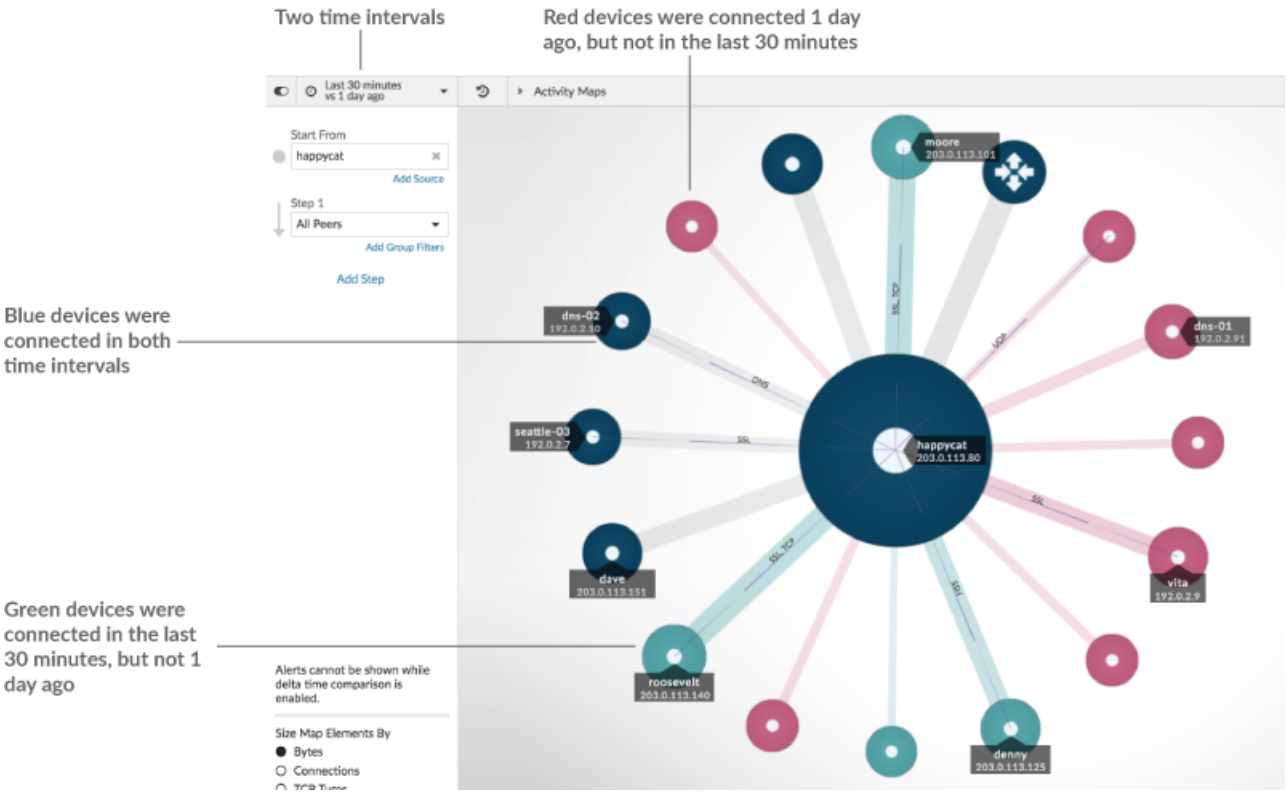
Pour voir le niveau de gravité d'une alerte pour un équipement sur votre carte, sélectionnez **Afficher le statut de l' alerte** dans le coin inférieur gauche ou sur la page, comme le montre la figure suivante. La couleur du cercle correspond alors à l'état le plus sévère pour toutes les alertes attribuées à un équipement pendant l'intervalle de temps. Si aucune alerte n'est attribuée à un équipement ou si le niveau d'alerte est informatif, la couleur du cercle par défaut est le vert.

Pour examiner l'alerte, cliquez sur le cercle, puis sélectionnez le nom de l'équipement dans Accédez à l'appareil... section. Sur la page de protocole de l'appareil, faites défiler la page jusqu'à voir la page Alertes.



Comparaison des intervalles de temps

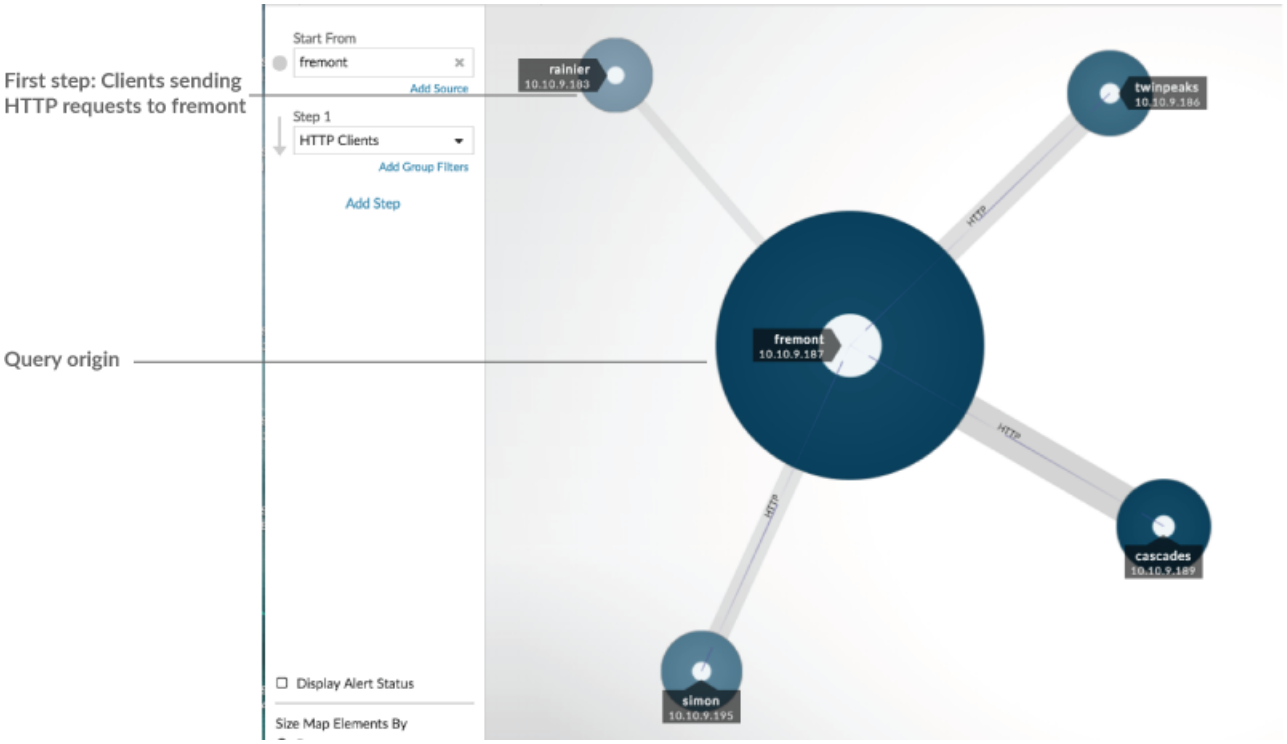
Lorsque vous comparez deux intervalles de temps pour trouver des deltas métriques, les différentes couleurs de la carte vous aident à déterminer à quel moment les connexions des équipements ont été établies ou à quel moment l'activité du protocole d'un équipement a changé. Par exemple, après avoir créé une comparaison entre **Hier** et le **Les 30 dernières minutes**, les nouvelles connexions à un équipement ou les activités qui apparaissent uniquement au cours de l'intervalle de temps le plus récent apparaissent en vert. Les connexions ou activités précédentes à l'équipement qui n'apparaissent que dans l'intervalle de temps précédent sont rouges. Les connexions des appareils qui n'ont pas changé entre les intervalles de temps sont bleues. Dans la figure suivante, les nouvelles connexions établies au cours des trente dernières minutes sont représentées par des cercles et des lignes verts.



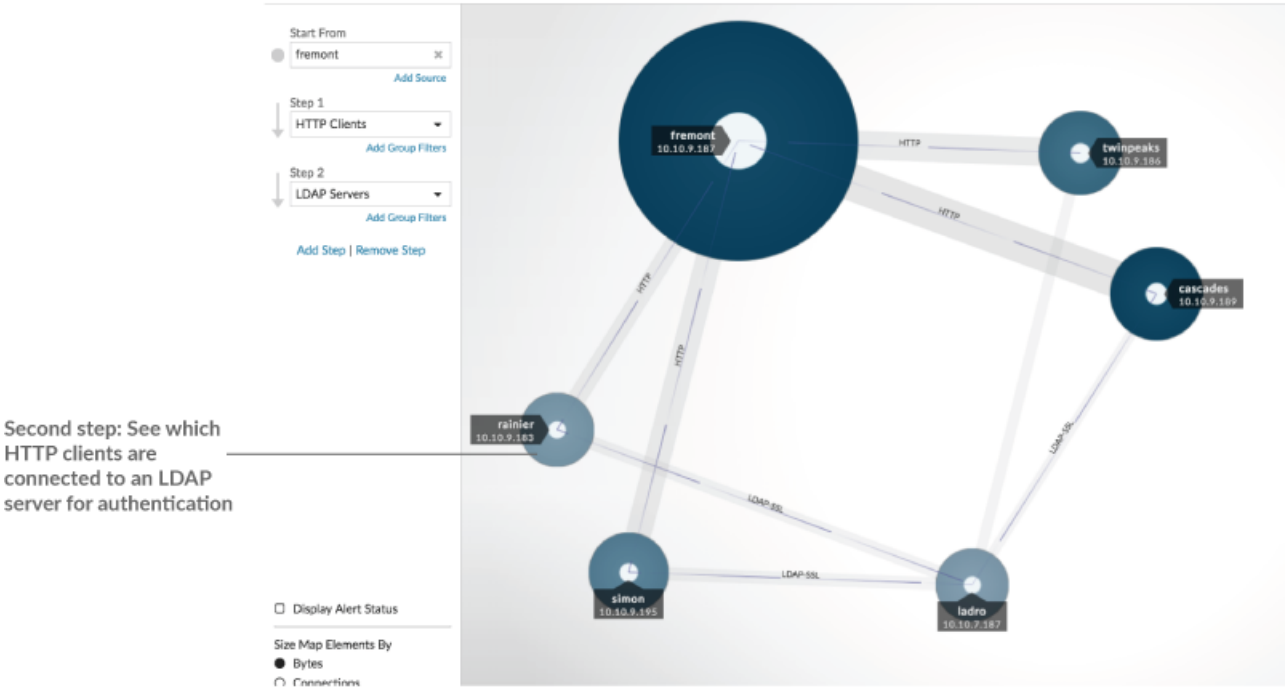
Note: Si tous les périphériques sont d'une seule couleur, par exemple le vert, cela signifie que la requête n'a pas produit de résultats dans l'intervalle de temps précédent. Par exemple, l'équipement d'origine n'avait aucune activité de protocole au cours de l'intervalle de temps précédent.

Ajouter des étapes et des filtres à une carte

Une étape est un niveau de connexions entre les appareils. Les appareils de chaque étape ont une relation avec les appareils de l'étape précédente. Ces relations sont définies par leur activité protocolaire.



Ajoutez une nouvelle étape à une carte dactivités pour ajouter une autre couche d'informations à votre carte. Cliquez sur la liste déroulante correspondant à une étape spécifique, puis sélectionnez une activité de protocole.



Vous pouvez également filtrer les appareils en une étape en fonction de leur appartenance au groupe. Par exemple, si vous sélectionnez des serveurs HTTP mais que vous souhaitez uniquement voir vos serveurs de

test sur la carte, vous pouvez filtrer les serveurs HTTP en fonction d'un groupe déquipements, tel que Mes serveurs de test.

Pour plus d'informations sur la façon d'ajouter des étapes et des filtres à une carte, voir Création d'une carte dactivitiés.

Gérez les cartes d'activités

Les options suivantes pour gérer votre carte dactivités sont disponibles dans le menu de commandes situé dans le coin supérieur droit :

- Enregistrez et partagez une carte dactivités
- Charger et gérer une carte dactivités enregistrée
- Exporter la carte dactivités sous forme de fichier PDF, PNG ou SVG

Meilleures pratiques pour étudier les données des cartes dactivités

Si vous trouvez sur votre carte un équipement qui mérite d'être étudié, plusieurs options s'offrent à vous pour recueillir plus d'informations sur cet équipement.

Trouvez les appareils récemment connectés

Cliquez sur l'intervalle de temps dans le coin supérieur gauche de la page, puis sur **Comparez**. Vous pouvez voir comment les connexions des équipements ont changé entre deux intervalles de temps différents.

Pour plus d'informations, voir Comparaison des intervalles de temps.

Accédez aux pages de protocole pour trouver l'activité métrique associée

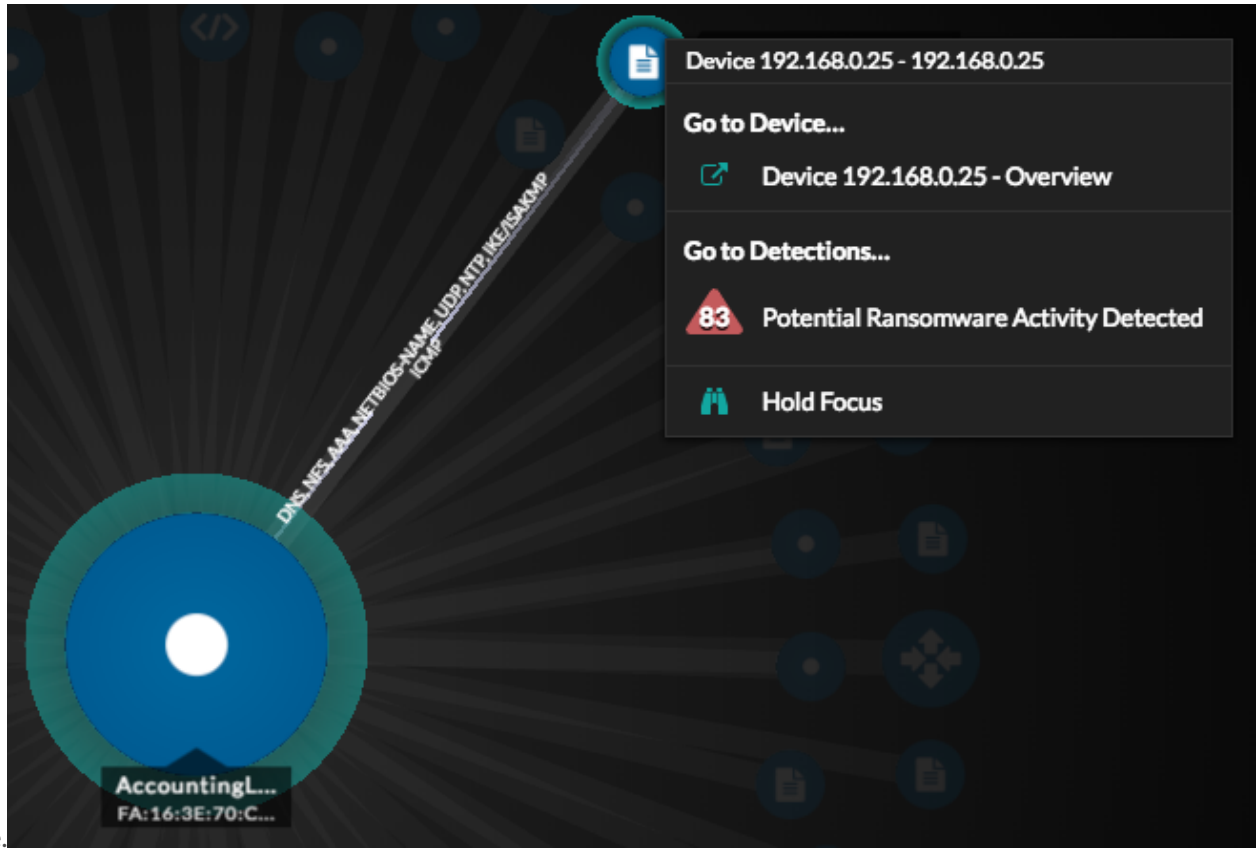
Cliquez sur un cercle ou une ligne pour accéder à un menu déroulant, comme illustré dans la figure suivante.

Sélectionnez le nom de l'équipement dans le menu pour afficher la page de présentation de l'appareil. Dans le volet de gauche, cliquez sur le nom d'un protocole pour afficher la page de protocole, qui contient un résumé des mesures de protocole importantes observées et associées à l'équipement. Sur une page de protocole, vous pouvez trouver des indicateurs connexes tels que les erreurs, les demandes, les réponses et le temps de traitement du serveur. Vous pouvez également accéder à une métrique depuis une page de protocole pour afficher les détails de la métrique, tels que l'adresse IP du serveur, l'adresse IP du client, les codes d'état, les méthodes et les URI.

Accédez aux détections identifiées sur l'équipement

Les appareils d'une carte dactivitiés associés à des détections sont affichés sous forme d'impulsions animées autour de l'étiquette circulaire. Cliquez sur un cercle avec ce

marqueur de détection pour accéder à un menu déroulant, comme illustré dans la figure suivante.



Sélectionnez un nom de détection dans le menu pour accéder à la page détaillée de cette détection. La page détaillée contient des informations sur le type de détection qui s'est produit et ce que cela signifie, ainsi que sur le moment où la détection s'est produite et la durée du problème. Pour plus d' informations, voir Page détaillée de détection.

Rechercher des enregistrements de transactions associés à une connexion (nécessite un espace de stockage des enregistrements configuré)

Cliquez sur un cercle ou une ligne pour accéder au menu déroulant. Cliquez **Enregistrements**. Une page de requête d'enregistrements s'ouvre et affiche tous les enregistrements de chaque équipement connecté, y compris tous les types d'enregistrements associés aux protocoles de connexion de l'équipement.

Création d'une carte dactivitiés

Une carte dactivités est un affichage interactif en 2D ou 3D des connexions d'équipements en temps réel basé sur l'activité des protocoles entre les appareils. Les cartes d'activité vous aident à visualiser les flux de trafic et à lancer le dépannage en fonction d'un point de données intéressant sur une carte.

Vous pouvez créer une carte d'activités pour un seul équipement actif ou un groupe d'équipements. Après avoir généré une carte de base, vous pouvez filtrer les appareils et les connexions sur votre carte.

Note: Vous pouvez créer des cartes d'activité pour les appareils dans Advanced, Standard, L2 Parent Analysis et Flow Analysis. Vous ne pouvez pas créer de carte dactivités pour les appareils en mode de découverte. Pour plus d'informations, voir Priorités d'analyse.

Créez une carte dactivitiés de base

Une carte dactivités de base vous indique une étape, ou un niveau, des connexions d'équipement entre les appareils d'origine et les appareils homologues de votre réseau.

Note: Vous pouvez créer des cartes d'activité pour les appareils dans Advanced, Standard, L2 Parent Analysis et Flow Analysis. Vous ne pouvez pas créer de carte dactivités pour les appareils en mode de découverte. Pour plus d'informations, voir Priorités d'analyse.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Actifs**.
3. Effectuez l'une des étapes suivantes en fonction du type d'origine de la carte d'activité :

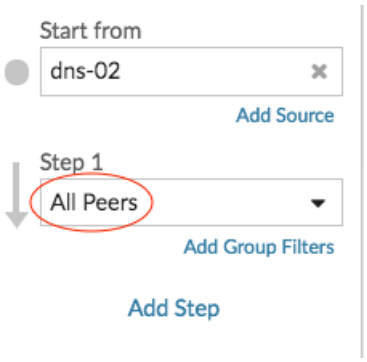
Option	Description
Pour un équipement	Cliquez **Appareils** dans le volet gauche, puis cliquez sur le nom d'un équipement individuel.
Pour un groupe d'équipements	Cliquez **Groupes d'appareils** dans le volet gauche, puis cliquez sur le nom d'un groupe déquipements.
Pour un groupe déquipements par activité de protocole	Cliquez **Activité** dans le volet gauche, puis cliquez sur le groupe de clients, de serveurs ou d'appareils correspondant au protocole de votre choix.

4. Cliquez sur l'un des liens suivants pour créer la carte dactivités :

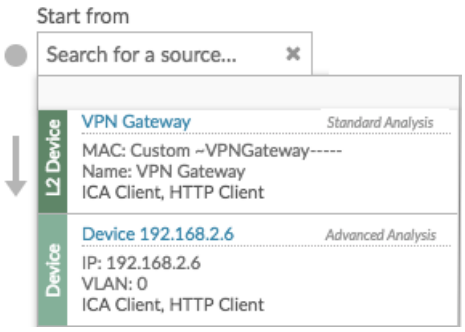
Option	Description
Pour un équipement	Cliquez **Appareils homologues**, situé en haut de la page.
Pour un groupe d'équipements	Cliquez **Carte des activités**, situé dans le coin supérieur droit de la page.

Note: Si l'équipement ou le groupe de dispositifs n'a aucune activité de protocole pendant l'intervalle de temps spécifié, la carte dactivités apparaît sans aucune donnée. Modifiez l'intervalle de temps ou votre sélection d'origine et réessayez.

5. À partir de la carte dactivités, filtrez les connexions par activité du protocole en effectuant les étapes suivantes :
   a) Cliquez sur la liste déroulante dans Étape 1 section du volet gauche, comme illustré dans la figure suivante.

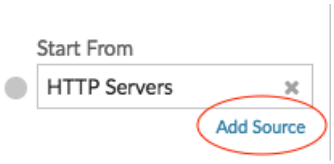


   b) En haut de la liste déroulante, recherchez et sélectionnez une activité et un rôle de protocole. Vous pouvez effectuer plusieurs sélections.
   c) Cliquez n'importe où en dehors de la liste déroulante.
6. Optionnel : Modifiez l'équipement d'origine principal en effectuant les étapes suivantes :
   a) Dans le Commencez à partir de dans le volet de gauche, cliquez sur le nom de l'équipement ou du groupe. Une liste déroulante apparaît.



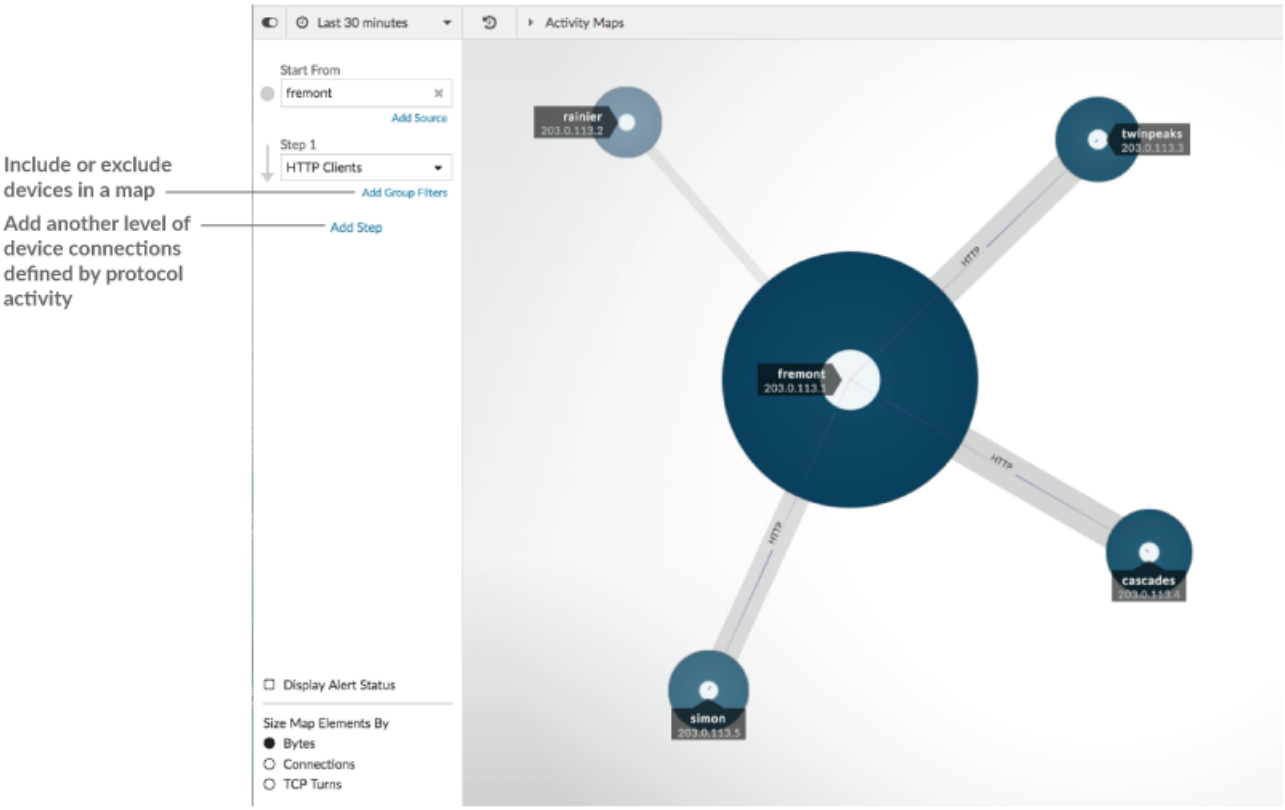
b) Recherchez et sélectionnez un autre équipement ou groupe pour mettre à jour dynamiquement l'origine de la carte que vous consultez.

7. Optionnel : Créez un groupe ad hoc de sources pour étudier rapidement le trafic provenant de plusieurs appareils sur la même carte. Cliquez **Ajouter une source**.



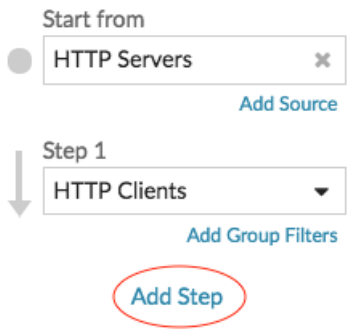
Ajoutez des connexions et filtrez les appareils sur votre carte

Pour mieux comprendre le trajet du trafic entre les appareils d'origine et les appareils en aval, vous pouvez ajouter des étapes supplémentaires à votre carte. Vous pouvez également créer des filtres pour inclure ou exclure des appareils de la carte. La figure suivante montre comment ajouter des étapes et créer des filtres.

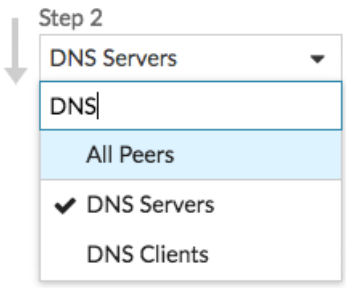


Ajoutez un autre niveau de connexions aux équipements
Une étape définit le niveau de connexion entre les appareils d'une carte. Les appareils de chaque étape ont une relation avec les appareils de l'étape précédente. Ces relations sont définies par leur activité protocolaire. Vous pouvez ajouter jusqu'à 5 étapes pour voir comment le trafic circule d'un équipement à l'autre.

1. Cliquez **Ajouter une étape**, comme le montre la figure suivante. **Tous les pairs** est sélectionné par défaut.



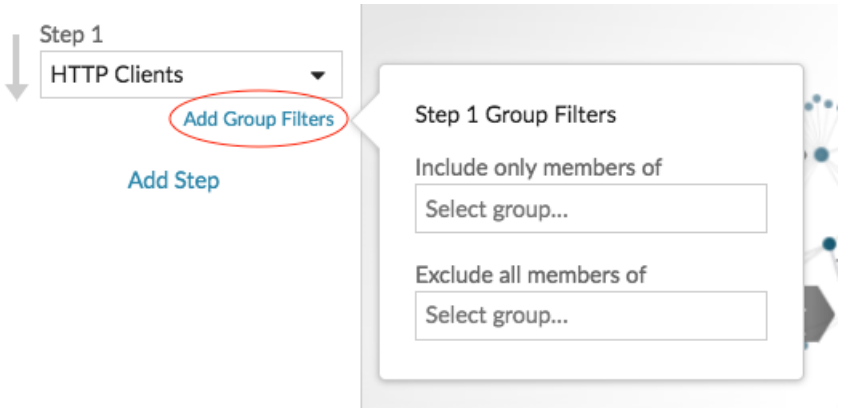
2. En haut de la liste déroulante, recherchez et sélectionnez une activité et un rôle de protocole. Vous pouvez effectuer plusieurs sélections.



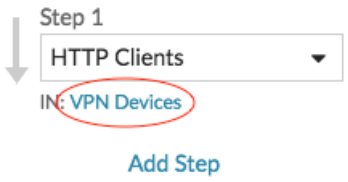
3. Cliquez n'importe où en dehors de la liste déroulante.

Inclure ou exclure des appareils
Vous pouvez filtrer les appareils en une étape en fonction de leur groupe d'équipements adhésion.

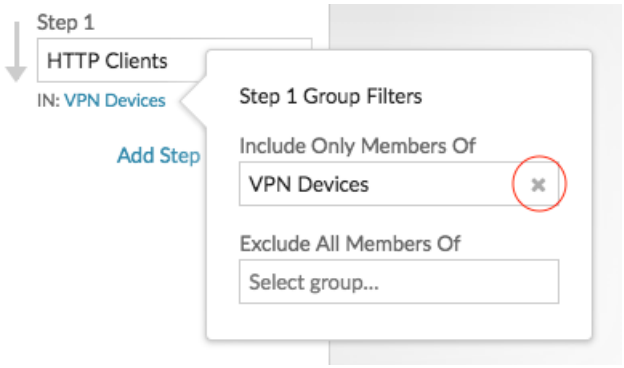
1. Cliquez **Ajouter un filtre de groupe**.



2. Cliquez sur une liste déroulante pour rechercher et sélectionner un groupe déquipements.
3. Cliquez n'importe où en dehors du menu des filtres pour appliquer vos filtres.
4. Pour supprimer ou modifier un filtre, procédez comme suit :
   a) Cliquez sur le nom du groupe d'équipements.



   b) Modifiez le filtre en cliquant sur la liste déroulante, puis en sélectionnant un autre groupe de déquipements.
   c) Supprimez le filtre en cliquant sur **x** icône, comme illustré dans la figure suivante.



d) Cliquez n'importe où en dehors du menu des filtres pour appliquer les mises à jour de vos filtres.

Prochaines étapes

- Enregistrez et partagez une carte dactivités

Enregistrez et partagez une carte dactivités

Vous pouvez enregistrer une carte dactivités et la partager avec d'autres personnes. Par défaut, toutes les cartes d'activité que vous créez sont privées, ce qui signifie qu'aucun utilisateur d'ExtraHop ne peut voir ou modifier votre carte. Cependant, vous pouvez partager votre carte lorsque vous l'enregistrez en accordant l'accès à la vue ou à la modification à d'autres utilisateurs et groupes d' ExtraHop.

Voici quelques points importants à prendre en compte concernant le partage de cartes d'activités :

- La manière dont un utilisateur interagit avec une carte dactivités et les informations qu'il peut consulter dans le système ExtraHop sont déterminées par les privilèges de l'utilisateur, qui sont attribués par l'administrateur ExtraHop. Pour plus d'informations, consultez le Privilèges utilisateur section du guide des administrateurs d' ExtraHop.
- Lorsque vous accordez un accès de modification à un utilisateur, celui-ci peut modifier et partager la carte d'activité avec d'autres personnes. Toutefois, les autres utilisateurs ne peuvent pas supprimer la carte dactivités. Seul le propriétaire de la carte peut supprimer une carte d'activités.
- Les informations de groupe sont importées dans le système ExtraHop depuis LDAP (tel qu'OpenLDAP ou Active Directory). Les informations utilisateur sont disponibles une fois qu'un utilisateur ExtraHop se connecte à son compte.
- Si vous supprimez un utilisateur, vous aurez la possibilité de transférer ses cartes d'activité à un autre utilisateur.

Les étapes suivantes vous indiquent comment enregistrer et partager une carte dactivités :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Création d'une carte dactivitiés.
3. Cliquez sur l'icône Enregistrer dans le coin supérieur droit de la page.
4. Tapez le nom de votre carte. Le nom doit être unique.
5. Optionnel : Entrez une description.
6. Optionnel : Changez le shortcode du permalien en un nom convivial.

   Par exemple, vous pouvez configurer une carte pour afficher les statuts des alertes et ajouter « /alerts » au shortcode pour indiquer aux utilisateurs que la carte enregistrée affiche les alertes par défaut.

   Note: Le shortcode ne peut pas contenir d'espaces et le shortcode doit être unique.

7. Partagez votre carte dactivités en suivant les étapes suivantes :
   a) Entrez un nom d'utilisateur ou un groupe.
   b) Effectuez l'une des sélections suivantes :

Type d'accès	Sélection
Les utilisateurs d'ExtraHop peuvent voir	Sélectionnez **Peut voir** puis cliquez sur **Ajouter**.
Les utilisateurs d'ExtraHop peuvent à la fois afficher et modifier	Cliquez **Peut voir** puis cliquez sur **Peut modifier**. Cliquez **Ajouter**.

8. Cliquez **Enregistrer**.

Conseil Vous pouvez également modifier les propriétés d'une carte enregistrée en cliquant sur le menu de commandes ⋮ puis en cliquant **Propriétés de la carte**. Pour modifier rapidement les autorisations de partage, cliquez sur le menu de commandes ⋮ puis cliquez sur **Partagez**.

Prochaines étapes

- Si vous avez partagé votre carte, copiez l'URL complète de la carte depuis votre navigateur, puis envoyez l'URL aux utilisateurs ayant accès à votre carte.
- Charger et gérer une carte dactivités enregistrée.
- Supprimer ou modifier l'accès à une carte dactivités

Supprimer ou modifier l'accès à une carte dactivités

Vous pouvez supprimer ou modifier l'accès à une carte dactivités que vous avez accordée aux utilisateurs et aux groupes. Vous devez d'abord créer une carte d'activités pour accéder aux options permettant de modifier les cartes d' activités enregistrées.

1. Création d'une carte dactivitiés, puis cliquez sur l'icône Ouvrir 🗁 dans le coin supérieur droit de la page.
2. Cliquez sur le nom de la carte dactivitiés.
3. Dans la section Partage, effectuez l'une des étapes suivantes :
   - Pour supprimer l'accès à des utilisateurs ou à des groupes, cliquez sur le bouton rouge Supprimer **x** icône à côté du nom de l'utilisateur ou du groupe.
   - Pour modifier l'accès d'un utilisateur ou d'un groupe existant, cliquez sur **Peut voir** ou **Peut modifier**, puis effectuez une autre sélection.
   - Pour ajouter un nouvel utilisateur ou un nouveau groupe, recherchez le nom d'utilisateur et cliquez dessus. Cliquez **Peut voir** ou **Peut modifier**, puis cliquez sur **Ajouter**.
4. Cliquez **Enregistrer**.

Charger et gérer une carte dactivités enregistrée

Vous pouvez afficher, mettre à jour ou supprimer des cartes d'activité enregistrées. Tout d'abord, vous devez créer une nouvelle carte pour accéder à une liste de cartes enregistrées et partagées.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Création d'une carte dactivitiés, puis cliquez sur l'icône Ouvrir 🗁 dans le coin supérieur droit de la page.
3. Choisissez l'une des options de carte dactivités suivantes :
   - Pour charger une carte, cliquez sur son nom. Si vous souhaitez modifier puis enregistrer à nouveau la carte, apportez vos modifications, puis cliquez sur **Enregistrer** icône.

     Conseil Vous pouvez également modifier les propriétés d'une carte enregistrée en cliquant sur le menu de commandes ⋮ puis en cliquant **Propriétés de la carte**.
   - Pour supprimer une carte, cliquez sur **Supprimer** à côté du nom de la carte.

Note: Les utilisateurs doivent disposer de privilèges pour afficher ou interagir avec les cartes d'activité. Voir Privilèges utilisateur dans le guide des administrateurs d' ExtraHop.

Détections

Le système ExtraHop applique des techniques d'apprentissage automatique et une surveillance basée sur des règles à vos données Wire Data afin d'identifier les comportements inhabituels et les risques potentiels pour la sécurité et les performances de votre réseau.

Avant de commencer
Les utilisateurs doivent être autorisés privilèges pour afficher les détections.

Lorsqu'un comportement anormal est identifié, le système ExtraHop génère une détection et affiche les données et les options disponibles. Les contrôles de la page Détections font apparaître des détections qui sont recommandé pour le triage et vous aider filtrer et trier vos points de vue, afin que vous puissiez vous concentrer rapidement sur les détections liées aux systèmes critiques en premier lieu.

Grâce à l'accès au module NPM, les détections peuvent vous aider à maintenir votre réseau de la manière suivante :

- Collectez des données exploitables de haute qualité pour identifier les causes profondes des problèmes de réseau.
- Identifiez les problèmes inconnus liés aux performances ou à l'infrastructure.

Grâce à l'accès au module NDR, les détections peuvent vous aider à défendre votre réseau de la manière suivante :

- Identifiez les comportements malveillants associés à différentes catégories d'attaques ou techniques MITRE.
- Consultez les détections associées ou créez les vôtres investigation pour regrouper les détections et suivre les campagnes d'attaques potentielles.
- Signalez les adresses IP, les noms d'hôte et les URI suspects identifiés par les renseignements sur les menaces .
- Mettez en évidence les meilleures pratiques en matière de renforcement de la sécurité.

En savoir plus sur optimisation des détections.

Important: Bien que les détections puissent vous informer sur les risques de sécurité et les problèmes de performances, elles ne remplacent pas la prise de décisions ou l'expertise concernant votre réseau. Révisez toujours sécurité et performance détections visant à déterminer la cause première d'un comportement inhabituel et à quel moment prendre des mesures.

Vidéos: Consultez les formations associées :

- Détections de sécurité
- Détections de performances

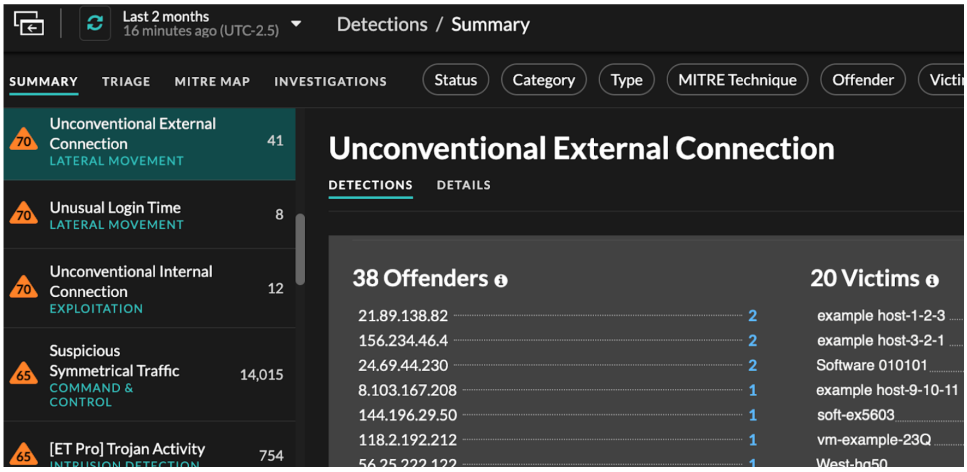
Affichage des détections

Dans le coin supérieur gauche de la page des détections, quatre options permettent de visualiser les détections : Résumé, Triage, Carte MITRE et Investigations. Ces options fournissent chacune une vue unique de votre liste de détections.

Résumé

Par défaut, les détections de la page Détections apparaissent dans la vue récapitulative, qui regroupe les informations relatives aux détections afin de mettre en évidence les modèles d'activité dans votre environnement. Vous pouvez trier et regrouper votre liste de détections dans la vue récapitulative afin de vous concentrer sur les types de détection les plus fréquents et sur les participants les plus actifs.

Note: Par défaut, le **Ouvert** le filtre d'état est appliqué au Détections page. Cliquez sur le **Ouvert** filtre pour accéder à d'autres options de filtre.



Tri des détections dans la vue récapitulative

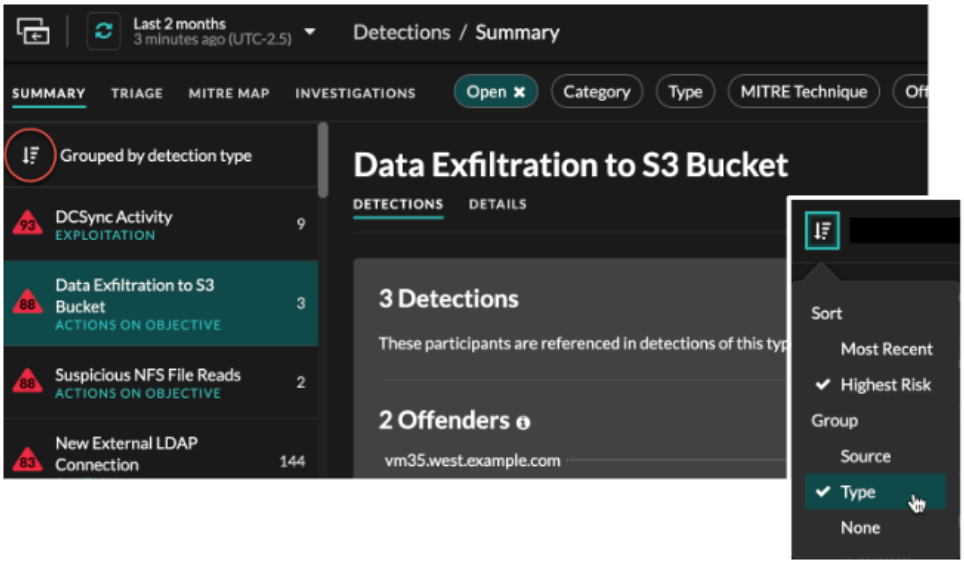
Vous pouvez trier les détections en fonction de l'indice de risque le plus élevé ou de l'événement le plus récent.

Une fois triées par score de risque, les détections qui sont recommandé pour le triage apparaissent en premier, suivies des détections présentant l'indice de risque le plus élevé.

Une fois triés par **Le plus récent**, les détections dont l' heure de fin est la plus récente apparaissent en premier. Si deux détections sont toujours en cours, la détection dont l'heure de mise à jour est la plus récente apparaît en premier. Cliquez sur l'icône de tri au-dessus de la liste des détections pour sélectionner une option.

Regroupement des détections dans la vue récapitulative

Vous pouvez regrouper les détections par type de détection (tel que Spike dans les sessions SSH) ou par source de détection (telle que l'adresse IP du délinquant), ou vous pouvez choisir de ne pas regrouper du tout votre liste de détections.



Grouper par type

Lorsque vous regroupez la vue récapitulative par **Type**, vous pouvez consulter des listes de valeurs associées aux détections survenues pendant l'intervalle de temps sélectionné, telles que les participants, les propriétés de détection ou les localisations du réseau.

Vous pouvez cliquer sur les valeurs des participants pour en savoir plus sur cet équipement ou cette adresse IP. Cliquez sur n'importe quelle valeur pour afficher uniquement les détections associées à cette valeur, ou suivre toutes les détections associées.

Les participants

Répertorie tous les délinquants et toutes les victimes du type de détection sélectionné. Les listes des délinquants et des victimes sont classées en fonction du nombre de détections dans lesquelles le participant apparaît.

Valeurs des propriétés

Répertorie les valeurs des propriétés associées au type de détection. La liste des valeurs de propriété est ordonnée en fonction du nombre de détections dans lesquelles la valeur de propriété apparaît.

Localités du réseau

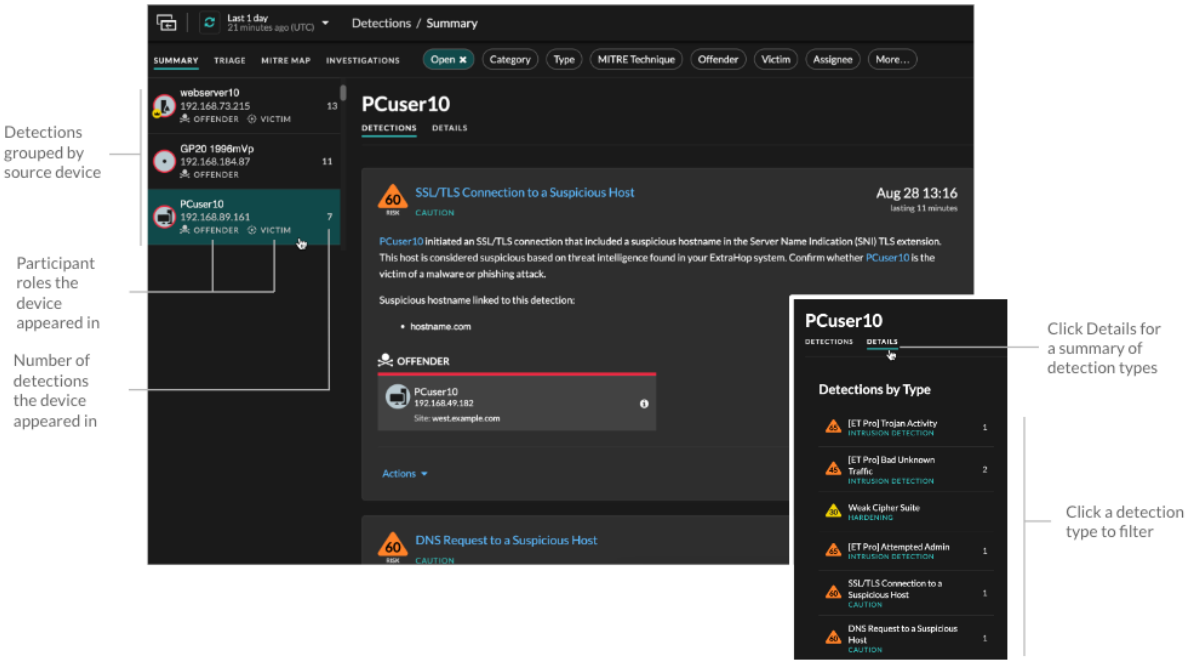
Répertorie les localités du réseau qui contiennent des détections du type sélectionné . La liste des localités du réseau est ordonnée en fonction du nombre de détections dans la localité du réseau.

Au bas du panneau récapitulatif se trouvent des liens qui vous permettent de suivre toutes les détections inclus dans le résumé. Tu peux créer une règle de réglage pour masquer toutes les détections incluses dans le résumé ou afficher les détections masquées de ce type de détection.

Vous pouvez faire défiler le panneau récapitulatif pour afficher les cartes de détection individuelles. Des détections qui sont recommandé pour le triage apparaissent en premier.

Grouper par source

Lorsque vous regroupez la vue récapitulative par source, vous pouvez afficher les participants à l'origine d'une détection, le nombre de détections étant affiché à côté du nom du participant. Cliquez sur une source pour afficher les détections dans lesquelles l'équipement est apparu en tant que délinquant ou en tant que victime. Cliquez **Détails** sous le nom de l'équipement pour afficher la liste des types de détection dans lesquels l'équipement est apparu, puis cliquez sur un type de détection pour filtrer selon ce type de détection.



Grouper par aucun

Lorsque vous regroupez par **Aucune** sur la page Détections, vous pouvez consulter un graphique chronologique du nombre total de détections identifiées dans l'intervalle de temps sélectionné. Chaque barre horizontale du graphique représente la durée d'une seule détection et est codée par couleur en fonction de l'indice de risque.

- Cliquez et faites glisser pour surligner une zone du graphique afin de zoomer sur une plage de temps spécifique. Les détections sont répertoriées pour le nouvel intervalle de temps.
- Passez le curseur sur une barre pour afficher l'indice de risque de détection.
- Cliquez sur une barre pour accéder directement à la page détaillée de détection.

Sous la chronologie, un organigramme affiche le nombre de détections associées à chaque catégorie d'attaque. Les catégories sont regroupées dans une chaîne dattacks qui décrit la progression des mesures prises par un attaquant pour atteindre son objectif, comme le vol de données sensibles. Cliquez sur une catégorie d' attaque pour afficher uniquement les détections correspondant à cette catégorie.

Triage

(module NDR uniquement) La vue Triage affiche les détections qu'ExtraHop recommande pour le triage sur la base d'une analyse contextuelle des facteurs de votre environnement, également connue sous le nom de Smart Triage.

Les fiches de détection recommandées pour le triage sont marquées d'une étiquette jaune et répertorient les facteurs qui ont conduit à la recommandation.

Implique un actif de valeur élevée

L'actif fournit une authentification ou des services essentiels, ou un actif qui était identifié manuellement comme valeur élevée.

Implique un délinquant de haut niveau

L'équipement ou l'adresse IP ont participé à de nombreuses détections et à divers types de détection.

Implique un type de détection rare

Le type de détection n'a jamais été récemment apparu dans votre environnement. Des types de détection peu courants peuvent indiquer un comportement malveillant unique.

Implique un nom d'hôte ou une adresse IP suspects

Le nom d'hôte ou l'adresse IP est référencé dans une collecte des menaces qui est activé sur votre système.

Implique une investigation recommandée

La détection fait partie d'une chaîne dproximative d'attaques dans un investigation recommandée.

Les détections recommandées pour le triage sont classées par ordre de priorité dans la vue Résumé et apparaissent en haut de votre liste de détections, quel que soit le tri.

Tu peux détections de filtres pour afficher uniquement les détections recommandées pour le triage et inclure Recommandé pour le triage comme critère pour un règle de notification.

Voici quelques considérations concernant les recommandations relatives au triage :

- Les recommandations basées sur des actifs de valeur élevée sont limitées à un maximum de cinq détections du même type de détection sur une période de deux semaines.
- Deux semaines de données provenant des sondes sont nécessaires avant que des recommandations ne soient formulées en fonction des principaux facteurs de détection ou des facteurs de détection rares.
- Recommandations basées sur renseignement sur les menaces sont limités à deux détections du même type de détection, pour le même indicateur de compromission, sur une période de trente jours.

Carte MITRE

Cliquez sur **Carte MITRE** voir si vous souhaitez afficher vos détections par technique d'attaque.

Chaque vignette de la matrice représente une technique d'attaque issue de la matrice MITRE ATT&CK® pour les entreprises. Si une vignette est surlignée, la détection associée à cette technique s'est produite pendant l'intervalle de temps sélectionné. Cliquez sur n'importe quelle vignette pour voir les détections correspondant à cette technique.

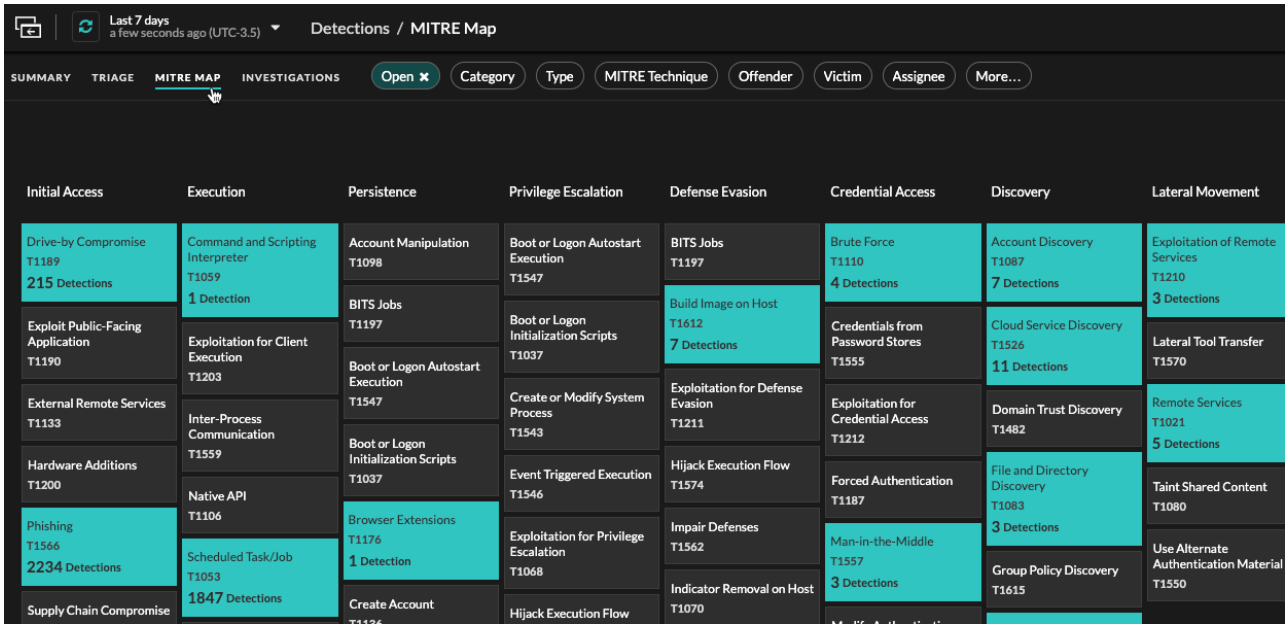


Tableau des enquêtes

La vue Enquêtes affiche toutes les enquêtes créées par l'utilisateur et recommandées qui ont été créées pendant l'intervalle de temps sélectionné.

Cliquez sur le nom d'une enquête pour l'ouvrir. En savoir plus sur Enquêtes.

Détections de filtrage

Vous pouvez filtrer la page Détections pour afficher uniquement les détections qui correspondent à vos critères spécifiés. Par exemple, vous ne serez peut-être intéressé que par les détections d'exfiltration effectuées via HTTP ou par les détections associées à des participants qui sont des serveurs importants.

État

Vous pouvez filtrer les détections ayant un statut de détection spécifique, tel que Reconnu, En cours ou Fermé. Par défaut, **Ouvrir** le filtre d'état est appliqué au Détections page. Cliquez sur **Ouvrir** filtre pour accéder à d'autres options de filtrage.

Vous pouvez sélectionner le **Caché** statut pour afficher uniquement les détections qui sont actuellement masqué par règles d'exceptions.

Catégorie

Vous pouvez filtrer par détection d'attaque ou de performance, ou vous pouvez sélectionner une catégorie plus spécifique pour affiner votre affichage de la page Détections. Lorsque vous cliquez sur le filtre de catégorie, la plupart des catégories sont répertoriées sous **Toutes les catégories d'attaques** et **Toutes les catégories de performance** les options sont triées en fonction du nombre de détections dans la catégorie. Les détections renforcées apparaissent toujours à la fin de la liste.

Les détections d'attaques incluent les catégories suivantes qui correspondent aux phases de la chaîne d'attaque.

Commande et contrôle

Un serveur externe qui a établi et maintenu la connexion à un équipement compromis de votre réseau. Les serveurs C&C peuvent envoyer des programmes malveillants, des commandes et des charges utiles pour soutenir l'attaque. Ces détections permettent de savoir quand un équipement interne communique avec un système distant qui semble agir comme un serveur C&C.

Reconnaissance

Un attaquant cherche des cibles de grande valeur et des faiblesses à exploiter. Ces détections permettent d'identifier les scans et les techniques d'énumération.

Note: Les détections peuvent identifier un scanner de vulnérabilité connu tel que Nessus et Qualys. Cliquez sur le nom de l'équipement pour vérifier s'il est déjà doté d'un rôle d'analyseur de vulnérabilités dans le système ExtraHop. Pour savoir comment masquer les détections liées à ces appareils, voir Détections de syntonisation.

Exploitation

Un attaquant profite d'une vulnérabilité connue de votre réseau pour exploiter activement vos actifs. Ces détections permettent d'identifier les comportements inhabituels et suspects associés aux techniques d'exploitation.

Mouvement latéral

Un attaquant s'est infiltré dans votre réseau et se déplace d'un équipement à l'autre à la recherche de cibles de plus grande valeur. Ces détections identifient le comportement inhabituel des équipements associé aux transferts de données et aux connexions du corridor est-ouest.

Actions par rapport à l'objectif

L'attaquant est sur le point d'atteindre son objectif, qui peut aller du vol de données sensibles au chiffrement de fichiers contre rançon. Ces détections permettent de savoir quand un attaquant est sur le point d'atteindre un objectif de campagne.

Mise en garde

Soulignez les activités qui ne présentent pas de menace imminente pour les opérations, mais qui doivent être traitées pour maintenir une posture de sécurité saine. Ces détections permettent également d'identifier les activités de participants suspects associées à des renseignements sur les menaces.

Rendement les détections incluent les catégories suivantes.

Authentification et contrôle d'accès

Mettez en évidence les tentatives infructueuses des utilisateurs, des clients et des serveurs pour se connecter ou accéder aux ressources. Ces détections identifient les problèmes Wi-Fi potentiels liés aux protocoles d'authentification, d'autorisation et d'audit (AAA), les erreurs LDAP excessives ou découvrent des appareils aux ressources limitées.

Base de données

Mettez en évidence les problèmes d'accès des applications ou des utilisateurs sur la base de l'analyse des protocoles de base de données. Ces détections identifient les problèmes de base de données, tels que les serveurs de base de données qui envoient un nombre excessif d'erreurs de réponse susceptibles de ralentir ou d'échouer des transactions.

Virtualisation des ordinateurs de bureau et des applications

Soulignez les longs temps de chargement ou les sessions de mauvaise qualité pour les utilisateurs finaux. Ces détections identifient des problèmes d'application, tels qu'un nombre excessif de Zero Windows, ce qui indique qu'un serveur Citrix est dépassé.

Infrastructure réseau

Mettez en évidence les événements inhabituels via les protocoles TCP, DNS et DHCP. Ces détections peuvent révéler des problèmes DHCP qui empêchent les clients d'obtenir une adresse IP auprès du serveur, ou révéler que les services n'ont pas pu résoudre les noms d'hôte en raison d'erreurs de réponse DNS excessives.

Dégradation du service

Soulignez les problèmes de service ou la dégradation des performances associés aux protocoles de voix sur IP (VoIP), de transfert de fichiers et de communication par courrier électronique. Ces détections peuvent indiquer des dégradations de service en cas d'échec des appels VoIP et fournir le code d'état SIP correspondant, ou indiquer que des appelants non autorisés ont tenté de faire plusieurs demandes d'appel.

Rangement

Soulignez les problèmes d'accès des utilisateurs à des fichiers et à des partages spécifiques détectés lors de l'évaluation du trafic du système de fichiers réseau. Ces détections peuvent indiquer que les utilisateurs n'ont pas pu accéder à des fichiers sur des serveurs Windows en raison de problèmes SMB, ou que les serveurs de stockage rattaché au réseau (NAS) n'ont pas pu être atteints en raison d'erreurs NFS.

Application Web

Soulignez les mauvaises performances du serveur Web ou les problèmes observés lors de l'analyse du trafic via le protocole HTTP. Ces détections peuvent indiquer que des problèmes internes au serveur sont à l'origine d'un nombre excessif d'erreurs de niveau 500, empêchant ainsi les utilisateurs d'accéder aux applications et aux services dont ils ont besoin.

Durcissement les détections identifient les risques de sécurité et les opportunités d'améliorer votre posture de sécurité.

Durcissement

Soulignez les meilleures pratiques de renforcement de la sécurité qui devraient être appliquées pour atténuer le risque d'exploitation. Ces détections identifient les possibilités d' améliorer la sécurité de votre réseau, par exemple en empêchant l'exposition des informations d'identification et en supprimant les certificats TLS expirés des serveurs. Après avoir cliqué sur une détection renforcée, vous pouvez appliquer des filtres supplémentaires pour afficher les détections spécifiques correspondant à ce type de détection renforcée. En savoir plus sur filtrage et réglage (durcissement, détections).

Système de détection d'intrusion (IDS) les détections identifient les risques de sécurité et les comportements malveillants.

Détection d'intrusion

Mettez en évidence le trafic réseau qui correspond à des signatures connues de pratiques dangereuses, à des tentatives d'exploitation et à des indicateurs de compromission liés à des programmes malveillants et à des activités de commande et de contrôle.

Important: Alors que les détections IDS incluent des liens vers des paquets pour tous les types de protocoles, les liens vers des enregistrements ne sont disponibles que pour les protocoles L7.

Tapez

Filtrez votre liste de détection en fonction d'un type de détection spécifique, tel que l'exfiltration de données ou les certificats de serveur SSL expirés. Vous pouvez également saisir un numéro d'identification CVE dans ce filtre pour afficher uniquement les détections relatives à une vulnérabilité de sécurité publique spécifique.

Technique MITRE

Mettez en évidence les détections qui correspondent à des identifiants de techniques MITRE spécifiques. Le framework MITRE est une base de connaissances largement reconnue sur les attaques.

Délinquant et victime

Les paramètres du délinquant et de la victime associés à une détection sont appelés participants. Vous pouvez filtrer votre liste de détection pour n'afficher que les détections concernant un participant spécifique, par exemple un délinquant dont l'adresse IP distante est inconnue ou une victime qui est un serveur important. Les périphériques de passerelle ou d'équilibrage de charge associés à des participants au point de terminaison externe peuvent également être spécifiés dans ces filtres.

Cessionnaire

Filtrez les détections effectuées par l'utilisateur affecté à la détection.

Plus de filtres

Vous pouvez également filtrer vos détections selon les critères suivants :

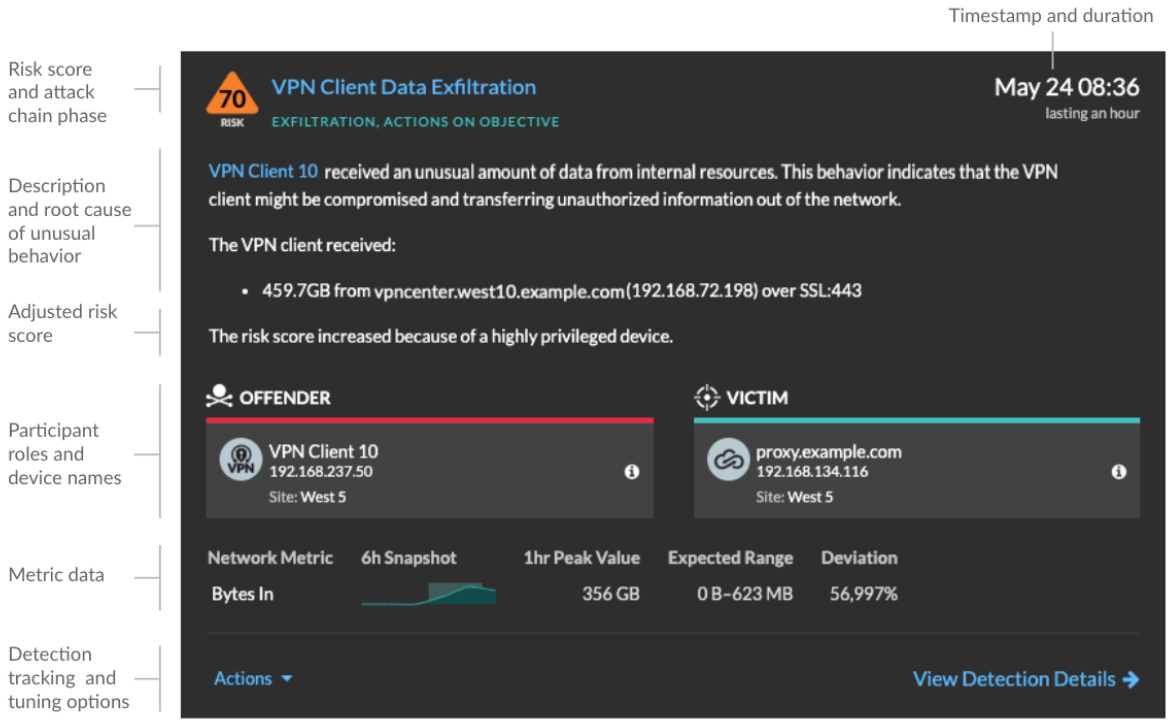
- Recommandé pour le triage
- Rôles des appareils
- Source
- Site (console uniquement)
- Filtre d'identification des tickets (suivi des billets par des tiers uniquement)
- Score de risque minimum

Naviguer dans les détections

Après avoir sélectionné la manière d'afficher, de regrouper et de filtrer votre liste de détections, cliquez sur n'importe quelle carte de détection pour accéder à la page détaillée de la détection.

Cartes de détection

Chaque carte de détection identifie la cause de la détection, la catégorie de détection, la date à laquelle la détection a eu lieu, ainsi que les participants à la victime et au délinquant. Les détections de sécurité incluent un indice de risque.



Score de risque

Mesure les probabilité, complexité et impact commercial d'une détection de sécurité. Ce score fournit une estimation basée sur des facteurs relatifs à la fréquence et à la disponibilité de certains vecteurs d'attaque par rapport au niveau de compétence requis d'un pirate informatique potentiel et aux conséquences d'une attaque réussie. L'icône est codée par couleur selon la gravité : rouge (80-99), orange (31-79) ou jaune (1-30).

Les participants

Identifie chaque participant (délinquant et victime) impliqué dans la détection par nom d'hôte ou adresse IP. Cliquez sur un participant pour afficher les informations de base et accéder aux liens. Les points de terminaison internes affichent un lien vers la page de présentation de l'appareil ; les terminaux externes affichent la géolocalisation de l'adresse IP, liens de recherche de point de terminaison tels que ARIN Whois et un lien vers la page détaillée de l'adresse IP. Si un participant est passé par un autre équipement tel qu'un équilibreur de charge ou une passerelle, le participant et l'équipement sont affichés sur la carte de participant, mais seul le point de terminaison d'origine est considéré comme un participant .

Note: Le déchiffrement TLS est requis pour afficher les points de terminaison d'origine si le protocole HTTPS est activé. En savoir plus sur Décryptage TLS.

Lors du regroupement par **Tapez**, un panneau récapitulatif apparaît sous le type de détection. Il détaille les détections par délinquant et par victime et vous permet de appliquer des filtres pour les participants.

Lors du regroupement par **Source**, les icônes de rôle de l'équipement interne sont surlignées en rouge si l' appareil était un délinquant lors d'une détection et en bleu sarcelle s'il s'agissait d'une victime. Vous pouvez cliquer **Détails** sous le nom de la source pour afficher un résumé des détections auxquelles cette source était participante. Ces informations relatives à l'équipement sont affichées à côté de la carte de détection sur de grands écrans (1 900 pixels ou plus).

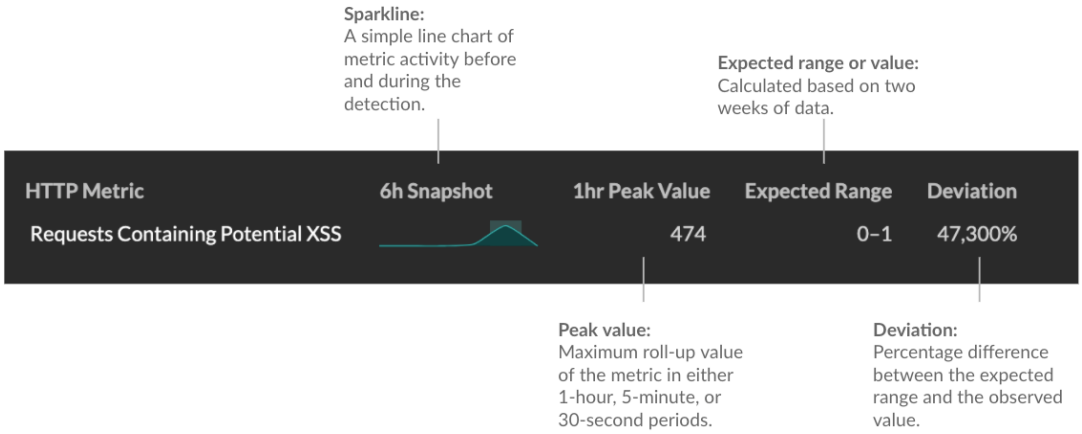
Durée

Identifie la durée pendant laquelle le comportement inhabituel a été détecté ou affiche EN COURS s'il se produit actuellement.

Les détections qui mettent en évidence les meilleures pratiques en matière de renforcement de la sécurité affichent deux dates : la première fois et la dernière fois que la violation a été identifiée.

Données métriques

Identifie des données métriques supplémentaires lorsque le comportement inhabituel est associé à une métrique ou à une clé spécifique. Si les données métriques ne sont pas disponibles pour la détection, le type d'activité anormale du protocole apparaît.



Gestion de la détection

Tu peux piste ou syntoniser la détection dans la liste déroulante Actions, ou cliquez sur **Afficher les détails de détection** pour accéder à la page détaillée de la détection.

Page détaillée de détection

La plupart des données dont vous avez besoin pour comprendre et valider une détection apparaissent sur la page détaillée de la détection : tableaux contenant les données métriques pertinentes, transactions d'enregistrement et liens vers des paquets bruts.

Les informations de la carte de détection sont suivies de toutes les sections disponibles pour la détection. Ces sections varient en fonction du type de détection.

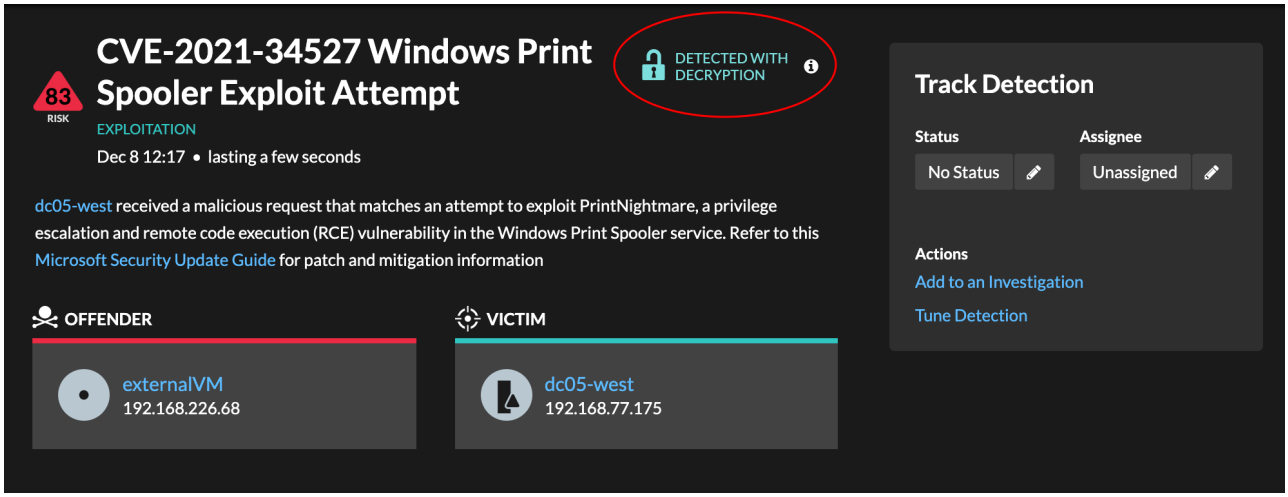
Détection de traces

Tu peux piste ou syntoniser la détection, ou cliquez sur **Ajouter à une enquête** pour inclure la détection dans un nouveau système ou dans un système existant investigation.

Si vous avez configuré un Intégration à CrowdStrike sur votre système ExtraHop, vous pouvez initier le confinement des appareils CrowdStrike qui participent à la détection. (RevealX 360 uniquement.)

Badge de déchiffrement

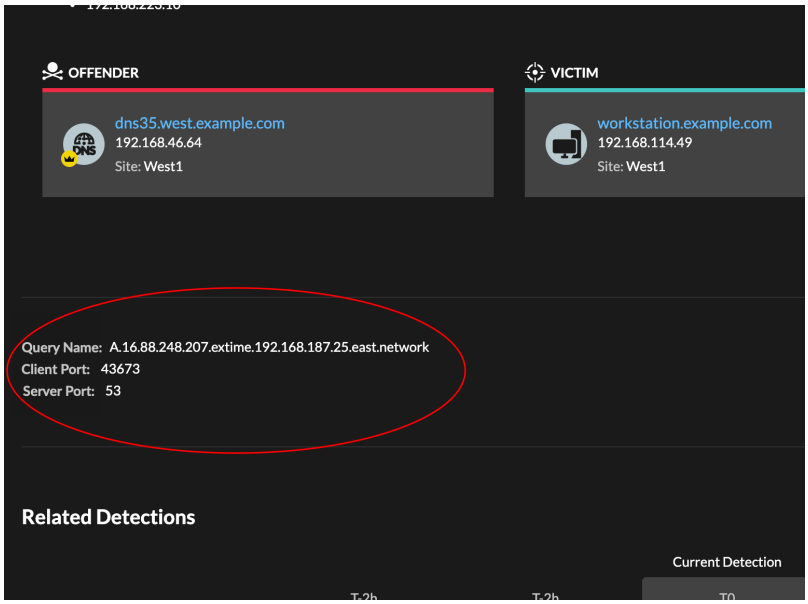
Lorsque le système ExtraHop identifie un comportement suspect ou une attaque potentielle dans les enregistrements de trafic déchiffrés, la page détaillée de la détection affiche un badge de déchiffrement à droite du nom de la détection.



En savoir plus sur Décryptage TLS et déchiffrement du trafic à l'aide d'un contrôleur de domaine Windows.

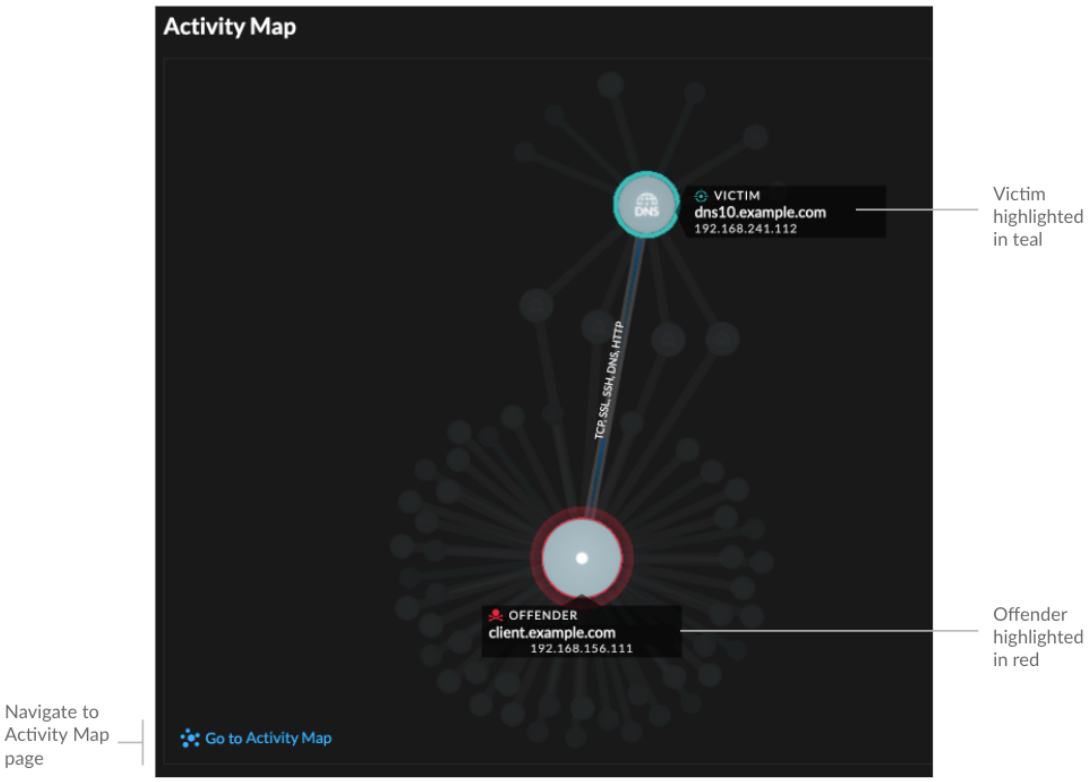
Propriétés de détection

Fournit une liste des propriétés pertinentes pour la détection. Par exemple, les propriétés de détection peuvent inclure une requête, un URI ou un outil de piratage au cœur de la détection.



Carte des activités

Fournit une carte d'activités qui met en évidence les participants impliqués dans la détection. La carte d'activité affiche le trafic est-ouest du protocole associé à la détection afin de vous aider à évaluer l'ampleur de l'activité malveillante. Cliquez sur la victime ou le délinquant pour accéder à un menu déroulant contenant des liens vers la page de présentation de l'appareil et d'autres détections auxquelles l'équipement est un participant.



Données de détection et liens

Fournit des données supplémentaires associées à la détection à examiner. Les types de données peuvent inclure des mesures connexes, des liens vers enregistrement des requêtes sur les transactions et un lien vers une page générale paquets requête. La disponibilité des métriques, des enregistrements et des paquets varie en fonction de la détection. Par exemple, les détections IDS incluent des liens vers des paquets pour tous les types de protocoles, mais les liens vers des enregistrements ne sont disponibles que pour les protocoles L7 .

Les données métriques et les transactions d'enregistrement sont affichées dans des tableaux. Dans un tableau de mesures, cliquez sur l'icône pour consulter les transactions d'enregistrement associées. Dans un tableau d'enregistrements, cliquez sur l'icône pour afficher la requête de paquet associée à une transaction.

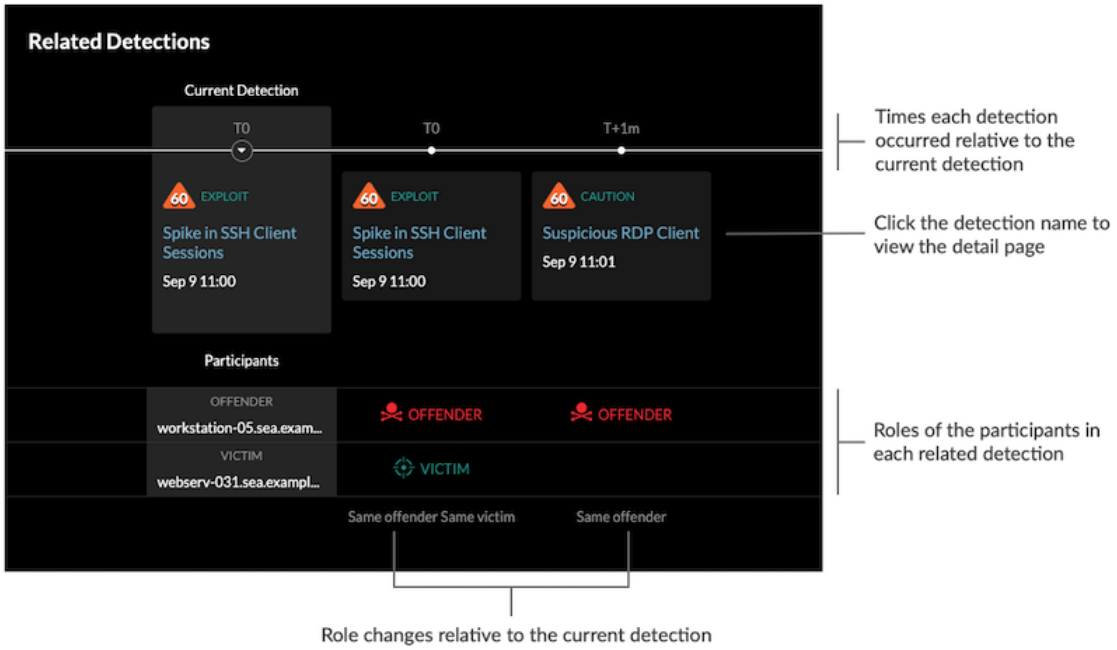
Note: UNE espace de stockage des enregistrements doit être configuré pour afficher les transactions et en continu PCAP doit être configuré pour télécharger des paquets.

Comparez les comportements

Fournit un graphique qui montre l'activité du délinquant à côté de l' activité d'appareils similaires au cours de la période au cours de laquelle la détection a eu lieu. Le graphique apparaît pour les détections liées à l'activité non conventionnelle d'un équipement et met en évidence les comportements inattendus en les affichant à côté du comportement des appareils du réseau ayant des propriétés similaires.

Détections associées

Fournit une chronologie des détections liées à la détection actuelle qui peut vous aider à identifier une campagne d'attaque plus importante. Les détections associées incluent le rôle du participant, la durée, l'horodateur et tout changement de rôle si le délinquant lors d'une détection devient la victime d'une autre détection. Cliquez sur une détection associée dans la chronologie pour afficher la page détaillée de cette détection.

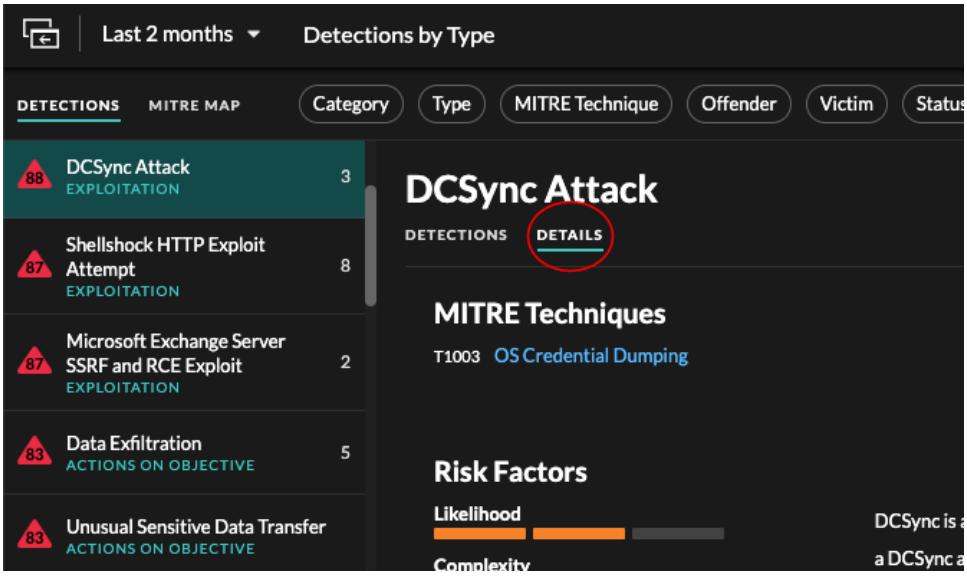


Détections associées incluses dans un investigation recommandée sont signalés par des liens dorés et peuvent être cliqués pour accéder à la page d'investigation.

Détails de détection

Fournit une description détaillée de la détection, notamment les techniques MITRE associées, les facteurs de risque, les antécédents et les diagrammes des attaques, les options d'atténuation et des liens de référence vers des organisations de sécurité telles que MITRE.

Ces informations sont affichées à côté de la carte de détection sur de grands écrans, ou vous pouvez y accéder en cliquant **Détails** sous le titre de la détection lorsque vous regroupez la page Détection par **Types**.



Pour certains types de détection, un Comment fonctionne ce détecteur La section fournit des réponses aux questions fréquemment posées sur les raisons pour lesquelles une détection apparaît dans votre système ExtraHop.

Conseil : Vous pouvez détection des partages pages détaillées avec d'autres utilisateurs d'ExtraHop.

Catalogue de détection

Le catalogue de détection fournit une liste complète de tous les types de détection du système ExtraHop, y compris les types de détection actuellement inactifs ou en cours de révision. Vous pouvez également gérer les types de détection personnalisés à partir de la page Catalogue des détections.

Vous pouvez accéder à la page du catalogue de détection en cliquant sur l'icône Paramètres du système.

Outre le nom d'affichage et l'auteur, vous pouvez filtrer la liste des types de détection par ID, statut, catégorie, techniques MITRE associées au type de détection et types de détection prenant en charge les données du flux capteurs.

Cliquez sur une détection créée par ExtraHop pour afficher le Paramètres du type de détection panneau, qui affiche le nom du type de détection, l'identifiant, l'auteur, l'état actuel du type de détection, la date à laquelle le type de détection a été mis en production pour la première fois (si disponible) et les catégories associées. Pour en savoir plus sur la détection, cliquez **Détails du type de détection**.

État du type de détection

Ce statut indique si une détection est disponible dans votre environnement.

Actif

Les types de détection actifs sont disponibles pour tous les capteurs et peuvent générer des détections dans votre environnement.

Inactif

Les types de détection inactifs ont été supprimés de tous les capteurs et ne généreront plus de détections. Lorsqu'un type de détection devient inactif, les détections existantes de ce type seront continuer à afficher.

En révision

Dans Review, les types de détection sont évalués sur un nombre limité de systèmes ExtraHop avant d'être disponibles pour tous les capteurs. Ces types de détection passent un examen approfondi en termes d'efficacité et de précision avant d'être mis à la disposition d'un nombre croissant de capteurs. La période de révision peut durer plusieurs semaines. Une fois l'examen terminé, l'état du type de détection passe à Actif.

Voici quelques points importants à prendre en compte pour déterminer si des détections d'un certain type sont visibles dans votre environnement :

- Si les détections actives ne s'affichent pas comme prévu, le type de détection peut nécessiter déchiffrement ou peut ne pas prendre en charge les capteurs de flux (RevealX 360 uniquement).
- Les systèmes RevealX Enterprise doivent être connectés à Services cloud pour recevoir des mises à jour fréquentes du catalogue de détection. Sans connexion aux services cloud, les mises à jour sont retardées jusqu'à ce que le firmware soit mis à jour.

Détections personnalisées

Vous pouvez consulter et gérer les détections personnalisées à partir de la page Catalogue des détections.

- Pour créer un type de détection personnalisé, cliquez sur **Créez** dans le coin supérieur droit de la page. L'ID du type de détection pour le nouveau type de détection doit correspondre à l'ID inclus dans le déclencheur de détection personnalisé. En savoir plus sur création d'une détection personnalisée.
- Pour modifier une détection personnalisée, cliquez sur la détection et modifiez le nom d'affichage, l'auteur, les catégories de détection et les techniques MITRE associées dans le Modifier le type de détection panneau. Vous ne pouvez pas modifier les détections dont ExtraHop est répertorié comme auteur.
- Pour supprimer une détection personnalisée, cliquez sur la détection, puis sur **Supprimer** à partir du Paramètres du type de détection panneau.
- Les détections personnalisées affichent toujours un tiret (-) sous État.

Enquêtes

(module NDR uniquement) Les enquêtes vous permettent d'ajouter et de visualiser plusieurs détections sur une seule chronologie et une seule carte. L'affichage d'un résumé des détections connectées peut vous aider à déterminer si un comportement suspect constitue une menace valable et si la menace provient d'une seule attaque ou s'inscrit dans le cadre d'une campagne d'attaque plus vaste.

Vous pouvez créer des enquêtes et les compléter à partir d'une page détaillée de détection ou du **Actions** menu sur chaque carte de détection. Votre système ExtraHop créera également enquêtes recommandées par le biais des enquêtes intelligentes, qui sont des enquêtes créées automatiquement en réponse à une activité malveillante potentielle.

Chaque page d'investigation inclut les outils suivants :

Chronologie de l'enquête

La chronologie des investigations apparaît sur le côté gauche de la page et répertorie les détections ajoutées, en commençant par la détection la plus récente. Les nouvelles détections ajoutées à l'enquête apparaissent dans la chronologie en fonction de l'heure et de la date de détection. Les participants à la détection sont affichés sous le titre de la détection et les informations de suivi de la détection, telles que la personne assignée et le statut, sont affichées à côté des participants.

Catégories d'attaques

Les catégories des détections ajoutées sont affichées en haut de la page d' investigation.

La chaîne de catégories d'attaques affiche le nombre de détections dans chaque catégorie, et non l'ordre dans lequel les détections ont eu lieu. Reportez-vous à la chronologie de l'enquête pour avoir une vision précise de la façon dont les détections se sont produites au fil du temps.

Visualisation des enquêtes

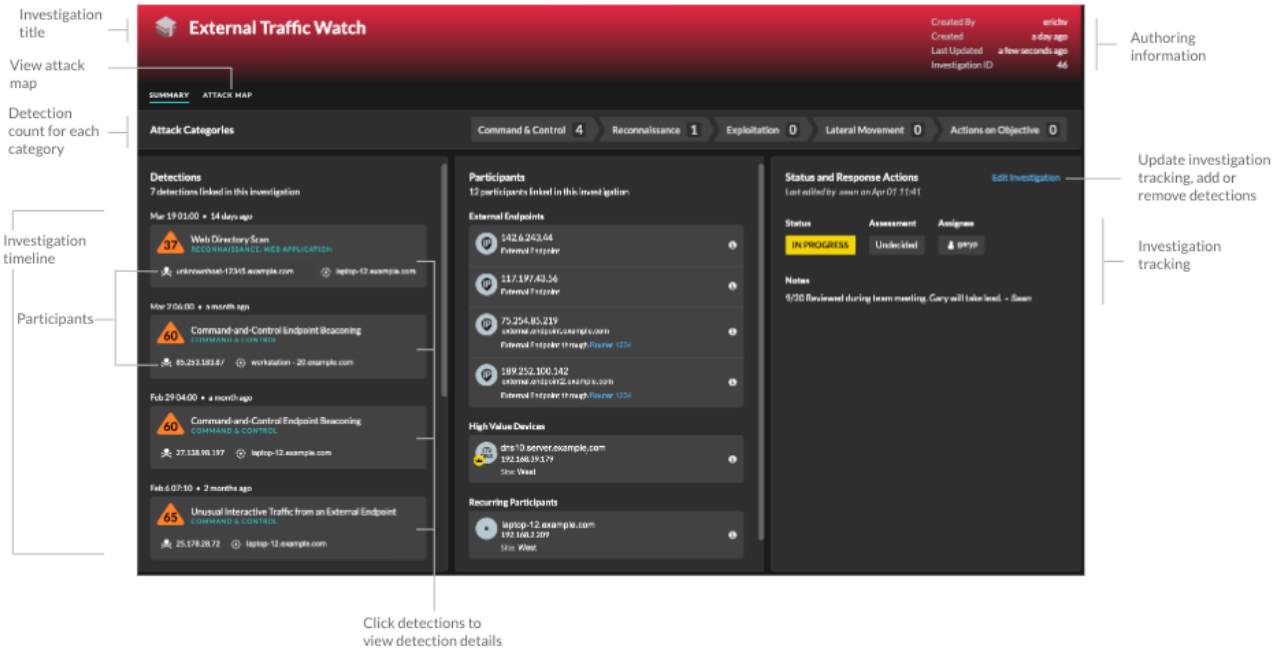
En haut de la page d'enquête, deux options permettent de visualiser l' enquête : Résumé et Carte des attaques. Les deux options offrent une vision unique de votre enquête.

Résumé

Par défaut, les enquêtes sont ouvertes dans **Résumé** vue, qui comprend la chronologie de détection, une liste agrégée des participants et un panneau permettant de suivre l'état de l'enquête et les mesures de réponse.

Vous pouvez cliquer sur une détection dans la chronologie de l'investigation pour l'afficher détails de détection, puis cliquez sur l'icône en forme de x pour fermer les détails de la détection et revenir au résumé de l' enquête. Vous pouvez également cliquer sur le bouton Aller à icône dans le coin supérieur droit pour afficher la page des détails de la détection dans un nouvel onglet.

Dans le panneau Participants, les participants à l'enquête sont regroupés par points de terminaison externes, appareils à valeur élevée et participants récurrents, c'est-à-dire des participants qui apparaissent dans plusieurs détections au cours de l'enquête. Cliquez sur un participant pour afficher les détails et accéder aux liens.

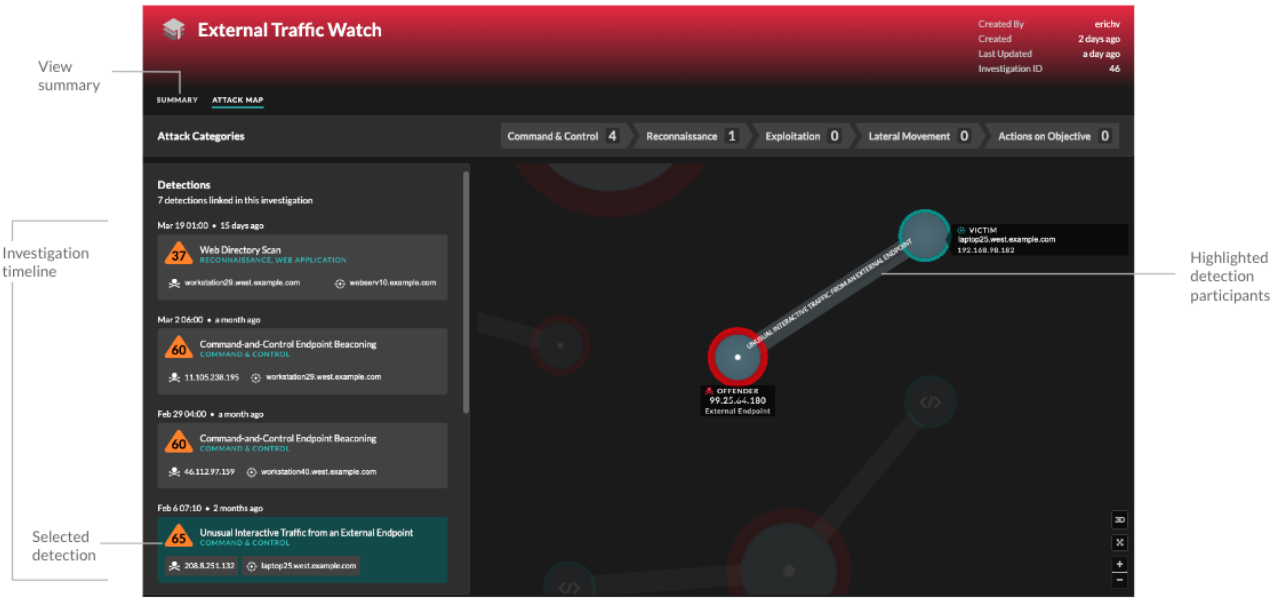


Dans le État et mesures de réponse panneau, cliquez sur **Modifier l'enquête** pour modifier le nom de l'enquête, définir le statut ou l'évaluation finale de l'enquête, spécifier un cessionnaire ou ajouter des notes.

Vous pouvez continuer suivre les détections individuelles après les avoir ajoutés à une enquête.

Carte d'attaque

Dans **Carte d'attaque** , le délinquant et la victime de chaque détection dans le cadre de l'enquête sont affichés sur une carte interactive à côté de la chronologie de l' enquête.



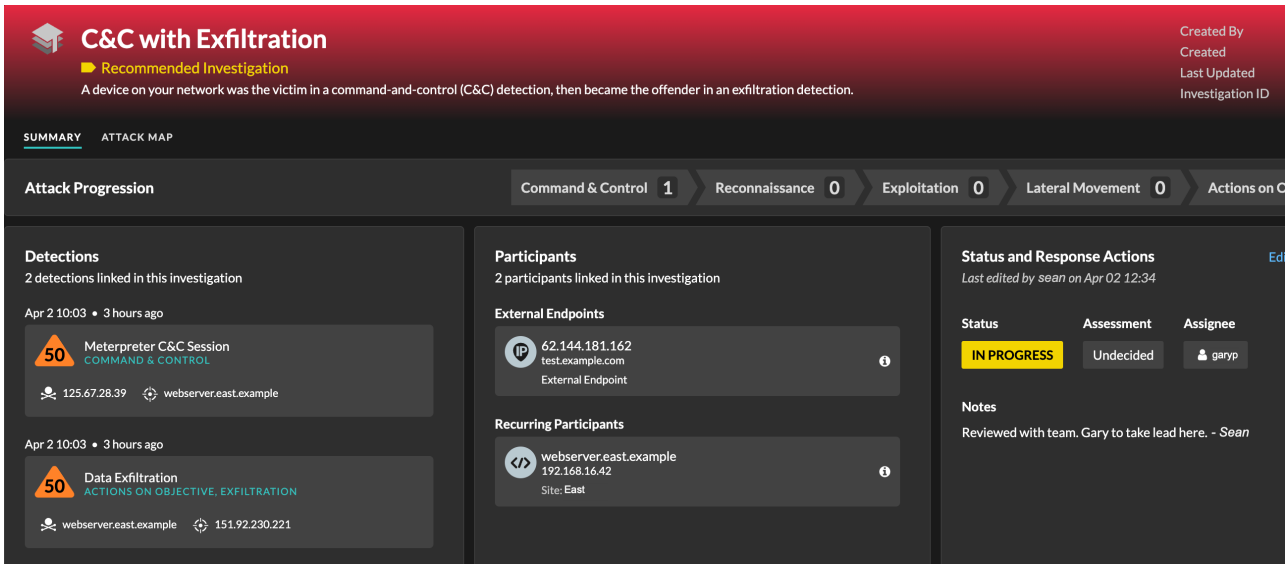
Les participants sont connectés par des lignes étiquetées selon le type de détection et les rôles des équipements sont représentés par une icône.

- Cliquez sur une détection dans la chronologie de l'enquête pour mettre en évidence les participants. Les cercles sont surlignés en rouge si l'équipement est apparu en tant que délinquant lors d'au moins une détection au cours de l'enquête et sont surlignés en bleu sarcelle s'il s'agit d'une victime. Les points forts sont mis à jour lorsque vous cliquez sur une autre détection pour vous aider à identifier le moment où un participant passe du statut de victime à celui de délinquant.
- Cliquez sur un cercle pour afficher des informations telles que le nom d'hôte, l' adresse IP ou l'adresse MAC de l'équipement, ou pour accéder aux détections associées ou au Page de présentation de l'appareil.
- Passez la souris sur un cercle ou une ligne pour afficher l'étiquette.

Enquêtes recommandées

Le service d'apprentissage automatique ExtraHop surveille l'activité du réseau à la recherche de combinaisons de techniques d' attaque susceptibles d'indiquer un comportement malveillant. Lorsqu'une combinaison est identifiée, le système ExtraHop crée une investigation recommandée, permettant à vos équipes de sécurité d' évaluer la situation et de réagir rapidement si un comportement malveillant est confirmé.

Par exemple, si un équipement est la victime d'une détection de la catégorie Commande et contrôle, mais devient le contrevenant lors d'une détection d'exfiltration, le système ExtraHop recommandera une enquête C&C avec exfiltration.



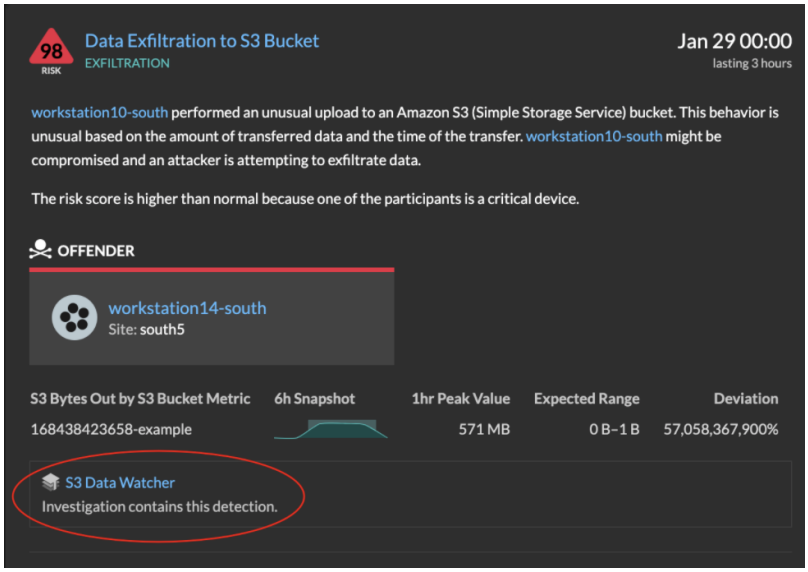
Vous pouvez interagir avec les enquêtes recommandées de la même manière que les enquêtes créées par les utilisateurs, par exemple en ajoutant ou en supprimant des détections, en spécifiant un destinataire et en définissant un statut et une évaluation.

Les investigations recommandées se trouvent dans le tableau des enquêtes. Vous pouvez trier les Créé par colonne pour rechercher les enquêtes créées par ExtraHop.

Gérer les enquêtes

Une fois qu'une détection est ajoutée à une enquête, un lien vers l'enquête apparaît au bas de la carte de détection et sur la page détaillée de la détection.

Cliquez sur le nom pour ouvrir l'enquête, puis sur le nom de la détection sur la page d' enquête pour revenir à la page détaillée de la détection.



Apprenez comment créer une enquête.

Recherche de détections dans le système ExtraHop

Bien que la page Détections fournisse un accès rapide à toutes les détections, il existe des indicateurs et des liens vers les détections dans l'ensemble du système ExtraHop.

Note: Les détections restent dans le système en fonction de votre capacité de rétrospective du système pour les mesures d'une heure, avec une durée de stockage minimale de cinq semaines. Les détections resteront dans le système sans mesures complémentaires si la capacité de rétrospective de votre système est inférieure à cinq semaines.

- Sur une page de présentation des appareils, cliquez sur Détections pour afficher la liste des détections associées. Cliquez sur le lien correspondant à une détection individuelle pour afficher la page des détails de la détection.
- Sur la page de présentation d'un groupe d'appareils, cliquez sur le lien Détections pour accéder à la page Détections. La liste des détections est filtrée en fonction des participants membres du groupe d'équipements.
- Sur une carte d'activités, cliquez sur un équipement qui affiche des impulsions animées autour de l'étiquette circulaire pour afficher la liste des détections associées. Cliquez sur le lien correspondant à une détection individuelle pour afficher les détails de la détection.
- À partir d'un graphique figurant sur un tableau de bord ou une page de protocole, passez la souris sur un marqueur de détection pour afficher le titre de la détection associée ou cliquez sur le marqueur pour afficher les détails de la détection.

Optimisation des détections

Voici quelques bonnes pratiques à mettre en œuvre pour améliorer vos détections : ajoutez des informations sur votre réseau, activez le système ExtraHop pour détecter le trafic potentiellement suspect et filtrez les pages affichées en fonction de vos priorités.

La plupart de ces paramètres fournissent un contexte sur votre réseau que vous pouvez fournir pour améliorer à la fois l'apprentissage automatique et les détections basées sur des règles. Ces paramètres sont parfois négligés et peuvent affecter la qualité de vos détections.

Configurer le déchiffrement

Le trafic HTTP chiffré est un vecteur courant d'attaques, en partie parce que les attaquants savent que le trafic est généralement masqué. Et si votre réseau est doté d'Active Directory, un certain nombre de détections sont masquées dans le trafic chiffré sur le domaine.

Nous vous recommandons vivement d'activer le déchiffrement pour TLS et Active Directory.

Configuration des paramètres de réglage

Ce paramètre améliore la précision des détections basées sur des règles. Vous fournir des détails au système ExtraHop sur votre environnement réseau afin de fournir un contexte sur les appareils observés.

Par exemple, une détection basée sur des règles est générée lorsqu'un équipement interne communique avec des bases de données externes. Si un trafic vers une base de données externe est attendu ou si la base de données fait partie d'une infrastructure de stockage ou de production légitime basée sur le cloud, vous pouvez définir un paramètre de réglage pour ignorer le trafic vers la base de données externe approuvée.

Configurer les localités du réseau

Ce réglage vous permet de classer interne ou externe des terminaux auxquels vous faites confiance, tels qu'un bloc CIDR d'adresses IP auquel vos appareils se connectent régulièrement. Les détections par apprentissage automatique et les mesures du système reposent sur la classification des équipements et du trafic .

Par exemple, si vos appareils se connectent régulièrement à un domaine inconnu mais fiable classé comme adresse IP externe, les détections sont supprimées pour ce domaine.

Création de règles d'exceptions

Ces paramètres vous permettent de masquer les détections une fois que le système les a générés. Si vous constatez une détection qui n'apporte aucune valeur ajoutée, vous pouvez réduire le bruit de votre vue d'ensemble.

Par exemple, si une détection est générée à partir d'un délinquant, d'une victime ou d'autres critères qui ne sont pas préoccupants pour votre réseau, vous pouvez masquer toutes les détections passées et futures utilisant ces critères.

Partagez des données externes en texte brut

Cette option permet au service d'apprentissage automatique de collecter des adresses IP, des noms d'hôtes et des domaines qui sont associés à des activités suspectes.

En activant cette option, vous ajoutez à un ensemble de données collectif de menaces potentielles qui peuvent vous aider et contribuer à la communauté de la sécurité.

Détections de traces

Cette option vous permet de attribuer une détection à un utilisateur, ajouter des notes et mettre à jour le statut de reconnu à fermé. Vous pouvez ensuite filtrer la page Détections pour effacer les problèmes résolus ou vérifier les détections.

Partager une détection

Vous pouvez envoyer l'URL d'une page détaillée de détection à d'autres utilisateurs du système ExtraHop.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Recherchez la détection que vous souhaitez partager, puis cliquez sur le titre de la détection.
4. En haut du navigateur, copiez l'URL complète.

Conseil Partagez un PDF de la page détaillée de détection en cliquant sur l' icône PDF dans le coin supérieur droit de la page.

Prochaines étapes

- Création d'une règle de notification de détection pour recevoir des notifications par e-mail concernant une détection.

Reconnaître les détections

Les remerciements constituent un moyen visuel d'identifier qu'une détection a été détectée. Vous pouvez accuser réception d'une détection pour informer les membres de l'équipe que vous étudiez un ticket ou que le problème a été trié et doit être classé par ordre de priorité pour le suivi. Vous pouvez également filtrer l'affichage des détections pour n'afficher que les détections non reconnues.

Avant de commencer
Les utilisateurs doivent avoir un nombre d'écriture limité ou supérieur privilèges pour accuser réception d'une détection ou effacer un accusé de réception.

Voici quelques points importants à prendre en compte concernant l'accusé de réception des détections :

- Un accusé de réception ne masque pas la détection.
- Une fois la détection confirmée, un horodateur et le nom d'utilisateur de la personne qui a accusé réception de la détection sont affichés.
- Un accusé de réception peut être effacé par n'importe quel utilisateur, même s'il ne s'agit pas de l'utilisateur qui a initialement accusé réception de la détection.

Pour accuser réception d'une détection, procédez comme suit :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez **Reconnaître** depuis le coin inférieur gauche de la carte de détection.

   La détection affiche le nom d'utilisateur et l'horodateur. Cliquez **Réinitialiser** pour effacer un accusé de réception.

Créer une investigation

Créez une investigation pour visualiser plusieurs détections sur une seule chronologie et une seule carte.

Vous pouvez accéder à la liste des enquêtes créées depuis **Enquêtes** icône dans le coin supérieur droit de la page Détections.

Avant de commencer

- Les utilisateurs doivent avoir accès au module NDR et disposer d'une capacité d'écriture limitée privilèges ou une version supérieure pour effectuer les tâches décrites dans ce guide.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez **Actions** depuis le coin inférieur gauche de la carte de détection.
4. Cliquez **Ajouter à une enquête...**.
5. Sélectionnez **Ajouter la détection à une nouvelle investigation**.
6. Cliquez **Suivant**.
7. Tapez un nom et ajoutez des notes à la nouvelle enquête.
8. Cliquez **Créez**.

Une fois que le nom de l'enquête apparaît en bas de la carte de détection, vous pouvez cliquer dessus pour afficher la chronologie et la carte.

- Pour ajouter une détection à l'investigation, cliquez sur **Actions**, puis cliquez sur **Ajouter à une enquête...**.

- Pour supprimer une détection d'une enquête, cliquez sur l'icône de suppression (X) sur la détection dans la chronologie de l'enquête.

Création d'une règle de notification de détection

Créez une règle de notification si vous souhaitez recevoir une notification concernant les détections correspondant à des critères spécifiques.

Vidéo: Consultez la formation associée : Configurer les notifications de détection

Lorsqu'une détection correspondant à vos critères est générée, une notification contenant des informations provenant du carte de détection.

Vous pouvez configurer le système pour envoyer un e-mail à une liste de destinataires ou appeler un webhook spécifique. Les utilisateurs de RevealX 360 peuvent créer une règle de notification qui appelle un webhook pour exporter les données de détection vers un intégration configurée.

Note: (RevealX 360 uniquement) Si vous créez une règle de notification pour exporter les données de détection vers une intégration SIEM , créez la notification directement depuis Intégrations page dans les paramètres d'administration pour pré-remplir les champs des règles de notification.

Avant de commencer

- Les utilisateurs doivent disposer d'un accès au module NDR ou NPM et disposer d'une écriture complète privilèges ou une version supérieure pour effectuer les tâches décrites dans ce guide.
- RevealX Enterprise nécessite un connexion aux services cloud ExtraHop pour envoyer des notifications par e-mail, mais vous pouvez envoyer une notification via un webhook sans connexion.
- Les notifications par e-mail sont envoyées via les services cloud ExtraHop et peuvent contenir des informations identifiables telles que des adresses IP, des noms d'utilisateur, des noms d'hôtes, des noms de domaine , des noms d'équipements ou des noms de fichiers. Les utilisateurs de RevealX Enterprise qui ont des exigences réglementaires interdisant les connexions externes peuvent configurer des notifications avec des appels Webhook pour envoyer des notifications sans connexion externe.
- Les notifications par e-mail sont envoyées depuis no-reply@notify.extrahop.com. Assurez-vous d'ajouter cette adresse à votre liste d'expéditeurs autorisés.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Règles de notification**.
3. Cliquez **Créez**.
4. Cliquez sur l'une des options suivantes :
   - Pour les modules NDR, sélectionnez **Détection de sécurité**.
   - Pour les modules NPM, sélectionnez **Détection des performances**.
5. Dans le Nom champ, saisissez un nom unique pour la règle de notification.
6. Dans le Descriptif champ, ajoutez des informations sur la règle de notification.
7. Dans le Critères section, cliquez sur **Ajouter des critères** pour spécifier les critères qui généreront une notification.
   - **Recommandé pour le triage**
   - **Score de risque minimum**
   - **Tapez**
   - **Catégorie**
   - **Technique MITRE** (NDR uniquement)
   - **Délinquant**
   - **Victime**
   - **Rôle de l'appareil**

- **Participant**
- **Site**

Les options de critères correspondent à options de filtrage sur la page Détections.

8. Dans le Cible section, sélectionnez le mode d' envoi de la notification parmi les options suivantes :

Option	Description
Envoyer un e-mail	Envoyez des notifications par e-mail à une liste de distribution.
Webhook personnalisé	Envoyez une charge utile JSON à l'URL d'un webhook.
Intégration	Exportez les données de détection vers une intégration configurée. Pour les intégrations, nous recommandons aux administrateurs d'ExtraHop de créer des règles de notification de détection à partir du Intégrations page.

9. Si vous avez sélectionné Envoyer un e-mail comme cible, procédez comme suit :
   a) Spécifiez les adresses e-mail individuelles, en les séparant par une virgule.
   b) Cliquez **Enregistrer**.
10. Si vous avez sélectionné Custom Webhook comme cible, procédez comme suit :
    a) Dans le URL de la charge utile dans ce champ, saisissez l'URL du webhook.
    b) Cliquez **Afficher les options de connexion avancées** pour configurer les éléments suivants :
       - Dans le En-têtes personnalisés section, cliquez sur **Ajouter un en-tête** pour spécifier des paires clé:valeur personnalisées.

         Des en-têtes personnalisés sont ajoutés à l' en-tête de la requête HTTP POST du webhook.
       - Sélectionnez un type d'authentification.
         - Aucune authentification
         - Authentification de base

           Entrez le nom d'utilisateur et le mot de passe de l' application cible.
         - Jeton Bearer

           Entrez le jeton d'accès pour l'application cible.
       - Configurez la méthode de connexion.
         - Sélectionnez cette option pour acheminer le webhook via un proxy global configuré. (RevealX Enterprise uniquement.)
         - Sélectionnez cette option pour ignorer la vérification du certificat du serveur.

    c) En dessous Comportement des notifications, sélectionnez le moment où le système ExtraHop enverra des notifications pour une détection.
       - **Envoyer pour chaque mise à jour de détection**

         Recevez une notification chaque fois que la détection est mise à jour.

         Cette sélection est recommandée si vous exportez des données de détection vers un SIEM et que vous souhaitez une visibilité complète de l'activité de détection.
       - **Envoyer une fois par détection**

         Recevez une seule notification lorsqu'une détection est créée.

         Cette sélection est optimale pour avertir un groupe lorsqu'une détection se produit sans surcharger le groupe de mises à jour ultérieures.

d) En dessous Options de charge utile, sélectionnez si vous souhaitez envoyer le charge utile par défaut ou saisissez une charge utile JSON personnalisée.

Si vous avez choisi d'envoyer des notifications une fois par détection sous Comportement des notifications, vous devez envoyer une charge utile personnalisée.

- **Charge utile par défaut**

  Remplissez la charge utile du webhook avec un ensemble de champs de détection de base.

  Dans la liste déroulante Ajouter des champs de charge utile, vous pouvez cliquer sur les champs supplémentaires que vous souhaitez inclure dans la charge utile.
- **Charge utile personnalisée**

  Renseignez la charge utile du webhook avec un JSON personnalisé.

  Vous pouvez modifier la charge utile personnalisée suggérée dans **Modifier la charge utile** fenêtre.

e) Cliquez **Enregistrer**.

f) Cliquez **Connexion de test**.

Un message intitulé Notification de test sera envoyé à l'URL de la charge utile pour confirmer la connexion.

Note: Après avoir testé la connexion, vérifiez que vous avez reçu la notification dans l'application cible. RevealX Enterprise affiche un message d'erreur si la notification de test n'a pas abouti.

11. Dans le Options section, la **Activer la règle de notification** la case à cocher est activée par défaut. Décochez la case pour désactiver la règle de notification.

Lorsqu'une détection correspond aux critères, une notification est envoyée.

Référence de notification du Webhook

Ce guide fournit des informations sur la rédaction de charges utiles personnalisées pour les notifications de sécurité ou de détection des performances avec des webhooks personnalisés ou des cibles d'intégration. Le guide contient une présentation de l'interface Payload (JSON), la charge utile par défaut pour les cibles de webhook, une liste de champs de charge utile que vous pouvez ajouter à la charge utile par défaut et des exemples de structure JSON pour les cibles de webhook courantes, telles que Slack, Microsoft Teams et Google Chat.

Voici quelques points à prendre en compte à propos des notifications de webhook :

- RevealX 360 ne peut pas envoyer d'appels Webhook aux terminaux de votre réseau interne. Les cibles Webhook doivent être ouvertes au trafic externe.
- RevealX Enterprise doit se connecter directement aux points de terminaison du webhook pour envoyer des notifications.
- Les cibles Webhook doivent disposer d'un certificat signé par une autorité de certification (CA) du programme de certificats Mozilla CA. Voir https://wiki.mozilla.org/CA/Included_Certificates pour les certificats émis par des autorités de certification publiques fiables.

Pour plus d'informations sur les règles de notification, voir Création d'une règle de notification de détection.

Charge utile JSON

Les webhooks ExtraHop sont formatés en JSON, alimentés par Moteur de création de modèles Jinja2. Lorsque vous créez une règle de notification de sécurité ou de détection des performances et que vous sélectionnez un webhook ou une intégration personnalisé comme cible, vous avez la possibilité de sélectionner une charge utile par défaut ou d'écrire votre propre charge utile personnalisée .

Charge utile par défaut
L'option de charge utile par défaut est disponible lorsque vous choisissez d'envoyer une notification pour chaque mise à jour de détection en tant que comportement de notification pour le webhook. La charge utile par défaut contient l'ensemble d'informations de base suivant concernant une détection.

```
{
    "title": "{{ title }}",
    "type": "{{ type }}",
    "src": {
        "type": "{{ src.type }}",
        "hostname": "{{ src.hostname }}",
        "ipaddr": "{{ src.ipaddr }}",
        "role": "{{ src.role }}",
        "endpoint": "{{ src.endpoint }}",
        "device": {
            "oid": {{ src.device.oid }},
            "name": "{{ src.device.name }}",
            "ipaddrs": {{ src.device.ipaddrs | safe }},
            "macaddr": "{{ src.device.macaddr }}"
        }
    },
    "dst": {
        "type": "{{ dst.type }}",
        "hostname": "{{ dst.hostname }}",
        "ipaddr": "{{ dst.ipaddr }}",
        "role": "{{ dst.role }}",
        "endpoint": "{{ dst.endpoint }}",
        "device": {
            "oid": {{ dst.device.oid }},
            "name": "{{ dst.device.name }}",
            "ipaddrs": {{ dst.device.ipaddrs | safe }},
            "macaddr": "{{ dst.device.macaddr }}"
        }
    },
    "additional_participants": {{ additional_participants | safe }},
    "properties": {{ properties }},
    "description": "{{ description }}",
    "categories_ids": {{ categories_ids | safe }},
    "mitre_techniques": {{ mitre_techniques | safe }},
    "recommended": "{{ recommended }}",
    "recommended_factors": {{ recommended_factors | safe }},
    "url": "{{ url }}",
    "risk_score": {{ risk_score }},
    "time": {{ time }},
    "id": {{ detection_id or id }}
}
```

Vous pouvez modifier la charge utile par défaut en sélectionnant des champs dans la liste déroulante Ajouter des champs de charge utile. Pour apporter des modifications personnalisées, vous pouvez modifier votre option de charge utile en **Charge utile personnalisée**, puis modifiez la charge utile suggérée dans **Modifier la charge utile** fenêtre.

Charge utile personnalisée
Sélectionnez l'option de charge utile personnalisée pour modifier le JSON suggéré pour un webhook de règles de notification.

Si vous choisissez d'envoyer une notification pour chaque mise à jour de détection sous Comportement des notifications, la charge utile personnalisée suggérée contient le JSON suivant :

```
{
    "title": "{{ title }}",
    "type": "{{ type }}",
```

```
    "src": {
        "type": "{{ src.type }}",
        "hostname": "{{ src.hostname }}",
        "ipaddr": "{{ src.ipaddr }}",
        "role": "{{ src.role }}",
        "endpoint": "{{ src.endpoint }}",
        "device": {
            "oid": {{ src.device.oid }},
            "name": "{{ src.device.name }}",
            "ipaddrs": {{ src.device.ipaddrs | safe }},
            "macaddr": "{{ src.device.macaddr }}"
        }
    },
    "dst": {
        "type": "{{ dst.type }}",
        "hostname": "{{ dst.hostname }}",
        "ipaddr": "{{ dst.ipaddr }}",
        "role": "{{ dst.role }}",
        "endpoint": "{{ dst.endpoint }}",
        "device": {
            "oid": {{ dst.device.oid }},
            "name": "{{ dst.device.name }}",
            "ipaddrs": {{ dst.device.ipaddrs | safe }},
            "macaddr": "{{ dst.device.macaddr }}"
        }
    },
    "additional_participants": {{ additional_participants | safe }},
    "properties": {{ properties }},
    "description": "{{ description }}",
    "categories_ids": {{ categories_ids | safe }},
    "mitre_techniques": {{ mitre_techniques | safe }},
    "recommended": "{{ recommended }}",
    "recommended_factors": {{ recommended_factors | safe }},
    "url": "{{ url }}",
    "risk_score": {{ risk_score }},
    "time": {{ time }},
    "id": {{ detection_id or id }}
}
```

Si vous choisissez d'envoyer une notification par mise à jour de détection sous Comportement des notifications, la charge utile personnalisée suggérée contient le JSON suivant :

```
{
    "title": "{{ title }}",
    "type": "{{ type }}",
    "url": "{{ url }}",
    "description": "{{ description }}",
    "api": {{ api | safe }},
    "categories_string": "{{ categories_string }}",
    "categories_array": {{ categories_array | safe }},
    "victims": {{ victims | safe }},
    "offenders": {{ offenders | safe }},
    "description_format": "{{ description_format }}",
    "victim_primary": {{ victim_primary | safe }},
    "offender_primary": {{ offender_primary | safe }}
}
```

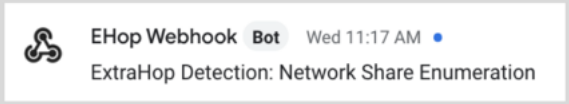
Conseil Avant de prendre le temps de saisir une longue charge utile personnalisée, nous vous recommandons de tester votre connexion à l'URL du webhook. De cette façon, vous pouvez être sûr que les problèmes ne sont pas dus à une erreur de connexion.

Validation de syntaxe
L'éditeur de webhook permet de valider les syntaxes JSON et Jinja2. Si vous tapez une ligne qui inclut une syntaxe JSON ou Jinja2 incorrecte, une erreur apparaît dans le champ Charge utile avec l'erreur.
Variables
Les variables de détection sont ajoutées à la charge utile en insérant le nom de la variable entre deux ensembles d'accolades ({{et}}).

Par exemple, l'échantillon de la charge utile inclut une variable pour le titre de détection :

```
"text": "ExtraHop Detection: {{title}}"
```

Lorsqu'une détection correspond à une règle de notification et à la variable, celle-ci est remplacée par le titre de la détection. Par exemple, si la règle de notification correspond à la détection pour Network Share Enumeration, la variable est remplacée par le titre de la notification, comme dans la figure suivante :



Consultez la liste des variables de détection.

Filtres
Les filtres vous permettent de modifier une variable.

Transmission de JSON

Si la variable renvoie une valeur formatée en JSON, la valeur est automatiquement échappée et traduite en chaîne. Si vous souhaitez transmettre un code JSON valide à votre cible de webhook, vous devez spécifier `safe` filtre :

```
{{<variable> | safe }}
```

Dans l'exemple suivant, la variable renvoie des données de détection au format JSON concernant les participants directement à la cible du webhook :

```
{{api.participants | safe }}
```

Déclarations IF
Une instruction IF permet de vérifier si une valeur est disponible pour la variable. Si la variable est vide, vous pouvez spécifier une variable alternative.

```
 {% if {{<variable>}} %}
```

Dans l'exemple suivant, l'instruction IF vérifie si une valeur est disponible pour la variable victim :

```
{% if victims %}
```

Dans l'exemple suivant, l'instruction IF vérifie si le nom du délinquant est disponible. S'il n'y a aucune valeur pour le nom du délinquant, la valeur de la variable d'adresse IP du délinquant est renvoyée à la place.

```
{% if offender.name %}{{offender.name}}{%else%}{{offender.ipaddr}}
{% endif %}
```

Boucles FOR
Une boucle FOR peut permettre à la notification d'afficher un tableau d'objets.

```
{% for <array-object-variable> in <array-variable> %}
```

Dans l'exemple suivant, une liste des noms de délinquants du tableau des délinquants est affichée dans la notification. Une instruction IF vérifie la présence d'autres éléments dans le tableau (`{% if not loop.last %}`) et ajoute un saut de ligne avant d'imprimer la valeur suivante (`\n`). Si le nom du délinquant est vide, le filtre par défaut renvoie « Nom inconnu » pour la valeur.

```
{% for offender in offenders %}
  {{offender.name | default ("Unknown Name")}}
  {% if not loop.last %}\n
  {% endif %}
{% endfor %}
```

Variables de détection disponibles

Les variables suivantes sont disponibles pour les notifications des webhooks concernant les détections.

titre : *Corde*

Titre de la détection.

description : *Corde*

Description de la détection.

type : *Corde*

Type de détection.

identifiant : *Numéro*

L'identifiant unique pour la détection.

url : *Corde*

URL de détection dans le système ExtraHop.

point_de risque : *Numéro*

L'indice de risque de la détection.

site : *Corde*

Le site où la détection a eu lieu.

texte_date_début : *Corde*

Heure à laquelle la détection a commencé.

texte_de_fin : *Corde*

Heure à laquelle la détection s'est terminée.

tableau_catégories : *Tableau de cordes*

Tableau de catégories auxquelles appartient la détection.

chaîne_catégories : *Corde*

Chaîne répertoriant les catégories auxquelles appartient la détection.

mitre_tactics : *Tableau de cordes*

Tableau d'identifiants tactiques MITRE associés à la détection.

mitre_tactics_string : *Corde*

Chaîne répertoriant les ID de tactiques MITRE associés à la détection.

mitre_techniques : *Tableau de cordes*

Un ensemble d'identifiants de techniques MITRE associés à la détection.

mitre_techniques_string : *Corde*

Chaîne répertoriant les identifiants de la technique MITRE associés à la détection.

délinquant principal : *Objet*

(Obsolète) Objet qui identifie le délinquant principal et qui contient les propriétés suivantes :

externe : *Booléen*

La valeur est `true` si l' adresse IP du délinquant principal est externe à votre réseau.

adresse iPad : ***Corde***

L'adresse IP du délinquant principal.

nom : ***Corde***

Le nom du délinquant principal.

délinquants : ***Tableau d'objets***

Un ensemble d'objets du délinquant associés à la détection. Chaque objet contient les propriétés suivantes :

externe : ***Booléen***

La valeur est `true` si l'adresse IP du contrevenant est externe à votre réseau.

adresse iPad : ***Corde***

L'adresse IP du délinquant. S'applique aux détections impliquant plusieurs délinquants.

nom : ***Corde***

Le nom du délinquant. S'applique aux détections impliquant plusieurs délinquants.

victime_principale : ***Objet***

(Obsolète) Objet qui identifie la victime principale et contient les propriétés suivantes :

externe : ***Booléen***

La valeur est `true` si l' adresse IP de la victime principale est externe à votre réseau.

adresse iPad : ***Corde***

L'adresse IP de la victime principale.

nom : ***Corde***

Le nom de la victime principale.

victimes : ***Tableau d'objets***

Un ensemble d'objets victimes associés à la détection. Chaque objet contient les propriétés suivantes :

externe : ***Booléen***

La valeur est `true` si l'adresse IP de la victime est externe à votre réseau.

adresse iPad : ***Corde***

L'adresse IP de la victime. S'applique aux détections impliquant plusieurs victimes.

nom : ***Corde***

Le nom de la victime. S'applique aux détections impliquant plusieurs victimes.

api : ***Objet***

Un objet qui contient tous les champs renvoyés par `GET /detections/{id}operation`. Pour plus d'informations, consultez Présentation de l'API REST ExtraHop.

Exemples de webhooks

Les sections suivantes fournissent des modèles JSON pour les cibles de webhook courantes.

Slack

Après avoir créé une application Slack et activé les webhooks entrants pour l'application, vous pouvez créer un webhook entrant. Lorsque vous créez un webhook entrant, Slack génère l' URL que vous devez saisir dans le champ URL de la charge utile de votre règle de notification.

L'exemple suivant montre la charge utile JSON d'un webhook Slack :

```
{
    "blocks": [
        {
            "type": "header",
            "text": {
                "type": "plain_text",
```

```
                "text": "Detection: {{ title }}"
             }
        },
        {
            "type": "section",
            "text": {
                "type": "mrkdwn",
                "text": "• *Risk Score:* {{ risk_score }}\n • *Category:*
 {{ categories_string }}\n • *Site:* {{ site }}\n • *Primary Offender:*
 {{ offender_primary.name}} ({{ offender_primary.ipaddr}})\n • *Primary
 Victim:* {{ victim_primary.name }} ({{ victim_primary.ipaddr }})\n"
            }
        },
        {
            "type": "section",
            "text": {
                "type": "plain_text",
                "text": "Detection ID: {{ id }}"
            },
            "text": {
                "type": "mrkdwn",
                "text": "<{{ url }}|View Detection Details>"
            }
        }
    ]
}
```

Microsoft Teams

Vous pouvez ajouter un webhook entrant à une chaîne Teams en tant que connecteur. Après avoir configuré un webhook entrant, Teams génère l'URL que vous pouvez saisir dans le champ URL de la charge utile de votre règle de notification.

L'exemple suivant montre la charge utile JSON pour un webhook Microsoft Teams :

```
{
   "type":"message",
   "attachments":[
      {
         "contentType":"application/vnd.microsoft.card.adaptive",
         "contentUrl":null,
         "content":{
            "$schema":"https://adaptivecards.io/schemas/adaptive-card.json",
            "type":"AdaptiveCard",
            "body":[
               {
                  "type":"ColumnSet",
                  "columns":[
                     {
                        "type": "Column",
                        "width":"16px",
                        "items":[
                           {
                              "type":"Image",
                              "horizontalAlignment":"center",
                              "url":"https://assets.extrahop.com/
favicon.ico",
                              "altText":"ExtraHop Logo"
                           }
                        ]
                     },
                     {
                        "type": "Column",
```

```
                        "width":"stretch",
                        "items":[
                           {
                              "type":"TextBlock",
                              "text":"ExtraHop RevealX",
                              "weight": "bolder"
                           }
                        ]
                     }
                  ]
               },
               {
                  "type":"TextBlock",
                  "text":"**{{ title }}**"
               },
               {
                  "type":"TextBlock",
                  "spacing":"small",
                  "isSubtle":true,
                  "wrap":true,
                  "text":"{{ description }}"
               },
               {
                  "type":"FactSet",
                  "facts":[
                     {
                        "title":"Risk Score:",
                        "value":"{{ risk_score }}"
                     },
                     {
                        "title":"Category:",
                        "value":"{{ categories_string }}"
                     },
                     {
                        "title":"Site:",
                        "value":"{{ site }}"
                     },
                     {
                        "title":"Primary Offender:",
                        "value":"{{ offender_primary.name }}
({{ offender_primary.ipaddr }})"
                     },
                     {
                        "title":"Primary Victim:",
                        "value":"{{ victim_primary.name }}
({{ victim_primary.ipaddr }})"
                     }
                  ]
               },
               {
                  "type":"ActionSet",
                  "actions":[
                     {
                        "type":"Action.OpenUrl",
                        "title":"View Detection Details",
                        "url":"{{ url }}"
                     }
                  ]
               }
            ]
         }
      }
   ]
```

```
}
```

Google Chat

Depuis un salon de discussion Google, vous pouvez cliquer sur la liste déroulante à côté du nom du salon et sélectionner Gérer les webhooks. Une fois que vous avez ajouté un webhook et que vous l'avez nommé, Google Chat génère l'URL que vous pouvez saisir dans le champ URL de la charge utile de votre règle de notification .

L'exemple suivant montre la charge utile JSON d'un webhook Google Chat :

```
{
    "cards": [
        {
            "header": {
                "title": "{{title}}"
            },
            "sections": [
                {
                    "widgets": [
                        {
                            "keyValue": {
                                "topLabel": "Risk score",
                                "content": "{{risk_score}}"
                            }
                        },
                        {
                            "keyValue": {
                                "topLabel": "Categories",
                                "content": "{{categories_string}}"
                            }
                        }
                        {% if offenders %}
                       ,{
                            "keyValue": {
                                "topLabel": "Offenders",
                                "contentMultiline": "true",
                                "content": "{% for offender in offenders %}
{% if offender.name %}{{offender.name}}{% else %}{{offender.ipaddr}}{% endif
 %}{% if not loop.last %}\n{% endif %}{% endfor %}"
                            }
                        }
                        {% endif %}
                        {% if victims %}
                       ,{
                            "keyValue": {
                                "topLabel": "Victims",
                                "contentMultiline": "true",
                                "content": "{% for victim in victims %}{%
 if victim.name %}{{victim.name}}{% else %}{{victim.ipaddr}}{% endif %}{% if
 not loop.last %}\n{% endif %}{% endfor %}"
                            }
                        }
                        {% endif %}
                    ]
                },
                {
                    "widgets": [
                        {
                            "buttons": [
                                {
                                    "textButton": {
```

```
                                    "text": "VIEW DETECTION DETAILS",
                                    "onClick": {
                                        "openLink": {
                                            "url": "{{url}}"
                                        }
                                    }
                                }
                            }
                        ]
                    }
                ]
            }
        ]
    ]
}
```

Création d'une règle de notification du catalogue de détection

Créez une règle de notification si vous souhaitez recevoir une notification lorsque de nouvelles détections sont actives sur votre système ExtraHop.

Lorsque l'état d'un type de détection dans le catalogue de détection est défini sur Actif, une notification contenant des informations sur la détection est envoyée, notamment le type et l'état de détection. La notification inclura également les dates de publication de la détection et de dernière mise à jour si ces dates sont disponibles.

Avant de commencer

- Les utilisateurs doivent disposer d'un accès au module NDR ou NPM et disposer d'une capacité d'écriture complète privilèges ou une version supérieure pour effectuer les tâches décrites dans ce guide.
- Le système ExtraHop doit être connecté à ExtraHop Cloud Services pour envoyer des notifications par e-mail.
- Les notifications par e-mail sont envoyées depuis no-reply@notify.extrahop.com. Assurez-vous d'ajouter cette adresse à votre liste d'expéditeurs autorisés.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Règles de notification**.
3. Cliquez **Créez**.
4. Cliquez sur l'une des options suivantes :
   - Pour les modules NDR, sélectionnez Security Detection Catalog.
   - Pour les modules NPM, sélectionnez Performance Detection Catalog.
5. Tapez un nom unique pour la règle de notification dans le champ Nom.
6. Dans le champ Description, ajoutez des informations sur la règle de notification.
7. Spécifiez les adresses e-mail individuelles, en les séparant par une virgule.
8. Dans le Options section, la **Activer la règle de notification** La case à cocher est activée par défaut. Décochez la case pour désactiver la règle de notification.
9. Cliquez **Enregistrer**.

Suivre une détection

Le suivi des détections vous permet d'attribuer des utilisateurs, de définir un statut et d'ajouter des notes à une fiche de détection.

Vous pouvez également filtrer votre affichage des détections par statut ou par personne assignée.

Vidéos Consultez la formation associée : Suivi de la détection

Avant de commencer
Les utilisateurs doivent avoir une écriture limitée privilèges ou une version supérieure pour effectuer les tâches décrites dans ce guide.

Vous pouvez attribuer à n'importe quel utilisateur du système la personne assignée, ajouter des notes et définir l'état d'une détection sur l'une des valeurs suivantes :

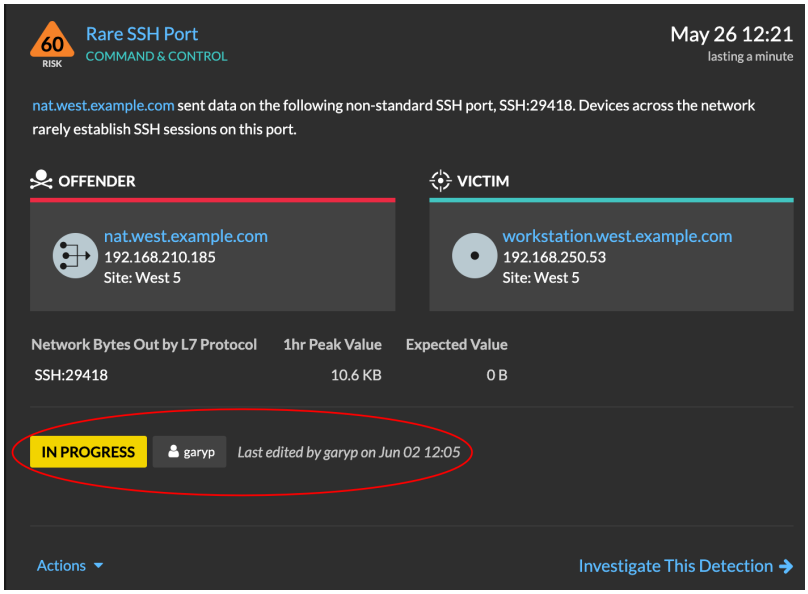
Ouvrir
La détection n'a pas été revue.

Reconnaître
La détection a été constatée et doit faire l'objet d'un suivi prioritaire.

En cours
La détection a été attribuée à un membre de l'équipe et est en cours de révision.

Clôturé : mesures prises
La détection a été revue et des mesures ont été prises pour faire face au risque potentiel.

Fermé - Aucune mesure n'a été prise
La détection a été revue et n'a nécessité aucune action.



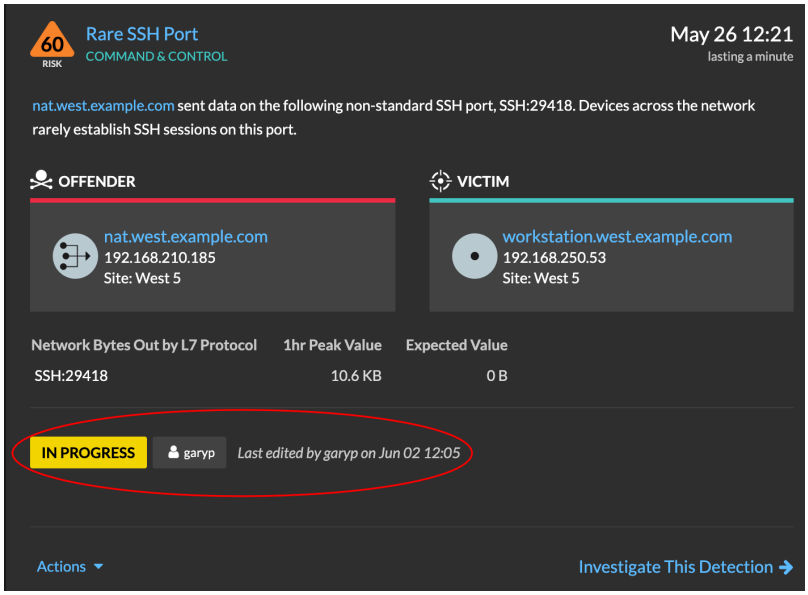
Voici quelques considérations importantes concernant le suivi des détections :

- Le statut Reconnu ou Fermé ne masque pas la détection.
- L'état de détection peut être mis à jour par n'importe quel utilisateur privilégié.
- Vous pouvez ajouter un suivi de détection avec ExtraHop et des systèmes tiers dans le Administration paramètres.

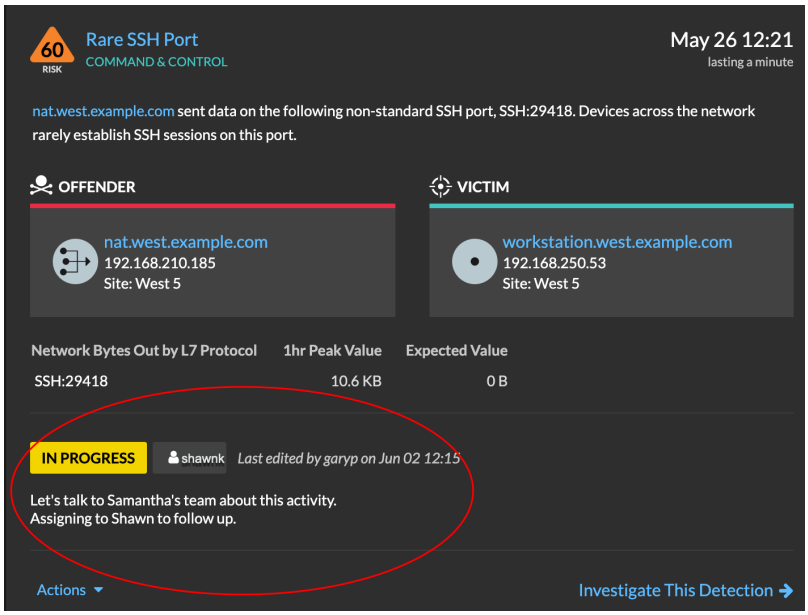
Pour suivre une détection, procédez comme suit :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez **Actions** depuis le coin inférieur gauche de la carte de détection.
4. Optionnel : Cliquez sur un état de détection pour l'ajouter à la détection.

Option	Description
Reconnaître	La détection a été constatée et doit faire l'objet d'un suivi prioritaire.
En cours	La détection a été attribuée à un membre de l'équipe et est en cours de révision.
Clôturé : mesures prises	La détection a été revue et des mesures ont été prises pour faire face au risque potentiel.
Fermé - Aucune mesure n'a été prise	La détection a été revue et n'a nécessité aucune action.



5. Cliquez **Détection de traces...** pour définir l'état de détection, attribuer la détection à un utilisateur et ajouter des notes à la carte de détection.



À partir du **Actions** menu déroulant, sélectionnez **Détection de traces...** et puis **Ouvrir** pour supprimer le statut de la détection ; le destinataire et les notes restent visibles.

Suivez une détection à partir d'une carte de détection

Vous pouvez suivre une détection en ajoutant un responsable, un statut et des notes à partir d'une carte de détection .

Pour suivre une détection, procédez comme suit :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez **Des actions** depuis le coin inférieur gauche de la carte de détection.
4. Optionnel : Cliquez sur un état de détection pour l'ajouter à la détection.
5. Cliquez **Détection de pistes...** pour définir l'état de détection, attribuer la détection à un utilisateur et ajouter des notes à la carte de détection.

   À partir du **Des actions** menu déroulant, sélectionnez **Détection de pistes...** et puis **Ouvert** pour supprimer le statut de la détection ; la personne assignée et les notes restent visibles.

Suivez un groupe de détections à partir d'un résumé des détections

Vous pouvez appliquer un statut, une personne assignée ou une note à plusieurs détections en même temps à partir du panneau récapitulatif de la page Détections.

Un panneau récapitulatif apparaît lorsque les détections sont regroupées par type dans la vue récapitulative de la page Détections.

Pour suivre un groupe de détections à partir d'un résumé des détections, procédez comme suit :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.

   Par défaut, la page doit être en mode récapitulatif avec les détections groupées par type. Si ce n'est pas le cas, cliquez sur le Vue récapitulative et ensuite groupe par type.
3. Cliquez sur un type de détection dans votre liste de détections.
4. Cliquez sur les critères selon lesquels vous souhaitez filtrer : participants, propriétés ou localités du réseau.
5. Dans le coin inférieur gauche du panneau récapitulatif, cliquez sur **Suivez toutes les détections**.

   Le lien indiquera le nombre de détections que vous êtes en train de mettre à jour. Par exemple, suivez les 14 détections. Ce lien n'apparaît pas dans le panneau récapitulatif si le filtre d' état masqué est appliqué.
6. Optionnel : Sélectionnez le statut que vous souhaitez appliquer à toutes les détections sélectionnées.
7. Optionnel : Sélectionnez le responsable que vous souhaitez appliquer à toutes les détections sélectionnées.
8. Optionnel : Indiquez si vous souhaitez ajouter une nouvelle note aux notes existantes des détections sélectionnées ou remplacer toutes les notes existantes.

   Lorsque vous ajoutez votre note à des notes existantes, la nouvelle note est ajoutée au-dessus des notes existantes.
9. Cliquez **Enregistrer**.

Empêcher les appareils CrowdStrike d'une détection

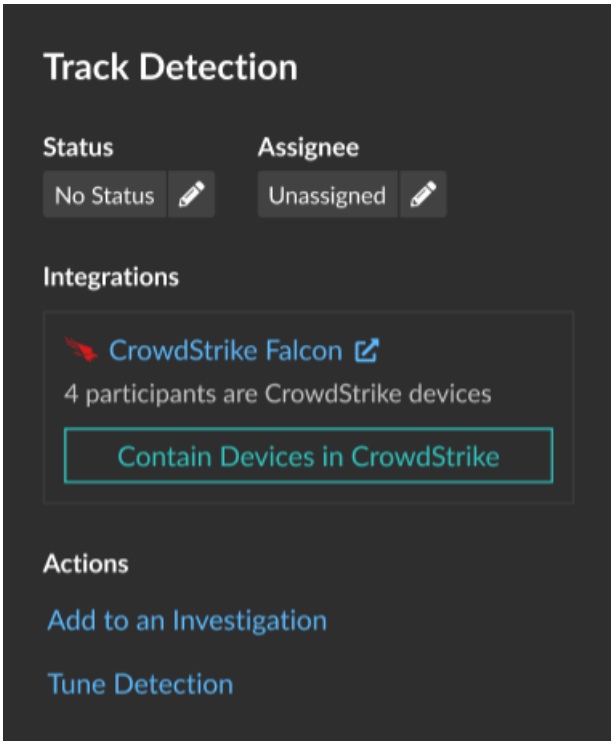
Vous pouvez initier le confinement des appareils CrowdStrike participant à une détection de sécurité. Le confinement empêche les appareils d'établir des connexions avec d'autres appareils de votre réseau.

Une fois que vous avez initié le confinement à la suite d'une détection, une demande est envoyée à CrowdStrike Falçon pour contenir les appareils et le statut Containment Pending apparaît à côté du participant. Le statut est mis à jour à Contained uniquement lorsque le système ExtraHop reçoit une réponse de CrowdStrike.

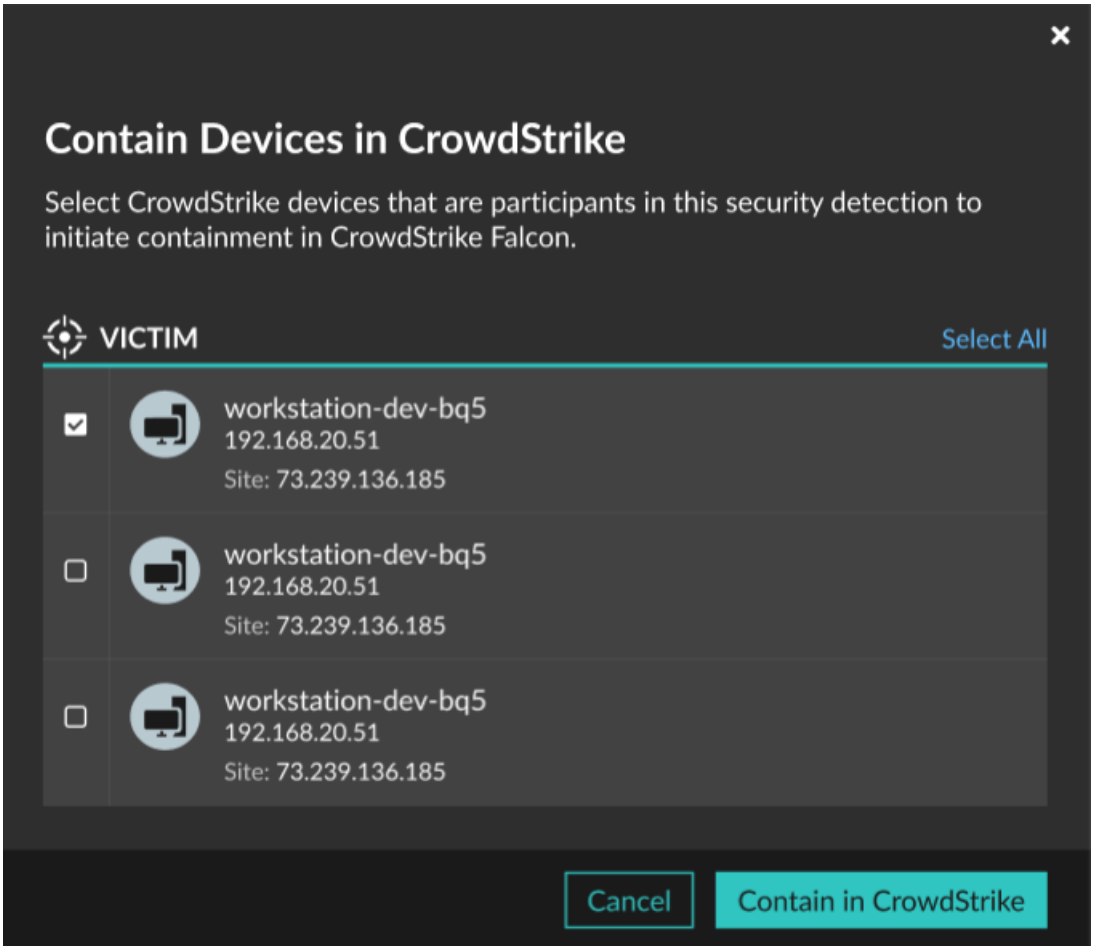
Avant de commencer

- Le confinement des appareils doit être activé pour Intégration à CrowdStrike.
- Les utilisateurs doivent avoir accès au module NDR et disposer d'un nombre d'écriture limité privilèges ou supérieur pour effectuer les tâches décrites dans ce guide.

1. <extrahop-hostname-or-IP-address>Connectez-vous au système ExtraHop via https ://.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez sur le titre d'une détection pour afficher la page détaillée de la détection.
   Le nombre d'appareils CrowdStrike participant à la détection apparaît dans la section Intégrations sous Track Detection.



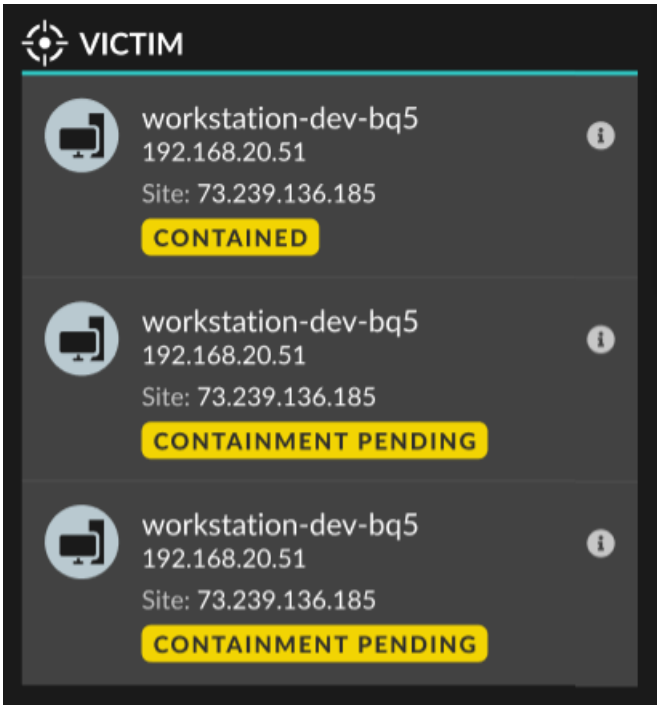
4. Cliquez **Contenir les appareils dans CrowdStrike**.
   La boîte de dialogue affiche les appareils CrowdStrike associés à la détection.



5. Sélectionnez les appareils que vous souhaitez contenir et cliquez sur **Contenu dans CrowdStrike**. Une demande est envoyée à CrowdStrike et le statut Containment Pending apparaît à côté de chaque participant sélectionné.

Prochaines étapes

- Vérifiez le confinement de l'équipement en vérifiant son état à partir des détails de détection. L'état du confinement apparaît également dans propriétés de l'équipement.



- Réessayez de contenir un équipement. Le statut Containment Pending n'apparaît plus lorsqu' une demande de confinement adressée à CrowdStrike est refusée ou expire.
- Libérez un équipement du confinement depuis la console CrowdStrike Falçon. Dans la section Intégrations, sous Détection des pistes, cliquez sur **CrowdStrike Falçon** pour ouvrir la console dans un nouvel onglet. L'état du confinement n'apparaît plus une fois que le système ExtraHop reçoit une réponse de CrowdStrike.

Création d'une détection personnalisée

Les détections personnalisées vous permettent de spécifier des critères qui génèrent des détections sur le système ExtraHop. L'apprentissage automatique et les détections basées sur des règles détectent les comportements inhabituels et les menaces courantes. Toutefois, en créant une détection personnalisée, vous pouvez cibler les appareils et les comportements essentiels pour votre réseau.

Lorsque vous créez une détection personnalisée, vous devez créer un déclencheur qui identifie l'événement système et les conditions que le système doit surveiller, puis vous pouvez attribuer le déclencheur aux appareils ou groupes d'équipements spécifiques que vous souhaitez surveiller. Lorsque l'événement se produit, une détection est générée.

Dans ce guide, nous fournissons les étapes et un exemple de script qui génère une détection personnalisée lorsque des connexions suspectes sont établies avec des sites Web spécifiques via Windows PowerShell.

Avant de commencer

- Vous devez avoir une certaine connaissance d'ExtraHop éléments déclencheurs. En particulier, considérez ces meilleures pratiques lors de l'écriture de votre script et de l'attribution de déclencheurs.
- Vous devez disposer d'un compte utilisateur auprès du privilèges nécessaire pour créer des déclencheurs.
- Si vous avez un console, créez un déclencheur sur le console et le déclencheur fonctionnera sur tous les capteurs connectés.

Création d'un déclencheur pour générer des détections personnalisées

Les déclencheurs génèrent des détections personnalisées en appelant le `commitDetection` fonction dans le script du déclencheur.

Dans l'exemple suivant, le déclencheur génère une détection personnalisée lorsqu' un client PowerShell accède à un site Web connu sous le nom de site intermédiaire pour les données exfiltrées.

Le déclencheur identifie les connexions PowerShell en recherchant les hachages JA3 du client TLS qui appartiennent à des clients PowerShell connus.

Si la connexion TLS est établie entre un client PowerShell et un hôte suspect, le déclencheur génère une détection. La détection inclut la version de PowerShell qui a initié la connexion, l'adresse IP du serveur et l'adresse IP du client.

Note: Pour plus d'informations sur le `commitDetection` fonction, voir Référence de l'API Trigger.

1. Cliquez sur l'icône Paramètres système puis cliquez sur **éléments déclencheurs**.
2. Cliquez **Créez**.
3. Spécifiez les paramètres de configuration du déclencheur suivants :

   Nom

   Tapez un nom pour votre déclencheur. Ce nom identifie votre déclencheur, pas la détection.

   Dans notre exemple, nous allons entrer le nom : `Détection personnalisée : connexion PowerShell à un site suspect`.

   Descriptif

   (Facultatif) Entrez la description du déclencheur. Cette description concerne le déclencheur et non la détection.

   Dans notre exemple, nous allons entrer la description : `Crée une détection chaque fois qu'un client PowerShell se connecte à pastebin, raw.githubusercontent.com ou Githack. Les clients PowerShell sont identifiés par des hachages JA3.`

   Évènements

   Sélectionnez l'événement sur lequel le déclencheur s'exécute.

   Dans notre exemple, nous allons sélectionner l'événement SSL_OPEN. Cet événement se produit lorsqu'une connexion TLS est établie pour la première fois.

   Devoirs

   Sélectionnez l'équipement ou le groupe dequipments que vous souhaitez surveiller. Dans un premier temps, attribuez votre déclencheur à un seul équipement à des fins de test. Après avoir vérifié que la détection personnalisée fonctionne correctement, attribuez le déclencheur à un groupe dproximatif contenant tous les appareils que vous souhaitez surveiller.

   PowerShell étant un outil de ligne de commande Windows, sélectionnez un serveur Microsoft pour tester le déclencheur. Une fois que vous avez vérifié que la détection personnalisée fonctionne correctement, modifiez l'attribution à un groupe dproximatif d'équipements contenant tous vos serveurs Microsoft critiques. Pour plus d'informations sur la création de groupes d'équipements, voir Création d'un groupe dproximatifs d'équipements.
4. Dans le volet droit, saisissez le code qui détermine le moment où votre détection personnalisée est générée.

   Dans notre exemple, le code de déclencheur suivant identifie le moment où un client initie une connexion à pastebin, githubusercontent ou githack :

```
if(SSL.host.match(/pastebin/i) || SSL.host.match(/
raw.githubusercontent.com/i) || SSL.host.match(/githack/i)) {
```

```
}
```

5. Tapez ensuite le code qui valide votre détection personnalisée. Le `commitDetection` la fonction doit être écrite dans le format suivant :

```
commitDetection('<detection type ID>', {
       title: '<title>',
       description: '<detection description>',
       categories: ['<category>'],
       riskScore: <risk score>,
       participants: [{
           object:<offender participant>,
           role: 'offender'
           }, {
           object: <victim participant>,
           role: 'victim'
           }],
       identityKey: '<identity key>',
       identityTtl: '<time period>',
       });
```

Entrez des valeurs pour chacun des paramètres suivants dans votre script.

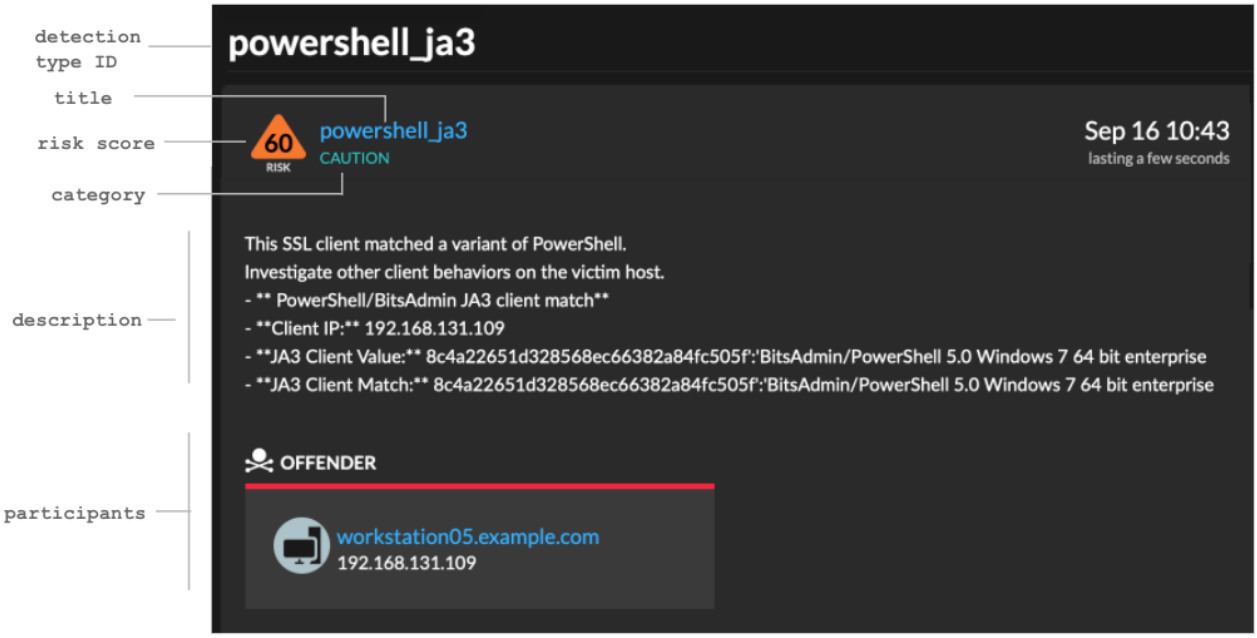
Valeur	Descriptif
ID du type de détection	Chaîne unique qui identifie votre détection personnalisée. Cette chaîne ne peut contenir que des lettres, des chiffres et des traits de soulignement.
titre	Texte qui apparaît en haut de la carte de détection. Tapez un titre descriptif facile à scanner. Ce titre apparaît dans le catalogue de détection en tant que nom d'affichage pour votre type de détection, précédé de `[personnalisé]`.
description de la détection	Texte qui apparaît sous le titre et la catégorie sur une carte de détection. Tapez les informations relatives à l'événement qui génère la détection. Ce champ prend en charge le markdown. Nous vous recommandons d'inclure des variables d'interpolation pour afficher des informations spécifiques concernant votre détection . Par exemple, les variables `$(Flow.client.ipaddr)` et `$(Flow.server.ipaddr)` afficher l' adresse IP du client et de l'équipement serveur dans le flux et `$(Flow.l7proto)` affiche le protocole L7. Inclure `\n` à la fin de chaque ligne de texte pour vous assurer que la description s'affiche correctement.
indice de risque	Chiffre qui mesure la probabilité, la complexité et l'impact commercial d'une détection de sécurité. L'icône de l'indice de risque apparaît en haut de la carte de détection et est codée par couleur selon

Valeur	Descriptif
	la gravité : rouge (80-99), orange (31-79) ou jaune (1-30). Tu peux trier les détections par risque.
délinquant participant victime participante	Tableau d'objets qui identifie les participants à la détection. Définissez le rôle du participant comme suit : `'offender'` ou `'victim'` et fournissez une référence à un équipement, une adresse IP ou un objet d'application pour ce rôle. Par exemple, le tableau suivant identifie le serveur en tant que délinquant et le client en tant que victime dans un flux : `participants: [ { role: 'offender', object: Flow.server.device}, { role: 'victim', object: Flow.client.device } ]` Pour plus d'informations sur l'équipement, l'adresse IP et les objets de l'application, consultez Référence de l'API Trigger.
clé d'identité	Chaîne qui permet d'identifier les détections en cours. Si plusieurs détections avec la même clé d'identité et le même type de détection sont générées dans le délai spécifié par `identityTtl` paramètre, les détections sont consolidées en une seule détection continue. Créez une chaîne clé d'identité unique en combinant les caractéristiques de la détection. Par exemple, la clé d'identité suivante est créée en combinant l'adresse IP du serveur et l' adresse IP du client : `identityKey: [Flow.server.ipaddr, Flow.client.ipaddr].join('!!')`
période	Durée pendant laquelle les détections dupliquées sont consolidées en une détection continue après la génération d'une détection. La période est réinitialisée et la détection ne prend fin qu'à l'expiration de cette période. Les périodes de validité suivantes sont les suivantes : • `hour` • `day` • `week` La période par défaut est `hour`.

L'exemple suivant montre la section de script terminée.

```
commitDetection('powershell_ja3', {
        title:
'PowerShell / BitsAdmin Suspicious Connection',
        description:
"This TLS client matched a variant of PowerShell." + "\n"+
"Investigate other client behaviors on the victim host." + "\n"+
"- ** PowerShell/BitsAdmin JA3 client match**" + "\n"+
"- **Client IP:** " + Flow.client.ipaddr + "\n"+
"- **JA3 Client Value:** " + ja3 + "\n"+
"- **JA3 Client Match:** " + suspect_ja3_hashes[ja3],
        riskScore: 60,
        participants: [{
            object:Flow.client.device,
            role: 'offender'
            }],
        identityKey: [
            Flow.server.ipaddr,
            Flow.client.ipaddr,
            hash
        ].join('!!'),
        identityTtl: 'hour',
});
```

Ces valeurs apparaissent dans la carte de détection, comme dans la figure suivante :



6. Cliquez **Enregistrer** puis cliquez sur **Terminé**.

   Voir Exemple de déclencheur de détection personnalisé pour un script annoté complet.

Votre détection personnalisée sera ajoutée au catalogue de détections lorsque votre déclencheur sera exécuté pour la première fois. Ajouter des catégories de détection et des techniques MITRE à la détection depuis le catalogue de détection.

Création d'un type de détection personnalisé

Après avoir créé un déclencheur pour générer votre détection personnalisée, vous pouvez créer un type de détection personnalisé dans le catalogue de détection pour ajouter des informations supplémentaires à votre détection.

Vous pouvez spécifier un nom d'affichage et ajouter des catégories de détection pour vous aider à localiser votre détection sur la page Détections. Vous pouvez également ajouter des liens MITRE, qui permettent à votre détection personnalisée d'apparaître dans la matrice de la page Grouper par technique MITRE.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Catalogue de détection**.
3. Sur la page Catalogue de détection, effectuez l'une des étapes suivantes :
   - Si votre déclencheur est déjà lancé, le système ajoute automatiquement votre détection personnalisée au catalogue avec le nom d'affichage spécifié dans le déclencheur précédé de `[personnalisé]`. Cliquez sur le type de détection à modifier.
   - Si votre type de détection n'a pas été créé, cliquez sur **Créez**.
4. Renseignez les champs suivants :

   Nom d'affichage

   Entrez un nom unique pour le titre de la détection.

   ID du type de détection

   Tapez la valeur que vous avez saisie pour l'ID du type de détection dans le déclencheur. Par exemple, si vous avez saisi : `commitDetection('network_segmentation_breach')`, l'ID du type de détection est « network_segmentation_breach ». Vous ne pouvez pas modifier l'ID du type de détection une fois le type de détection enregistré.

   Auteur

   Entrez l'auteur de la détection personnalisée.

   Technique MITRE

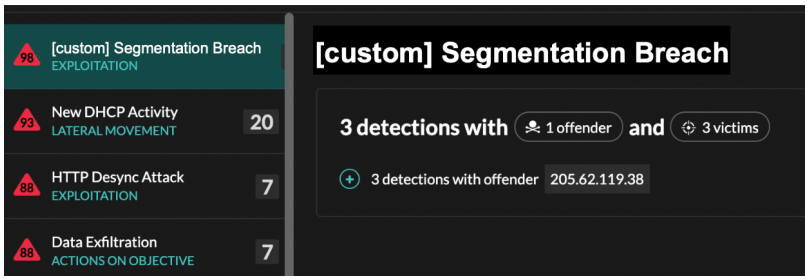
   Dans la liste déroulante, sélectionnez une ou plusieurs techniques MITRE que vous souhaitez associer à la détection.
5. Cliquez **Enregistrer**.

Afficher les détections personnalisées

Vous pouvez consulter les détections personnalisées sur le Détections page avec d'autres détections intégrées.

Regroupez la page des détections par type. Toutes les détections de la liste de détection sont regroupées par type de détection.

Par exemple, si votre nom d'affichage de détection est `[custom]Segmentation Breach`, l'entrée apparaîtrait dans la liste de détection comme dans la figure suivante :



En haut à gauche de la page, sélectionnez **Carte MITRE**. Les techniques MITRE liées à la détection personnalisée sont mises en évidence dans la matrice.

Prochaines étapes

Création d'une règle de notification de détection. Par exemple, vous pouvez configurer le système ExtraHop pour qu'il vous envoie un e-mail lorsque votre détection personnalisée se produit.

Exemple de déclencheur de détection personnalisé

Le script suivant est l'exemple complet de PowerShell/JA3 auquel il est fait référence dans ces instructions.

```
// If the server is internal, exit
if ( ! Flow.server.ipaddr.isExternal ) {
    return;
}
// If the TLS host name is not set, exit
if(SSL.host === null) { return; }

// Continue only if the TLS hostname belongs to one of the suspicious sites
if(SSL.host.match(/pastebin/i) || SSL.host.match(/raw.githubusercontent.com/
i) || SSL.host.match(/githack/i)) {

    // List of common PowerShell JA3 hashes
    let suspect_ja3_hashes = cache('suspect_ja3_hashes', () => ({
        '13cc575f247730d3eeb8ff01e76b245f':'PowerShell/BitsAdmin/PowerShell
 4.0 Windows Server 2012RT',
        '5e12c14bda47ac941fc4e8e80d0e536f':'PowerShell/BitsAdmin/PowerShell
 4.0 Windows Server 2012RT',
        '2c14bfb3f8a2067fbc88d8345e9f97f3':'PowerShell/BitsAdmin Windows
 Server 2012RT',
        '613e01474d42ebe48ef52dff6a20f079':'PowerShell/BitsAdmin Windows
 Server 2012RT',
        '05af1f5ca1b87cc9cc9b25185115607d':'BitsAdmin/PowerShell 5.0 Windows
 7 64 bit enterprise',
        '8c4a22651d328568ec66382a84fc505f':'BitsAdmin/PowerShell 5.0 Windows
 7 64 bit enterprise',
        '235a856727c14dba889ddee0a38dd2f2':'BitsAdmin/PowerShell 5.1 Server
 2016',
        '17b69de9188f4c205a00fe5ae9c1151f':'BitsAdmin/PowerShell 5.1 Server
 2016',
        'd0ec4b50a944b182fc10ff51f883ccf7':'PowerShell/BitsAdmin (Microsoft
 BITS/7.8) Server 2016',
        '294b2f1dc22c6e6c3231d2fe311d504b':'PowerShell/BitsAdmin (Microsoft
 BITS/7.8) Server 2016',
        '54328bd36c14bd82ddaa0c04b25ed9ad':'BitsAdmin/PowerShell 5.1 Windows
 10',
        'fc54e0d16d9764783542f0146a98b300':'BitsAdmin/PowerShell 5.1 Windows
 10',
        '2863b3a96f1b530bc4f5e52f66c79285':'BitsAdmin/PowerShell 6.0 Windows
 Server 2012RT',
        '40177d2da2d0f3a9014e7c83bdeee15a':'BitsAdmin/PowerShell 6.0 Windows
 Server 2012RT',
        '36f7277af969a6947a61ae0b815907a1':'PowerShell/BitsAdmin Windows 7
 32 bit enterprise',
    }));
    // Store the client JA3 hash in a variable
    const hash = SSL.ja3Hash;

    // Iterate through each PowerShell JA3 hash
    for ( let ja3 in suspect_ja3_hashes ) {

        // If the client JA3 hash is from PowerShell,
        // commit the detection
        if ( hash.includes(ja3) ) {
```

```
            commitDetection('PowerShell_JA3', {
                categories: ['sec.caution'],
                title: "PowerShell / BitsAdmin Suspicious Connection",
                // Specify the offender as the device object of the client
                participants: [
                    { role: 'offender', object: Flow.client.device }
                ],
                description:
                    "This TLS client matched a variant of PowerShell." +
 "\n"+
                    "Investigate other client behaviors on the victim host."
 + "\n"+
                    "- ** PowerShell/BitsAdmin JA3 client match**" + "\n"+
                    "- **Client IP:** " + Flow.client.ipaddr + "\n"+
                    "- **Server IP:** " + Flow.server.ipaddr + "\n"+
                    "- **JA3 Client Value:** " + ja3 + "\n"+
                    "- **JA3 Client Match:** " + suspect_ja3_hashes[ja3],
                // Create the identity key by combining the server IP
 address, client IP address, and PowerShell JA3 hash
                identityKey: [
                    Flow.server.ipaddr,
                    Flow.client.ipaddr,
                    hash
                ].join('!!'),
                riskScore: 60,
                identityTtl: 'hour'
            });
        }
    }
}
```

Télécharger des règles IDS personnalisées

Vous pouvez télécharger un ensemble personnalisé de règles IDS vers les capteurs IDS ExtraHop. Le système ExtraHop convertit les règles en types de détection qui génèrent des détections que vous pouvez consulter et examiner.

Ajoutez des règles formatées conformément aux directives de Suricata à un ou plusieurs fichiers .rules et téléchargez-les dans un fichier .zip. Lors du téléchargement, le système ExtraHop traite chaque règle, qui est affichée dans un tableau qui affiche l'ID de signature, le nom de chaque règle et l'un des statuts de règle suivants.

• **Accepté:** Le système ExtraHop a correctement traité la règle.

• **Rejeté:** Le système ExtraHop n'a pas pu traiter la règle. La règle peut contenir une erreur de mise en forme ou contenir une action, un protocole ou une option qui n'est pas actuellement pris en charge par le système ExtraHop. Contacter Assistance ExtraHop pour vous renseigner sur la prise en charge future de la règle.

• **Mise à niveau requise:** UNE une version plus récente du firmware ExtraHop est requise pour soutenir la règle. La version du système requise s' affiche.

Voici quelques considérations concernant les règles IDS personnalisées :

- Les règles IDS personnalisées doivent être formatées comme étant valides Fichier Suricata .rules.
- Un ou plusieurs fichiers Suricata .rules doivent être ajoutés à un seul fichier .zip pour le téléchargement.
- Vous ne pouvez pas télécharger plus de 10 000 règles IDS personnalisées.
- La suppression d'un fichier entraîne la suppression de toutes les règles associées au fichier chargé et peut prendre plusieurs minutes. Les utilisateurs peuvent continuer à voir des détections basées sur ces règles jusqu'à ce que la suppression soit terminée.

- Le remplacement d'un fichier supprime toutes les règles associées au fichier précédemment chargé, puis traite les règles du nouveau fichier.
- Les règles IDS intégrées ne sont ni supprimées ni remplacées lorsque vous gérez vos règles IDS personnalisées. Votre système ExtraHop est connecté à ExtraHop Cloud Services et les dernières règles intégrées sont automatiquement téléchargées sur le système lorsque des versions mises à jour sont disponibles.

  Note: ExtraHop peut revoir les règles téléchargées afin de vérifier l' exactitude des conversions et de guider l'amélioration du produit en termes de conversion, d'exactitude et de performances des règles Suricata.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Règles IDS personnalisées**.
3. Cliquez **Télécharger un fichier**.
4. Cliquez **Choisissez un fichier**, sélectionnez le fichier .zip de votre choix, puis cliquez sur **Télécharger un fichier**.
   Le processus de téléchargement peut prendre plusieurs minutes. L'état du fichier et ses horodatages sont mis à jour une fois le traitement terminé.

Prochaines étapes
Cliquez **Détections** depuis la page du menu de navigation supérieure pour afficher les détections générées à partir de règles IDS personnalisées. Ces détections indiquent que la règle a été fournie par un fichier IDS personnalisé et inclut l'ID de signature de la règle.

Détections de syntonisation

Le réglage de la détection vous permet de réduire le bruit et de détecter les détections critiques nécessitant une attention immédiate.

Il existe deux manières de régler les détections : vous pouvez ajouter des paramètres de réglage qui empêchent la génération de détections, ou vous pouvez créer des règles d'exceptions qui masquent les détections existantes en fonction du type de détection, des participants ou des propriétés de détection.

Vidéo: Consultez la formation associée : Configurer les règles de réglage

Paramètres de réglage

Les paramètres de réglage vous permettent de spécifier des domaines connus et fiables, des serveurs DNS et des cibles HTTP CONNECT qui ne doivent pas générer de détection. Vous pouvez également activer des paramètres de réglage qui suppriment les détections fréquentes et redondantes associées aux périphériques de passerelle et aux nœuds Tor.

Les paramètres de réglage sont gérés à partir du Paramètres de réglage page.

Règles de réglage

Les règles de réglage vous permettent de spécifier des critères qui masquent les détections qui ont été générées, mais dont la valeur est faible et qui ne nécessitent aucune attention.

Note: Les règles de réglage peuvent ne pas masquer certaines détections si vos capteurs de paquets n'utilisent pas la même version de microprogramme que celle de votre console.

Les règles de réglage masquent toutes les détections passées, en cours et futures et les participants qui correspondent aux critères spécifiés et affectent les zones système suivantes :

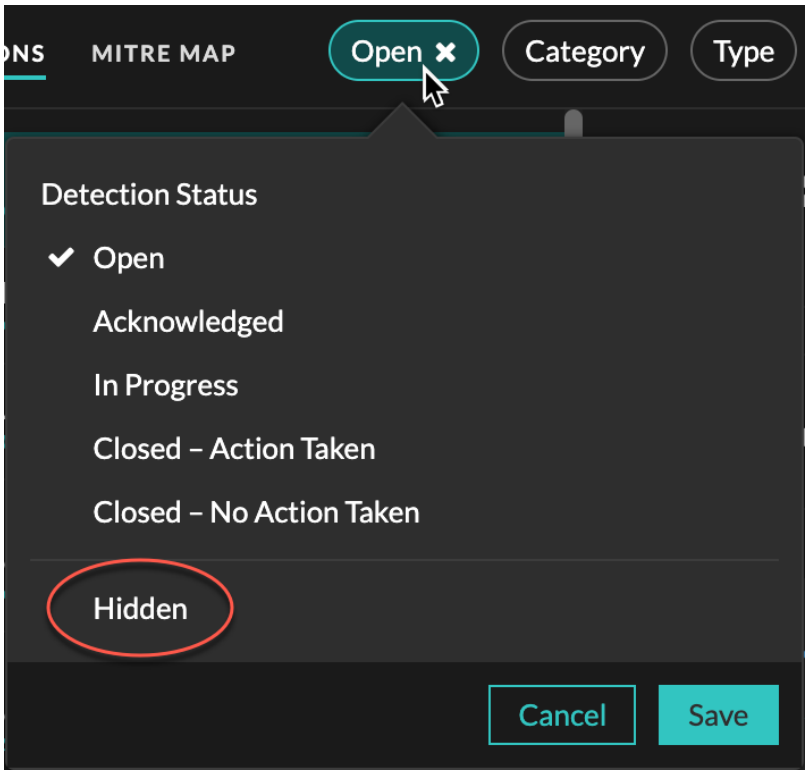
- Les détections masquées n'entraînent pas l'exécution de déclencheurs et d'alertes associés lorsque la règle est activée.
- Les détections masquées n'apparaissent pas en tant que marqueurs de détection dans les graphiques.
- Les détections masquées n'apparaissent pas sur les cartes d'activité, mais les participants cachés apparaîtront sur les cartes d'investigation.

- Les détections masquées n'apparaissent pas dans le nombre de détections sur les pages associées, telles que la page Aperçu de l'appareil ou la page Activité.
- Les détections et les participants masqués n'apparaissent pas dans le rapport sur les opérations de sécurité.
- Les détections masquées ne sont pas incluses dans les notifications par e-mail et par webhook.
- Les détections masquées ne sont pas exportées vers un SIEM ou un SOAR intégré.

Note: Si vous ne voyez aucun marqueur de détection pour une détection, vérifiez que marqueurs de détection n'ont pas été désactivés.

Afficher les détections masquées
En appliquant le statut Masqué sur la page Détections, vous pouvez afficher les détections actuellement masquées par une règle de réglage.

Le filtre Ouvrir est sélectionné par défaut sur la page Détections. Cliquez sur le **Ouvert** filtre pour accéder à d'autres options de filtrage. Si le filtre Ouvrir n'est pas appliqué, cliquez sur **État** pour afficher les options de filtre, puis cliquez sur **Caché**. Le résumé des détections masquées s'affiche uniquement.



Le résumé identifie les règles de réglage qui masquent actuellement les détections sélectionnées, les participants masqués, les propriétés de détection et les localisations du réseau.

Cliquez sur une règle de réglage, un participant, une propriété ou une valeur de localité du réseau pour afficher un résumé des détections masquées associées à la valeur sélectionnée.

Les participants

Répertorie à la fois les délinquants et les victimes qui sont actuellement masqués. Les listes des délinquants et des victimes sont classées en fonction du nombre de détections où le participant est caché.

Valeurs des propriétés

Répertorie les valeurs des propriétés associées au type de détection masqué. La liste des valeurs de propriété est ordonnée en fonction du nombre de détections où la valeur de propriété est masquée.

Localités du réseau concernées

Répertorie les localités du réseau qui contiennent des détections masquées du type sélectionné . La liste des localités du réseau concernées est ordonnée en fonction du nombre de détections masquées dans la localité du réseau.

En filtrant les résultats pour une seule règle de réglage, un seul participant, une propriété ou une localité, vous pouvez afficher le nombre de détections masquées associées à la valeur spécifiée. Cliquez sur le **Afficher les détections** bouton pour afficher les cartes de détection individuelles.

Meilleures pratiques de réglage

Il est préférable de créer un paramètre ou une règle unique plus large au lieu de créer plusieurs paramètres et règles qui se chevauchent.

Voici quelques recommandations qui vous aideront à optimiser le réglage de votre détection :

- Commencez par ajouter des paramètres de réglage pour éviter les détections impliquant des agents connus ou fiables. N'oubliez pas de consulter le Paramètres de réglage et Localités du réseau pages pour les paramètres existants afin d'éviter la redondance.
- Déterminez si vous souhaitez masquer toutes les détections pour un participant spécifique, tel qu'un analyseur de vulnérabilités, et sélectionnez **Tous les types de détection**. Si vous souhaitez masquer les données par rôle d'équipement, augmentez la portée jusqu'à un groupe d'équipements.
- Quand un **Adresse IP ou bloc CIDR** est sélectionné dans la liste déroulante du délinquant ou de la victime, ajoutez ou supprimez des entrées de la liste dans le champ Adresses IP pour augmenter ou réduire la portée de la règle de réglage.
- Par défaut, les règles d'exceptions expirent au bout de 8 heures. Vous pouvez sélectionner un autre délai d'expiration dans la liste déroulante ou sélectionner un nouveau délai d'expiration après avoir réactivé une règle expirée dans le Règles de réglage page.
- Le système ExtraHop supprime automatiquement les détections qui sont dans le système depuis 21 jours depuis l'heure de début de la détection, qui ne sont pas en cours et qui sont masquées. Si une règle de réglage récemment créée ou modifiée masque une détection qui correspond à ce critère, la détection concernée ne sera pas supprimée pendant 48 heures.
- Lorsque vous ajoutez une règle de réglage, si vous identifiez un équipement qui n'est pas classé correctement, vous pouvez modifier le rôle de l'équipement.
- Certaines détections peuvent nécessiter une règle de réglage précise basée sur une propriété spécifique de la détection. Sous l'en-tête Propriété, cliquez sur la case à cocher à côté d'une propriété pour spécifier une valeur ou une expression régulière et ajouter des critères pour une règle de réglage ciblée.
- Appliquez le **Caché** filtre d'état vers le Détections page pour afficher les détections qui sont actuellement masqué par des règles d'exceptions.

Apprenez comment supprimer les détections à l'aide de paramètres de réglage et masquer les détections à l'aide de règles de réglage .

Supprimez les détections à l'aide de paramètres de réglage

Fournissez des informations sur votre environnement réseau afin que le système ExtraHop puisse empêcher la génération de détections de faible valeur ou redondantes.

Vous pouvez ajouter des critères à partir du Paramètres de réglage page ou directement depuis une carte de détection. De plus, vous pouvez spécifier les localités du réseau, qui classent les plages d'adresses IP comme internes ou externes à votre réseau.

En savoir plus sur détections de réglage.

Vidéos Consultez la formation associée : Configuration des paramètres de réglage

Spécifier les paramètres de réglage pour les détections et les métriques

Spécifiez les paramètres de réglage pour améliorer les métriques et empêcher la génération de détections de faible valeur.

Si votre déploiement ExtraHop inclut une console, nous vous recommandons gestion des transferts de tous les capteurs connectés à la console.

Note: Les champs de cette page peuvent être ajoutés, supprimés ou modifiés au fil du temps par ExtraHop.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Paramètres de réglage**.
3. Spécifiez des valeurs pour l'un des paramètres suivants disponibles sur la page.

Option	Description
Appareils Gateway	Par défaut, les périphériques de passerelle sont ignorés par les détections basées sur des règles car elles peuvent entraîner des détections redondantes ou fréquentes. Sélectionnez cette option pour identifier les problèmes potentiels liés aux périphériques de passerelle tels que vos pare-feux, routeurs et passerelles NAT. Ce paramètre n'affecte pas les détections par apprentissage automatique.
Nœuds Tor sortants	Par défaut, les connexions sortantes vers des nœuds Tor connus sont ignorées par les détections basées sur des règles car elles peuvent entraîner des détections de faible valeur dans des environnements avec un trafic Tor minimal. Sélectionnez cette option pour identifier les détections sur les connexions sortantes vers des nœuds Tor connus si votre environnement observe un trafic Tor sortant important.
Nœuds Tor entrants	Par défaut, les connexions entrantes provenant de nœuds Tor connus sont ignorées par les détections basées sur des règles car elles peuvent entraîner des détections de faible valeur dans des environnements avec un trafic Tor minimal. Sélectionnez cette option pour identifier les détections sur les connexions entrantes provenant de nœuds Tor connus si votre environnement détecte un trafic Tor entrant important.
Détection de balisage accélérée	Par défaut, le système ExtraHop détecte les événements de balisage potentiels via HTTP et TLS. Sélectionnez cette option pour détecter les événements de balisage plus rapidement que la détection par défaut.

Option	Description
	Notez que l'activation de cette option peut améliorer la détection des événements de balisage qui ne sont pas malveillants.
Détections IDS	Par défaut, les systèmes ExtraHop connectés Capteurs du système de détection d'intrusion (IDS) ne détectez que le trafic à l'intérieur de votre réseau. Sélectionnez cette option pour générer des détections IDS pour le trafic entrant depuis un point de terminaison externe. Notez que l'activation de cette option peut augmenter considérablement le nombre de détections IDS.
Comptes Active Directory privilégiés	Spécifiez des expressions régulières (regex) qui correspondent aux comptes Active Directory privilégiés de votre environnement. La liste de paramètres inclut une liste par défaut d'expressions régulières pour les comptes privilégiés courants que vous pouvez modifier. Le système ExtraHop identifie les comptes privilégiés et suit l' activité des comptes dans les enregistrements et mesures Kerberos.
Serveurs DNS publics autorisés	Spécifiez les serveurs DNS publics autorisés dans votre environnement que vous souhaitez que les détections basées sur des règles ignorent. Spécifiez une adresse IP ou un bloc CIDR valide.
Cibles HTTP CONNECT autorisées	Spécifiez les URI auxquels votre environnement peut accéder via la méthode HTTP CONNECT. Les URI doivent être formatés comme *<hostname>: <numéro de port>* . Les caractères génériques et Regex ne sont pas pris en charge. Si vous ne spécifiez aucune valeur, aucune détection basée sur ce paramètre n'est générée.
Domaines fiables	Ajoutez des domaines connus légitimes à la liste des domaines de confiance afin de supprimer les détections futures ciblant des activités malveillantes pour ce domaine. Tapez un seul nom de domaine par champ. Si vous spécifiez un nom de domaine, le paramètre de réglage supprime les détections pour tous les sous-domaines. Par exemple, si vous ajoutez exemple.com en tant que domaine sécurisé, les détections impliquant vendor.example.com comme étant le contrevenant sont également supprimées. Si vous ajoutez un sous-domaine tel que vendor.example.com, le paramètre supprime

Option	Description
	uniquement les détections où le participant se termine par ce sous-domaine exact. Dans cet exemple, test.vendor.example.com serait supprimé mais pas test.example.com. Les caractères génériques et Regex ne sont pas pris en charge. Pour ajouter plusieurs noms de domaine fiables, cliquez sur **Ajouter un domaine**. Pour les détections associées à un domaine, vous pouvez également ajouter un domaine de confiance directement à partir d'une carte de détection.

4. Cliquez **Enregistrer**.

Prochaines étapes
Cliquez **Détections** depuis le menu de navigation supérieur pour voir les détections.

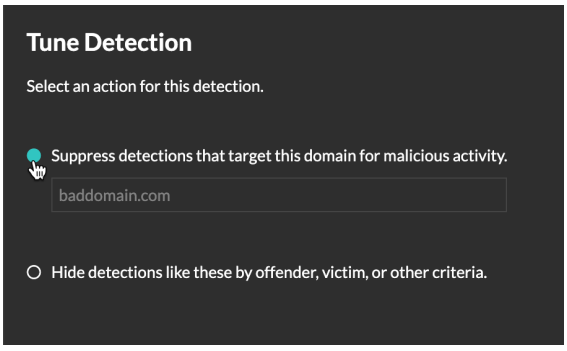
Ajouter un paramètre de réglage à partir d'une carte de détection

Si vous rencontrez une détection de faible valeur, vous pouvez ajouter des paramètres de réglage directement à partir d'une carte de détection pour empêcher la génération de détections similaires.

Avant de commencer
Les utilisateurs doivent disposer d'une écriture complète ou supérieure privilèges pour régler une détection.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez **Actions** depuis le coin inférieur gauche de la carte de détection.
4. Cliquez **Détection des réglages...**.

   Si le type de détection est associé à un paramètre de réglage, l' option permettant de supprimer la détection en ajoutant un paramètre de réglage s'affiche. Si aucun paramètre de réglage n'est associé à la détection, vous pouvez masquer la détection à l'aide d'une règle de réglage.



5. Cliquez sur **Supprimer les détections...** option et cliquez **Enregistrer**.

   La confirmation de l'ajout d'un paramètre de réglage s'affiche et le nouveau paramètre est ajouté au Paramètres de réglage page.

Masquer les détections à l'aide de règles d'exceptions

Les règles de réglage vous permettent de masquer les détections qui correspondent à des critères spécifiques.

Pour éviter de créer des règles redondantes, assurez-vous d'abord d'ajouter des informations sur votre environnement réseau au système ExtraHop en spécification des paramètres de réglage.

En savoir plus sur détections de réglage.

Création d'une règle de réglage

Créez des règles de réglage pour rationaliser votre liste de détection en spécifiant des critères qui masquent les détections passées, présentes et futures qui sont de faible valeur et ne nécessitent pas d'attention.

Avant de commencer
Les utilisateurs doivent avoir une écriture complète ou supérieure privilèges pour créer une règle de réglage.

En savoir plus sur meilleures pratiques de réglage.

Ajouter une règle de réglage à partir d'une carte de détection
Si vous rencontrez une détection de faible valeur, vous pouvez créer une règle de réglage directement à partir d'une carte de détection pour masquer les détections similaires dans le système ExtraHop.

Avant de commencer
Les utilisateurs doivent avoir une écriture complète ou supérieure privilèges pour régler une détection.

En savoir plus sur meilleures pratiques de réglage.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez **Actions** depuis le coin inférieur gauche de la carte de détection.
4. Cliquez **Détection des réglages...**.

   Si le type de détection est associé à un paramètre de réglage, vous verrez apparaître une option pour supprimer la détection. Si vous souhaitez toujours créer une règle de réglage, sélectionnez l'option Masquer les détections comme celles-ci... et cliquez sur Enregistrer.
5. Spécifiez le critères des règles de réglage et cliquez **Créez**.

   La règle est ajoutée à la page Règles de réglage. En savoir plus sur gestion des règles de réglage.

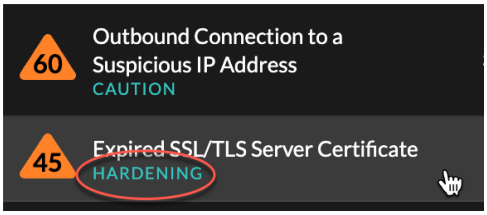
Ajouter une règle de réglage à partir d'une détection de durcissement
Cliquez sur une détection renforcée pour afficher un résumé de tous les actifs, propriétés de détection et emplacements réseau associés à ce type de détection. Vous pouvez filtrer le résumé en cliquant sur l'une des valeurs associées, puis créer une règle de réglage pour masquer les détections en fonction des résultats affichés.

Avant de commencer
Les utilisateurs doivent avoir une écriture complète ou supérieure privilèges pour régler une détection.

En savoir plus sur filtrage et réglage des détections de durcissement.

En savoir plus sur meilleures pratiques de réglage.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez sur n'importe quelle détection de renforcement dans la liste de détection.



4. Filtrez les résultats sur la page récapitulative du durcissement.
   a) Cliquez sur un actif affecté pour afficher uniquement les détections où cet actif participe à une détection.
   b) Cliquez sur une valeur de propriété pour afficher uniquement les détections associées à la valeur de propriété de détection sélectionnée.
   c) Cliquez sur une localité du réseau pour afficher uniquement les détections où le participant se trouve dans la localité du réseau sélectionnée.
5. Cliquez **Création d'une règle de réglage**.

   Critères des règles de réglage sont automatiquement renseignés pour refléter les résultats filtrés de la page de résumé du durcissement.
6. Cliquez **Créez**.

   La règle est ajoutée à la page Règles de réglage. En savoir plus sur gestion des règles de réglage.

Ajouter une règle de réglage depuis la page Règles de réglage
Créez des règles d'exceptions pour masquer les détections par type de détection, participant ou propriétés de détection spécifiques.

Avant de commencer
Les utilisateurs doivent disposer d'une écriture complète ou supérieure privilèges pour régler une détection.

En savoir plus sur bonnes pratiques de réglage.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Règles de réglage**.
3. Cliquez **Créez**.
4. Spécifiez critères des règles de réglage et cliquez **Enregistrer**.

   La règle est ajoutée au tableau Règles de réglage.

Critères des règles de réglage

Sélectionnez l'un des critères suivants pour déterminer quelles détections sont masquées par une règle de réglage.

Type de détection

Créez une règle de réglage qui s'applique à un seul type de détection ou choisissez de l'appliquer à tous les types de détection de sécurité ou de performance, en fonction du module système. Les règles qui englobent tous les types de détection de sécurité sont généralement réservées aux activités associées aux scanners de vulnérabilités.

Les participants

Créez une règle de réglage qui masque les détections en fonction de participants spécifiques au délinquant et à la victime.

Spécifiez les participants à une règle de réglage à l'aide de l'une des sélections suivantes.

Tout délinquant ou victime

Vous pouvez spécifier N'importe quel délinquant ou N'importe quelle victime pour masquer tous les participants. Cette option est efficace pour masquer les détections lors de tests planifiés ou d'analyses de vulnérabilités.

Groupe d'appareils ou appareils

Vous pouvez spécifier un équipement découvert ou groupe d'équipements pour masquer les participants. Par exemple, vous pouvez spécifier le groupe déquipements intégré pour les scanners de vulnérabilité afin de masquer les détections auxquelles un scanner interne est participant.

Note: Les règles de réglage sont appliquées lorsque des détections ou des règles de réglage sont créées ou mises à jour. Les règles de réglage ne sont pas appliquées rétroactivement aux détections existantes lorsqu'un participant est ajouté ou retiré d'un groupe dequipments dynamique.

Service de numérisation externe

Vous pouvez spécifier un service de numérisation externe en tant que participant à une règle de réglage. Le système ExtraHop masque les services de numérisation externes en fonction de la plage d'adresses IP associée au service.

Adresse IP ou bloc CIDR

Vous pouvez spécifier une adresse IP unique ou un bloc d' adresses IP CIDR pour masquer tout participant compris dans cette plage. Par exemple, si une équipe effectue un test dintrusion sur un sous-réseau spécifique, vous pouvez créer une règle de réglage avec les adresses IP du sous-réseau afin d'éviter un pic de détections liées aux outils d'énumération et de piratage.

Note: Les détections sont masquées en fonction de l'adresse IP au moment de la détection. Étant donné que les adresses IP des appareils découverts et des points de terminaison externes peuvent changer de manière dynamique, la spécification d'une adresse IP unique n'est fiable que si le point de terminaison possède une adresse IP statique.

Nom d'hôte ou domaine

Vous pouvez spécifier un nom d'hôte, un nom de domaine ou une indication de nom de serveur (SNI) pour masquer un participant qui n'a pas été découvert par le système ExtraHop. Si vous spécifiez un nom de domaine, la règle de réglage masquera tous les sous-domaines. Par exemple, si vous créez une règle de réglage avec vendor.com comme délinquant, la règle de réglage masquera les détections avec example.vendor.com comme délinquant. Si vous spécifiez un sous-domaine tel que example.vendor.com, la règle de réglage masquera uniquement les détections où le participant se termine par ce sous-domaine exact. Dans cet exemple, test.example.vendor.com serait masqué mais pas test.vendor.com.

Note: Les règles de réglage ne masqueront pas les appareils découverts par nom d'hôte. Vous pouvez ajouter des appareils découverts en tant que critères de règle de réglage en spécifiant une adresse IP, un équipement ou un groupe déquipements.

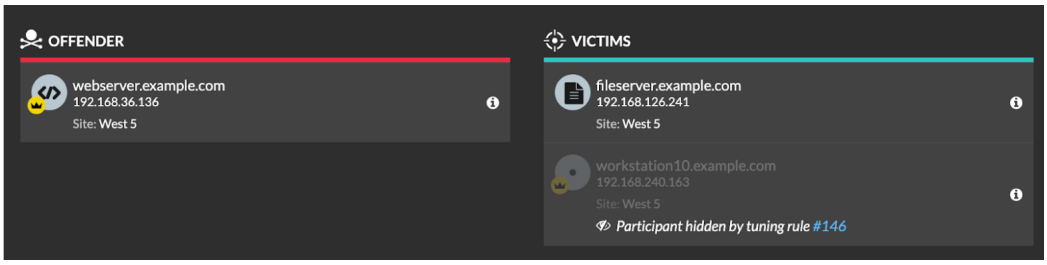
Localité du réseau

Vous pouvez spécifier localité du réseau pour masquer les participants à l'adresse IP de cette localité.

Note: Les règles de réglage masqueront uniquement les participants dont les adresses IP spécifiques sont incluses dans la localité du réseau. Si une autre adresse IP est attribuée à un équipement en dehors du bloc CIDR de localité du réseau, cet équipement ne sera pas masqué.

Voici quelques considérations importantes concernant le réglage des participants :

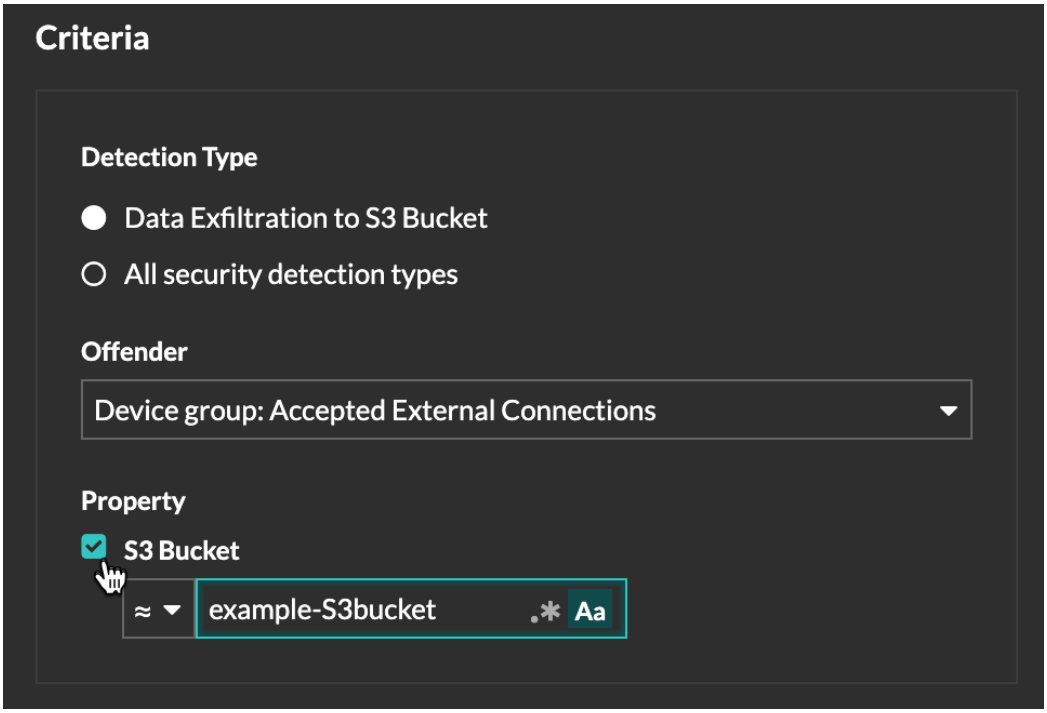
- Lorsque les critères de participation pour une règle de réglage ne correspondent qu'à une partie de la liste des participants d'une détection, le système masque les participants spécifiés dans la règle de réglage sans masquer la totalité de la détection.



- Les participants spécifiés comme critères de réglage, y compris les blocs CIDR et les services d'analyse externes, seront masqués même s'ils se connectent via une passerelle ou un équilibreur de charge.

Propriétés de détection

Créez une règle de réglage qui masque les détections par une propriété spécifique. Par exemple, vous pouvez masquer les détections de ports SSH rares pour un numéro de port unique, ou l'exfiltration de données vers les détections de compartiment S3 pour un compartiment S3 spécifique.



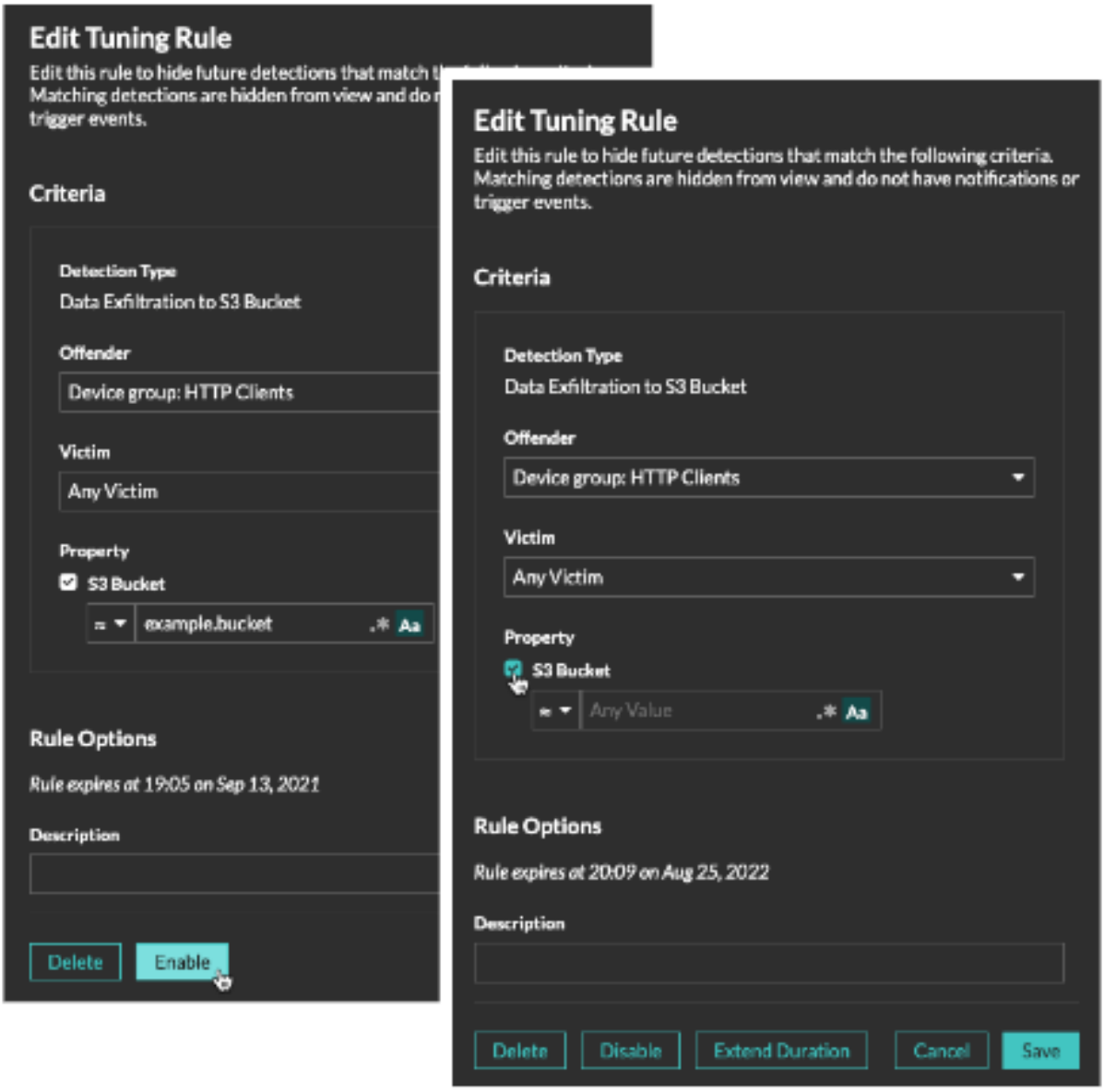
Gérer les règles de réglage

Vous pouvez modifier les critères ou prolonger la durée d'une règle, réactiver une règle et désactiver ou supprimer une règle.

En haut de la page, cliquez sur l'icône Paramètres du système et sélectionnez **Règles de réglage**.

Cliquez sur une règle de réglage dans Règles de réglage table pour ouvrir le Modifier la règle de réglage panneau. Mettez à jour les participants, les critères de règle ou les propriétés pour ajuster la portée de la

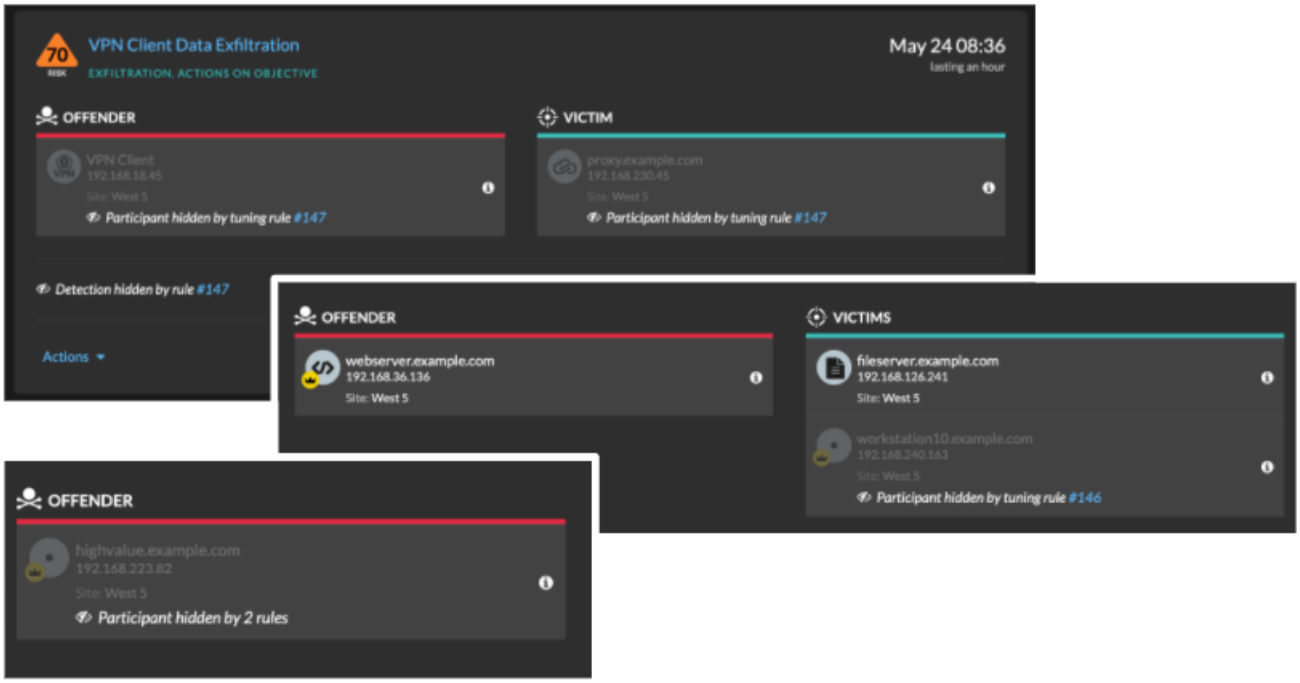
règle. Cliquez sur les boutons situés en bas du panneau pour supprimer, désactiver, activer ou prolonger la durée d'une règle.



- Une fois que vous avez désactivé ou supprimé une règle, celle-ci expire immédiatement et les déclencheurs et alertes associés reprennent.
- Une fois que vous avez désactivé une règle, les détections précédemment masquées restent masquées ; les détections en cours apparaissent.
- La suppression d'une règle affiche les détections précédemment masquées.
- Le système ExtraHop supprime automatiquement les détections présentes sur le système depuis 21 jours depuis le début de la détection, qui ne sont pas en cours et qui sont masquées. Si une règle de réglage nouvellement créée ou modifiée masque une détection répondant à ces critères, la détection concernée ne sera pas supprimée pendant 48 heures.

Vous pouvez appliquer le Statut masqué à la page Détections pour afficher uniquement les détections qui sont actuellement masqué par une règle de réglage.

Chaque détection ou participant masqué inclut un lien vers la règle de réglage associée et affiche le nom d'utilisateur de l'utilisateur qui a créé la règle. Si la détection ou le participant est masqué par plusieurs règles, le nombre de règles applicables apparaît.



Filtrer et régler les détections de durcissement

Les détections de la catégorie Renforcement contribuent à atténuer le risque d'exploitation. Vous pouvez trier un grand nombre de détections de durcissement en filtrant et en ajustant la page Détections.

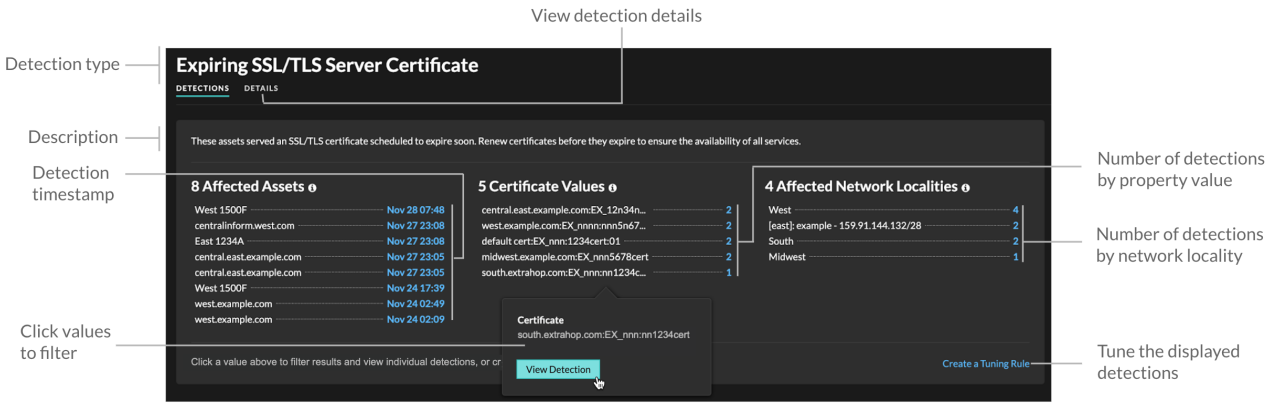
Avant de commencer

Les utilisateurs doivent être autorisés privilèges pour afficher les détections et doit disposer de privilèges d'écriture complets ou supérieurs pour créer une règle de réglage.

En savoir plus sur détections de réglage.

En savoir plus sur bonnes pratiques de réglage.

Cliquez sur une détection de durcissement dans Détections page pour consulter le résumé. Les résumés de détection renforcés identifient le type de détection, les actifs qui participent aux détections de ce type, les propriétés de détection et les localités du réseau qui contiennent les actifs concernés.



Cliquez sur n'importe quelle valeur d'actif, de propriété ou de localité de réseau pour afficher les détections individuelles associées à cette valeur.

Actifs concernés

Liste des actifs participant au renforcement des détections du type sélectionné. La liste des actifs concernés est triée selon l'heure la plus récente à laquelle la détection a eu lieu.

Valeurs des propriétés

Liste des valeurs de propriétés clés associées au type de détection. Par exemple, le type de détection Weak Cipher Suite répertorie les suites de chiffrement référencées dans les détections, et la détection des certificats de serveur TLS expirant répertorie les certificats dont l'expiration est programmée. La liste des valeurs de propriété est triée en fonction du nombre de détections contenant la valeur de propriété.

Localités du réseau touchées

Liste des localités du réseau contenant des détections de durcissement du type sélectionné. La liste des localités du réseau concernées est triée en fonction du nombre de détections dans la localité du réseau.

En filtrant les résultats sur un actif, une propriété ou une localité unique, vous pouvez identifier les détections qui affectent des systèmes critiques ou créer une règle de réglage qui masque les détections de faible valeur similaires aux résultats filtrés.

Activer le suivi des détections

Le suivi des détections vous permet d'attribuer une détection à un utilisateur, de définir son statut et d' ajouter des notes. Vous pouvez suivre les détections directement dans le système ExtraHop, avec un système de billetterie externe tiers, ou avec les deux méthodes.

Note: Vous devez activer le suivi des tickets sur tous les capteurs connectés.

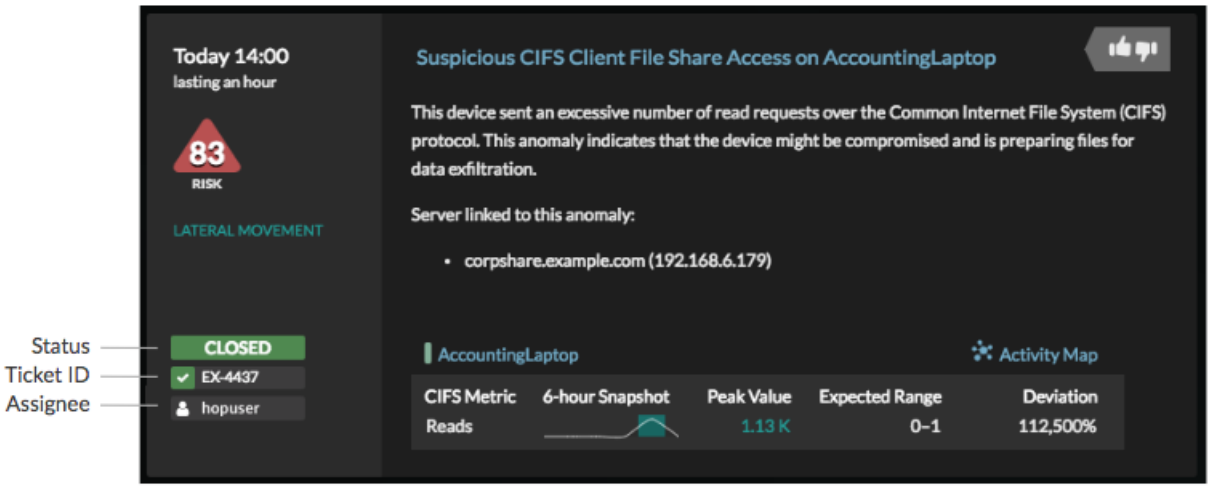
Avant de commencer

- Vous devez avoir accès à un système ExtraHop avec un compte utilisateur doté de Privilèges d'administration.
- Après avoir activé le suivi externe des tickets, vous devez configurer le suivi des tickets par des tiers en écrivant un déclencheur pour créer et mettre à jour des tickets sur votre système de billetterie, puis activez les mises à jour des tickets sur votre système ExtraHop via l'API REST.
- Si vous désactivez le suivi externe des tickets, les informations de statut et de ticket des destinataires précédemment stockées sont converties en suivi de détection ExtraHop. Si le suivi de détection depuis le système ExtraHop est activé, vous pourrez consulter les tickets qui existaient déjà lorsque vous avez désactivé le suivi des tickets externes, mais les modifications apportées à ce ticket externe n'apparaîtront pas dans le système ExtraHop.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Suivi de la détection**.
3. Sur la page de présentation, cliquez sur **Paramètres du système** puis cliquez sur **Toute l'administration**.
4. À partir du Paramètres de la console section, cliquez sur **Suivi de la détection**.
5. Sélectionnez l'une des méthodes suivantes ou les deux pour suivre les détections :
   - Sélectionnez **Permettre aux utilisateurs d'ExtraHop de suivre les détections depuis le système ExtraHop**.
   - Sélectionnez **Activez des intégrations externes, telles que les systèmes SOAR ou de suivi des tickets, pour suivre les détections via l'API ExtraHop Rest** .

6. Optionnel : Après avoir sélectionné l'option permettant d'activer les intégrations externes, spécifiez le modèle d'URL pour votre système de billetterie et ajoutez le *$ticket_id* variable à l'endroit approprié. Par exemple, saisissez une URL complète telle que `https://jira.example.com/browse/$ticket_id`. Le *$ticket_id* La variable est remplacée par l'identifiant du ticket associé à la détection.

   Une fois le modèle d'URL configuré, vous pouvez cliquer sur l'ID du ticket dans une détection pour ouvrir le ticket dans un nouvel onglet de navigateur.



Prochaines étapes
Si vous avez activé les intégrations externes de suivi des tickets, vous devez passer à la tâche suivante :

- Configurer le suivi des tickets par des tiers pour les détections

Configurer le suivi des tickets par des tiers pour les détections

Le suivi des tickets vous permet de connecter les tickets, les alarmes ou les dossiers de votre système de suivi du travail aux détections ExtraHop. Tout système de billetterie tiers capable d'accepter les requêtes Open Data Stream (ODS), tel que Jira ou Salesforce, peut être lié aux détections ExtraHop.

Avant de commencer

- Tu dois avoir a sélectionné l'option de suivi de la détection par des tiers dans les paramètres d'administration.
- Vous devez avoir accès à un système ExtraHop avec un compte utilisateur doté de Privilèges d'administration du système et des accès.
- Vous devez être familiarisé avec l'écriture de ExtraHop Triggers. Voir éléments déclencheurs et les procédures de Créez un déclencheur.
- Vous devez créer une cible ODS pour votre serveur de suivi des tickets. Consultez les rubriques suivantes concernant la configuration des cibles ODS : HTTP, Kafka, MongoDB, syslog, ou données brutes.
- Vous devez être familiarisé avec l'écriture de scripts d'API REST et disposer d'une clé d'API valide pour effectuer les procédures ci-dessous. Voir Générer une clé API.

Rédigez un déclencheur pour créer et mettre à jour des tickets concernant les détections sur votre système de billetterie
Cet exemple montre comment créer un déclencheur qui exécute les actions suivantes :

- Créez un nouveau ticket dans le système de billetterie chaque fois qu'une nouvelle détection apparaît sur le système ExtraHop.
- Attribuer de nouveaux tickets à un utilisateur nommé `escalations_team` dans le système de billetterie.
- Exécuté chaque fois qu'une détection est mise à jour sur le système ExtraHop.

- Envoyez des mises à jour de détection via un flux de données ouvert (ODS) HTTP au système de billetterie.

L'exemple de script complet est disponible à la fin de cette rubrique.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Nouveau**.
4. Spécifiez un nom et une description facultative pour le déclencheur.
5. Dans la liste des événements, sélectionnez **MISE À JOUR DE DÉTECTION**.

   L'événement DETECTION_UPDATE s'exécute chaque fois qu'une détection est créée ou mise à jour dans le système ExtraHop.
6. Dans le volet droit, spécifiez Classe de détection paramètres d'un objet JavaScript. Ces paramètres déterminent les informations envoyées à votre système de billetterie.

   L'exemple de code suivant ajoute l'identifiant de détection, la description, le titre, les catégories, les techniques et tactiques MITRE, ainsi que l'indice de risque à un objet JavaScript appelé `payload`:

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
 Detection.title;
const description = "ExtraHop has detected the following event on your
 network: " + Detection.description
const payload = {
    "fields": {
        "summary": summary,
        "assignee": {
            "name": "escalations_team"
        },
        "reporter": {
            "name": "ExtraHop"
        },
        "priority": {
            "id": Detection.riskScore
        },
        "labels": Detection.categories,
        "mitreCategories": Detection.mitreCategories,
        "description": description
    }
};
```

7. Définissez ensuite les paramètres de requête HTTP dans un objet JavaScript situé sous l'objet JavaScript précédent.

   L'exemple de code suivant définit une requête HTTP pour la charge utile décrite dans l'exemple précédent : définit une requête avec une charge utile JSON :

```
const req = {
    'path': '/rest/api/issue',
    'headers': {
        'Content-Type': 'application/json'
    },
    'payload': JSON.stringify(payload)
};
```

   Pour plus d'informations sur les objets de requête ODS, voir Classes de flux de données ouvertes.
8. Enfin, spécifiez la requête HTTP POST qui envoie les informations à la cible ODS. L'exemple de code suivant envoie la requête HTTP décrite dans l'exemple précédent à une cible ODS nommée ticket-server :

```
Remote.HTTP('ticket-server').post(req);
```

Le code du déclencheur complet doit ressembler à l'exemple suivant :

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
 Detection.title;
const description = "ExtraHop has detected the following event on your
 network: " + Detection.description
const payload = {
    "fields": {
        "summary": summary,
        "assignee": {
            "name": "escalations_team"
        },
        "reporter": {
            "name": "ExtraHop"
        },
        "priority": {
            "id": Detection.riskScore
        },
        "labels": Detection.categories,
        "mitreCategories": Detection.mitreCategories,
        "description": description
    }
};

const req = {
    'path': '/rest/api/issue',
    'headers': {
        'Content-Type': 'application/json'
    },
    'payload': JSON.stringify(payload)
};

Remote.HTTP('ticket-server').post(req);
```

Envoyer les informations de ticket aux détections via l'API REST
Après avoir configuré un déclencheur pour créer des tickets à détecter dans votre système de suivi des tickets, vous pouvez mettre à jour les informations relatives aux tickets sur votre système ExtraHop via l'API REST .

Les informations relatives aux tickets apparaissent dans les détections sur la page Détections du système ExtraHop. Pour plus d'informations, consultez Détections sujet.

L'exemple de script Python suivant extrait les informations de ticket d'un tableau Python et met à jour les détections associées sur le système ExtraHop.

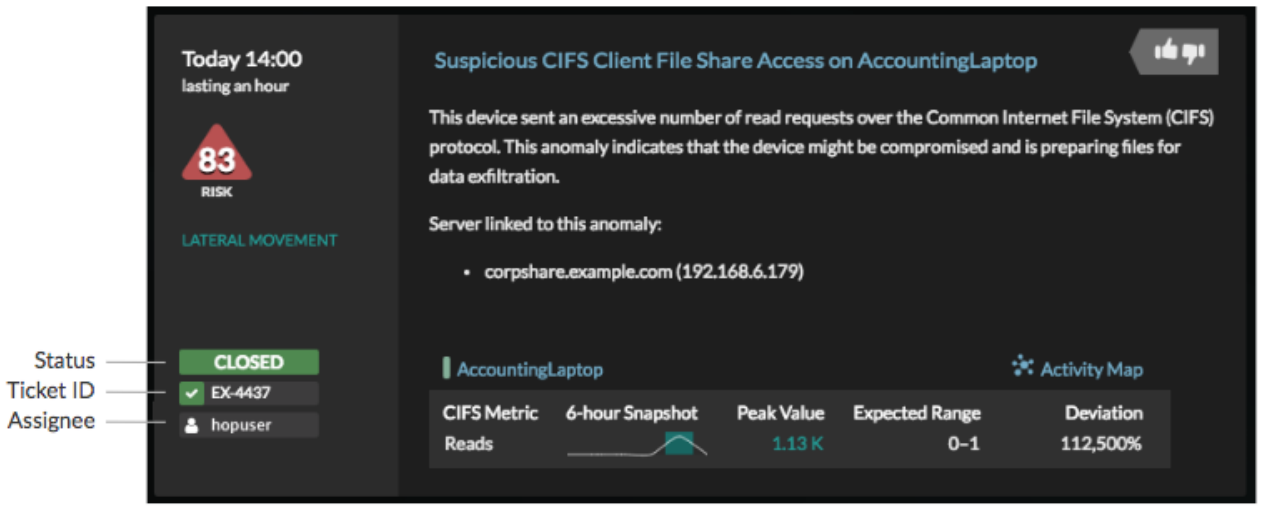
```
#!/usr/bin/python3

import json
import requests
import csv

API_KEY = '123456789abcdefghijklmnop'
HOST = 'https://extrahop.example.com/'

# Method that updates detections on an ExtraHop system
def updateDetection(detection):
    url = HOST + 'api/v1/detections/' + detection['detection_id']
    del detection['detection_id']
    data = json.dumps(detection)
    headers = {'Content-Type': 'application/json',
               'Accept': 'application/json',
               'Authorization': 'ExtraHop apikey=%s' % API_KEY}
```

```
    r = requests.patch(url, data=data, headers=headers)
    print(r.status_code)
    print(r.text)

# Array of detection information
detections = [
                {
                    "detection_id": "1",
                    "ticket_id": "TK-16982",
                    "status": "new",
                    "assignee": "sally",
                    "resolution": None,
                },
                {
                    "detection_id": "2",
                    "ticket_id": "TK-2078",
                    "status": None,
                    "assignee": "jim",
                    "resolution": None,
                },
                {
                    "detection_id": "3",
                    "ticket_id": "TK-3452",
                    "status": None,
                    "assignee": "alex",
                    "resolution": None,
                }
            ]

for detection in detections:
    updateDetection(detection)
```

Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat TLS a échoué, assurez-vous que un certificat fiable a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter `verify=False` option permettant de contourner la vérification des certificats. Cependant, cette méthode n'est pas sûre et n'est pas recommandée. Le code suivant envoie une requête HTTP GET sans vérification du certificat :

```
requests.get(url, headers=headers, verify=False)
```

Une fois le suivi des tickets configuré, les détails des tickets sont affichés dans le volet gauche des détails de détection, comme dans la figure suivante :



État

État du ticket associé à la détection. Le suivi des tickets prend en charge les statuts suivants :

- Nouveau
- En cours
- Fermé
- Clôturé avec mesures prises
- Clôturé sans qu'aucune mesure n'ait été prise

ID du billet

L'identifiant du ticket associé à la détection dans votre système de suivi du travail. Si vous avez configuré un modèle d'URL, vous pouvez cliquer sur l'identifiant du ticket pour ouvrir le ticket dans votre système de suivi du travail.

Cessionnaire

Le nom d'utilisateur attribué au ticket associé à la détection. Les noms d'utilisateur en gris indiquent un compte qui n'est pas ExtraHop.

Étudier les détections de sécurité

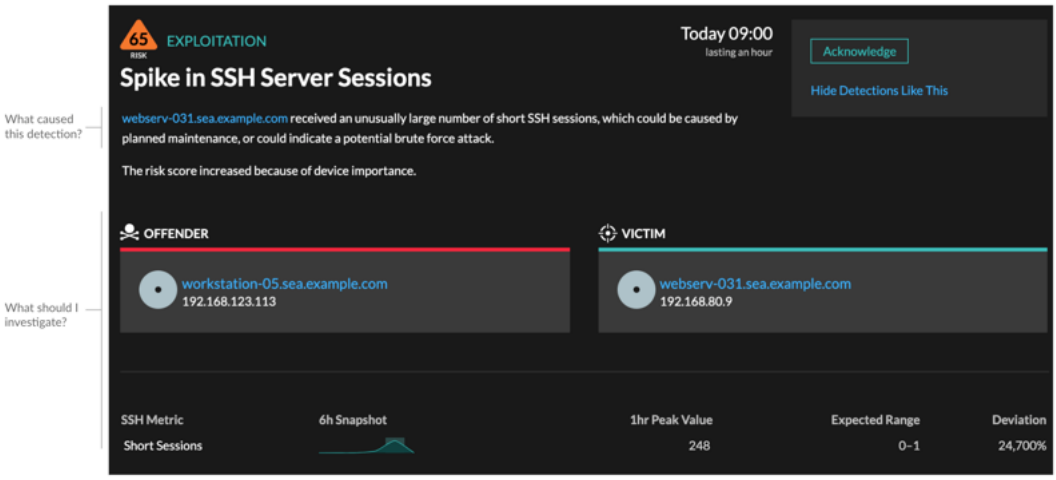
Lorsqu'une détection intéressante apparaît, vous devez déterminer si le comportement détecté indique un problème peu prioritaire ou un risque de sécurité potentiel. Vous pouvez démarrer votre enquête directement à partir de la carte de détection, qui fournit des liens vers les données du système ExtraHop.

Il existe un certain nombre de outils qui peuvent vous aider à filtrer votre vue pour voir les détections que vous souhaitez prioriser dans le cadre d'une enquête. Pour commencer, observez les tendances suivantes :

- Des détections se sont-elles produites à des moments inhabituels ou inattendus, tels que l'activité des utilisateurs le week-end ou en dehors des heures de bureau ?
- Des détections apparaissent-elles dans de grands groupes sur la chronologie ?
- Des détections apparaissent-elles pour des points de terminaison de grande valeur ?
- Y a-t-il des détections présentant des scores de risque élevés ?
- Les appareils utilisés lors de la détection participent-ils également à d'autres détections ?
- Les indicateurs de compromission sont-ils identifiés à partir d'une collecte des menaces associée à la détection ?

Commencez votre investigation

Consultez le titre et le résumé de la détection pour découvrir la cause de la détection.



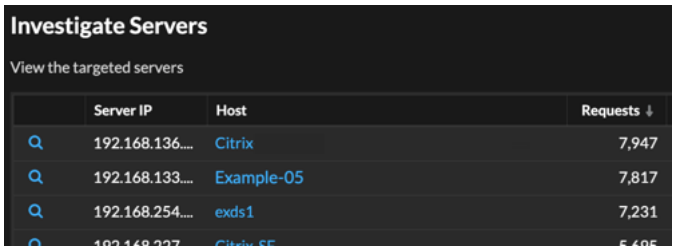
Affinez votre investigation

Les fiches détaillées de détection présentent les données associées à la détection. La disponibilité des données dépend des appareils et des mesures associés à la détection. Après avoir cliqué sur un lien, vous pouvez revenir à la fiche de détection en cliquant sur le nom de la détection dans le chemin de navigation. Chaque option d'investigation est décrite dans les sections ci-dessous.

Examiner les données d'enquête

La plupart des données dont vous avez besoin pour comprendre, valider et étudier une détection sont affichées sur la page détaillée de la détection : tableaux contenant les données métriques pertinentes, transactions d'enregistrement et liens vers des paquets bruts.

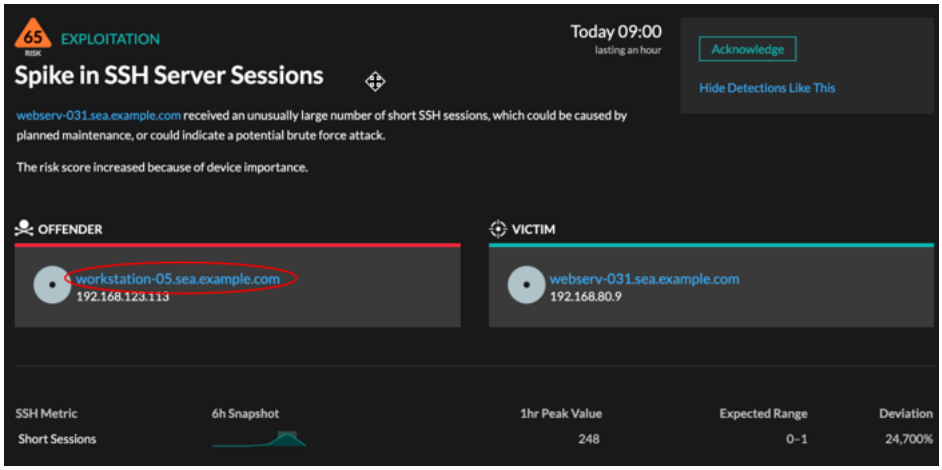
Cliquez sur le nom d'un hôte pour accéder à la page de présentation des appareils, ou cliquez avec le bouton droit pour créer un graphique avec cet équipement comme source et les mesures pertinentes.



Nom de l'appareil

Cliquez sur le nom d'un équipement pour accéder à la page Présentation de l'appareil, qui contient le rôle, les utilisateurs et les balises associés à cet équipement. Dans le volet de gauche, cliquez sur le nom d'un protocole pour afficher toutes les mesures de protocole associées à l'équipement. La page de protocole vous donne une image complète de ce que faisait cet équipement au moment de la détection.

Par exemple, si vous obtenez la détection d'un scan de reconnaissance, vous pouvez savoir si le rôle d'analyseur de vulnérabilités est attribué à l'équipement associé au scan.



Disponibilité

Les liens vers les noms des appareils ne sont disponibles que pour les appareils qui ont été découverts automatiquement par le système ExtraHop. Les appareils distants situés en dehors de votre réseau sont représentés par leur adresse IP.

Carte des activités

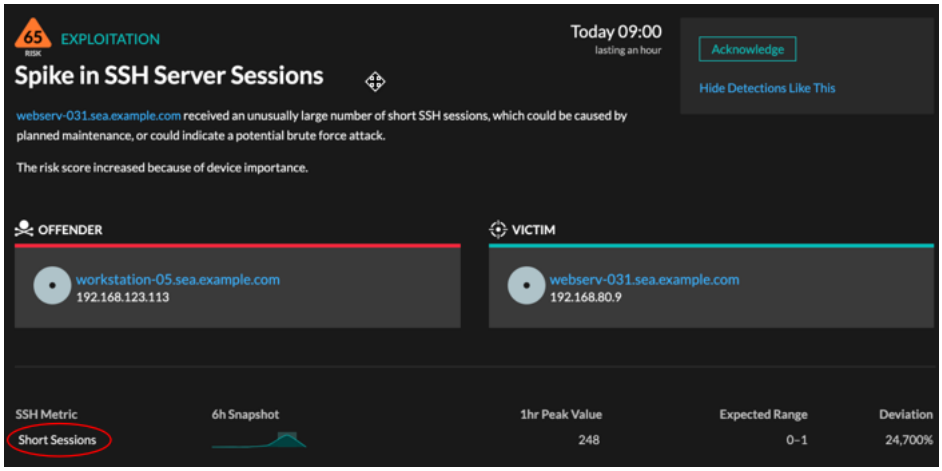
Cliquez sur l'icône de la carte d'activité à côté du nom d'un équipement pour voir les connexions de l'équipement par protocole au moment de la détection. Par exemple, si vous recevez une détection de mouvement latéral, vous pouvez savoir si l'équipement suspect a établi des connexions via un protocole de contrôle à distance avec d'autres clients, serveurs informatiques ou contrôleurs de domaine de votre réseau.

Disponibilité

Une carte d'activité est disponible lorsqu'un seul client ou serveur est associé à une activité inhabituelle du protocole L7, telle qu'un nombre élevé d'erreurs HTTP ou des délais d'attente de requêtes DNS.

Analyse métrique détaillée vers le bas

Cliquez sur le lien d'une métrique détaillée pour accéder à une valeur métrique vers le bas. Une page de mesures détaillées apparaît, qui répertorie les valeurs métriques par clé, telle que l'adresse IP du client, l'adresse IP du serveur, la méthode ou l'erreur. Par exemple, si vous obtenez une détection par scan de reconnaissance, effectuez une exploration vers le bas pour savoir quelles adresses IP des clients étaient associées au nombre anormalement élevé de codes d'état 404 lors de la détection.

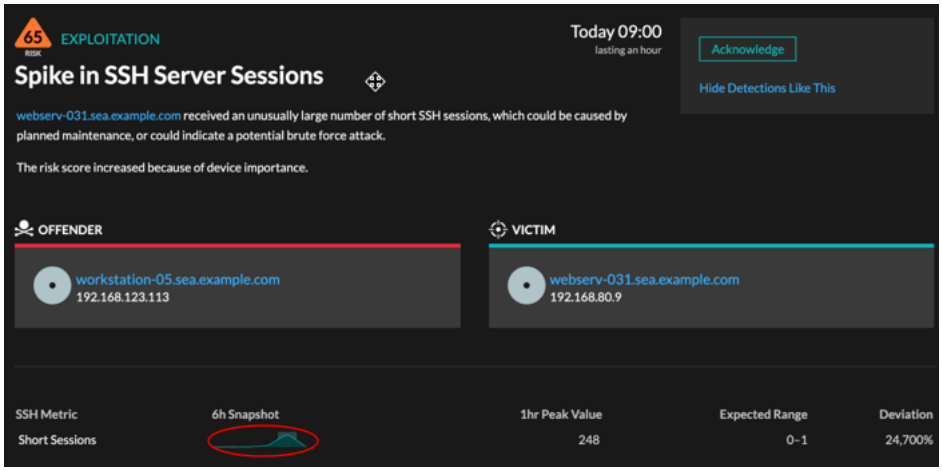


Disponibilité

L'option d'exploration vers le bas est disponible pour les détections associées à topnset des métriques détaillées.

Sparkline

Cliquez sur la ligne d'étincelle pour créer un graphique qui inclut la source, l'intervalle de temps et les détails détaillés de la détection, que vous pouvez ensuite ajouter à un tableau de bord à des fins de surveillance. Par exemple, si vous recevez une détection concernant un nombre inhabituel de sessions à distance, créez un graphique avec les sessions SSH pour ce serveur, puis ajoutez-le à un tableau de bord concernant la gestion des sessions.

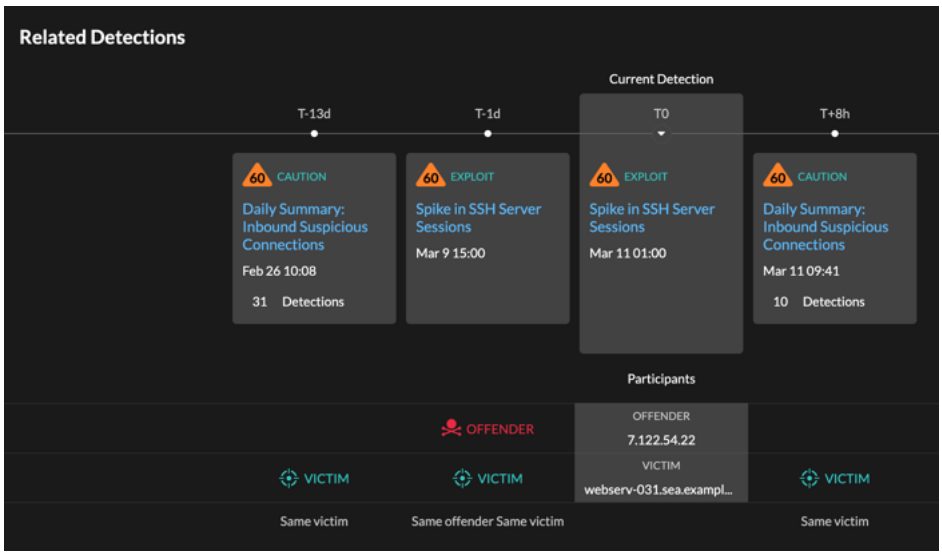


Disponibilité

L'option sparkline est disponible pour les détections associées à des métriques et dont la durée est supérieure à une heure. Pour les mesures d'une seconde, un sparkline est disponible lorsque la durée était supérieure à 30 secondes.

Détections associées

Cliquez sur l'une des détections associées pour obtenir des informations sur les comportements suspects et les attaques émergentes résultant de plusieurs détections impliquant des participants partagés. Par exemple, une victime de la détection en cours qui participe en tant que délinquant à une détection ultérieure peut indiquer que l'équipement est compromis. Vous pouvez consulter les détails de détection associés pour déterminer si les événements de détection sont similaires et pour voir quels autres appareils sont concernés.



Disponibilité

La chronologie des détections associée est disponible si certaines détections concernent la même victime ou le même délinquant que la détection en cours. Les détections associées peuvent avoir eu lieu avant ou après la détection en cours.

Renseignements sur les menaces

Cliquez sur l'icône rouge d'une caméra pour accéder à des renseignements sur les menaces détaillés concernant un indicateur de compromission.

Le renseignement sur les menaces fournit des données connues sur les adresses IP, les noms d'hôte et les URI suspects qui peuvent aider à identifier les risques auxquels votre organisation est exposée. Ces ensembles de données, appelés collections de menaces, sont disponibles par défaut dans votre système RevealX et auprès de sources gratuites et commerciales de la communauté de la sécurité.

Disponibilité

Le renseignement sur les menaces doit être activé sur votre système RevealX pour que vous puissiez voir ces indicateurs.

Étudier les détections de performances

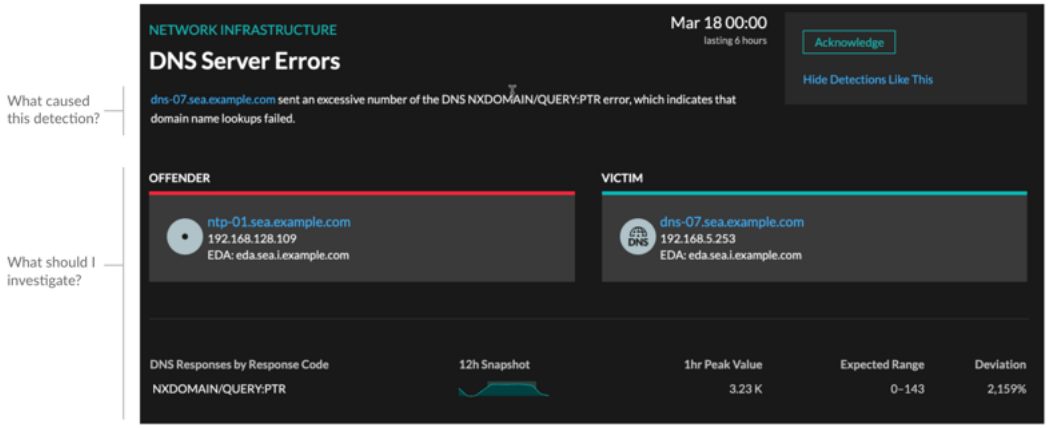
Lorsqu'une détection intéressante apparaît, vous devez déterminer si le comportement détecté indique un problème peu prioritaire ou un problème potentiel. Vous pouvez démarrer votre enquête directement à partir de la carte de détection, qui fournit des liens vers les données du système ExtraHop.

Il existe un certain nombre de outils qui peuvent vous aider à filtrer votre vue pour voir les détections que vous souhaitez prioriser dans le cadre d'une enquête. Pour commencer, observez les tendances suivantes :

- Des détections se sont-elles produites à des moments inhabituels ou inattendus, tels que l'activité des utilisateurs le week-end ou en dehors des heures de bureau ?
- Des détections apparaissent-elles dans de grands groupes sur la chronologie ?
- Des détections apparaissent-elles pour des points de terminaison de grande valeur ?
- Les appareils utilisés lors de la détection participent-ils également à d'autres détections ?

Commencez votre investigation

Consultez le titre et le résumé de la détection pour découvrir la cause de la détection.



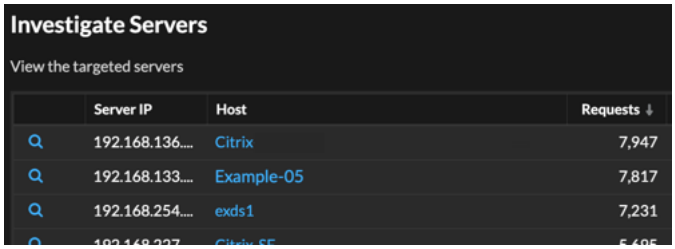
Affinez votre investigation

Les fiches détaillées de détection présentent des données associées à la détection. La disponibilité des données dépend des appareils et des métriques associés à la détection. Après avoir cliqué sur un lien, vous pouvez revenir à la carte de détection en cliquant sur le nom de la détection dans le chemin de navigation. Chaque option d'investigation est décrite dans les sections ci-dessous.

Examiner les données d'enquête

La plupart des données dont vous avez besoin pour comprendre, valider et étudier une détection sont affichées sur la page détaillée de la détection : tableaux contenant les données métriques pertinentes, transactions d'enregistrement et liens vers des paquets bruts.

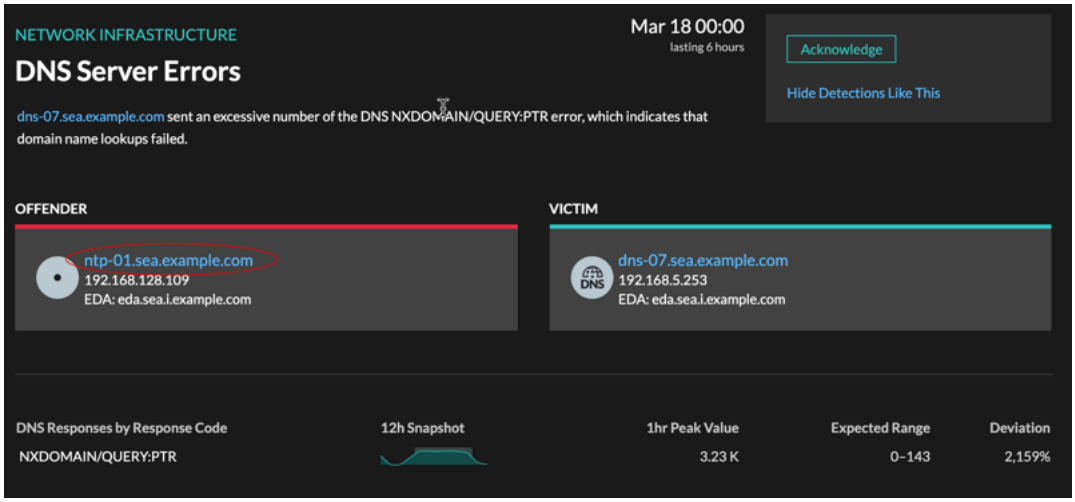
Cliquez sur le nom d'un hôte pour accéder à la page de présentation du périphérique, ou cliquez avec le bouton droit de la souris pour créer un graphique avec cet équipement comme source et les mesures pertinentes.



Nom de l'appareil

Cliquez sur le nom d'un équipement pour accéder à la page de présentation de l'équipement, qui contient le rôle, les utilisateurs et les tags associés à cet équipement. Dans le volet de gauche, cliquez sur le nom d'un protocole pour afficher toutes les mesures de protocole associées à l'équipement. La page de protocole vous donne une image complète de ce que faisait cet équipement au moment de la détection.

Par exemple, si un échec de transaction de base de données est détecté, vous pouvez en savoir plus sur d'autres activités associées au serveur hébergeant l'instance de base de données.



Disponibilité

Les liens vers les noms d'appareils ne sont disponibles que pour les appareils qui ont été automatiquement découverts par le système ExtraHop. Les appareils distants situés en dehors de votre réseau sont représentés par leur adresse IP.

Carte des activités

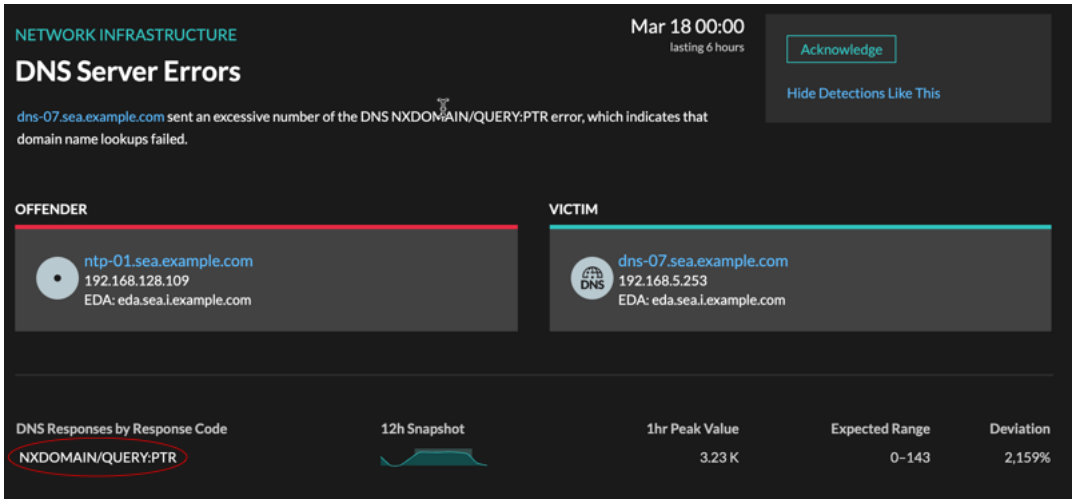
Cliquez sur l'icône de la carte d'activité à côté du nom d'un équipement pour voir les connexions des équipements par protocole au moment de la détection. Par exemple, si des erreurs d'authentification LDAP sont détectées, vous pouvez créer une carte dactivités pour savoir quels appareils étaient connectés à un serveur LDAP lors de la détection.

Disponibilité

Une carte dactivités est disponible lorsqu'un seul client ou serveur est associé à une activité inhabituelle liée au protocole L7, telle qu'un nombre élevé d'erreurs HTTP ou des délais d'expiration des requêtes DNS.

Exploration métrique détaillée

Cliquez sur un lien métrique détaillé pour accéder à une valeur métrique vers le bas. Une page détaillée des mesures apparaît, qui répertorie les valeurs métriques par clé, telles que l'adresse IP du client, l'adresse IP du serveur, la méthode ou l'erreur. Par exemple, si vous recevez une détection d'authentification concernant un serveur LDAP, effectuez une analyse détaillée pour savoir quelles adresses IP des clients ont soumis les informations dÂ'identification non valides qui ont contribué au nombre total d'erreurs LDAP.

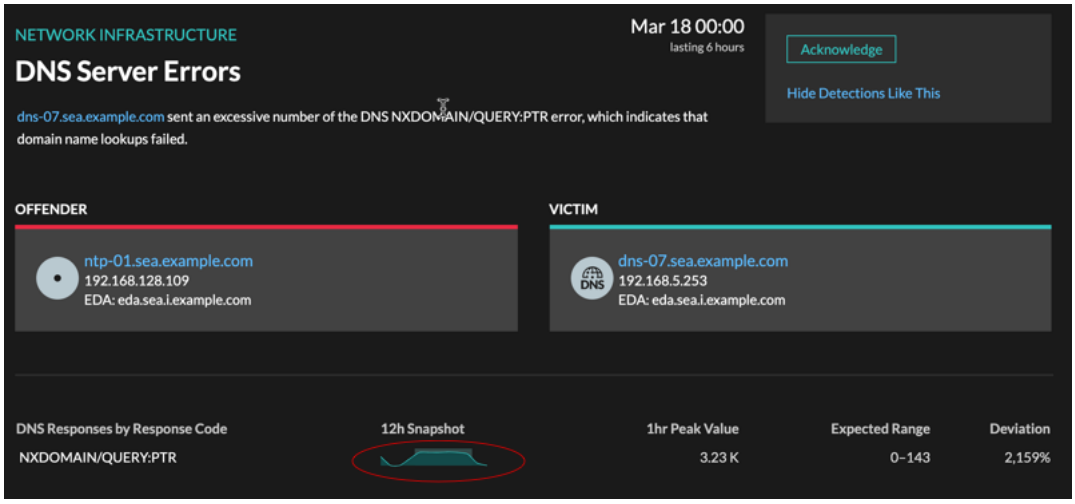


Disponibilité

L'option d'exploration vers le bas est disponible pour les détections associées à topnset métriques détaillées.

Sparkline

Cliquez sur le sparkline pour créer un graphique qui inclut la source, l'intervalle de temps et les détails détaillés de la détection, que vous pouvez ensuite ajouter à un tableau de bord pour une surveillance supplémentaire. Par exemple, si vous recevez une détection concernant des problèmes de serveur Web, vous pouvez créer un graphique avec les 500 codes d'état envoyés par le serveur Web, puis ajouter ce graphique à un tableau de bord concernant les performances du site Web.

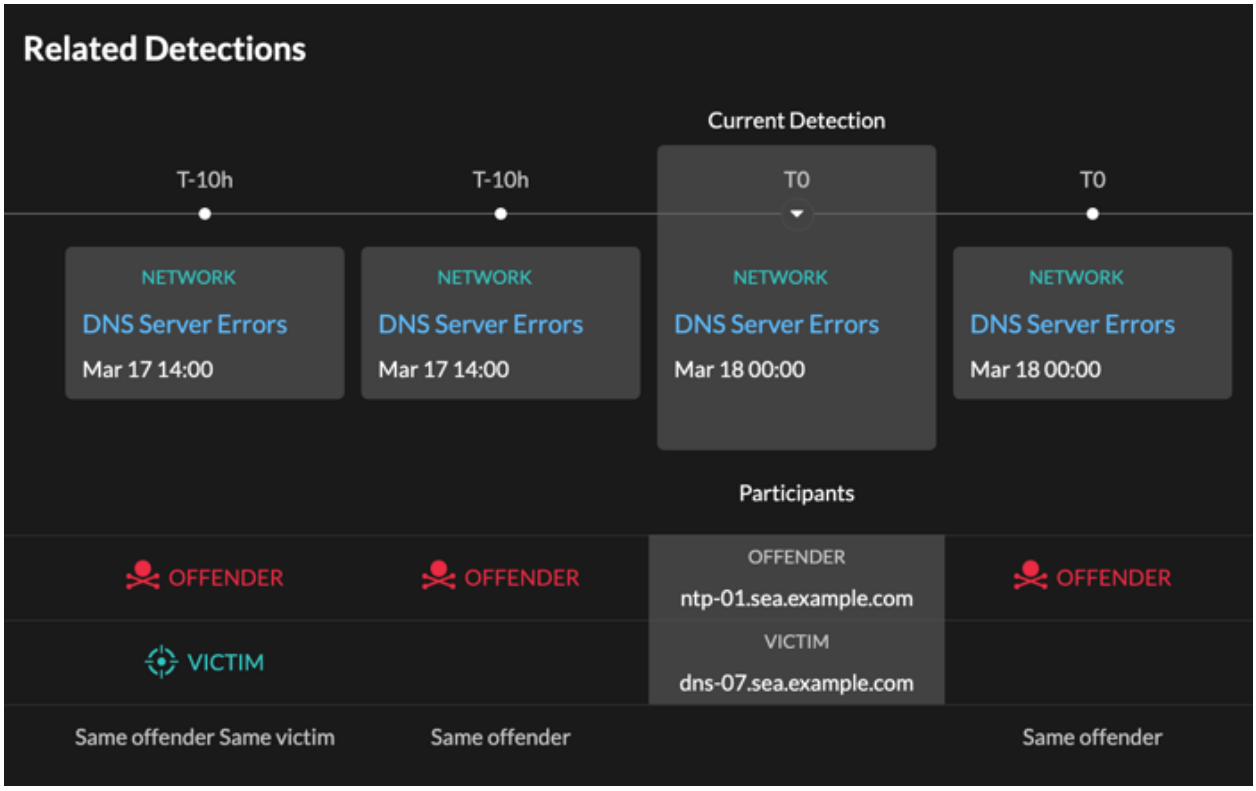


Disponibilité

L'option sparkline est disponible pour les détections associées à des métriques.

Détections associées

Cliquez sur une détection associée pour obtenir des informations sur les problèmes de réseau, d'application et d'infrastructure rencontrés lors de plusieurs détections impliquant des participants communs. Par exemple, un équipement identifié comme étant un délinquant est probablement à l'origine d'un problème, tel qu'un serveur de bases de données envoyant un nombre excessif d' erreurs de réponse. Un équipement identifié comme victime est généralement affecté négativement par le problème, par exemple lorsque les clients rencontrent des transactions de base de données lentes ou échouées. Vous pouvez consulter les détails de détection associés pour déterminer si les événements de détection sont similaires, voir quels autres appareils sont concernés et consulter les données métriques.



Disponibilité

La chronologie des détections associée est disponible si certaines détections concernent la même victime ou le même délinquant que la détection actuelle. Les détections associées peuvent s'être produites avant ou après la détection en cours.

Exposés sur les menaces

Les informations sur les menaces fournissent des conseils sur les menaces potentielles qui pèsent sur votre réseau.

Les exposés sur les menaces portent sur les événements suivants :

- Événements de sécurité à l'échelle du secteur, au cours desquels le système ExtraHop détecte des détections liées à des compromissions connues.
- Briefings d'analyse de sécurité, qui fournissent une analyse d'apprentissage automatique spécifique à votre réseau.
- (RevealX 360 uniquement.) Briefings d'analyse rétrospective des menaces, qui détectent de nouveaux indicateurs de compromission dans des collections actualisées de renseignements sur les menaces organisées par ExtraHop.

Les briefings sur les menaces contiennent des détections de scans, d'exploits et d'indicateurs de compromission (IOC) liés à la menace. Les informations contenues dans chaque briefing varient en fonction du type de menace. Les informations relatives au briefing sont mises à jour dans le cloud au fur et à mesure que des détails apparaissent sur les indicateurs de compromission, les vecteurs d'attaque potentiels et les risques connus.

Les briefings sur les menaces sont disponibles dans le coin supérieur gauche du Aperçu de la sécurité page. Cliquez sur n'importe quel titre pour accéder à la page détaillée de ce briefing. La page détaillée est mise à jour au fur et à mesure que de nouvelles informations sont découvertes.

Voici quelques moyens de suivre les briefings sur les menaces :

- Création d'une règle de notification d'informations sur les menaces pour recevoir des e-mails lorsqu'une nouvelle information sur les menaces apparaît.
- Cliquez **Créer une enquête** depuis la page détaillée pour ajouter les détections associées au briefing à une enquête.
- Cliquez **Exposé sur les archives** depuis la page détaillée lorsque vous ne souhaitez plus suivre le briefing ; le briefing est automatiquement restauré et un e-mail de notification est envoyé en cas de mise à jour du briefing. Vous pouvez consulter les anciens briefings dans la section Archivé de la page Threat Briefing. Cliquez **Restaurer le briefing** sur la page détaillée pour revenir à la section Active de la page d'information sur les menaces.

Création d'une règle de notification d'informations sur les menaces

Vous pouvez créer une règle de notification qui envoie un e-mail à une liste de destinataires chaque fois qu'un nouveau briefing sur les menaces est publié ou automatiquement restauré. Les briefings sont automatiquement restaurés s' ils sont mis à jour avec des modifications de contenu ou de nouvelles détections.

Avant de commencer

- Les utilisateurs doivent avoir accès au module NDR et disposer d'une capacité d'écriture complète privilèges ou une version supérieure pour effectuer les tâches décrites dans ce guide.
- Le système ExtraHop doit être connecté à ExtraHop Cloud Services pour envoyer des notifications par e-mail.
- Les notifications par e-mail sont envoyées depuis no-reply@notify.extrahop.com. Assurez-vous d'ajouter cette adresse à votre liste d'expéditeurs autorisés.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Règles de notification**.
3. Cliquez **Créez**.

4. Cliquez **Exposé sur les menaces**.
5. Tapez un nom unique pour la règle de notification dans le champ Nom.
6. Dans le champ Description, ajoutez des informations sur la règle de notification.
7. Spécifiez les adresses e-mail individuelles, en les séparant par une virgule.
8. Dans le Options section, la **Activer la règle de notification** La case à cocher est activée par défaut. Décochez la case pour désactiver la règle de notification.
9. Cliquez **Enregistrer**.

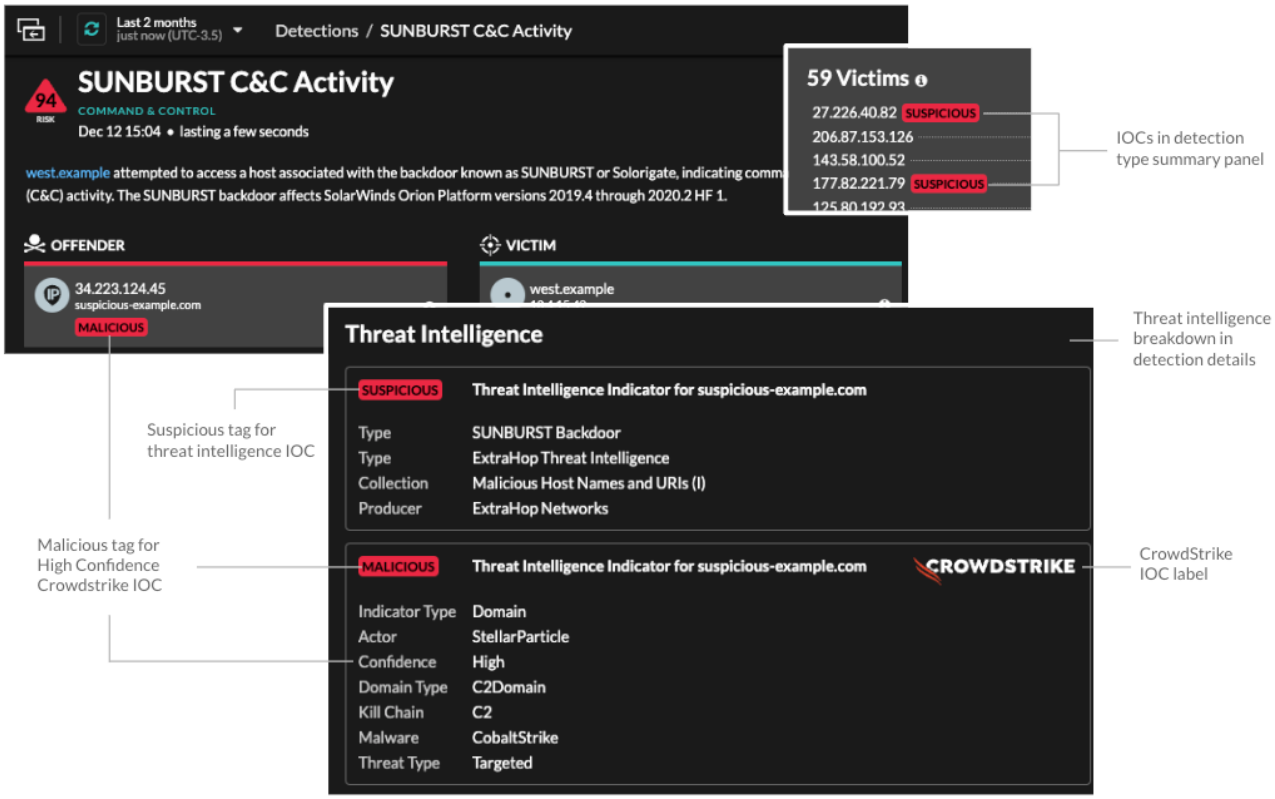
Renseignements sur les menaces

Le renseignement sur les menaces fournit des données connues sur les adresses IP, les domaines, les noms d'hôte et les URI suspects qui peuvent aider à identifier les risques pour votre organisation.

Vidéo: Consultez la formation associée : Renseignements sur les menaces

Les ensembles de données de renseignement sur les menaces, appelés collections de menaces, contiennent des listes de terminaux suspects appelés indicateurs de compromission (IOC).

Les participants correspondant à une collecte des menaces sont marqués comme suspects dans les détections, les résumés des détections, les diagrammes des systèmes et les enregistrements. (Pour les IoC Crowdstrike où le niveau de confiance est élevé, le participant est marqué comme malveillant.) Les enregistrements contenant l'entrée suspecte sont signalés par une icône représentant une caméra . Dans de nombreux cas, une correspondance d'indicateur génère également la détection de la connexion suspecte.



Collections de menaces

Le système ExtraHop prend en charge la collecte de menaces provenant de plusieurs sources.

Collections de menaces intégrées

Des collections de menaces organisées par ExtraHop et CrowdStrike Falçon sont disponibles par défaut dans votre système ExtraHop. Les collections intégrées sont mises à jour toutes les 6 heures. Tu peux activer ou désactiver les collections de menaces intégrées depuis la page Threat Intelligence.

Téléversement de fichiers STIX

Important: Les téléchargements de fichiers STIX sont désormais obsolètes et la date de suppression est prévue pour mars 2025.

Les collections gratuites et commerciales proposées par la communauté de la sécurité et formatées au format STIX (Structured Threat Information eXpression) sous forme de fichiers TAR compressés , tels que .TGZ ou TAR.GZ, peuvent être chargé manuellement ou via l' API REST aux systèmes ExtraHop. Les versions 1.0 à 1.2 de STIX sont actuellement prises en charge. Vous devez télécharger chaque collecte des menaces individuellement sur votre console et sur tous les capteurs connectés.

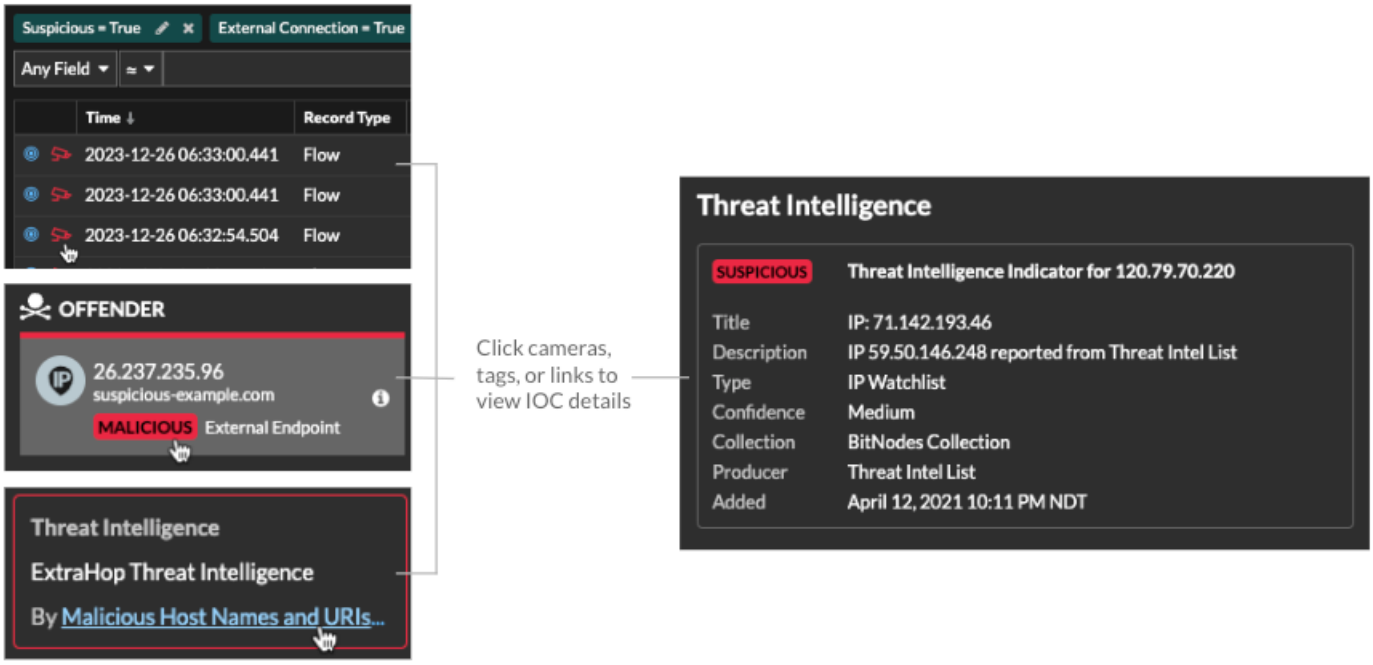
Fil TAXII

Les collections de menaces peuvent être transmises à votre environnement à partir d'une source fiable via le protocole TAXII (Trusted Automated Exchange of Intelligence Information). Un flux TAXII peut fournir un flux constant d'indicateurs de menace mis à jour. Tu peux ajouter un flux TAXII à partir du Renseignements sur les menaces page.

Étant donné que les renseignements sur les cybermenaces sont gérés par la communauté, il existe de nombreuses sources externes pour la collecte des menaces. Les données de ces collections peuvent varier en termes de qualité ou de pertinence par rapport à votre environnement. Pour garantir la précision et réduire le bruit, nous vous recommandons de limiter le téléchargement de vos fichiers STIX à des données de renseignements sur les menaces de haute qualité qui se concentrent sur un type d'intrusion spécifique, comme une collection pour les programmes malveillants et une autre pour les botnets. De même, nous vous recommandons de limiter les flux TAXII à des sources fiables et de haute qualité.

Enquête sur les menaces

Une fois que le système RevealX a observé un indicateur de compromission, l' adresse IP, le domaine, le nom d'hôte ou l'URI suspects sont marqués comme suspects ou malveillants dans les résumés de détection et sur les fiches de détection individuelles. Dans les tableaux et les graphiques, les indicateurs de compromission sont signalés par une icône représentant une caméra, ce qui vous permet d'effectuer des recherches directement à partir des tableaux et des graphiques que vous consultez.



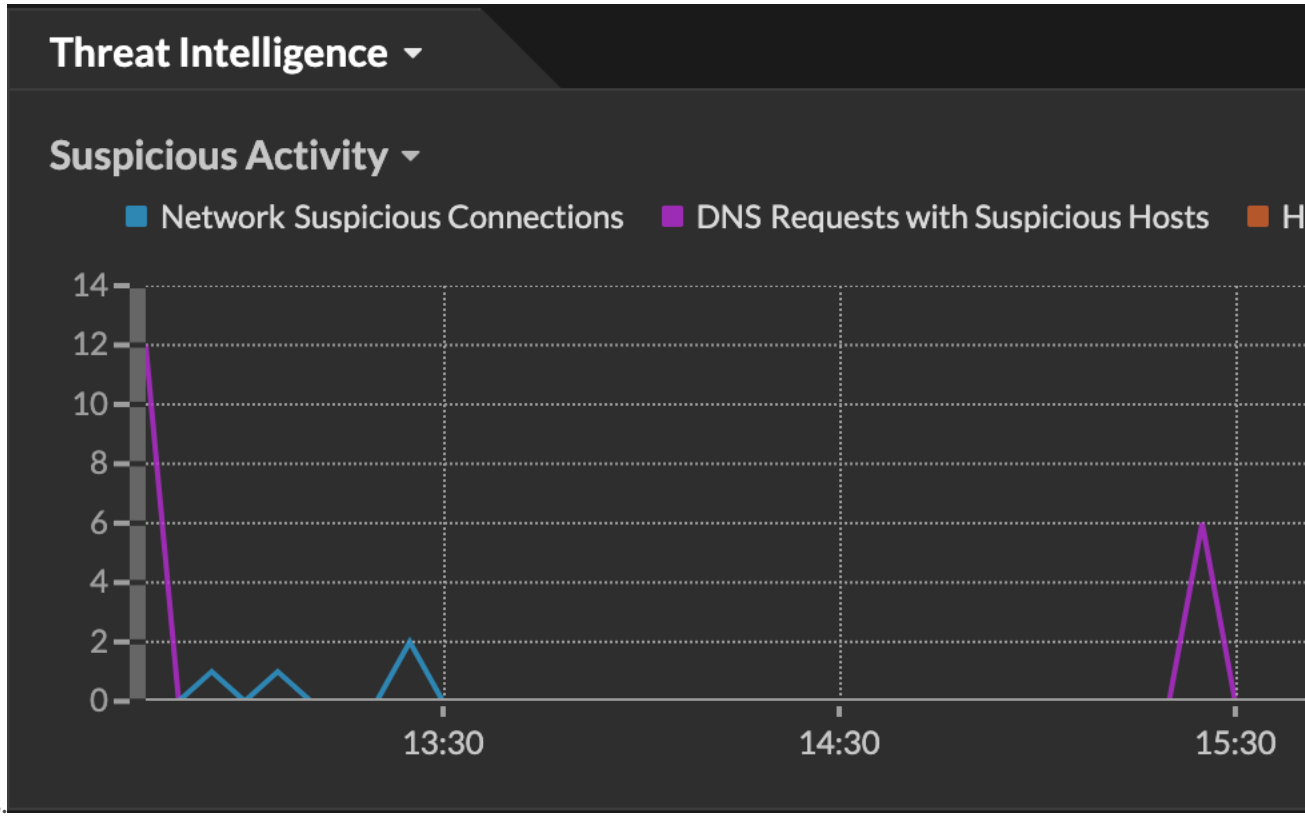
- Si la collecte des menaces est ajoutée ou mise à jour après que le système a détecté l' activité suspecte, les renseignements sur les menaces ne sont pas appliqués à cette adresse IP, à ce nom d'hôte ou à cet URI jusqu'à ce que l'activité suspecte se reproduise.

- (RevealX 360 uniquement) Si une collecte des menaces ExtraHop ou CrowdStrike intégrée est mise à jour, le système ExtraHop effectue une détection rétrospective automatisée (ARD), qui recherche les nouveaux domaines, noms d'hôtes, URL et adresses IP qui indiquent une compromission dans les enregistrements des 7 derniers jours. Si une correspondance est trouvée, le système génère une détection rétrospective.
- Si vous désactivez ou supprimez une collecte des menaces, tous les indicateurs sont supprimés des métriques et des enregistrements associés dans le système. Les détections dont le triage est recommandé sur la base de renseignements sur les menaces resteront dans le système une fois la collecte associée désactivée.

Voici quelques sections du système RevealX qui présentent les indicateurs de compromission détectés dans vos collections de menaces :

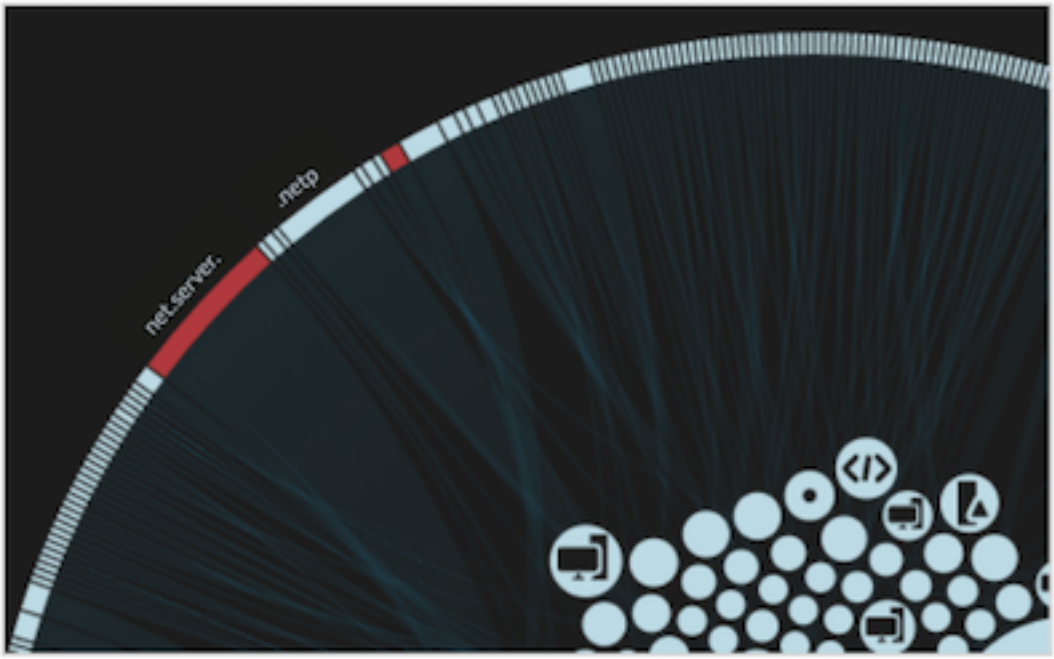
Tableau de bord de renforcement de la sécurité

Le région de renseignement sur les menaces contient des mesures relatives aux activités suspectes qui correspondent aux données de vos collections de menaces. En cliquant sur n'importe quelle métrique, telle que Requêtes HTTP avec des hôtes suspects, vous pouvez effectuer une recherche détaillée sur la métrique ou interroger des enregistrements pour les transactions associées.



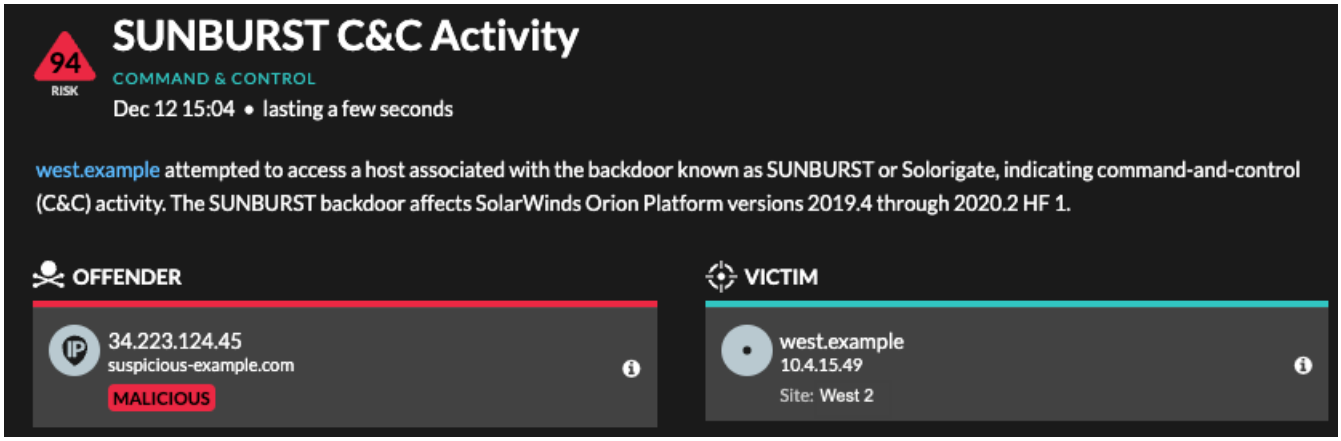
Vue d'ensemble du périmètre

Dans la visualisation du halo, tous les points de terminaison correspondant aux entrées de collecte des menaces sont surlignés en rouge.



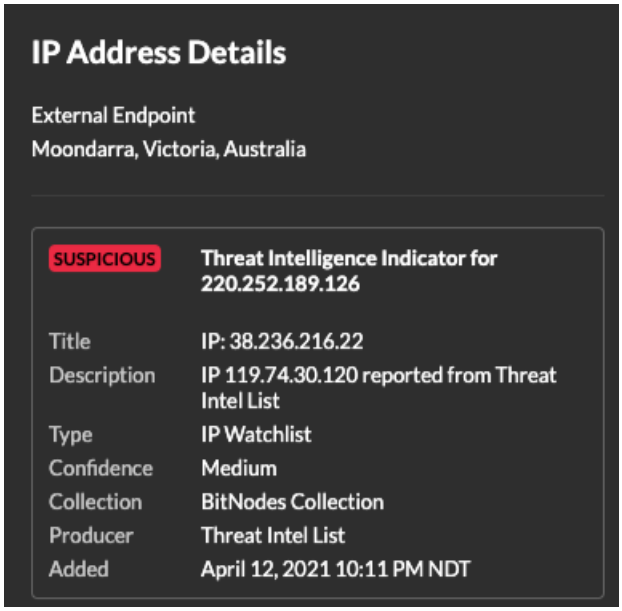
Détections

Une détection apparaît lorsqu'un indicateur de compromission provenant d'une collecte des menaces est identifié dans le trafic réseau.



Détails de l'adresse IP

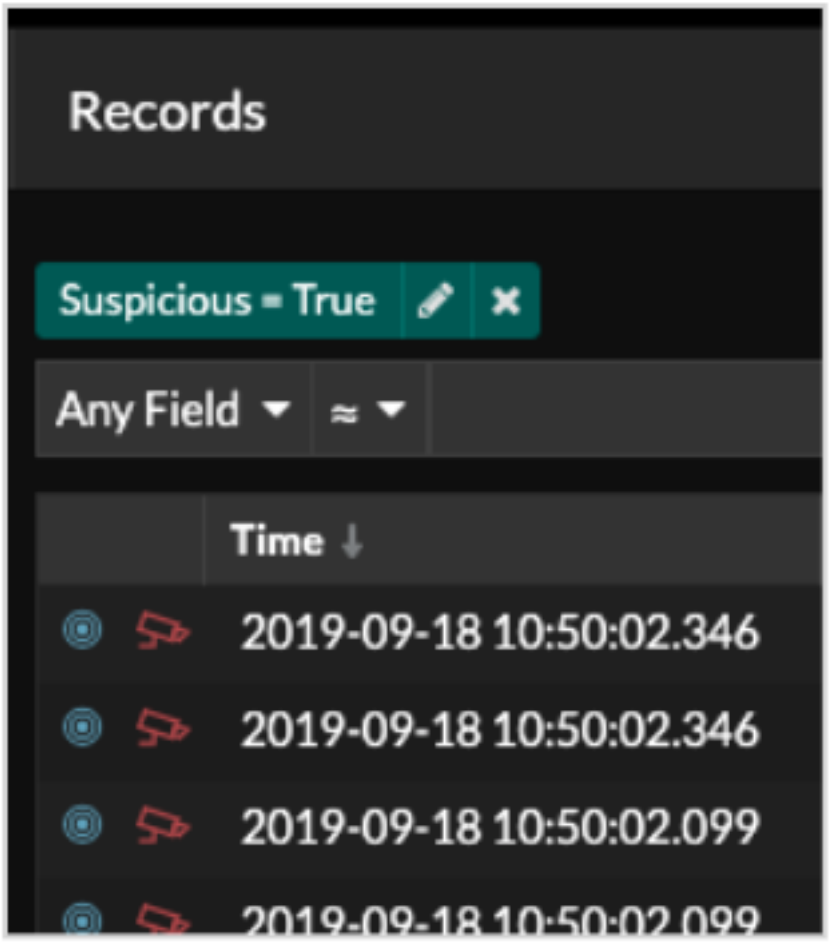
Les pages détaillées des adresses IP affichent des renseignements sur les menaces complets pour les indicateurs de compromission des adresses IP.



Disques

La page Enregistrements vous permet de rechercher directement les transactions qui correspondent aux entrées de collecte des menaces.

- Sous la facette Suspect, cliquez sur **Vrai** pour filtrer tous les enregistrements contenant des transactions correspondant à des adresses IP, des noms d'hôte et des URI suspects.
- Créez un filtre en sélectionnant Suspect, Adresse IP suspecte, Domaine suspect ou URI suspect dans la liste déroulante à trois champs, un opérateur et une valeur.
- Cliquez sur l'icône rouge de la caméra pour consulter les renseignements sur les menaces.



Gérez les collections de menaces

ExtraHop RevealX peut s'appliquer renseignement sur les menaces à l'activité de votre réseau en fonction des collections de menaces fournies par Extrahop, CrowdStrike ou d'autres sources gratuites et commerciales.

Avant de commencer

- En savoir plus sur renseignements sur les menaces.
- Tu dois avoir Privilèges d'administration du système et des accès sur chaque console et sonde pour gérer les collections de menaces.
- Si votre déploiement ExtraHop inclut une console, nous vous recommandons gestion des transferts de tous les capteurs connectés à la console pour activer ou désactiver les collectes de menaces intégrées sur l'ensemble de votre système.

Activer ou désactiver les collections de menaces intégrées

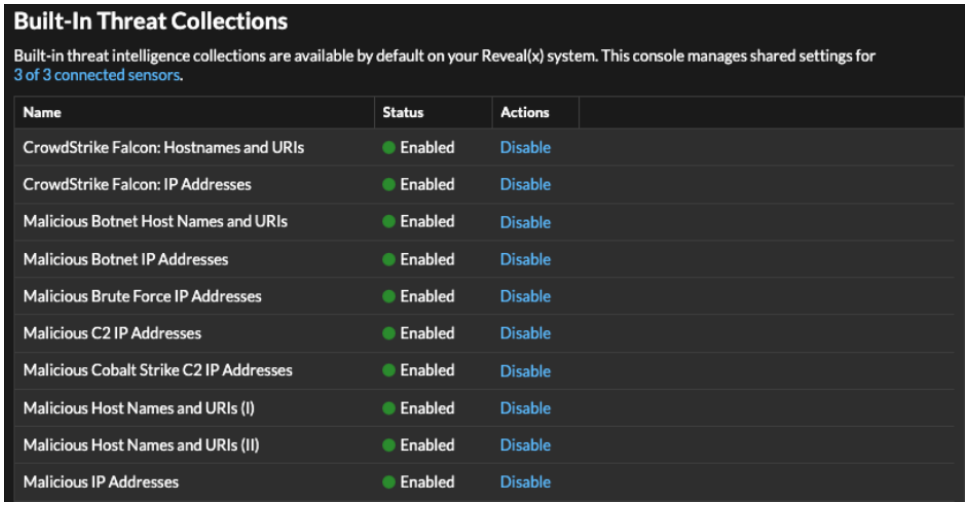
Les collections de menaces intégrées d'ExtraHop et de CrowdStrike identifient les indicateurs de compromission dans l'ensemble du système.

Les collections de menaces activées mettent automatiquement à jour les systèmes connectés aux services cloud ExtraHop. Vous pouvez confirmer la connectivité sur Services cloud ExtraHop page dans les paramètres d'administration.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.

2. Cliquez sur l'icône Paramètres système puis cliquez sur **Renseignements sur les menaces**.
3. Dans le tableau des collections de menaces intégrées, cliquez sur **Activer** ou **Désactiver** dans la colonne Actions.

   Le système vérifie automatiquement les mises à jour des collections de menaces ExtraHop et CrowdStrike toutes les 6 heures.



Télécharger une collecte des menaces

Téléchargez des collections de menaces provenant de sources gratuites et commerciales pour identifier les indicateurs de compromission dans l'ensemble du système ExtraHop. Étant donné que les données relatives aux renseignements sur les menaces sont mises à jour fréquemment (parfois quotidiennement), il se peut que vous deviez mettre à jour une collecte des menaces avec les données les plus récentes. Lorsque vous mettez à jour une collecte des menaces avec de nouvelles données, la collection est supprimée et remplacée, et n'est pas ajoutée à une collection existante.

> **Important:** Les téléchargements de fichiers STIX sont désormais obsolètes et la date de suppression est prévue pour mars 2025.

Vous devez télécharger les collections de menaces individuellement sur votre console et sur tous les capteurs connectés.

Voici quelques considérations concernant le téléchargement de collections de menaces.

- Les collections de menaces personnalisées doivent être formatées dans STIX (Structured Threat Information Expression) sous forme de fichiers TAR compressés, tels que .TGZ ou TAR.GZ. RevealX prend actuellement en charge le téléchargement des versions 1.0 à 1.2 des fichiers STIX.
- Vous pouvez télécharger directement des collections de menaces sur RevealX 360 pour une gestion autonome capteurs. Contactez le support ExtraHop pour télécharger une collection de menaces sur ExtraHop Managed capteurs.
- Le nombre maximum d'observables qu'une collecte des menaces peut contenir dépend de la mémoire et de la licence de votre sonde. Pour garantir la réussite des téléchargements dans les limites de vos capteurs et de votre licence, nous vous recommandons de diviser les collections en fichiers de moins de 3 000 observables, avec une taille totale de collection inférieure à 1 million d'observables. Contactez votre représentant ExtraHop pour plus d'informations sur les limites de licence et de plate-forme pour le téléchargement de collections de menaces.
- Tu peux télécharger des fichiers STIX via l'API REST.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Renseignements sur les menaces**.
3. Cliquez **Gérer les collections personnalisées**.

4. Cliquez **Télécharger une nouvelle collection**.
5. Dans le champ ID de collection, saisissez un identifiant de collection unique. L'identifiant ne peut contenir que des caractères alphanumériques et les espaces ne sont pas autorisés.
6. Cliquez **Choisissez un fichier** et sélectionnez un `.tgz` fichier contenant un fichier STIX.
7. Tapez un nom d'affichage dans le champ Nom d'affichage.
8. Cliquez **Collection de téléchargements**.
9. Répétez ces étapes pour tous consoles et chacun connecté sonde.

Ajouter un flux TAXII

Les collections de menaces peuvent être transmises à votre environnement via le protocole TAXII (Trusted Automated Exchange of Intelligence Information).

Les flux TAXII peuvent varier en termes de qualité ou de pertinence par rapport à votre environnement. Pour maintenir la précision et réduire le bruit, nous vous recommandons de n'ajouter que des flux provenant de sources fiables fournissant des renseignements sur les menaces de haute qualité.

Avant de commencer

- Les indicateurs de flux TAXII sont traités par ExtraHop Cloud Services. Le système ExtraHop doit être connecté à ExtraHop Cloud Services pour ajouter un flux TAXII.
- Les flux TAXII ne peuvent être gérés depuis une console que par les utilisateurs disposant de l'accès et de l'administration du module NDR privilèges.
- Les indicateurs d'alimentation TAXII ne sont fournis qu'aux capteurs connectés exécutant les versions 9.6.0 et ultérieures du firmware.
- RevealX prend actuellement en charge les flux TAXII pour les versions 2.0 à 2.1 de TAXII qui contiennent des versions de fichiers STIX 2.0 à 2.1

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Renseignements sur les menaces**.
3. Dans la section flux TAXII, cliquez sur **Ajouter un flux TAXII**.
4. Dans le champ Nom, saisissez un nom unique pour le flux TAXII.
5. Dans le champ URL de découverte du serveur TAXII, saisissez l'URL de découverte de votre fournisseur de flux TAXII.
6. Dans la liste déroulante des versions de TAXII, sélectionnez la version du protocole TAXII du flux.
7. Sélectionnez un type d'authentification.
   - Pas d'authentification
   - Authentification de base

     Entrez le nom d'utilisateur et le mot de passe du flux cible.
8. Spécifiez un certificat pour le flux cible.
   - Pas de certificat
   - Certificat de base

     Copiez et collez le contenu de la chaîne de certificats codée PEM dans le champ du certificat de base. Un chemin de confiance valide doit exister entre le certificat et une racine sécurisée.
9. Cliquez **Connexion de test** pour confirmer les paramètres d'URL, d'authentification et de certificat.
10. Cliquez **Suivant**.
11. Dans la liste déroulante Collections à enrichir, sélectionnez les collections de menaces qui produiront une étiquette suspecte en cas de correspondance d'indicateurs.
12. Dans la liste déroulante Collections pour la création de détections, sélectionnez les collections de menaces qui entraîneront une détection en cas de correspondance d'indicateurs .

Note: Vous pouvez affecter une collection à la fois à l'enrichissement et à la création de détections. Si aucune collection n'est affectée à l' option d'enrichissement, la collection ne sera pas mise à jour lors du sondage et les indicateurs de la collection n'apparaîtront pas dans votre système.

13. Dans le champ Maximum Lookback, saisissez le nombre de jours passés pendant lesquels vous souhaitez accepter les indicateurs de la collecte des menaces.

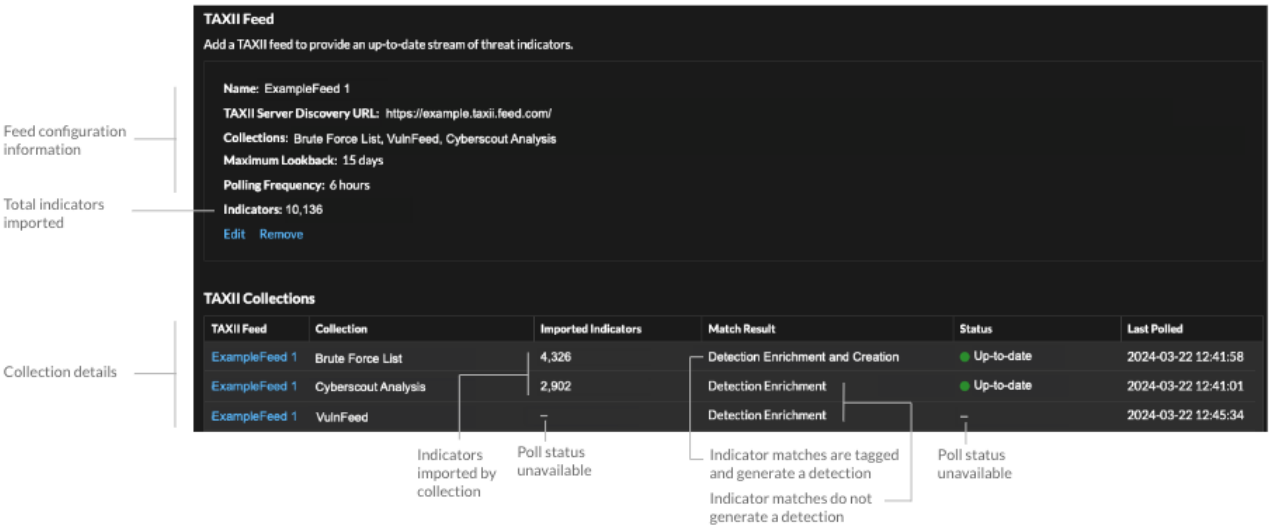
    Vous pouvez définir cette valeur sur une valeur comprise entre 1 et 15 jours. Le flux n' acceptera que les indicateurs créés au cours de cette période rétrospective.

14. Dans le champ Fréquence d'interrogation, saisissez le nombre d'heures entre l'interrogation du fil TAXII pour les mises à jour de la collecte des menaces.

    Vous pouvez définir cette valeur sur une valeur comprise entre 1 et 24 heures.

15. Cliquez **Enregistrer**.

Les informations de configuration du flux TAXII s'affichent dans la section Fil TAXII de la page Threat Intelligence, y compris la période de référence spécifiée, la fréquence d'interrogation et le nombre total d'indicateurs contenus dans le flux. Le tableau des collections TAXII contient des informations sur les différentes collections du flux.



Voici quelques considérations concernant les flux TAXII :

- Le temps nécessaire pour interroger les indicateurs d'alimentation et de traitement TAXII est basé sur le nombre d'indicateurs contenus dans le flux. À titre de référence, l'interrogation d'un flux contenant 500 000 indicateurs au cours de la période de référence spécifiée peut prendre une heure ou plus.
- Les types d'indicateurs qui ne sont pas reconnus par le système ExtraHop, les indicateurs de point de terminaison bénins et les indicateurs marqués comme révoqués seront supprimés du flux lors du sondage.
- Dans le tableau des collections TAXII, l'état de la collecte sera affiché par un tiret (-) jusqu'à ce que la collection soit à jour. Si ce statut ne passe pas à jour, testez votre connexion au serveur TAXII, puis vérifiez auprès de votre fournisseur de flux TAXII que la collection existe toujours dans le flux, que vos informations dcidentification autorisent l'accès à la collection et que vous n' avez pas dépassé les limites de sondage définies par le fournisseur. Un état de mise à jour partielle s'affiche si une collection n'est pas complètement mise à jour pendant le sondage. Des mises à jour partielles peuvent se produire si le sondage a été interrompu de façon inattendue ou si la limite de débit d'un fournisseur a été atteinte.

Alertes

Les alertes permettent de savoir facilement quand des événements importants se produisent sur votre réseau ou si certaines zones ne se comportent pas comme prévu, comme des violations du contrat de licence logicielle (SLA) ou des temps de réponse lents de la base de données.

Vidéo: Consultez la formation associée : Alertes

Les conditions d'alerte configurées déterminent le moment où une alerte est générée. Les conditions d'alerte sont une combinaison de paramètres, tels qu'un intervalle de temps, une valeur métrique et des calculs métriques effectués sur des sources de données attribuées. Les alertes de seuil ou de tendance sont basées sur la valeur de la métrique surveillée.

Configuration des alertes

Configurez une alerte pour surveiller certaines conditions et générer des alertes lorsque ces conditions sont remplies sur les sources de données attribuées.

Alertes de seuil

Des alertes basées sur des seuils sont générées lorsqu'une métrique surveillée dépasse une valeur définie dans un intervalle de temps spécifié.

Créez une alerte de seuil pour surveiller les événements tels que les taux d'erreur supérieurs à un pourcentage confortable ou les violations des SLA. Découvrez comment configurer une alerte de seuil.

Alertes de tendance

Des alertes basées sur les tendances sont générées lorsqu'une métrique surveillée s'écarte des tendances normales observées par le système. Les alertes de tendance sont plus complexes que les alertes de seuil et sont utiles pour surveiller les tendances métriques, telles que les temps d'aller-retour anormalement élevés ou les serveurs de stockage dont le trafic est anormalement faible, ce qui peut indiquer un échec de sauvegarde.

Créez une alerte de tendance pour surveiller lorsqu'une métrique s'écarte du comportement normal et lorsque les seuils sont difficiles à définir. Découvrez comment configurer une alerte de tendance.

En outre, vous pouvez configurer une alerte avec les options suivantes :

- Définissez un intervalle d'exclusion pour supprimer les alertes pendant certaines périodes, par exemple pendant une période de maintenance.
- Configuration des notifications pour recevoir un e-mail lorsqu'une alerte est générée.

Afficher les alertes

La page Alertes affiche la liste de toutes les alertes générées pendant l' intervalle de temps spécifié.

Sélectionnez l'un des filtres en haut de la page pour ajuster la liste ou cliquez sur le nom d'une alerte pour afficher les détails de l'alerte.

Type de source

Filtrez les alertes attribuées aux applications ou aux appareils.

Sévérité

Filtrez les alertes par niveau de gravité.

Type d'alerte

Filtrez par seuil, tendance ou alertes de détection.

Important: Les alertes de détection sont obsolètes et seront supprimées dans une prochaine version. Pour recevoir des notifications concernant les détections, créer une règle de notification.

Site

Filtrez par sites connectés. (Disponible uniquement auprès d'un console.)

La page Alertes affiche les informations suivantes concernant chaque alerte :

Sévérité

Indicateur codé par couleur du niveau de gravité de l'alerte. Vous pouvez définir les niveaux de gravité suivants : urgence, alerte, critique, erreur, avertissement, notification, information et débogage.

Nom de l'alerte

Nom de l'alerte configurée. Cliquez sur le nom de l'alerte pour afficher les détails de l'alerte.

La source

Nom de la source de données dans laquelle les conditions d'alerte se sont produites. Cliquez sur le nom de la source pour accéder à la page d'aperçu de la source.

Heure

Heure à laquelle les conditions d'alerte se sont produites le plus récemment.

Type d'alerte

Indique une alerte de tendance ou de seuil.

Pour plus d'informations sur l'affichage des alertes, consultez les rubriques suivantes

- Ajouter un widget Alertes à un tableau de bord
- FAQ sur les alertes

Configuration d'une alerte de seuil

Configurez une alerte de seuil pour surveiller le moment où une métrique spécifique franchit une limite définie. Par exemple, vous pouvez générer une alerte lorsqu'un code d'état HTTP 500 est observé plus de 100 fois au cours d'une période de dix minutes.

Avant de commencer
Tu dois avoir privilèges d'écriture complets ou supérieur.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Alertes**.
3. Cliquez **Créez**.
4. Entrez un nom unique pour la configuration de l'alerte dans **Nom** champ.
5. Dans le **Descriptif** champ, ajoutez des informations sur l' alerte.

   Conseil: Les descriptions des alertes prennent en charge le Markdown, une syntaxe de formatage simple qui convertit le texte brut en HTML. Pour plus d'informations, consultez le FAQ sur les alertes.
6. Dans le **Type d'alerte** section, cliquez **Alerte de seuil**.
7. Dans le **Sources assignées** dans ce champ, saisissez le nom d'un équipement, d'un groupe d'équipements ou d'une application, puis sélectionnez-le dans les résultats de recherche.

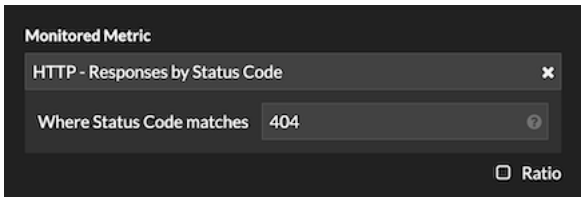
   Pour rechercher un site, un réseau de flux ou une interface de flux, sélectionnez ce type de source dans le menu déroulant en haut des résultats de recherche.
8. Optionnel : Cliquez **Ajouter une source** pour attribuer l'alerte à plusieurs sources. Plusieurs sources doivent être du même type, par exemple uniquement des appareils et des groupes d'équipements ou uniquement des applications.

Conseil Attribuez une alerte à un groupe déquipements pour gérer efficacement les assignations à plusieurs appareils.

9. Dans le **Métrique surveillée** champ, tapez le nom d'une métrique, puis sélectionnez-la dans les résultats de recherche.

   La métrique doit être compatible avec les sources assignées. Par exemple, si vous attribuez l'alerte à une application, vous ne pouvez pas sélectionner de métrique d'équipement.

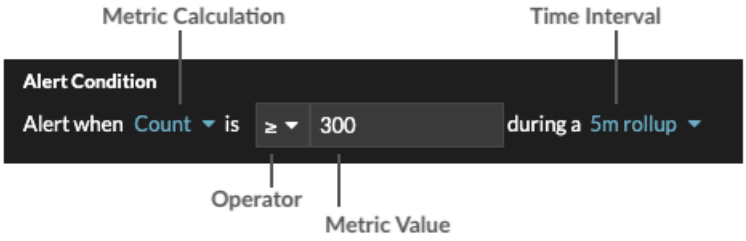
   Note: Si vous sélectionnez un métrique de détail, vous pouvez spécifier une valeur clé. Par exemple, vous pouvez sélectionner HTTP - Réponses par code d'état, puis spécifier 404 comme valeur clé. Une alerte est générée uniquement lorsque des réponses HTTP contenant des codes d'état 404 se produisent.



10. Optionnel : Pour surveiller la valeur d'une métrique divisée par une métrique secondaire, cliquez sur **Ratio** puis sélectionnez une métrique secondaire.

    Par exemple, vous pouvez surveiller le pourcentage d'erreurs HTTP survenant dans les réponses en divisant les erreurs de réponse HTTP par les réponses HTTP.

11. Dans la section Condition d'alerte, spécifiez les conditions de génération d'une alerte.



a) Sélectionnez un calcul métrique pour spécifier comment calculer la valeur métrique dans l'intervalle de temps. Les options disponibles dépendent du type de données.

Compter	• Compter • Débit par seconde • Tarif par minute • Tarif par heure
Ensemble de données	• Minimum • 25e percentile • Médiane

	• 75e percentile • Maximum
Set d'échantillons	• Méchant • +1 à +7 écarts types • -1 à -7 écarts types
Maximum, instantané	Aucune mesure ; l'opérateur compare la valeur métrique réelle.

b) Sélectionnez un opérateur pour spécifier comment comparer le calcul de la métrique à la valeur de la métrique.
c) Spécifiez la valeur métrique à comparer au calcul de la métrique.
d) Sélectionnez l'intervalle de temps pendant lequel la valeur métrique est observée et les données métriques sont agrégées ou cumulées. Vous pouvez sélectionner un intervalle de temps compris entre 30 secondes et 30 minutes.

Par exemple, pour générer une alerte lorsque plus de 300 erreurs de réponse HTTP se produisent dans les 5 minutes, spécifiez les conditions suivantes :

- Calcul métrique : nombre
- Opérateur : >
- Valeur métrique : 300
- Intervalle de temps : cumul de 5 m

12. Optionnel : Dans la section Notifications, ajouter une notification par e-mail à une alerte pour recevoir des e-mails ou des interruptions SNMP lorsqu'une alerte est générée.
13. Dans la section État, cliquez sur une option pour activer ou désactiver l'alerte.
14. Optionnel : Ajouter un intervalle d'exclusion pour supprimer les alertes à des moments précis.
15. Cliquez **Enregistrer**.

Configuration d'une alerte de tendance

Configurez une alerte de tendance pour surveiller lorsqu'une métrique spécifique s'écarte des tendances normales. Les alertes de tendance sont utiles pour surveiller les tendances métriques, telles que les temps d' aller-retour anormalement élevés ou les serveurs de stockage dont le trafic est anormalement faible, ce qui peut indiquer un échec de sauvegarde. Par exemple, vous pouvez configurer une alerte de tendance qui génère des alertes lorsqu'un pic (75e centile) du temps de traitement du serveur Web HTTP dure plus de 10 minutes et lorsque la valeur métrique du temps de traitement est 100 % supérieure à la tendance.

Avant de commencer
Tu dois avoir privilèges d'écriture complets ou supérieur.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Alertes**.
3. Cliquez **Créez**.
4. Entrez un nom unique pour la configuration de l'alerte dans **Nom** champ.
5. Dans le **Descriptif** champ, ajoutez des informations sur l' alerte.

   Conseil Les descriptions des alertes prennent en charge le Markdown, une syntaxe de formatage simple qui convertit le texte brut en HTML. Pour plus d'informations, consultez le FAQ sur les alertes.
6. Dans le **Type d'alerte** section, cliquez **Alerte de tendance**.
7. Dans le **Sources assignées** dans ce champ, saisissez le nom d'un équipement, d'un groupe d'équipements ou d'une application, puis sélectionnez-le dans les résultats de recherche.

Pour rechercher un site, un réseau de flux ou une interface de flux, sélectionnez ce type de source dans le menu déroulant en haut des résultats de recherche.

8. Optionnel : Cliquez **Ajouter une source** pour attribuer l'alerte à plusieurs sources. Plusieurs sources doivent être du même type, par exemple uniquement des appareils et des groupes d'équipements ou uniquement des applications.

   Conseil : Attribuez une alerte à un groupe d'équipements pour gérer efficacement les assignations à plusieurs appareils.

9. Dans le **Métrique surveillée** champ, tapez le nom d'une métrique, puis sélectionnez-la dans les résultats de recherche.

   La métrique doit être compatible avec les sources assignées. Par exemple, si vous attribuez l'alerte à une application, vous ne pouvez pas sélectionner de métrique d'équipement.

   Si vous sélectionnez une métrique de jeu de données telle que le temps de traitement du serveur HTTP, vous devez spécifier l'une des méthodes d'agrégation de données suivantes :

Fusionner	Agrégez toutes les valeurs du jeu de données métriques et appliquez le modèle de pondération des tendances à un sur-ensemble de données. Par exemple, un cumul agrégé de 30 secondes, ou cycle métrique, contient un seul jeu de données pour chaque intervalle de 30 secondes. Par conséquent, un intervalle de 30 minutes comporte 60 ensembles de données.
Méchant	Agrégez la moyenne de chaque jeu de données métriques.
Percentile	Agrégez le percentile de chaque jeu de données métriques en fonction de la valeur que vous spécifiez pour **Percentile**.
Écart type absolu	Agrégez le jeu de données métriques à son écart type sous forme de constante.
Écart type relatif	Agrégez le jeu de données métriques à son écart type par rapport à la moyenne.

10. Optionnel : Pour surveiller la valeur d'une métrique divisée par une métrique secondaire, cliquez sur **Ratio** puis sélectionnez une métrique secondaire.

    Par exemple, divisez les erreurs de réponse HTTP par les réponses HTTP pour suivre l'évolution du pourcentage d'erreurs HTTP.

11. Dans la section Définition de la tendance, spécifiez le mode de calcul de la tendance :
    a) Dans la liste déroulante Modèle de pondération des tendances, sélectionnez un modèle. Le modèle de pondération agrège les valeurs métriques historiques pour calculer une tendance.

Méchant	Calculez une tendance en faisant la moyenne de toutes les valeurs métriques, pondérées de manière égale.
Valeur minimale	Calculez une tendance à partir des mesures les plus faibles.
Valeur médiane	Calculez une tendance à partir des valeurs métriques historiques médianes.
Valeur maximale	Calculez une tendance à partir des indicateurs de valeur les plus élevés.
Percentile	Calculez une tendance à partir du percentile de chaque métrique en fonction de la valeur que vous spécifiez pour **Valeur percentile**.
Écart type absolu	Calculez une tendance en comparant l' écart type sous forme de valeur constante à la tendance actuelle. À partir du **Type de déviation** liste déroulante, sélectionnez un type : • Basé sur des échantillons • Basé sur la population
Écart type relatif	Calculez une tendance en comparant l' écart type sous forme de valeur par rapport à la moyenne de la tendance actuelle. À partir du **Type de déviation** liste déroulante, sélectionnez un type : • Basé sur des échantillons • Basé sur la population
Régression linéaire	Calculez une tendance linéaire en fonction des valeurs métriques précédentes.
Régression polynomiale du 2e degré	Calculez une tendance quadratique en projetant une courbe avec l'équation suivante : `y=ax^2+bx+c`
Moyenne exponentielle unique	Calcule une tendance en faisant la moyenne des valeurs métriques basées sur le poids . Dans le **Calcul récent de la valeur et du poids** champ, spécifiez un grand nombre pour donner plus de poids aux valeurs métriques les plus récentes ou spécifiez un petit nombre pour donner plus de poids aux valeurs métriques les plus anciennes.
Moyenne exponentielle double	Calcule une tendance en faisant la moyenne des valeurs métriques basées sur le poids . Dans le **Calcul récent de la valeur et du poids** champ, spécifiez un grand nombre pour donner plus de poids aux valeurs métriques les plus récentes ou spécifiez un petit nombre pour

	donner plus de poids aux valeurs métriques les plus anciennes. Notez que les calculs de moyenne exponentielle doubles sont plus précis pour prédire la trajectoire de la tendance.
Valeur statique	Calculez une tendance en fonction d'une valeur métrique statique par rapport à un calcul métrique. Spécifiez une valeur statique et sélectionnez un calcul métrique : • Tarif par heure • Tarif par minute • Compter Ce modèle est utile pour tracer des lignes constantes pour les SLA.
Trimean	Calculez une tendance en fonction de la moyenne pondérée des valeurs métriques des 25e, 50e et 75e percentiles.
Delta temporel	Calculez une tendance en comparant les valeurs métriques actuelles aux données historiques.
Moyen Winsorisé	Calculez une tendance en récupérant les valeurs métriques aux pourcentages bas et élevés spécifiés et en les remplaçant par les valeurs restantes les plus faibles et les plus élevées. Par exemple, les valeurs métriques supérieures au 90e percentile deviennent les mêmes valeurs que le 90e, et les valeurs métriques inférieures au 10e percentile deviennent les mêmes valeurs que le 10e percentile. À partir du **Winsorisation** liste déroulante, sélectionnez une paire de pourcentages : • 5/95e percentile • 10/90e percentile • 25/75e percentile

b) À partir du **Fenêtre de tendance** liste déroulante, sélectionnez une fenêtre de calcul.

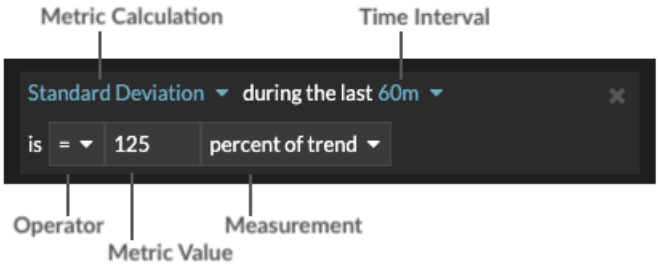
Même heure de la semaine	Calculez une tendance en comparant les statistiques recueillies au cours de la même fenêtre d'une heure chaque semaine.
Même heure du jour	Calculez une tendance en comparant les indicateurs collectés chaque jour sur la même fenêtre d'une heure.
Moyenne mobile par minute	Calculez une tendance en faisant la moyenne des valeurs métriques recueillies chaque minute

	dans un laps de temps spécifié à partir de l'heure actuelle.
Moyenne mobile par heure	Calculez une tendance en faisant la moyenne des valeurs métriques recueillies chaque heure dans un laps de temps spécifié à partir de l'heure actuelle.

c) Dans le **Rétrospective des tendances** champ, spécifiez la fenêtre temporelle des données historiques que le système ExtraHop examinera pour calculer la tendance. Les valeurs rétrospectives valides sont déterminées par la fenêtre de tendance sélectionnée.

- Spécifiez une valeur comprise entre 1 et 45 jours si la même heure du jour est sélectionnée.
- Spécifiez une valeur comprise entre 1 et 15 semaines si la même heure de la semaine est sélectionnée.
- Spécifiez une valeur comprise entre 1 et 48 heures si la moyenne mobile horaire est sélectionnée.
- Spécifiez une valeur comprise entre 1 et 999 minutes si la moyenne mobile par minute est sélectionnée.

12. Dans la section Condition d'alerte, spécifiez les conditions de génération d'une alerte.



a) À partir du **Tout faire correspondre** liste déroulante, sélectionnez une option pour générer une alerte lorsque toutes les conditions d'alerte, certaines ou aucune d'entre elles sont remplies.

b) Sélectionnez un calcul métrique pour spécifier comment calculer la valeur métrique dans l'intervalle de temps.

Méchant	Calculez la valeur moyenne de la métrique.
Médiane	Calculez la valeur du 50e percentile de la métrique .
25e percentile	Calculez la valeur du 25e percentile de la métrique .
75e percentile	Calculez la valeur du 75e percentile de la métrique.
Écart type	Calculez l'écart type par rapport à la métrique. L'écart type est l'ampleur de la variation par rapport à la tendance.
Compter	Spécifiez le total absolu de la métrique. Aucune mesure n'est requise.

c) Sélectionnez l'intervalle de temps pendant lequel la valeur métrique est observée. Vous pouvez sélectionner un intervalle compris entre 30 secondes et 30 minutes.

d) Sélectionnez un opérateur pour spécifier comment le calcul de la métrique est comparé à la valeur de la métrique.

e) Spécifiez la valeur métrique à comparer au calcul de la métrique.

f) Spécifiez le mode de mesure de la valeur métrique.

- Pourcentage de tendance
- Absolu
- Par seconde
- Par minute

g) Optionnel : Cliquez **Ajouter une condition** pour ajouter d'autres critères de condition ou cliquez sur **Ajouter un groupe de conditions** aux critères d' état du nid.

Par exemple, pour générer une alerte lorsque l'écart type de la métrique observée sur un intervalle de 60 minutes est égal à une valeur de tendance de 25 %, spécifiez les conditions suivantes :

- Calcul métrique : écart type
- Intervalle de temps : 60 m
- Opérateur : =
- Valeur métrique : 125
- Mesure : pourcentage de tendance

13. Optionnel : Dans la section Notifications, ajouter une notification par e-mail à une alerte pour recevoir des e-mails ou des interruptions SNMP lorsqu'une alerte est générée.
14. Dans la section État, cliquez sur une option pour activer ou désactiver l'alerte.
15. Optionnel : Ajouter un intervalle d'exclusion pour supprimer les alertes à des moments précis.
16. Cliquez **Enregistrer**.

Ajouter une notification à une configuration d'alerte

Configurez une alerte pour envoyer une notification lorsque la condition d'alerte est remplie.

Ajouter une notification d'alerte (RevealX Enterprise)

Vous pouvez ajouter une notification à une configuration d'alerte qui enverra un e-mail à une adresse e-mail ou à un groupe d'e-mails spécifié lorsque l'alerte se produira. L'e-mail contient les détails de l'alerte et un lien permettant d'afficher la source de l'alerte. Vous pouvez également envoyer des notifications à un écouteur SNMP .

Avant de commencer

- Tu dois avoir privilèges d'écriture complets ou supérieur.
- Votre système ExtraHop doit être configuré pour envoyer des notifications.
- Si vous souhaitez qu'une alerte soit envoyée à plusieurs adresses e-mail, configurer un groupe de messagerie.
- Si vous souhaitez envoyer des notifications via SNMP, configurer l'écouteur SNMP.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Alertes**.
3. Dans le tableau Alertes, cliquez sur l'alerte de votre choix.
4. Dans la section Notifications, spécifiez les groupes de messagerie et les adresses auxquels vous souhaitez envoyer une notification lorsque l'alerte se produit.
   - Cliquez **Sélectionnez un groupe de notifications par e-mail** et cliquez sur un ou plusieurs groupes de messagerie.
   - Tapez des adresses e-mail individuelles. Les adresses multiples doivent être séparées par une virgule.
5. Optionnel : Cliquez **Envoyer un trap SNMP** pour envoyer des notifications à un écouteur SNMP .
6. Optionnel : Ajoutez des mesures supplémentaires à la notification par e-mail.

   L'e-mail inclut la valeur de ces mesures lorsque l'alerte s'est produite.

a) Cliquez **Afficher les options avancées**.
b) À partir du Mesures supplémentaires dans les notifications par e-mail section, cliquez sur **Ajouter une métrique**.
c) Dans le champ de recherche, saisissez le nom d'une métrique, puis sélectionnez-la dans les résultats de recherche.

   La métrique doit être compatible avec le type de source attribué et la métrique surveillée, telle que les appareils et les métriques des équipements.

7. Cliquez **Enregistrer**.

Ajouter une notification d'alerte (RevealX 360)

Vous pouvez ajouter une notification à une configuration d'alerte qui enverra un e-mail à une ou plusieurs adresses e-mail spécifiées lorsque l'alerte se produira. L'e-mail contient les détails de l'alerte et un lien permettant d'afficher la source de l'alerte.

Avant de commencer
Tu dois avoir privilèges d'écriture complets ou supérieur.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Alertes**.
3. Dans le tableau Alertes, cliquez sur l'alerte de votre choix.
4. Dans la section Notifications, spécifiez les adresses e-mail à notifier lorsque l' alerte se produit.

   Tapez des adresses e-mail individuelles. Les adresses multiples doivent être séparées par une virgule.
5. Optionnel : Ajoutez des mesures supplémentaires à la notification par e-mail.

   L'e-mail inclut la valeur de ces mesures lorsque l'alerte s'est produite.
   a) Cliquez **Afficher les options avancées**.
   b) Dans la section Mesures supplémentaires dans les notifications par e-mail, cliquez sur **Ajouter une métrique**.
   c) Dans le champ de recherche, saisissez le nom d'une métrique, puis sélectionnez-la dans les résultats de recherche.

      La métrique doit être compatible avec le type de source attribué et la métrique surveillée, telle que les appareils et les métriques des équipements.
6. Cliquez **Enregistrer**.

Ajouter un intervalle d'exclusion à une alerte

Les intervalles d'exclusion vous permettent de supprimer une ou plusieurs alertes pendant des plages de temps spécifiques. Par exemple, vous pouvez supprimer une alerte après les heures de bureau, le week-end ou pendant les périodes de maintenance.

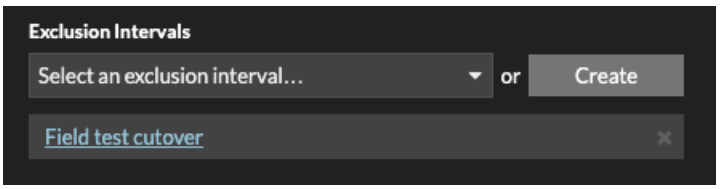
Créez un nouvel intervalle d'exclusion lorsque vous créez ou modifiez une alerte. Après avoir créé un intervalle d'exclusion, vous pouvez l'appliquer aux alertes existantes et nouvelles.

Avant de commencer
Tu dois avoir privilèges d'écriture complets ou supérieur.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Alertes**.
3. Dans le tableau Alertes, cliquez sur l'alerte de votre choix.
4. Dans la section Modifier l'alerte, cliquez sur **Afficher les options avancées**.
5. Dans la section Intervalles d'exclusion, ajoutez un intervalle existant ou créez-en un nouveau.

Option	Description
Ajouter un intervalle d'exclusion existant	1. Cliquez sur la liste déroulante des intervalles d'exclusion et sélectionnez un intervalle. 2. Répétez l'opération pour ajouter un intervalle supplémentaire à l'alerte.
Création d'un nouvel intervalle d'exclusion	1. Cliquez **Créez**. 2. Entrez un nom unique pour l'intervalle d'exclusion dans **Nom** champ. 3. Dans le **Descriptif** champ, ajoutez des informations sur l'intervalle. 4. Dans la section Exclure, spécifiez un intervalle et entrez une plage de temps : • Cliquez **Tous les jours à partir de** pour définir un intervalle récurrent quotidien. • Cliquez **Chaque semaine à partir de** pour définir un intervalle récurrent hebdomadaire. • Cliquez **Plage de temps personnalisée** pour définir un intervalle unique. 5. Facultatif : Dans la section Attributions, sélectionnez une option d'attribution globale : • Cliquez **Attribuer à toutes les alertes** pour ajouter l'intervalle à toutes les configurations d'alerte existantes et futures. • Cliquez **Affecter à toutes les tendances** pour exclure l'activité métrique pendant l'intervalle des calculs de tendance. 6. Cliquez **Enregistrer** pour créer l'intervalle et l'ajouter à l'alerte.

Conseil : Dans la liste des intervalles d'exclusion ajoutés, cliquez sur le nom d'un intervalle pour modifier les propriétés, ou cliquez sur l'icône de suppression (X) pour supprimer l'intervalle de l'alerte.



6. Cliquez **Enregistrer** puis cliquez sur **Terminé**.

Disques

Les enregistrements sont des informations structurées sur les flux de transactions, de messages et de réseaux qui sont générées et envoyées depuis le système ExtraHop vers un espace de stockage des enregistrements. Une fois vos enregistrements collectés et stockés, vous pouvez les rechercher dans le système ExtraHop.

Les enregistrements sont collectés à deux niveaux de protocole : L3 et L7. Les enregistrements L3 (ou flux) indiquent les transactions de couche réseau entre deux appareils via le protocole IP. Les enregistrements L7 présentent des transactions basées sur des messages (comme ActiveMQ, DNS et DHCP), transactionnelles (telles que HTTP, SMB et NFS) et basées sur des sessions (telles que TLS et ICA).

Par exemple, si vous avez rencontré cinquante erreurs HTTP 503, les transactions HTTP associées contiendraient des informations sur l'URL, le serveur Web, le client qui a envoyé la demande, etc. Ces informations peuvent vous aider à identifier le problème sous-jacent.

Vidéos Consultez la formation associée : Disques

Avant de commencer

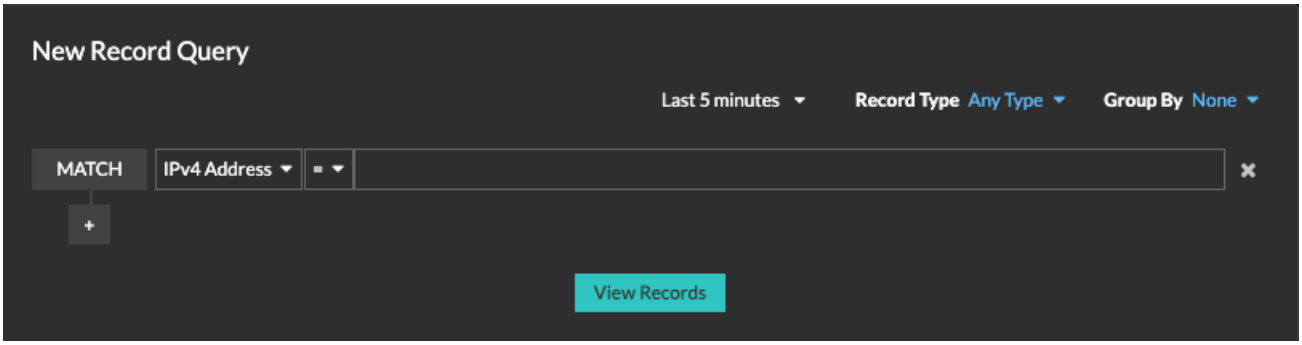
- Vous devez disposer d'un espace de stockage des enregistrements configuré, tel qu'un espace de stockage des enregistrements ExtraHop, Splunk, Google BigQuery, ou Balance à journaux CrowdStrike Falçon.
- Vous ne pouvez configurer qu'un seul espace de stockage des enregistrements pour le système ExtraHop.
- Votre système ExtraHop doit être configuré pour collecter et stocker enregistrements de flux ou records L7.

Naviguer dans les enregistrements

La page principale des enregistrements propose plusieurs méthodes pour rechercher des enregistrements stockés. Cliquez **Disques** depuis le menu supérieur pour commencer.

Recherche standard

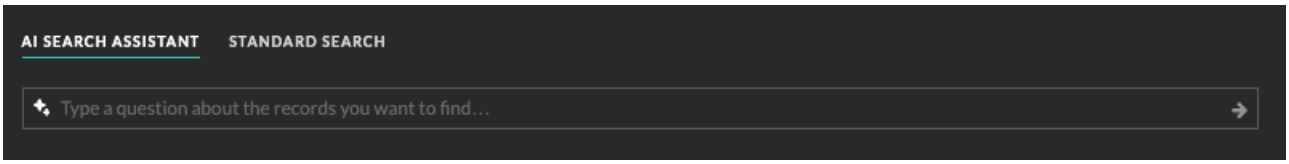
Recherchez des enregistrements à l'aide d'une recherche standard pour créer un filtre complexe en combinant les opérateurs « ET » et « OU » avec des options de filtre supplémentaires telles que le type d'enregistrement et l'intervalle de temps. En savoir plus sur l'interrogation d'enregistrements à l'aide d'une recherche standard.



Assistant de recherche IA

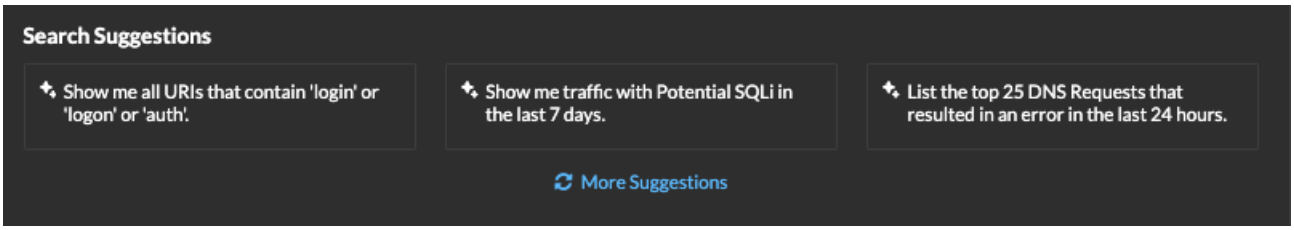
AI Search Assistant vous aide à rechercher des enregistrements contenant des questions rédigées dans un langage naturel et courant afin de créer rapidement des requêtes complexes par rapport à

la création d'une requête de recherche standard avec les mêmes critères. L'assistant de recherche AI doit être activé par votre administrateur ExtraHop.En savoir plus sur la recherche d'enregistrements avec AI Search Assistant.



Suggestion de recherche

Le système ExtraHop propose plusieurs recherches suggérées avec des filtres prédéfinis qui vous aident à effectuer plus efficacement des recherches d'enregistrements courantes. Cliquez sur une recherche suggérée pour appliquer la requête et afficher immédiatement les enregistrements ou cliquez sur **Plus de suggestions** pour plus d'options.



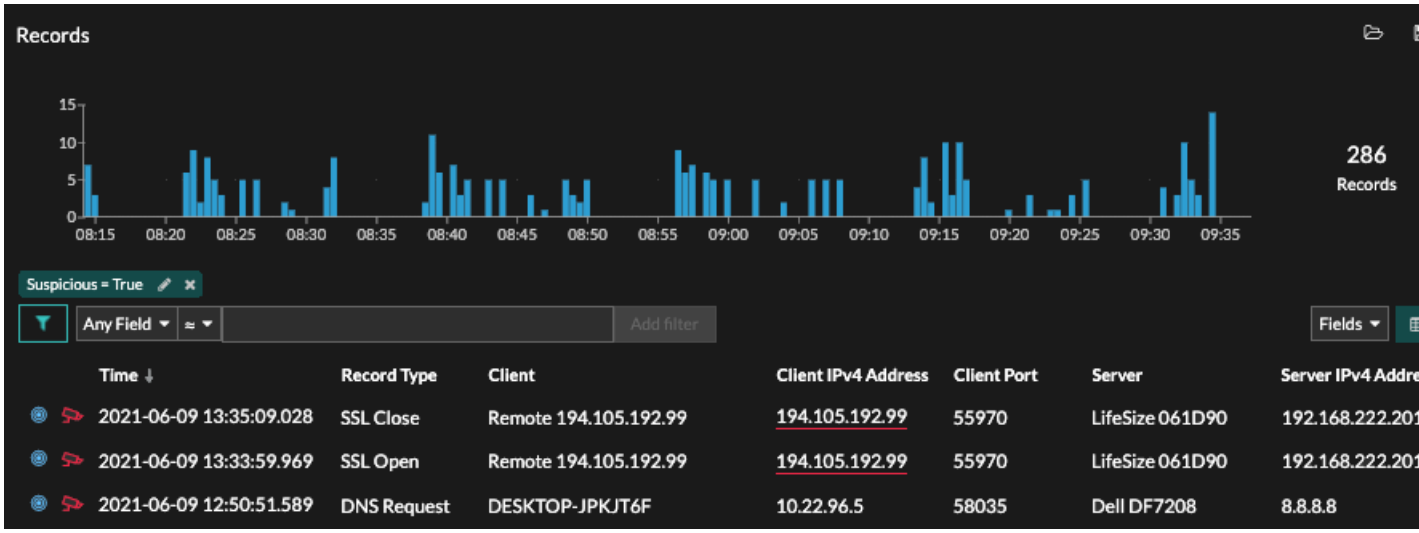
Requêtes enregistrées

Vous pouvez également sélectionner une requête précédemment enregistrée dans la liste de la page Enregistrements et afficher immédiatement les enregistrements, ou vous pouvez cliquer sur l'icône du dossier dans le coin supérieur droit de la page pour afficher toutes les requêtes enregistrées.

Note: Pour créer une requête d'enregistrement pour une métrique personnalisée, vous devez d'abord définir la relation entre les enregistrements en lier la métrique personnalisée à un type d'enregistrement.

Affichage des résultats d'une requête d'enregistrement

Une fois que vous avez soumis la requête, les résultats apparaissent sur la page principale des enregistrements.



Note: Une requête peut renvoyer des millions d'enregistrements en fonction de l' intervalle de temps et des critères de filtre. Si une requête dépasse le nombre maximum de résultats de requête, un nombre tronqué d'enregistrements apparaît (espace de stockage des enregistrements ExtraHop uniquement). Par exemple, les requêtes provenant du filtre Any Field par défaut génèrent souvent un très grand nombre de résultats et peuvent avoir un impact sur les performances.

Voici quelques méthodes pour explorer les résultats des requêtes d'enregistrement :

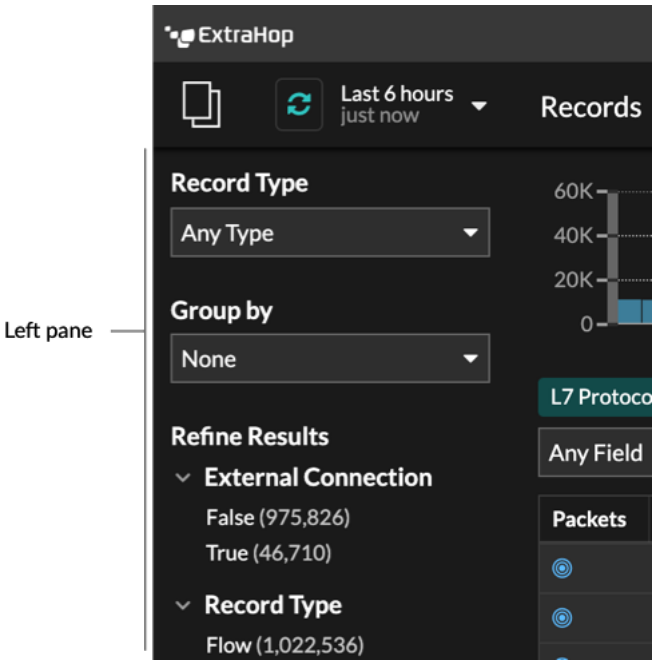
- Dans le graphique des enregistrements, passez la souris sur un intervalle de temps pour afficher le nombre d' enregistrements, ou cliquez et faites glisser le pointeur sur le graphique pour limiter les résultats de la requête d'enregistrement à un intervalle de temps spécifique.
- Cliquez sur un nom d'hôte ou une adresse IP pour afficher les détails de l'équipement ou du point de terminaison externe.
- Les enregistrements contenant des adresses IP, des noms d'hôte et des URI suspects apparaissent avec une icône de caméra rouge. Cliquez sur l'icône de la caméra pour voir renseignements sur les menaces pour l' enregistrement.
- Cliquez sur l'icône d'un paquet pour démarrer requête de paquet qui est filtré par cet enregistrement.
- Les résultats des enregistrements apparaissent dans un tableau par défaut. Cliquez sur la vue tabulaire ou la vue détaillée  icônes pour basculer l'affichage.
- Une requête s'arrête automatiquement si le nombre d'octets d'enregistrement scannés ou renvoyés est extrêmement important. En cas de pause, la requête affiche les enregistrements les plus récents. Cliquez **Poursuivre la requête** pour reprendre la recherche.
- Cliquez sur **Champs** liste déroulante pour ajouter des informations d'enregistrement supplémentaires à la vue des enregistrements.
- Dans la vue sous forme de tableau, cliquez et faites glisser les en-têtes de colonne pour organiser les informations d'enregistrement.
- Postulez simple ou filtres avancés pour détecter les problèmes potentiels, tels que des délais de traitement trop longs ou des tailles de réponse inhabituelles.

Affinez votre filtre de requête d'enregistrement

Vous pouvez affiner votre filtre de recherche d'enregistrements de plusieurs manières pour trouver les enregistrements exacts que vous recherchez. Les sections ci-dessous décrivent chaque méthode et présentent des exemples avec lesquels vous pouvez commencer pour vous familiariser.

Filtrer les résultats de l'enregistrement depuis le volet de gauche

Une fois que tous les enregistrements disponibles pour l'intervalle de temps que vous avez sélectionné apparaissent sur la page Enregistrements, vous pouvez filtrer depuis le volet de gauche pour affiner vos résultats.



Le **Type d'enregistrement** le menu déroulant affiche une liste de tous les types d' enregistrements que votre système ExtraHop est configuré pour collecter et stocker. Un type d'enregistrement détermine quelles données sont collectées et stockées dans l'espace de stockage des enregistrements.

Note: Comme vous devez créer un déclencheur pour collecter des enregistrements, vous avez besoin d'un moyen d' identifier le type de données que vous allez collecter. Il existe des types d'enregistrement intégrés qui collectent tous les champs connus disponibles pour un protocole. Vous pouvez commencer avec un type d' enregistrement intégré (tel que HTTP) et créer un déclencheur pour ne collecter que les champs du protocole qui vous intéressent (tels que l'URI et le code dstatus). Les utilisateurs avancés peuvent également créer un type d'enregistrement personnalisé s'ils ont besoin de collecter des informations propriétaires qui ne sont pas disponibles via un type d'enregistrement intégré.

Le **Regrouper par** La liste déroulante vous donne une liste de champs permettant de filtrer davantage le type d'enregistrement.

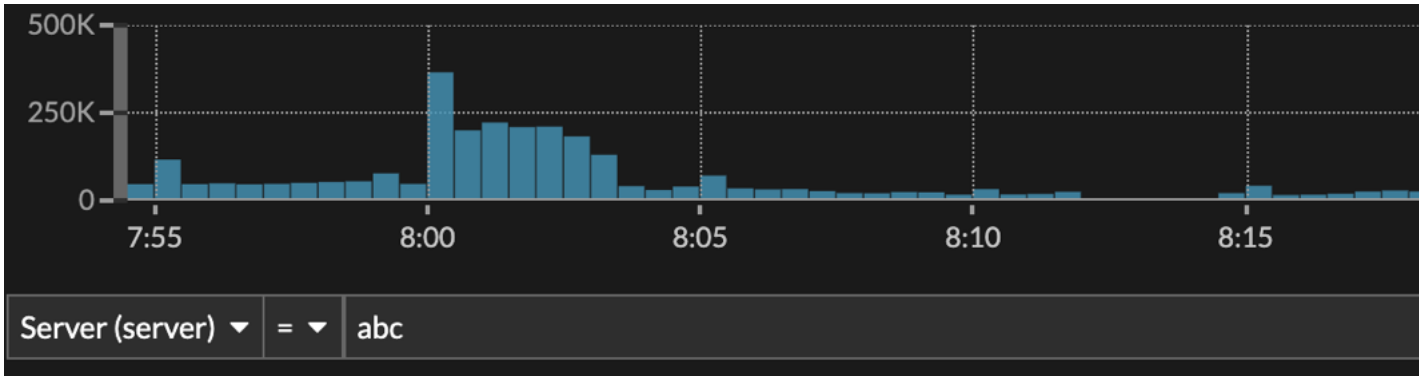
Le **Affiner les résultats** La section affiche une liste des filtres d'enregistrement courants pour le type d'enregistrement sélectionné avec le nombre d'enregistrements correspondant au filtre entre parenthèses.

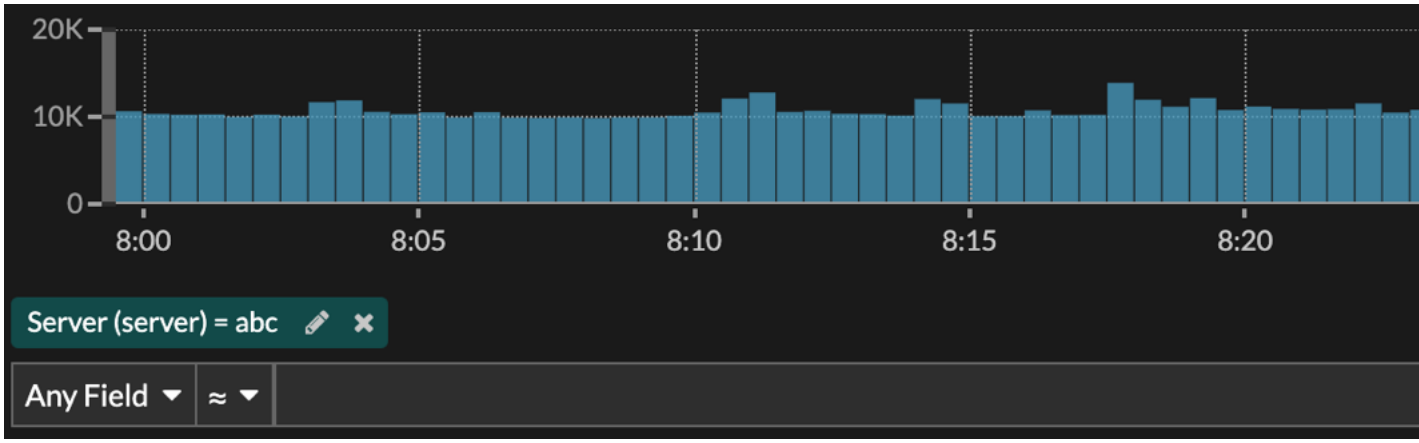
Filtrer les résultats de l'enregistrement via le trifield

Cliquez sur l'icône en forme de crayon pour modifier un filtre existant ou cliquez sur le bouton Ajouter un filtre avancé pour ajouter un nouveau filtre.

Dans le **Nom d'affichage du filtre** champ, vous pouvez spécifier un nom descriptif pour identifier l'objectif général de la requête.

Sélectionnez une option de critère dans le menu déroulant (l'option par défaut est Adresse IPv4), sélectionnez un opérateur (tel que le signe égal (=)), puis saisissez la valeur de recherche . Cliquez **Ajouter un filtre**, et le filtre est ajouté au-dessus de la barre de filtre.





Vos résultats n'affichent que les enregistrements correspondant au filtre.

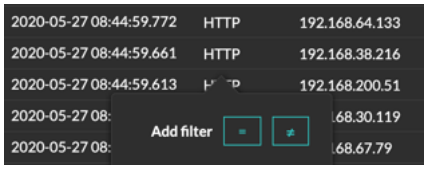
Les opérateurs suivants peuvent être sélectionnés en fonction du nom du champ sélectionné :

Opérateur	Descriptif
=	Égaux
≠	N'est pas égal
≈	Inclut Si les enregistrements sont stockés sur un espace de stockage des enregistrements ExtraHop, l'opérateur includes fait correspondre les mots entiers délimités par des espaces et des signes de ponctuation. Par exemple, une recherche sur « www.extra » correspondrait à « www.extra.com » mais pas à « www.extrahop.com ». Pour toutes les autres librairies, l'opérateur includes fait correspondre les sous-chaînes, y compris les espaces et la ponctuation. Par exemple, une recherche pour « www.extra » correspondrait à « www.extrahop.com », mais une recherche pour « www extra » ne correspondrait pas à « www.extrahop.com ».

Opérateur	Descriptif
	Les caractères Regex et les caractères génériques ne sont pas pris en charge.
≈/	Exclut Si les enregistrements sont stockés sur un espace de stockage des enregistrements ExtraHop, l'opérateur d'exclusion fait correspondre les mots entiers délimités par des espaces et des signes de ponctuation. Par exemple, une recherche sur « extra » exclurait « www.extra.com » mais pas « www.extrahop.com ». Pour toutes les autres librairies, l'opérateur d'exclusion fait correspondre les sous-chaînes, y compris les espaces et la ponctuation. Par exemple, une recherche sur « www.extra » exclurait « www.extrahop.com », mais une recherche sur « www extra » n'exclurait pas « www.extrahop.com ». Les caractères Regex et les caractères génériques ne sont pas pris en charge.
<	Moins de
≤	Inférieur ou égal à
>	Plus grand que
≥	Supérieur ou égal à
commence par	Commence par
existe	Existe
ne sort pas	N'existe pas

Filtrer directement à partir des résultats de l'enregistrement

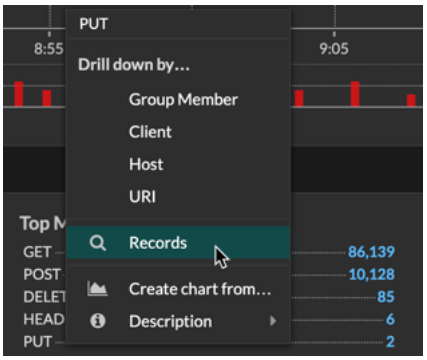
Vous pouvez sélectionner n'importe quelle entrée de champ affichée en mode tableau ou en affichage détaillé dans les résultats de votre enregistrement, puis cliquer sur l'opérateur contextuel pour ajouter le filtre. Les filtres sont affichés sous le résumé du graphique (à l'exception du champ de type d'enregistrement, qui est modifié dans le volet de gauche).



Recherche d'enregistrements dans le système ExtraHop

- Tapez un terme de recherche dans le champ de recherche global en haut de l'écran et cliquez sur Rechercher des enregistrements pour lancer une recherche sur tous les enregistrements stockés.

- Sur la page de présentation de l'équipement, cliquez sur **Enregistrements** pour démarrer une requête filtrée par cet équipement.
- Sur la page de présentation d'un groupe déquipements, cliquez sur **Afficher les enregistrements** pour démarrer une requête filtrée en fonction de ce groupe déquipements.
- À partir d'une carte de détection, cliquez sur Afficher les enregistrements pour lancer une requête filtrée avec les transactions associées à la détection.
- Cliquez sur l'icône Records à partir d'un widget graphique, comme illustré dans la figure suivante.



- Cliquez sur l'icône Records à côté d'une métrique détaillée après avoir exploré une métrique de niveau supérieur. Par exemple, après avoir étudié les réponses HTTP par serveur, cliquez sur l'icône Enregistrements pour créer une requête pour les enregistrements contenant une adresse IP de serveur spécifique.

Requête pour les enregistrements stockés

Vous pouvez interroger les enregistrements stockés dans l'espace de stockage des enregistrements à l'aide d'une recherche standard ou à l' aide de l'assistant de recherche AI.

- En savoir plus sur l'interrogation d'enregistrements à l'aide d'une recherche standard.
- En savoir plus sur la recherche d'enregistrements avec AI Search Assistant.
- Pour savoir comment rechercher un enregistrement spécifique, consultez notre procédure pas à pas pour Découvrir les ressources Web manquantes.
- Vous pouvez également automatiser cette tâche via l' API REST.

Prochaines étapes

Note: Pour créer une requête d'enregistrement pour une métrique personnalisée, vous devez d'abord définir la relation entre les enregistrements en lier la métrique personnalisée à un type d'enregistrement.

Interroger des enregistrements avec une recherche standard

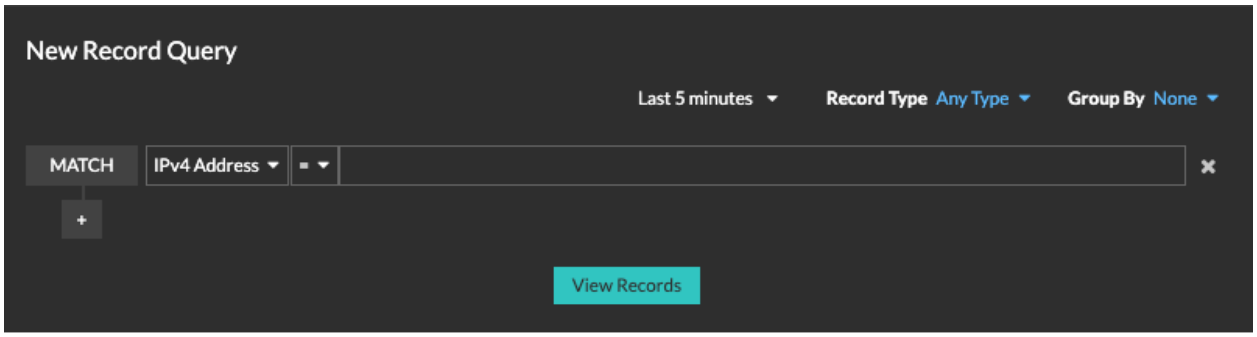
La page Enregistrements vous permet de créer un filtre complexe pour rechercher des enregistrements.

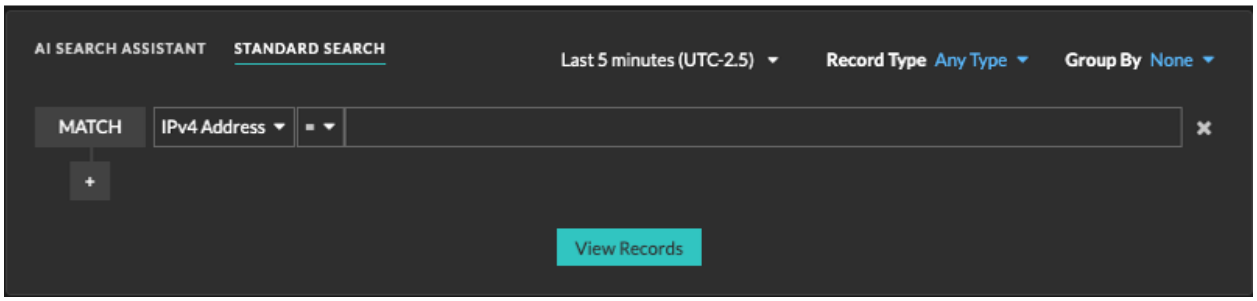
Voici quelques informations importantes à propos des requêtes d'enregistrement avec la recherche standard :

- Vous pouvez spécifier plusieurs critères à l'aide des opérateurs OR (Match Any), AND (Match All) et NOT.
- Vous pouvez regrouper les filtres et les imbriquer à quatre niveaux au sein de chaque groupe.
- Vous pouvez modifier un groupe de filtres après l'avoir créé pour affiner les résultats de recherche.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Disques**.

Si l'assistant de recherche AI n'est pas activé, la section Requête d'un nouvel enregistrement s' affiche. Si AI Search Assistant est activé, cliquez sur **Recherche standard**.



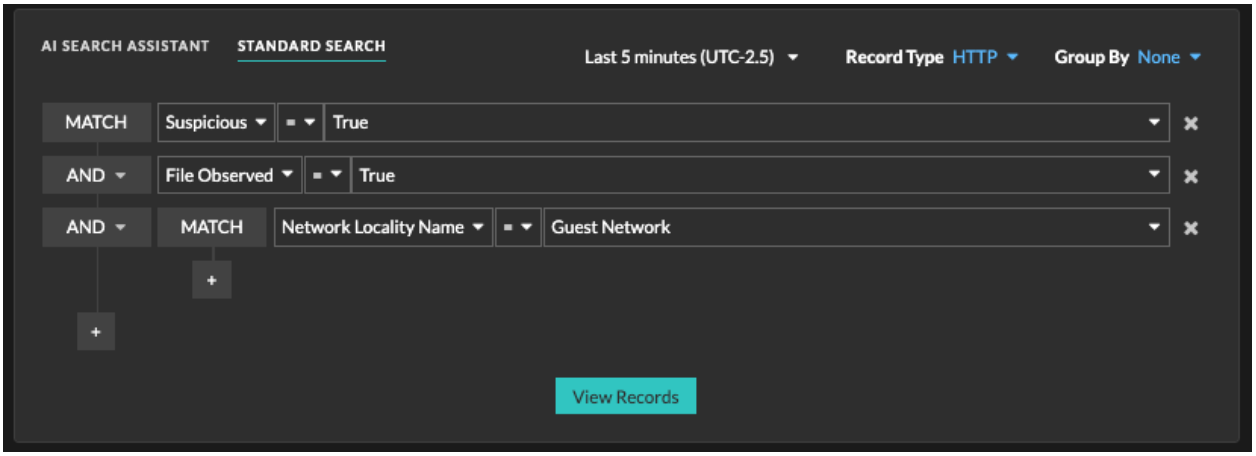


3. Sélectionnez l'intervalle de temps que vous souhaitez rechercher.

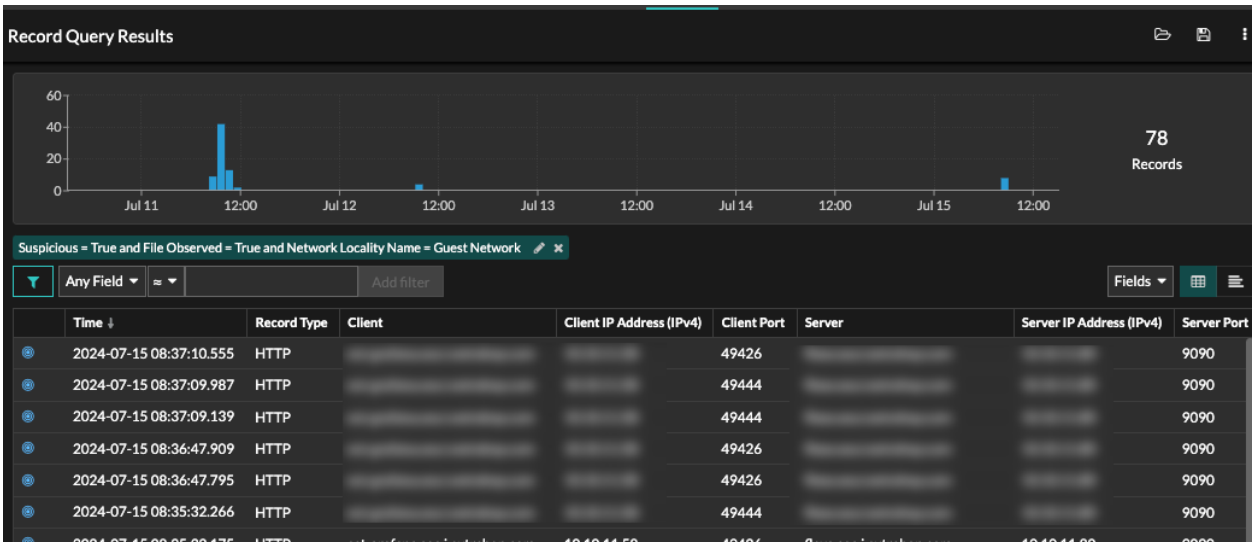
   L'intervalle de temps que vous sélectionnez modifie l'heure définie dans sélecteur de temps global.
4. À partir du **Type d'enregistrement** menu déroulant, sélectionnez un ou plusieurs types d'enregistrements que votre système ExtraHop est configuré pour collecter et stocker.
5. À partir du **Regrouper par** menu déroulant, sélectionnez une option pour spécifier la manière dont vous souhaitez regrouper les résultats. Les options affichées sont associées aux types d'enregistrement que vous avez sélectionnés.

   Par exemple, si vous regroupez les enregistrements HTTP par client, le tableau des résultats affiche les clients trouvés dans les transactions d'enregistrement, classés selon le nombre de fois que ce client a été trouvé.
6. Dans le menu déroulant des critères de filtre (la valeur par défaut est Adresse IPv4), sélectionnez les premiers critères auxquels vous souhaitez que le filtre corresponde. Les options affichées sont associées aux types d'enregistrement que vous avez sélectionnés.
7. Optionnel : Cliquez sur l'icône plus et sélectionnez **Ajouter un filtre** ou **Ajouter un groupe de filtres** pour spécifier d'autres critères au niveau supérieur ou secondaire du filtre.

   Un nouveau groupe de filtres ajoute des critères au résultat du filtre d'origine. Par exemple, si vous recherchez des transactions HTTP suspectes et contenant des fichiers, vous pouvez ajouter un groupe de filtres pour limiter les résultats aux enregistrements associés à une localité réseau spécifiée.



8. Cliquez **Afficher les enregistrements**.
   Les résultats des enregistrements sont affichés sur la page principale des enregistrements.



Prochaines étapes

- Tu peux afficher et explorer les résultats des requêtes d'enregistrement.
- Tu peux affinez votre filtre de requête d'enregistrement.
- Vous pouvez cliquer sur l'icône Enregistrer en haut à droite de la page pour enregistrer votre filtre pour une prochaine fois.
- Vous pouvez cliquer sur l'icône d'un paquet à côté d'un enregistrement pour démarrer requête de paquet qui est filtré par cet enregistrement ou cliquez sur le lien de requête en bas du tableau pour lancer une requête par paquet pour tous les enregistrements affichés.

Interrogez des enregistrements avec AI Search Assistant

L'assistant de recherche AI vous permet de rechercher des enregistrements contenant des questions rédigées dans un langage naturel courant afin de créer rapidement des requêtes complexes par rapport à la création d'une requête de recherche standard avec les mêmes critères.

Par exemple, si vous recherchez « Y a-t-il eu des transactions HTTP suspectes avec des fichiers au cours des 7 derniers jours ? » , la requête suivante de l'assistant de recherche AI s'affiche :

```
Time Interval = Last 2 days and Record Type = [HTTP]
```

```
Suspicious = True and File Observed = True
```

Voici quelques éléments à prendre en compte lors de la recherche d'appareils avec AI Search Assistant :

- Les invites sont associées aux mêmes critères de filtre d'enregistrement que ceux que vous spécifiez lors de la création d'une recherche standard.
- Les invites peuvent inclure des plages temporelles absolues et relatives, telles que « Afficher le trafic avec Potential SQLi au cours des 7 derniers jours ». L'année en cours est appliquée si une année n' est pas incluse pour une date.
- Les instructions doivent être aussi claires et concises que possible et nous vous recommandons d'essayer d' écrire quelques variantes pour optimiser vos résultats.
- Le système ExtraHop peut ne pas être en mesure de traiter une requête contenant des demandes d'informations d' enregistrement qui ne sont pas incluses dans les filtres disponibles.
- Le système ExtraHop peut conserver les instructions des utilisateurs à des fins d'amélioration du produit ; nous vous recommandons de ne pas inclure de données exclusives ou confidentielles dans vos invites.
- Vous pouvez modifier les critères du filtre de requête pour affiner les résultats de recherche.

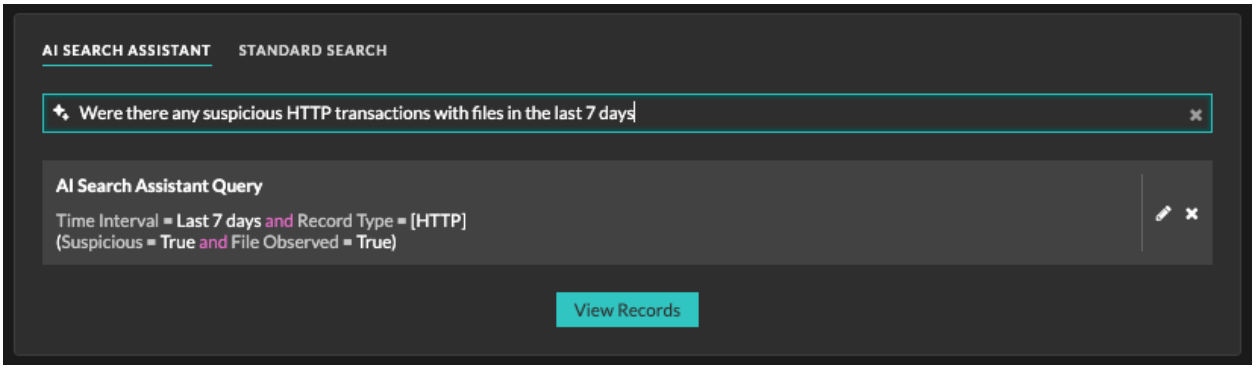
Avant de commencer

- Votre système ExtraHop doit être connecté à ExtraHop Cloud Services.
- L'assistant de recherche AI doit être activé par votre administrateur ExtraHop.

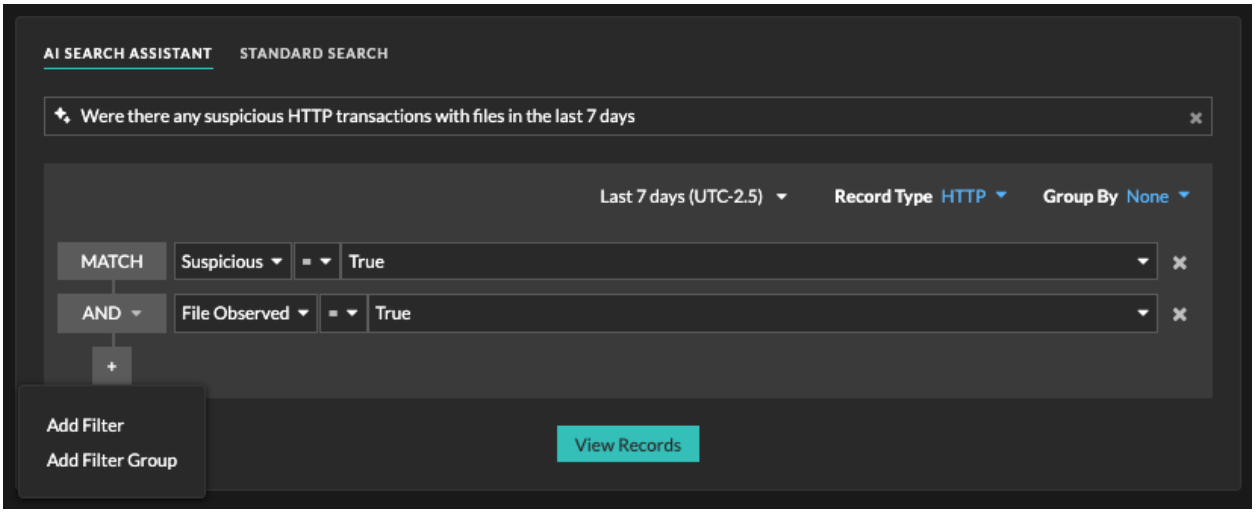
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Disques**.
3. Écrivez une invite dans le champ AI Search Assistant et appuyez sur ENTER.

   Conseil Cliquez sur le champ d'invite de recherche pour sélectionner une requête récente ou une recherche suggérée.

   Le filtre de requête AI Search Assistant s'affiche.



4. Optionnel : Dans la section Requête de l'assistant de recherche AI, cliquez sur l'icône de modification pour affiner les critères de votre filtre de requête.



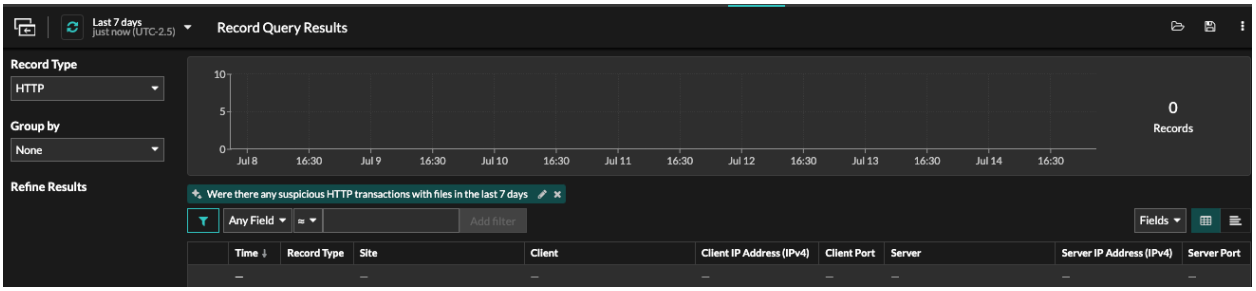
a) Dans la rangée supérieure, modifiez l'intervalle de temps, **Type d'enregistrement** ou **Grouper par** options.

b) Cliquez sur l'icône plus et sélectionnez **Ajouter un filtre** ou **Ajouter un groupe de filtres** pour spécifier d'autres critères au niveau supérieur ou secondaire du filtre.

Un nouveau groupe de filtres ajoute des critères au résultat du filtre d'origine. Par exemple, si vous recherchez des enregistrements HTTP suspects et contenant des fichiers, vous pouvez ajouter un groupe de filtres pour limiter les résultats aux enregistrements associés à une localité réseau spécifiée.

c) Cliquez **Terminé**.

5. Cliquez **Afficher les enregistrements**.
Les résultats des enregistrements sont affichés sur la page principale des enregistrements. Le nom d'affichage du filtre AI Search Assistant est l'invite que vous avez saisie et s'affiche au-dessus des trois champs.



Prochaines étapes

- Tu peux afficher et explorer les résultats des requêtes d'enregistrement.
- Tu peux affinez votre filtre de requête d'enregistrement.
- Vous pouvez cliquer sur l'icône Enregistrer en haut à droite de la page pour enregistrer votre filtre pour une prochaine fois.
- Vous pouvez cliquer sur l'icône d'un paquet à côté d'un enregistrement pour démarrer requête de paquet qui est filtré par cet enregistrement ou cliquez sur le lien de requête en bas du tableau pour lancer une requête par paquet pour tous les enregistrements affichés.

Collectez des records

La collecte de certains types d'enregistrements est activée par défaut. Vous pouvez ajouter ou supprimer les types d'enregistrements collectés et envoyés à votre espace de stockage des enregistrements depuis le Réglages/Enregistrements page. Ces enregistrements contiennent principalement des informations sur les messages, les transactions et les sessions envoyés via les protocoles L7 courants tels que DNS, HTTP et TLS.

Si vous souhaitez collecter uniquement des informations spécifiques sur les transactions, vous pouvez créer des enregistrements personnalisés via le API ExtraHop Trigger.

Note: Tu peux gérer ces paramètres de manière centralisée depuis une console.

En savoir plus sur Enregistrements ExtraHop.

Avant de commencer
Vous devez disposer d'un espace de stockage des enregistrements configuré, tel qu'un espace de stockage des enregistrements ExtraHop, Splunk, ou Google BigQuery.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Collection de disques**.
3. Sur le Disques page, cochez la case à côté des types de transactions que vous souhaitez capturer et stocker dans l'espace de stockage des enregistrements, puis cliquez sur **Activer**.
4. Cliquez **Disques** dans le menu supérieur, puis cliquez sur **Afficher les enregistrements** pour lancer une requête.

   Si vous ne voyez aucun enregistrement, patientez quelques minutes et réessayez. Si aucun enregistrement n' apparaît après cinq minutes, vérifiez votre configuration ou contactez Assistance ExtraHop.

Collecter des enregistrements de flux

Vous pouvez collecter et stocker automatiquement tous les enregistrements de flux, qui sont des communications au niveau réseau entre deux appareils via un protocole IP. Si vous activez ce paramètre, mais que vous n'ajoutez aucune adresse IP ni plage de ports, tous les enregistrements de flux détectés sont capturés. La configuration des enregistrements de flux pour la collecte automatique est assez simple et peut être un bon moyen de tester la connectivité à votre espace de stockage des enregistrements.

Avant de commencer
Vous devez avoir accès à un système ExtraHop avec Privilèges d'administration du système et des accès.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Disques section, cliquez sur **Enregistrements de flux automatiques**.
3. Sélectionnez le **Activé** case à cocher.
4. Dans le Intervalle de publication dans ce champ, saisissez un nombre compris entre 60 et 21600.

   Cette valeur détermine la fréquence à laquelle les enregistrements d'un flux actif sont envoyés à l'espace de stockage des enregistrements. La valeur par défaut est de 1800 secondes.
5. Dans le Adresse IP dans le champ, saisissez une seule adresse IP ou une plage d' adresses IP au format IPv4, IPv6 ou CIDR.
6. Cliquez sur le signe plus vert (**+**) icône.

   Vous pouvez supprimer une entrée en cliquant sur le bouton rouge « Supprimer » (**X**) icône.
7. Dans le Gammes de ports dans le champ, saisissez un seul port ou une plage de ports, puis cliquez sur le signe vert plus (**+**) icône.
8. Cliquez **Enregistrer**.

Les enregistrements de flux qui répondent à vos critères sont désormais automatiquement envoyés vers l'espace de stockage des enregistrements que vous avez configuré. Attendez quelques minutes que les enregistrements soient collectés.

9. Dans le système ExtraHop, cliquez sur **Disques** dans le menu supérieur, puis cliquez sur **Afficher les enregistrements** pour lancer une requête.

   Si vous ne voyez aucun enregistrement, patientez quelques minutes et réessayez. Si aucun enregistrement n' apparaît après cinq minutes, vérifiez votre configuration ou contactez Assistance ExtraHop.

Collectez des records L7 à l'aide d'un déclencheur

Les protocoles L7 peuvent être validés (collectés et stockés) sous forme d'enregistrement via une fonction de déclencheur globale. Les enregistrements L7 incluent les messages, les transactions et les sessions envoyés via les protocoles L7 courants tels que DNS, HTTP et TLS.

Dans les étapes suivantes, vous allez apprendre à collecter des enregistrements pour tout équipement qui envoie ou reçoit une Réponse HTTP.

En savoir plus sur Enregistrements ExtraHop.

Tout d'abord, nous allons écrire un déclencheur pour collecter des informations à partir du type d'enregistrement HTTP intégré avec la méthode commitRecord (), qui est disponible sur tous classes de protocoles. La syntaxe de base du déclencheur est `<protocol>.commitRecord()`. Ensuite, nous attribuerons le déclencheur à un serveur Web. Enfin, nous vérifierons que les enregistrements sont envoyés à l'espace de stockage des enregistrements.

Avant de commencer

- Vous devez disposer d'un espace de stockage des enregistrements configuré, tel qu'un espace de stockage des enregistrements ExtraHop, Splunk, ou Google BigQuery
- Ces instructions supposent une certaine familiarité avec Déclencheurs ExtraHop, qui nécessitent de l'expérience avec JavaScript. Alternativement, vous pouvez configurer la collection d'enregistrements L7 via le système ExtraHop.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système, puis cliquez sur **éléments déclencheurs**.
3. Cliquez **Créez**.
4. Dans le Créer un déclencheur volet, complétez vos informations, comme dans l'exemple suivant :
   - **Nom:** `Réponses HTTP`
   - **Descriptif:** `Ce déclencheur collecte les réponses HTTP.`
5. Cochez la case à côté de **activer le journal de débogage**.
6. Dans la liste déroulante Événements, sélectionnez **HTTP_RESPONSE**.
7. Dans le **Devoirs** zone de texte, recherchez un serveur Web actif pour lequel vous souhaitez collecter des enregistrements et sélectionnez le serveur.
8. Dans le volet droit, saisissez l'exemple de code suivant :

```
HTTP.commitRecord();
debug ("committing HTTP responses");
```

   Ce code génère des enregistrements pour le type d'enregistrement HTTP lorsque `HTTP_RESPONSE` l'événement se produit et correspond au format d'enregistrement intégré pour HTTP.
9. Cliquez **Enregistrer**.

Prochaines étapes

Attendez quelques minutes que les enregistrements soient collectés, puis vérifiez que vos enregistrements sont collectés à l'étape suivante en cliquant sur **Disques** dans le menu supérieur, puis cliquez sur **Afficher les enregistrements** pour lancer une requête.

Si aucun enregistrement HTTP ne s'affiche au bout de 5 minutes, cliquez sur **Journal de débogage** onglet en bas de la page dans l'éditeur de déclencheurs pour voir s' il existe des erreurs que vous pouvez résoudre. Si le déclencheur est en cours d'exécution, le message « validation des réponses HTTP » s'affiche. Si aucun enregistrement n'apparaît après l'exécution du déclencheur, contactez Assistance ExtraHop.

Collectez des enregistrements personnalisés

Vous pouvez personnaliser le type de détails d'enregistrement que vous générez et stockez dans un espace de stockage des enregistrements en écrivant un déclencheur. Nous vous recommandons également de créer un format dac.enregistrement pour contrôler la façon dont les enregistrements s'affichent dans le système ExtraHop.

Avant de commencer

- Ces instructions supposent une certaine familiarité avec ExtraHop DÉCLENCHEURS.
- Si vous êtes connecté à un espace de stockage des enregistrements Google BigQuery, le nombre de champs d'enregistrements personnalisés est limité à 300.

Dans l'exemple suivant, vous allez apprendre à stocker uniquement les enregistrements pour les transactions HTTP qui génèrent un code dstate 404. Tout d'abord, nous allons écrire un déclencheur pour collecter des informations à partir du type d'enregistrement HTTP intégré. Ensuite, nous assignerons le déclencheur à un serveur Web. Enfin, nous allons créer un format d'enregistrement pour afficher les champs d' enregistrement sélectionnés dans la vue tabulaire pour les résultats de nos requêtes d'enregistrement.

Écrire et attribuer un déclencheur

Notez que le déclencheur doit être créé sur chaque sonde auprès duquel vous souhaitez collecter ces types d'enregistrements. Vous pouvez créer le déclencheur sur un console pour collecter vos enregistrements personnalisés auprès de tous les connectés capteurs.

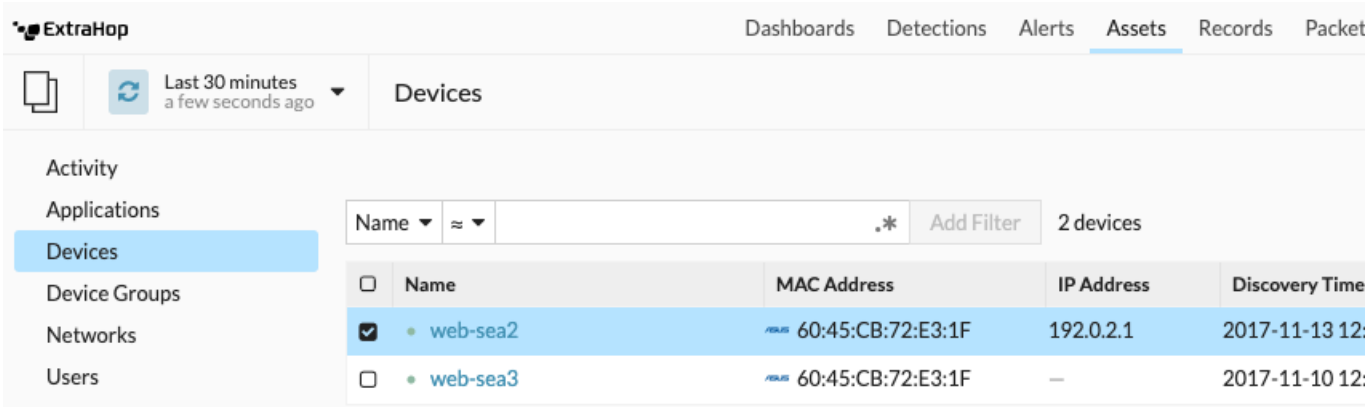
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système, puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Créez**.
4. Dans le Créer un déclencheur volet, complétez vos informations, comme dans l'exemple suivant :
   - **Nom:** `Erreurs HTTP 404`
   - **Descriptif:** `Suivez les erreurs 404 sur le serveur Web principal.`
   - **Activer le journal de débogage:** Cochez la case pour activer le débogage.
   - **Évènements:** `HTTP_RESPONSE`
5. Cliquez sur le **Rédacteur** onglet pour écrire les spécifications du déclencheur.

   La figure suivante montre un exemple de configuration qui collecte des enregistrements uniquement lorsqu'un code ddiligétat 404 est détecté. Nous avons également défini un nom (`web404`) pour ces types d'enregistrements afin de les identifier dans une requête d'enregistrement et d'ajouter des informations d'identification pour le débogage.

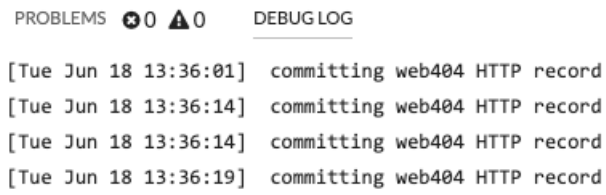
```
1  if (HTTP.statusCode === 404) {
2      commitRecord("web404", HTTP.record);
3      debug("committing web404 HTTP record");
4  }
```

Dans les étapes suivantes, attribuez le déclencheur à un équipement ou à un groupe d'équipements pour lequel vous souhaitez surveiller les codes d'état 404.

6. Cliquez **Actifs** depuis le menu supérieur.
7. Cliquez **Appareils** puis cliquez sur **Appareils actifs** graphique.
8. Cochez la case correspondant à un équipement dans la liste. Pour notre exemple, nous allons sélectionner un serveur Web appelé `web2-sea`.
9. Cliquez sur l'icône Attribuer des déclencheurs, sélectionnez le déclencheur que vous avez créé lors des étapes précédentes, puis cliquez sur **Assigner des déclencheurs**. Dans la figure suivante, nous avons sélectionné notre serveur Web, `web2-sea`.



Après avoir assigné le déclencheur, revenez au **Paramètres système > Déclencheur** page et sélectionnez le déclencheur que vous avez créé. Tout d'abord, assurez-vous que votre équipement est actif. Cliquez ensuite sur le **Journal de débogage** onglet pour voir si le déclencheur est en train de valider vos enregistrements. Dans l'exemple suivant, nous avons visité intentionnellement des pages Web non disponibles pour générer des erreurs 404.



Créez un format d'enregistrement personnalisé pour afficher les résultats de votre enregistrement dans un tableau

Les formats d'enregistrement sont la méthode recommandée pour afficher vos enregistrements avec uniquement les champs que vous souhaitez voir. Sans format d'enregistrement personnalisé, les champs de votre enregistrement personnalisé n'apparaîtront dans aucune liste sélectionnable, telle que la liste Grouper par.

Le moyen le plus rapide de créer un format d'enregistrement personnalisé consiste à copier-coller le schéma lors de la lecture à partir d'un format d'enregistrement intégré dans un nouveau format d'enregistrement. Si vous avez plusieurs capteurs, vous devez créer le format d'enregistrement personnalisé sur chaque appliance sur laquelle les résultats des enregistrements sont visualisés. Vous pouvez créer le format d'enregistrement sur une console pour formater un enregistrement personnalisé sur tous les capteurs connectés.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Formats d'enregistrement**.

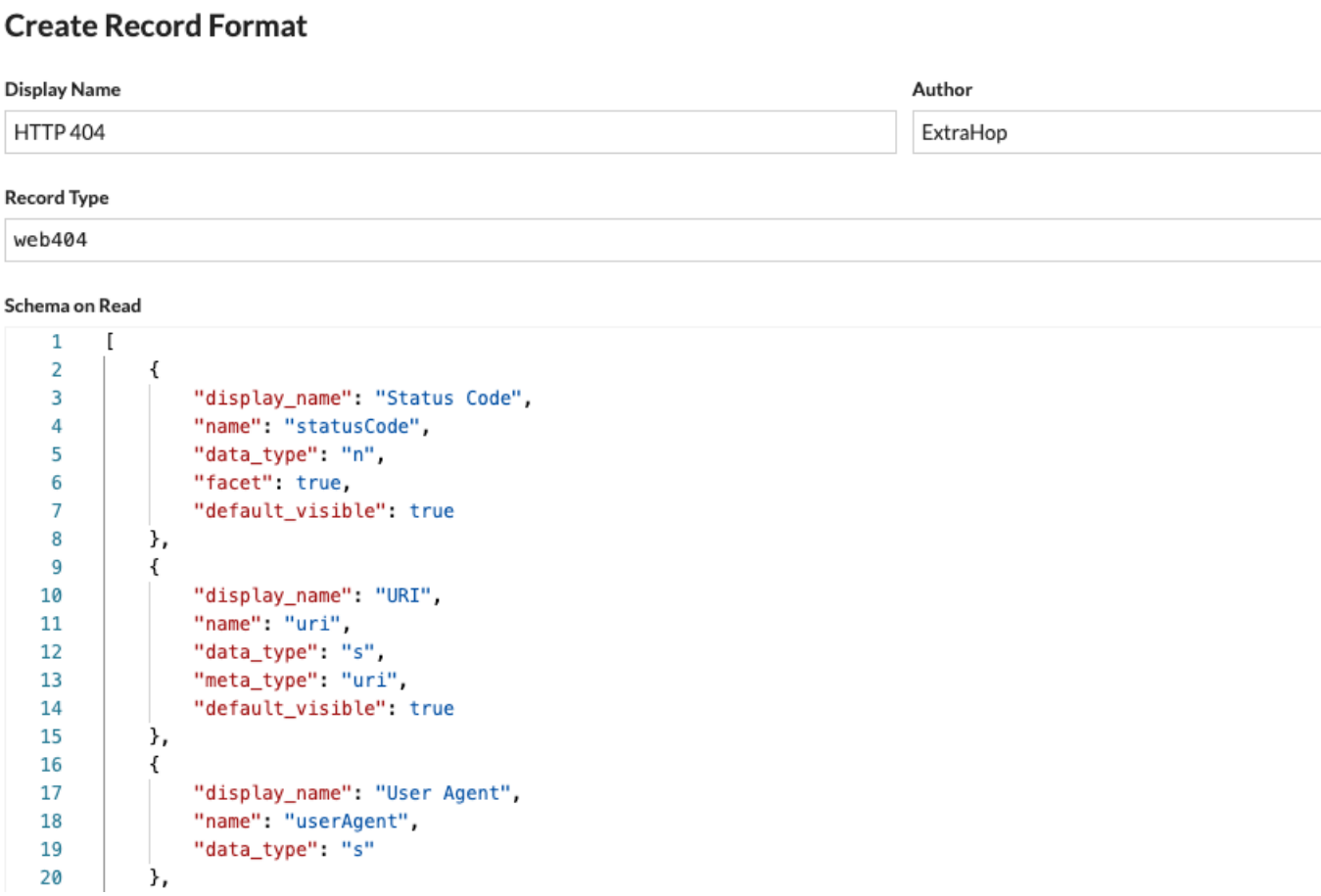
3. Cliquez sur le type d'enregistrement que vous souhaitez copier. Pour notre exemple, nous allons copier le format d'enregistrement HTTP.
4. Copiez le contenu dans la zone de texte ci-dessous Schéma en cours de lecture.
5. Cliquez **Nouveau format d'enregistrement**.
6. Renseignez les champs suivants :

   • **Nom d'affichage:** Entrez un nom unique pour votre format dac.enregistrement.

   • **Auteur:** Identifiez l'auteur du format dac.enregistrement.

   • **Type d'enregistrement:** Entrez le même identifiant de type d'enregistrement que celui que vous avez créé dans le déclencheur. Dans notre exemple, cette valeur est `web404`.

   • **Schéma en cours de lecture:** Collez le contenu copié de l'étape 4 dans la zone de texte. Modifiez la case pour supprimer tous les champs indésirables. Dans l'exemple de la figure ci-dessous, nous n'avons conservé que les champs suivants : client, serveur, méthode, code d' état, URI et temps de traitement.



Recherchez votre type d'enregistrement personnalisé

1. Cliquez **Enregistrements** depuis le menu supérieur.
2. Cliquez sur **N'importe quel type d'enregistrement** dans une liste déroulante, sélectionnez le format d'enregistrement que vous venez de créer.
3. Cliquez **Afficher les enregistrements**.
4. Cliquez sur **Vue verbeuse** icône.
5. Cliquez **Champs** puis cliquez sur **Tout sélectionner**.
   Toutes les informations collectées par le déclencheur concernant ces enregistrements sont affichées dans les résultats de la requête.

Paramètres du format d'enregistrement

Le Paramètres du format d'enregistrement La page affiche une liste de tous les formats d'enregistrement intégrés et personnalisés disponibles sur vos capteurs ou votre console ExtraHop. Si vous devez créer un format d'enregistrement personnalisé, nous vous recommandons de copier-coller le schéma des informations lues à partir d'un format d'enregistrement intégré. Les utilisateurs avancés souhaiteront peut-être créer un format d'enregistrement personnalisé avec leurs propres paires champ-valeur et devraient appliquer le matériel de référence fourni dans cette section.

Les formats d'enregistrement comprennent les paramètres suivants :

Nom d'affichage

Nom affiché pour le format d'enregistrement dans le système ExtraHop. S'il n'existe aucun format d'enregistrement pour l'enregistrement, le type d'enregistrement est affiché.

Auteur

(Facultatif) L'auteur du format d'enregistrement. Affichage de tous les formats d'enregistrement intégrés `ExtraHop` en tant qu'auteur.

Type d'enregistrement

Un nom alphanumérique unique qui identifie le type d'informations contenues dans le format d'enregistrement associé. Le type d'enregistrement lie le format d'enregistrement aux enregistrements envoyés à l'espace de stockage des enregistrements. Les formats d'enregistrement intégrés ont un type d'enregistrement qui commence par un tilde (~). Les formats d'enregistrement personnalisés ne peuvent pas comporter de type d'enregistrement commençant par un tilde (~) ou un symbole arobase (@).

Schéma en lecture

Tableau au format JSON contenant au moins un objet, composé d'un nom de champ et d'une paire de valeurs. Chaque objet décrit un champ de l'enregistrement et chaque objet doit avoir une combinaison unique de nom et de type de données pour ce format d'enregistrement. Vous pouvez créer les objets suivants pour un format d'enregistrement personnalisé :

nom

Le nom du champ.

nom_affichage

Le nom d'affichage du champ. Si le `display_name` le champ est vide, `name` le champ s'affiche.

description

(Facultatif) Informations descriptives sur le format d'enregistrement. Ce champ est limité à la page Paramètres du format d'enregistrement et n'est affiché dans aucune requête d'enregistrement.

visible par défaut

(Facultatif) Si réglé sur `true`, ce champ s'affiche dans le système ExtraHop sous forme d'en-tête de colonne par défaut dans la vue tabulaire.

facette

(Facultatif) Si réglé sur `true`, les facettes de ce champ s'affichent dans le système ExtraHop. Les facettes sont une courte liste des valeurs les plus courantes du champ sur lesquelles il est possible de cliquer pour ajouter un filtre.

type_de données

Abréviation qui identifie le type de données stockées dans ce champ. Les types de données suivants sont pris en charge :

Type de données	Abréviation	Descriptif
application	`app`	ID de l'application ExtraHop (chaîne)

Type de données	Abréviation	Descriptif
booléen	`b`	Valeur booléenne
équipement	`dev`	ID d'équipement ExtraHop (chaîne)
interface de flux	`fint`	ID de l'interface de flux
réseau de flux	`fnet`	Identifiant du réseau Flow
IPv4	`addr4`	Adresse IPv4 au format quadrilatère à points. Plus ou moins de filtres sont pris en charge.
IPv6	`addr6`	Une adresse IPv6. Seuls les filtres orientés chaînes sont pris en charge.
nombre	`n`	Nombre (entier ou virgule flottante)
chaîne	`s`	Chaîne générique

méta_type

La sous-classification du type de données qui détermine en outre la manière dont les informations sont affichées dans le système ExtraHop. Les méta-types suivants sont pris en charge pour chacun des types de données associés :

Type de données	Type de méta
Corde	• `domain` • `uri` • `user`
Numéro	• `bytes` • `count` • `expiration` • `milliseconds` • `packets` • `timestamp`

Activer les requêtes d'enregistrement pour les métriques personnalisées

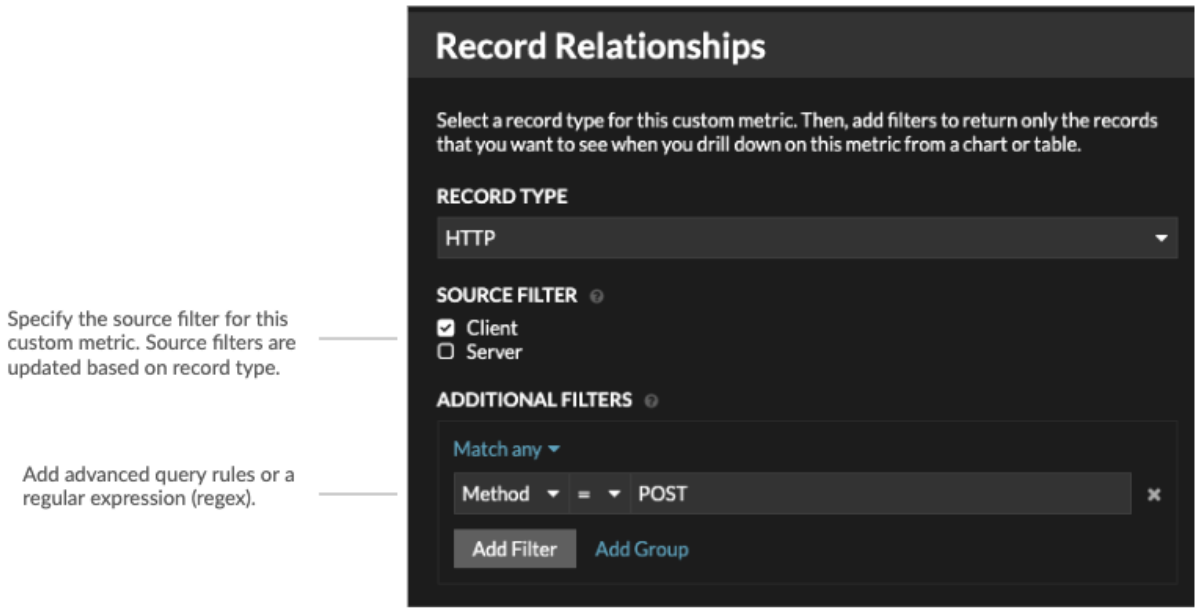
Les métriques personnalisées sont généralement créées pour collecter des informations spécifiques sur votre environnement. Vous pouvez configurer des paramètres qui vous permettent d'interroger et de récupérer des enregistrements au niveau des transactions associés à une métrique personnalisée. Dans le catalogue de mesures, la section Relations d'enregistrement vous permet d'associer une métrique personnalisée à un type d'enregistrement. Si vous demandiez des enregistrements à partir de cette métrique personnalisée, vous renverriez des résultats pour tous les enregistrements de ce type d'enregistrement, quels que soient les autres attributs configurés pour votre métrique personnalisée. Nous vous recommandons d'ajouter des filtres afin de renvoyer des résultats significatifs pour vos requêtes d'enregistrement.

En définissant un filtre de source dans le catalogue de mesures, vous filtrez automatiquement les enregistrements en fonction de la source à partir de laquelle vous avez effectué l'exploration. Par exemple, si vous cochez une case à côté de Serveur, lorsque vous recherchez des enregistrements pour cette métrique personnalisée à partir d'un serveur Web nommé `example-web-sea`, un filtre est automatiquement ajouté à votre requête qui ne renvoie des résultats que pour les transactions où `example-web-sea` agit en tant que serveur.

En définissant des filtres avancés, vous filtrez automatiquement les enregistrements selon les critères spécifiés. Les filtres avancés sont complexes et peuvent être imbriqués sur quatre niveaux.

Avant de commencer
Création d'une métrique personnalisée

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Catalogue métrique**.
3. Dans le coin supérieur gauche, tapez le nom de la métrique personnalisée, puis cliquez sur le nom de la métrique personnalisée dans les résultats.
   Les paramètres de la métrique personnalisée apparaissent dans le volet droit.
4. Dans le volet droit, faites défiler la page jusqu'à la section Record Relationships et cliquez sur la liste déroulante RECORD TYPE.
5. Cliquez sur un ou plusieurs types d'enregistrement dans la liste, puis cliquez en dehors de la liste pour appliquer vos sélections. Des options supplémentaires permettant de filtrer les champs d'enregistrement apparaissent sous les types d'enregistrement sélectionnés.



6. Optionnel : Dans la section FILTRE SOURCE, cochez la case à côté du type de source, tel que Client ou Application. Ces sources sont mises à jour de manière dynamique en fonction des types d'enregistrement sélectionnés.
7. Optionnel : Dans le champ FILTRES SUPPLÉMENTAIRES, spécifiez plusieurs critères avec les opérateurs OR (Match Any), AND (Match All) et NONE pour créer un filtre de requête avancé ou entrez un expression régulière (regex) pour filtrer les enregistrements afin d'obtenir des mesures détaillées personnalisées.
8. Cliquez **Mettre à jour**.

Vous pouvez désormais rechercher des enregistrements à partir de n'importe quel graphique ou page de détail à l'aide de la métrique personnalisée.

Prochaines étapes

- Créez une requête d'enregistrement pour votre métrique personnalisée en cliquant sur la métrique dans un graphique, puis en cliquant sur **Enregistrements**.

Paquets

Un paquet réseau est une petite quantité de données envoyée sur les réseaux TCP/IP (Transmission Control Protocol/Internet Protocol). Le système ExtraHop vous permet de collecter, rechercher et télécharger en permanence ces paquets à l'aide d'une appliance Trace, ce qui peut être utile pour détecter les intrusions sur le réseau et autres activités suspectes.

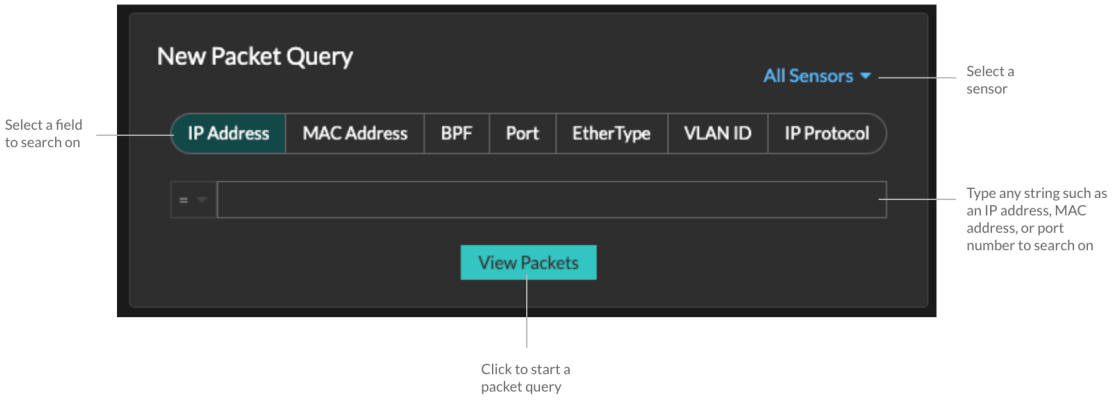
Vous pouvez rechercher et télécharger des paquets depuis la page Paquets du système ExtraHop et via Recherche par paquets ressource dans l' API REST ExtraHop. Les paquets téléchargés peuvent ensuite être analysés via un outil tiers, tel que Wireshark.

Note: Si vous ne possédez pas d'appliance Trace, vous pouvez toujours collecter des paquets via déclencheurs. Voir Initiez des captures de paquets de précision pour analyser les conditions de fenêtre zéro pour un exemple.

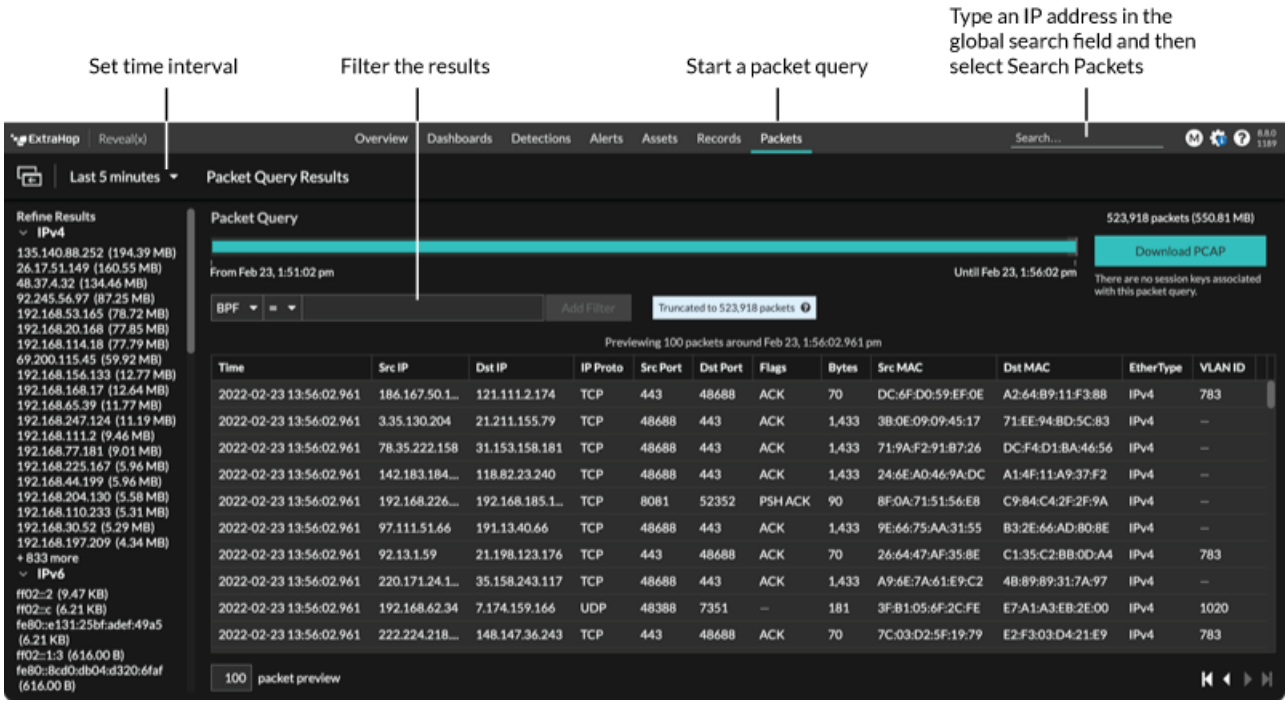
Vidéos: Consultez la formation associée : Paquets

Navigation dans les paquets

Cliquez **Paquets** depuis le menu supérieur pour créer une nouvelle requête de paquet. Sur la page Nouvelle requête de paquet, vous pouvez spécifier un filtre.



Les résultats apparaissent sur la page principale Paquets page. Lancez une autre requête de paquet en cliquant sur **Paquets** à nouveau depuis le menu supérieur.



Si vous modifiez l'intervalle de temps, la requête recommence. Chaque extrémité de la barre grise affiche un horodateur, qui est déterminé par l'intervalle de temps actuel. L'heure de droite indique le point de départ de la requête et l'heure de gauche indique le point de terminaison de la requête. La barre bleue indique l'intervalle de temps pendant lequel le système a détecté des paquets. Vous pouvez faire glisser le pointeur pour zoomer sur la barre bleue afin d'exécuter à nouveau une requête pour l'intervalle de temps sélectionné.

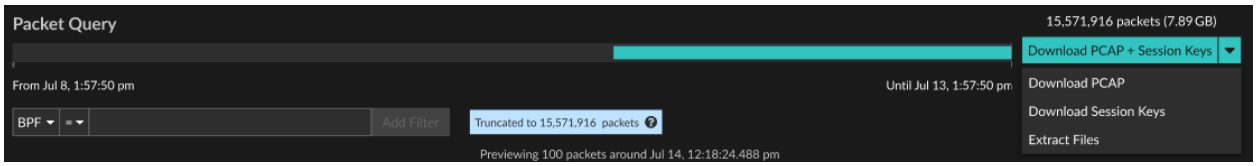
Conseil: Filtrer les paquets avec la syntaxe du filtre de paquets Berkeley.

Note: Vous ne pouvez afficher que les paquets correspondant aux privilèges accordés par votre administrateur ExtraHop. Si les résultats de votre requête ne s'affichent pas, contactez votre administrateur ExtraHop.

Téléchargement de paquets

Vous pouvez télécharger les résultats des requêtes dans un fichier de capture de paquets (PCAP) à des fins d'analyse, ainsi que les clés de session TLS et les fichiers associés aux paquets.

Les options de téléchargement sont disponibles dans le menu déroulant en haut à droite. Cliquez sur une option pour permettre à votre navigateur de télécharger le fichier sur votre ordinateur local.



Voici quelques considérations concernant le téléchargement de paquets et l'extraction de fichiers :

- Les options de téléchargement affichées dans le menu déroulant dépendent des résultats de votre requête. Par exemple, si aucune clé de session n'est associée aux paquets, il se peut que seules les options de téléchargement du PCAP et d'extraction de fichiers s'affichent.
- Les téléchargements contiennent uniquement des paquets correspondant aux privilèges accordés par votre administrateur ExtraHop . Par exemple, si vous interrogez deux capteurs mais que votre

administrateur vous a attribué un accès limité à l'un des capteurs, votre téléchargement ne contiendra que les en-têtes de paquets provenant du capteur à accès limité.

- Si vous télécharger les clés de session, vous pouvez ouvrir le fichier de capture de paquets dans un outil tel que Wireshark, qui peut appliquer les clés de session et afficher les paquets déchiffrés.
- L'extraction de fichiers (également appelée découpage de fichiers) est disponible si des fichiers sont observés sur des paquets contenant des enregistrements HTTP ou SMB.

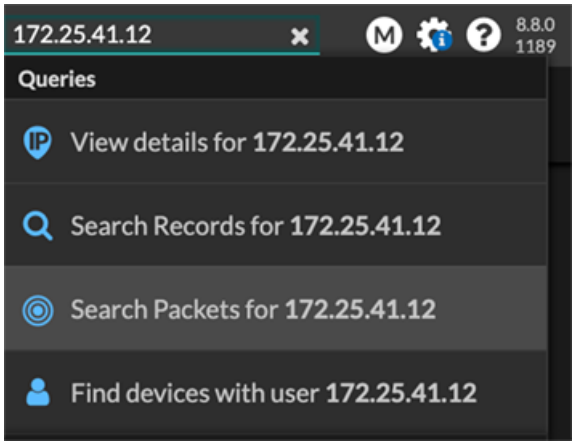
  Conseil: Sur la page Enregistrements, vous pouvez rechercher des types d'enregistrements HTTP ou SMB et filtrer par fichier observé. Cliquez sur l'icône des paquets à côté de l'enregistrement qui contient les fichiers que vous souhaitez extraire.
- Les fichiers extraits sont téléchargés dans un fichier .zip et contiennent un contenu original non chiffré susceptible d'inclure des données malveillantes. Un mot de passe est nécessaire pour ouvrir les fichiers .zip extraits. Le mot de passe est spécifié dans RevealX Enterprise ou RevealX 360 Les paramètres d'administration peuvent être obtenus auprès de votre administrateur ExtraHop.
- Si les options de téléchargement attendues ne s'affichent pas, contactez votre administrateur ExtraHop . Vous n'aurez aucun accès ou un accès limité aux capteurs qui ne vous sont pas attribués par le biais du contrôle d'accès aux capteurs. De plus, vos options de téléchargement peuvent être limitées par l'accès au module et les privilèges utilisateur. L'accès au module et les privilèges requis pour chaque option de téléchargement sont décrits dans le tableau suivant :

Option de téléchargement	Module requis	Privilèges Packet Forensics requis
Télécharger PCAP + Session Keys	NDR ou NPM	Paquets et clés de session
Télécharger PCAP	NDR ou NPM	Paquets uniquement
Télécharger PCAP Headers	NDR ou NPM	En-têtes de paquets uniquement
Télécharger PCAP Slices	NDR ou NPM	Tranches en sachets uniquement
Télécharger les clés de session	NDR ou NPM	Paquets et clés de session
Extraire des fichiers	NDR	Paquets uniquement ou Paquets et clés de session

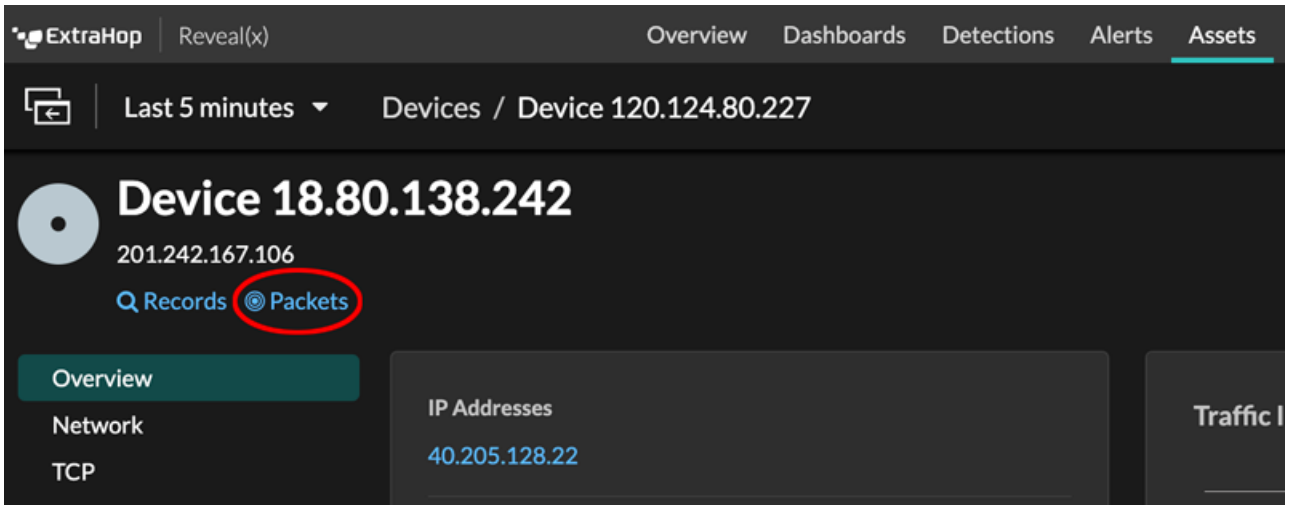
Paquets de requêtes dans le système ExtraHop

Bien que la page Paquets fournisse un accès rapide pour interroger tous les paquets, il existe des indicateurs et des liens à partir desquels vous pouvez lancer une requête de paquets dans le système ExtraHop.

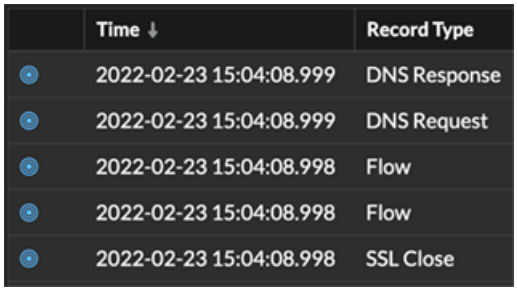
- Tapez une adresse IP dans le champ de recherche global, puis sélectionnez l' icône Rechercher des paquets .



- Cliquez **Paquets** sur la page d'un équipement.

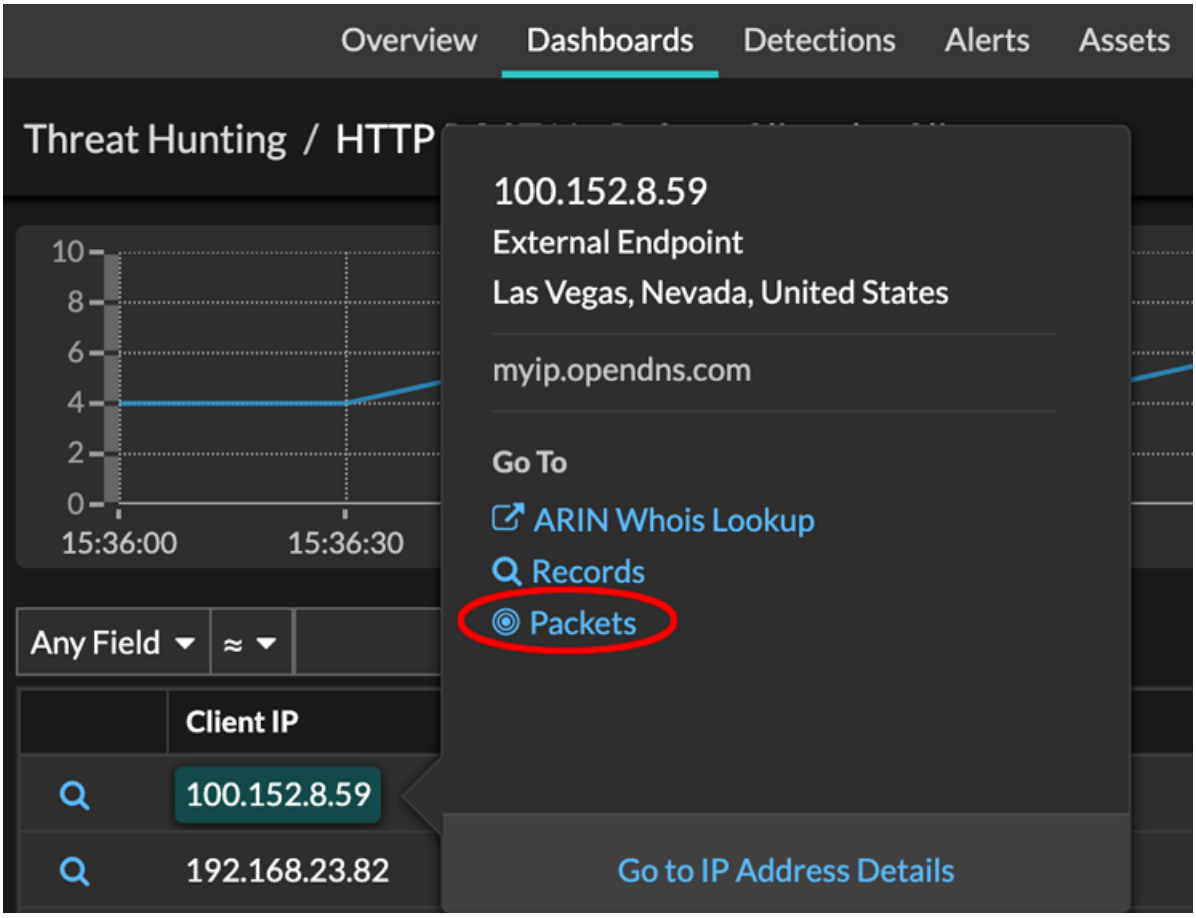


- Cliquez sur l'icône Paquets à côté de n'importe quel enregistrement sur la page de résultats d'une requête d'enregistrement.



	Time ↓	Record Type
	2022-02-23 15:04:08.999	DNS Response
	2022-02-23 15:04:08.999	DNS Request
	2022-02-23 15:04:08.998	Flow
	2022-02-23 15:04:08.998	Flow
	2022-02-23 15:04:08.998	SSL Close

- Cliquez sur une adresse IP ou un nom d'hôte dans n'importe quel graphique contenant des mesures pour les octets du réseau ou les paquets par adresse IP pour afficher un menu contextuel. Cliquez ensuite sur l'icône Paquets pour rechercher l'équipement et l'intervalle de temps.



Configuration d'une PCAP globale

Une PCAP globale collecte chaque paquet envoyé au système ExtraHop pendant la durée correspondant aux critères.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Captures de paquets section, cliquez sur **Capture globale de paquets**.

   Lors de la configuration des captures de paquets, il vous suffit de spécifier les critères que vous souhaitez pour la capture de paquets.
3. Dans le Nom dans le champ, saisissez un nom pour identifier la capture de paquets.
4. Dans le Nombre maximum de paquets dans le champ, saisissez le nombre maximum de paquets à capturer.
5. Dans le Nombre maximum d'octets dans ce champ, saisissez le nombre maximum d'octets à capturer.
6. Dans le Durée maximale (millisecondes) champ, saisissez la durée maximale de la PCAP en millisecondes.

   ExtraHop recommande la valeur par défaut de 1000 (1 seconde). La valeur maximale est de 60 000 millisecondes (1 minute).
7. Dans le Snäplen champ, saisissez le nombre maximum d'octets copiés par image.

   La valeur par défaut est de 96 octets, mais vous pouvez définir cette valeur sur un nombre compris entre 1 et 65535.
8. Cliquez **Démarrer**.

Conseil Notez l'heure à laquelle vous commencez la capture pour faciliter la localisation des paquets.

9. Cliquez **Arrête** pour arrêter la capture de paquets avant que l'une des limites maximales ne soit atteinte.

Téléchargez votre capture de paquets.

- Sur les systèmes RevealX Enterprise, cliquez sur **Paquets** dans le menu supérieur, puis cliquez sur **Télécharger PCAP**.

  Pour vous aider à localiser votre capture de paquets, cliquez et faites glisser le pointeur sur la chronologie de la requête par paquets pour sélectionner la plage de temps au cours de laquelle vous avez commencé la capture de paquets.
- Sur les systèmes ExtraHop Performance, cliquez sur l'icône Paramètres du système, cliquez **Toute l'administration**, puis cliquez sur **Afficher et télécharger les captures de paquets** dans la section Capture de paquets.

Analyser un fichier de capture de paquets

Le mode de capture hors ligne permet aux administrateurs de télécharger et d'analyser un fichier de capture enregistré par un logiciel d'analyse de paquets, tel que Wireshark ou tcpdump, dans le système ExtraHop.

Voici quelques points importants à prendre en compte avant d'activer le mode de capture hors ligne :

- Lorsque la capture est définie en mode hors ligne, la banque de données système est réinitialisée. Toutes les mesures enregistrées précédemment sont supprimées de la banque de données. Lorsque le système est configuré en mode en ligne, la banque de données est à nouveau réinitialisée.
- En mode hors ligne, aucune métrique n'est collectée depuis l'interface de capture tant que le système n'est pas reconfiguré en mode en ligne.
- Seuls les fichiers de capture au format pcap sont pris en charge. Les autres formats tels que pcapng ne sont pas pris en charge.

Définissez le mode de capture hors ligne

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez **Capturez**.
3. Cliquez **Fichier de capture hors ligne**.
4. Sélectionnez **Uploader** puis cliquez sur **Enregistrer**.
5. Cliquez **OK.** pour confirmer la réinitialisation de la banque de données.
   Le processus de capture est arrêté, l'état de capture est défini sur Hors ligne et toutes les données de la banque de données sont supprimées. Lorsque le système a mis la capture en mode hors ligne, le Fichier de capture hors ligne la page apparaît.
6. Cliquez **Choisissez un fichier**, naviguez jusqu'au fichier de capture que vous souhaitez télécharger, sélectionnez-le, puis cliquez sur **Ouvert**.
7. Cliquez **Uploader**.
   Le système ExtraHop affiche la page des résultats de capture hors ligne lorsque le fichier de capture est téléchargé avec succès.
8. Cliquez **Afficher les résultats** pour analyser le fichier de capture de paquets comme vous le feriez lorsque le système est en mode capture en direct.

Remettre le système en mode Live Capture

1. Dans le Configuration du système section, cliquez **Capture (hors ligne)**.
2. Cliquez **Redémarrer la capture**.

3. Sélectionnez **En direct**, puis cliquez sur **Enregistrer**.

Le système supprime les mesures de performance collectées dans le fichier de capture précédent et prépare la banque de données pour une analyse en temps réel à partir de l'interface de capture.

Filtrer les paquets avec la syntaxe du filtre de paquets Berkeley

Recherchez des paquets à l'aide de la syntaxe du filtre de paquets de Berkeley (BPF) uniquement ou en combinaison avec les filtres intégrés.

Les filtres de paquets Berkeley constituent une interface brute pour les couches de liaison de données et constituent un outil puissant pour l'analyse de détection des intrusions. La syntaxe BPF permet aux utilisateurs d'écrire des filtres qui explorent rapidement des paquets spécifiques pour afficher les informations essentielles.

Le système ExtraHop construit un en-tête de paquet synthétique à partir des données d'index des paquets, puis exécute les requêtes de syntaxe BPF par rapport à l'en-tête du paquet pour garantir que les requêtes sont beaucoup plus rapides que le scan de la charge utile complète du paquet. Notez qu'ExtraHop ne prend en charge qu'un sous-ensemble de la syntaxe BPF. Voir Syntaxe BPF prise en charge.

La syntaxe BPF consiste en une ou plusieurs primitives précédées d'un ou de plusieurs qualificatifs. Les primitives se composent généralement d'un identifiant (nom ou numéro) précédé d'un ou de plusieurs qualificatifs. Il existe trois types de qualifications différents :

type

Des qualificatifs qui indiquent le type auquel le nom ou le numéro d'identification fait référence. Par exemple, `host`, `net`, `port`, et `portrange`. S'il n'y a pas de qualificatif, `host` est supposé.

dir

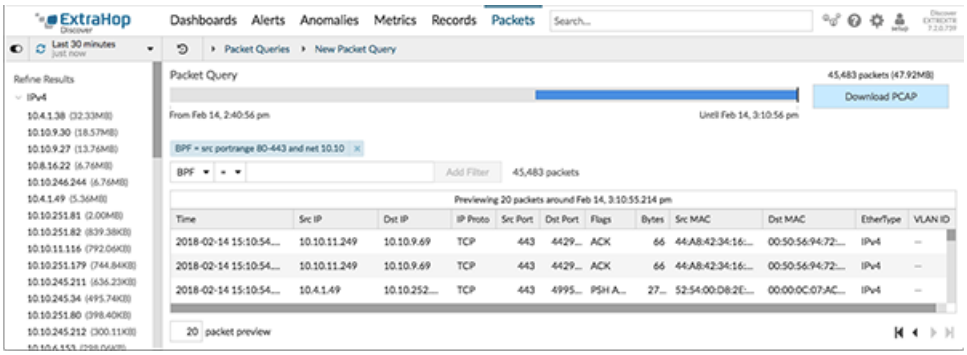
Qualificatifs qui spécifient une direction de transfert particulière vers ou depuis un identifiant. Les directions possibles sont `src`, `dst`, `src and dst`, et `src or dst`. Par exemple, `dst net 128.3`.

proto

Qualificatifs qui limitent la correspondance au protocole en question. Les protocoles possibles sont `ether`, `ip`, `ip6`, `tcp`, et `udp`.

Ajouter un filtre avec la syntaxe BPF

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le menu supérieur, cliquez sur **Paquets**.
3. Dans la section du filtre à trois champs, sélectionnez **BPF**, puis tapez la syntaxe de votre filtre. Par exemple, tapez `src portrange 80-443 and net 10.10`.
4. Cliquez **Télécharger PCAP** pour enregistrer la capture du paquet avec vos résultats filtrés.



Syntaxe BPF prise en charge

Le système ExtraHop prend en charge le sous-ensemble suivant de la syntaxe BPF pour le filtrage des paquets.

Note:
- ExtraHop ne prend en charge que les recherches d'adresses IP numériques. Les noms d'hôtes ne sont pas autorisés.
- Indexation dans les en-têtes, `[...]`, n'est pris en charge que pour `tcpflags` et `ip_offset`. Par exemple, `tcp[tcpflags] & (tcp-syn|tcp-fin) != 0`
- ExtraHop prend en charge les valeurs numériques et hexadécimales pour les champs VLAN ID, EtherType et IP Protocol. Préfixez les valeurs hexadécimales par 0x, par exemple 0x11.

Primitif	Exemples	Descriptif
`[src|dst] host <host ip>`	`host 203.0.113.50` `dst host 198.51.100.200`	Correspond à un hôte en tant que source IP, destination, ou l'une ou l'autre des deux. Ces expressions d'hôte peuvent être spécifiées conjointement avec d'autres protocoles tels que ip, arp, rarp ou ip6.
`ether [src|dst] host <MAC>`	`ether host 00:00:5E:00:53:00` `ether dst host 00:00:5E:00:53:00`	Fait correspondre un hôte en tant que source Ethernet, destination ou l'une des deux.
`vlan <ID>`	`vlan 100`	Correspond à un VLAN. Les numéros d'identification valides sont `0-4095`. Les bits de priorité du VLAN sont nuls. Si le paquet d'origine comportait plusieurs balises VLAN, le paquet synthétique auquel le BPF correspond n'aura que la balise VLAN la plus interne.

`[src|dst] portrange <p1>-<p2>`
ou
`[tcp|udp] [src|dst] portrange <p1>-<p2>`
	`src portrange 80-88`
	`tcp dst portrange 1501-1549`
		Fait correspondre les paquets à destination ou en provenance d'un port dans la plage donnée. Des protocoles peuvent être appliqués à une plage de ports pour filtrer des paquets spécifiques dans cette plage.

`[ip|ip6][src|dst] proto <protocol>`	`proto 1`
	`src 10.4.9.40 and proto ICMP`
	`ip6 and src fe80::aebc:32ff:fe84:70b7 and proto 47`
	`ip and src 10.4.9.40 and proto 0x0006`
		Correspond aux protocoles IPv4 ou IPv6 autres que TCP et UDP. Le protocole peut être un numéro ou un nom.

Primitif	Exemples	Descriptif
`[ip|ip6][tcp|udp] [src|dst] port <port>`	`udp and src port 2005` `ip6 and tcp and src port 80`	Correspond aux paquets IPv4 ou IPv6 sur un port spécifique.

`[src|dst] net <network>`	`dst net 192.168.1.0`
	`src net 10`
	`net 192.168.1.0/24`
		Fait correspondre les paquets à destination ou en provenance d'une source ou d'une destination ou de l'une ou l'autre, qui résident sur un réseau. Un numéro de réseau IPv4 peut être spécifié sous la forme de l'une des valeurs suivantes :
		• Quad pointillé (x.x.x.x)
		• Triple en pointillés (x.x.x)
		• Paire pointillée (x.x)
		• Numéro unique (x)

`[ip|ip6] tcp tcpflags & (tcp-[ack|fin|syn|rst|push|urg|)`	`tcp[tcpflags] & (tcp-ack) !=0`
	`tcp[13] & 16 !=0`
	`ip6 and (ip6[40+13] & (tcp-syn) != 0)`
		Correspond à tous les paquets avec l'indicateur TCP spécifié

Paquets IPv4 fragmentés (ip_offset ! = 0)	`ip[6:2] & 0x3fff != 0x0000`	Correspond à tous les paquets contenant des fragments.

Stockez les clés de session TLS dans les magasins de paquets connectés

Lorsque le transfert de clé de session est configuré sur un système ExtraHop connecté à un magasin de paquets, le système ExtraHop peut stocker des clés de session cryptées avec les paquets collectés.

Avant de commencer
En savoir plus sur déchiffrer des paquets avec des clés stockées.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Stockage des clés de session SSL**.
4. Sélectionnez **Activer le stockage des clés de session SSL**.
5. Cliquez **Enregistrer**.

Prochaines étapes

Pour plus d'informations sur le téléchargement des clés de session, voir Télécharger les clés de session avec captures de paquets.

Télécharger les clés de session avec captures de paquets

Vous pouvez télécharger le fichier PCAP Next Generation (pcapng) qui inclut toutes les clés de session TLS capturées et les paquets chiffrés. Vous pouvez ensuite ouvrir le fichier de capture de paquets dans un outil tel que Wireshark, qui peut appliquer les clés de session et afficher les paquets déchiffrés.

Avant de commencer

- Vous devez disposer d'un stockage des paquets ou d'un disque de capture de paquets configuré pour pouvoir télécharger des paquets et des clés de session à partir d'un sonde ou un console. Consultez notre guides de déploiement pour commencer.
- Le console doit être titulaire d'une licence pour TLS Shared Secrets.
- Le Stockage des clés de session TLS le réglage doit être activé sur la sonde.
- Les utilisateurs de RevealX Enterprise doivent disposer d'un accès au système et d'une administration privilèges ou des privilèges limités avec accès aux paquets et aux clés de session. Les utilisateurs de RevealX 360 doivent avoir accès aux paquets et aux clés de session.

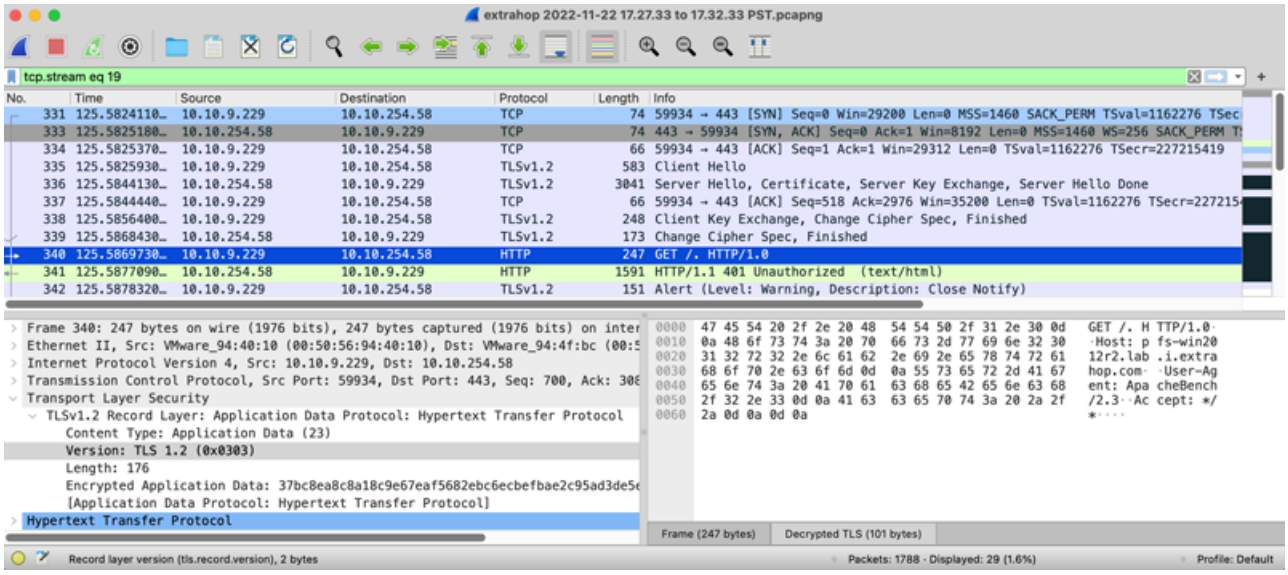
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le menu supérieur, cliquez sur **Paquets**.
3. Optionnel : Appliquez des filtres pour affiner la requête de paquets.
4. Lorsque la requête est terminée, cliquez sur **Télécharger PCAP + Session Keys** .
5. Cliquez **Télécharger PCAP + Session Keys**.
   Le fichier pcapng est automatiquement téléchargé sur votre ordinateur et l'opération de téléchargement de la clé de session est enregistrée dans journal d'audit.

   Si aucune clé de session n'est disponible pour la PCAP téléchargée, **Télécharger PCAP + Session Keys** le bouton n'apparaît pas.

Afficher la charge utile déchiffrée dans Wireshark

1. Démarrez l'application Wireshark.
2. Ouvrez le fichier de capture de paquets (pcapng) téléchargé dans Wireshark.

Lorsqu'une trame cryptée SSL est sélectionnée, **SSL déchiffré** l'onglet apparaît en bas de la fenêtre Wireshark. Cliquez sur l'onglet pour afficher les informations déchiffrées de la PCAP sous forme de texte brut.



éléments déclencheurs

Les déclencheurs sont composés d'un code défini par l'utilisateur qui s'exécute automatiquement sur les événements du système via l'API ExtraHop Trigger. Vous pouvez écrire un déclencheur, qui est un bloc de JavaScript, via l'API de déclenchement pour extraire, stocker et visualiser des événements et des mesures de Wire Data personnalisés qui sont spécifiques à votre entreprise, à votre infrastructure, à votre réseau, à vos clients et à vos applications métier.

Parmi les flux de travail les plus courants que vous pouvez exécuter à l'aide de déclencheurs, citons les opérations suivantes :

- Créez un application conteneur dans lequel les métriques sont collectées pour des appareils spécifiques. Les conteneurs d'applications augmentent les vues basées sur les appareils que le système ExtraHop construit par défaut.
- Créez métriques personnalisées et enregistrez-les dans la banque de données ExtraHop. Par exemple, les données des agents utilisateurs générées par un HTTP request n'est pas une métrique intégrée au système ExtraHop. Cependant, l'API ExtraHop Trigger fournit une propriété HTTP d'agent utilisateur, qui vous permet d'écrire un déclencheur qui collecte les données de l'agent utilisateur sous forme de métrique personnalisée.
- Générez disques et écrivez-les dans une banque de données pour un stockage et une extraction à long terme.
- Envoyez des données à des utilisateurs Syslog, tels que Splunk, ou à des bases de données tierces, telles que MongoDB ou Kafka, par le biais d'un flux de données ouvert.
- Effectuez une analyse universelle de la charge utile (UPA) pour accéder aux charges utiles TCP et UDP non prises en charge et les analyser protocoles.
- Lancez des captures de paquets pour enregistrer des flux individuels en fonction de critères spécifiés par l'utilisateur. Votre système ExtraHop doit disposer d'une licence pour la capture de paquets pour accéder à cette fonctionnalité.

Pour afficher tous les déclencheurs, cliquez sur **Paramètres du système** icône puis cliquez sur **éléments déclencheurs**. À partir de la page Déclencheurs, vous pouvez créer un déclencheur ou cochez la case à côté d'un déclencheur pour modifier la configuration du déclencheur ou modifier le script du déclencheur.

Planifier un déclencheur

La création d'un déclencheur pour collecter des métriques personnalisées est un moyen puissant de surveiller les performances de votre application et de votre réseau. Cependant, les déclencheurs consomment des ressources système et peuvent affecter les performances du système, et un déclencheur mal écrit peut entraîner une charge système inutile. Avant de créer un déclencheur, évaluez ce que vous voulez qu'il accomplisse, identifiez les événements et les appareils nécessaires pour extraire les données dont vous avez besoin et déterminez s'il existe déjà une solution.

- Identifiez les informations spécifiques que vous devez collecter en posant les types de questions suivants :
  - Quand est-ce que mes certificats TLS expireront ?
  - Mon réseau est-il connecté à des ports non autorisés ?
  - Combien de transactions sont lentes sur mon réseau ?
  - Quelles données dois-je envoyer à Splunk via un flux de données ouvert ?
- Passez en revue le Catalogue métrique pour déterminer s'il existe déjà une métrique intégrée qui extrait les données dont vous avez besoin. Les métriques intégrées ne créent pas de charge supplémentaire sur le système.
- Identifier quel système événements produisez les données que vous souhaitez collecter. Par exemple, un déclencheur qui surveille l'activité des applications cloud dans votre environnement peut s'exécuter

sur les réponses HTTP et lors de l'ouverture et de la fermeture de connexions TLS. Pour obtenir la liste complète des événements du système, consultez le Référence de l'API ExtraHop Trigger.

- Familiarisez-vous avec les méthodes et propriétés de l'API disponibles dans Référence de l'API ExtraHop Trigger. Par exemple, avant d' aller trop loin dans la planification de votre déclencheur, vérifiez la référence pour vous assurer que la propriété que vous souhaitez extraire est disponible ou pour savoir quelles propriétés sont collectées dans un enregistrement SMB par défaut.
- Déterminez comment vous souhaitez visualiser ou stocker les données collectées par le déclencheur. Par exemple, vous pouvez consulter les statistiques d'un tableau de bord ou par protocole, vous pouvez envoyer des enregistrements vers l'espace de stockage des enregistrements.
- Déterminez s'il existe déjà un déclencheur qui répond à vos besoins ou qui pourrait être facilement modifié ; commencez toujours par un déclencheur préexistant dans la mesure du possible. Recherchez un déclencheur existant dans les ressources suivantes :
  - Déclencheurs existants sur la page Déclencheurs
  - Les forums de la communauté ExtraHop

Créer des déclencheurs

Si vous déterminez que vous devez créer un nouveau déclencheur, familiarisez-vous avec les tâches suivantes à effectuer :

- Configurer le déclencheur pour fournir des informations telles que le nom du déclencheur et indiquer si le débogage est activé. Plus important encore, spécifiez les événements système sur lesquels le déclencheur s'exécutera. Par exemple, si vous souhaitez que votre déclencheur s'exécute chaque fois qu'une connexion SSH est ouverte, vous devez spécifier `SSH_OPEN` comme événement déclencheur.
- Écrivez le script du déclencheur, qui spécifie les instructions que le déclencheur exécutera lorsqu'un événement système configuré pour le déclencheur se produit. Le script déclencheur peut fournir des instructions pour une tâche simple, telle que la création d'une métrique personnalisée du nombre d'équipements appelée « slow_rsp », ou pour une tâche plus complexe, telle que la surveillance et la collecte de statistiques sur les applications cloud accessibles dans votre environnement.

Une fois le déclencheur terminé et en cours d'exécution, il est important de vérifier qu'il fonctionne comme prévu.

- Afficher le journal de débogage pour le résultat attendu des instructions de débogage du script de déclencheur. Le journal affiche également toutes les erreurs d'exécution et les exceptions que vous devez corriger.
- Surveillez le coût des performances en suivant le nombre de cycles consommés par le déclencheur.
- Consultez les graphiques de santé du système pour les exceptions liées aux déclencheurs, les sorties de la file d'attente des déclencheurs et les activités inattendues.
- Vérifiez que le script du déclencheur est conforme à Guide des meilleures pratiques relatives aux déclencheurs.

Parcourez les déclencheurs

La page Déclencheurs contient une liste des déclencheurs actuels avec les informations suivantes :

Nom
Le nom du déclencheur défini par l'utilisateur.

Auteur
Le nom de l'utilisateur qui a créé le déclencheur. Les déclencheurs par défaut affichent ExtraHop pour ce champ.

Descriptif
Description du déclencheur définie par l'utilisateur.

Devoirs
Les appareils ou groupes d'appareils auxquels le déclencheur est attribué.

État

Si le déclencheur est activé. Si le déclencheur est activé, le nombre d'attributions d' équipements s'affiche également.

Journal de débogage

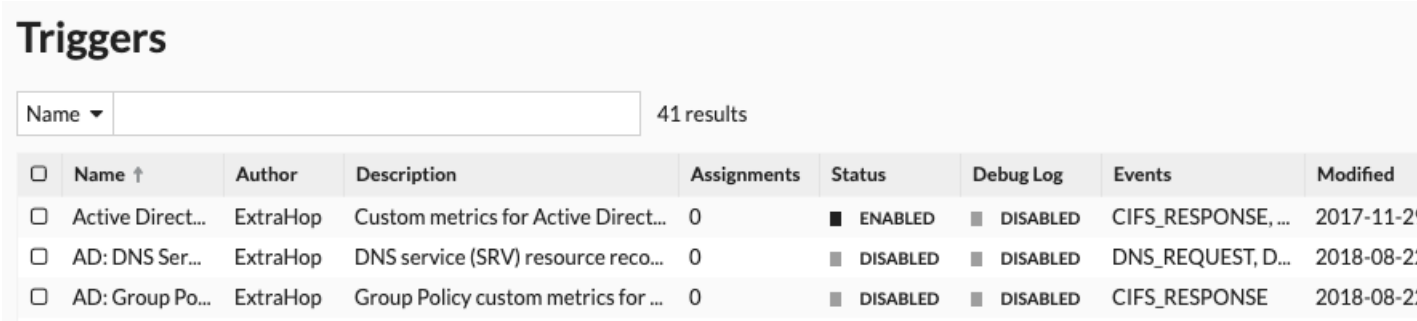
Indique si le débogage est activé. Si le débogage est activé, les résultats des instructions de débogage du script de déclencheur sont enregistrés dans le sortie du journal de débogage.

Évènements

Les événements système qui provoquent l'exécution du déclencheur, tels que `HTTP_RESPONSE`.

Modifié

La dernière fois que le déclencheur a été modifié.



Créez un déclencheur

Les déclencheurs fournissent des fonctionnalités étendues à votre système ExtraHop. Les déclencheurs vous permettent de créer des métriques personnalisées, de générer et de stocker des enregistrements ou d'envoyer des données à un système tiers. Comme vous écrivez le script de déclenchement, vous contrôlez les actions entreprises par le déclencheur lors d'événements système spécifiés.

Pour créer un déclencheur, vous devez créer une configuration de déclencheur, écrire le script du déclencheur, puis affecter le déclencheur à une ou plusieurs sources métriques. Le déclencheur ne s'exécute pas tant que toutes les actions ne sont pas terminées.

Avant de commencer
Connectez-vous au système ExtraHop avec un compte utilisateur disposant de l'écriture complète privilèges nécessaire pour créer des déclencheurs.

Si vous êtes novice en matière de déclencheurs, familiarisez-vous avec le processus de planification du déclencheur, ce qui vous aidera à affiner le champ de votre déclencheur ou à déterminer s'il est vraiment nécessaire de créer un déclencheur. Ensuite, suivez le processus de création d'un déclencheur en complétant le Procédure pas à pas des déclencheurs.

Configurer les paramètres du déclencheur

La première étape pour créer un déclencheur consiste à fournir un nom de déclencheur, à déterminer si le débogage est activé et, surtout, à identifier les événements système sur lesquels le déclencheur sera exécuté .

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **déclencheurs**.
3. Cliquez **Créez**.
4. Spécifiez les paramètres de configuration du déclencheur suivants :

   Nom

   Nom du déclencheur.

Auteur

Nom de l'utilisateur qui a écrit le déclencheur. Les déclencheurs par défaut affichent ExtraHop.

Descriptif

Description facultative du déclencheur.

Missions

Les appareils ou groupes d'équipements auxquels le déclencheur est attribué. Un déclencheur ne s'exécute pas tant qu'il n'est pas attribué à un équipement, et le déclencheur collecte des données métriques uniquement auprès des appareils auxquels il est attribué.

Avertissement: L'exécution de déclencheurs sur des appareils et des réseaux inutiles épuise les ressources du système. Minimisez l'impact sur les performances en affectant un déclencheur uniquement aux sources spécifiques auprès desquelles vous devez collecter des données.

Important: Les déclencheurs comportant les événements suivants s'exécutent chaque fois que l'événement se produit. Les déclencheurs qui s'exécutent uniquement lors de ces événements ne peuvent pas être attribués à des appareils ou à des groupes d'équipements.

- ALERT_RECORD_COMMIT
- MISE À JOUR DE DÉTECTION
- METRIC_CYCLE_BEGIN
- METRIC_CYCLE_END
- METRIC_RECORD_COMMIT
- NOUVELLE_APPLICATION
- NOUVEL_APPAREIL
- EXPIRATION DE SESSION
- MINUTER_30 SECONDES

Activer le journal de débogage

Case à cocher qui active ou désactive le débogage. Si vous ajoutez des instructions de débogage au script du déclencheur, cette option vous permet de afficher la sortie de débogage dans le journal de débogage lorsque le déclencheur est en cours d'exécution.

Évènements

Les événements sur lesquels le déclencheur s'exécute. Le déclencheur s'exécute chaque fois que l' un des événements spécifiés se produit sur un équipement assigné ; vous devez donc attribuer au moins un événement à votre déclencheur. Vous pouvez cliquer dans le champ ou commencer à saisir le nom d'un événement pour afficher une liste filtrée des événements disponibles.

Options avancées

Options de déclencheur avancées varient en fonction des événements sélectionnés. Par exemple, si vous sélectionnez `HTTP_RESPONSE` événement, vous pouvez définir le nombre d'octets de charge utile à mettre en mémoire tampon sur ces événements.

Écrire un script de déclencheur

Le script de déclenchement spécifie les instructions que le déclencheur exécutera lorsqu' un événement système configuré pour le déclencheur se produit.

Avant de commencer

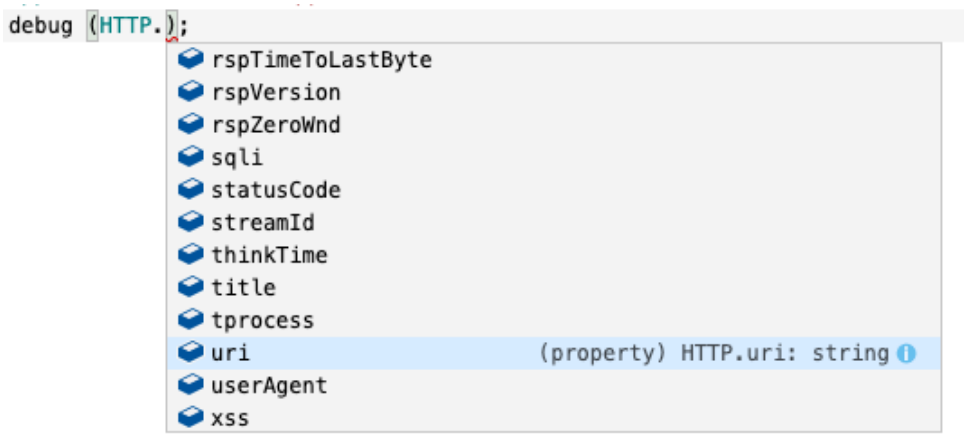
Nous vous recommandons d'ouvrir Référence de l'API ExtraHop Trigger, qui contient les événements, les méthodes et les propriétés dont vous avez besoin pour votre déclencheur. Un lien est également disponible depuis la fenêtre de l'éditeur du déclencheur du système ExtraHop.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système, puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Créez**.

4. Dans le volet droit, tapez le script du déclencheur dans une syntaxe de type JavaScript avec les événements, les méthodes et les propriétés du Référence de l'API ExtraHop Trigger.

   La figure suivante montre un exemple de script saisi dans l'onglet Editeur :

   L'éditeur fournit une fonction de saisie semi-automatique qui affiche une liste de propriétés et de méthodes en fonction de l' objet de classe sélectionné. Par exemple, tapez le nom d'une classe, puis tapez un point (.) pour afficher la liste des propriétés et méthodes disponibles, comme illustré dans la figure suivante :

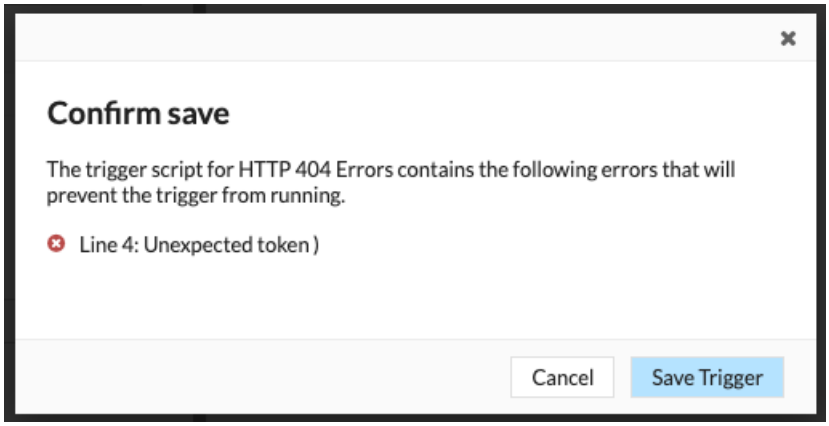


5. Cliquez **Enregistrer**.

   L'éditeur permet de valider la syntaxe de votre script. Lorsque vous enregistrez le déclencheur, le validateur signale les actions non valides, les erreurs de syntaxe ou les éléments obsolètes du script. S'il est disponible, le validateur affiche les remplacements des éléments obsolètes.

   Avertissement : Pour éviter de mauvaises performances du déclencheur, des résultats incorrects ou un dysfonctionnement du déclencheur , nous vous recommandons vivement de corriger le code ou de remplacer l'élément obsolète.

   La figure suivante montre un exemple de message d'erreur généré par le validateur de syntaxe :



Options de déclencheur avancées

Vous devez configurer les déclencheurs pour qu'ils s'exécutent sur au moins un événement. En fonction de l' événement sélectionné, le volet Create Trigger affiche des options de configuration avancées. Par exemple, en sélectionnant le HTTP_RESPONSE cet événement vous permet de définir le nombre d'octets de charge utile à mettre en mémoire tampon chaque fois qu'un événement se produit sur le système.

Le tableau suivant décrit les options avancées disponibles et les événements qui prennent en charge chaque option.

Option	Descriptif	Événements pris en charge
Octets par paquet à capturer	Spécifie le nombre d'octets à capturer par paquet. La capture commence par le premier octet du paquet. Spécifiez cette option uniquement si le script déclencheur effectue une capture de paquets. La valeur 0 indique que la capture doit collecter tous les octets de chaque paquet.	Tous les événements sont pris en charge à l'exception de la liste suivante : • ALERT_RECORD_COMMIT • METRIC_CYCLE_BEGIN • METRIC_CYCLE_END • FLOW_REPORT • NEW_APPLICATION • NEW_DEVICE • SESSION_EXPIRE
Octets de charge utile L7 vers la mémoire tampon	Spécifie le nombre maximum d'octets de charge utile à mettre en mémoire tampon. **Note:** Si plusieurs déclencheurs sont exécutés sur le même événement, le déclencheur dont la valeur L7 Payload Octets to Buffer est la plus élevée détermine la charge utile maximale pour cet événement pour chaque déclencheur.	• CIFS_REQUEST • CIFS_RESPONSE • HTTP_REQUEST • HTTP_RESPONSE • ICA_TICK • LDAP_RESPONSE
Octets du presse-papiers	Spécifie le nombre d'octets à mettre en mémoire tampon lors	• ICA_TICK

Option	Descriptif	Événements pris en charge
	d'un transfert dans le presse-papiers Citrix.	
Cycle métrique	Spécifie la durée du cycle métrique, exprimée en secondes. La seule valeur valide est `30sec`.	• `METRIC_CYCLE_BEGIN` • `METRIC_CYCLE_END` • `METRIC_RECORD_COMMIT`
Types de métriques	Spécifie le type de métrique par le nom brut de la métrique, tel que `extrahop.device.http_server`. Spécifiez plusieurs types de métriques dans une liste séparée par des virgules.	• `ALERT_RECORD_COMMIT` • `METRIC_RECORD_COMMIT`
Exécuter le déclencheur à chaque tour de flux	Permet la capture de paquets sur chaque flux tourner. L'analyse par tour analyse en continu la communication entre deux terminaux pour extraire un seul point de données de charge utile du flux. Si cette option est activée, toutes les valeurs spécifiées pour **Chaîne correspondant au client** et **Chaîne correspondante au serveur** les options sont ignorées.	• `SSL_PAYLOAD` • `TCP_PAYLOAD`
Plage de ports clients	Spécifie la plage de ports du client. Les valeurs valides sont comprises entre 0 et 65535.	• `SSL_PAYLOAD` • `TCP_PAYLOAD` • `UDP_PAYLOAD`
Octets du client vers la mémoire tampon	Spécifie le nombre d'octets du client à mettre en mémoire tampon. La valeur de cette option ne peut pas être définie sur 0 si la valeur du **Octets du serveur à mettre en mémoire tampon** l'option est également définie sur 0.	• `SSL_PAYLOAD` • `TCP_PAYLOAD`
Chaîne de recherche Client Buffer	Spécifie la chaîne de format qui indique quand commencer à mettre en mémoire tampon les données du client. Renvoie le paquet entier en cas de correspondance de chaîne. Vous pouvez spécifier la chaîne sous forme de texte ou de	• `SSL_PAYLOAD` • `TCP_PAYLOAD` • `UDP_PAYLOAD`

Option	Descriptif	Événements pris en charge
	nombres hexadécimaux. Par exemple, les deux `ExtraHop` et `\x45\x78\x74\x72\x61\x48\x6F\x70` sont équivalents. Les nombres hexadécimaux ne font pas la distinction entre majuscules et minuscules. Toute valeur spécifiée pour cette option est ignorée si **Par tour** ou **Exécuter le déclencheur sur tous les protocoles UDP** l'option de paquets est activée.	
Plage de ports du serveur	Spécifie la plage de ports du serveur. Les valeurs valides sont comprises entre 0 et 65535.	• SSL_PAYLOAD • TCP_PAYLOAD • UDP_PAYLOAD
Octets du serveur vers la mémoire tampon	Spécifie le nombre d'octets du serveur à mettre en mémoire tampon. La valeur de cette option ne peut pas être définie sur 0 si la valeur du **Octets du client à mettre en mémoire tampon** l'option est également définie sur 0.	• SSL_PAYLOAD • TCP_PAYLOAD
Chaîne de recherche dans la mémoire tampon du serveur	Spécifie la chaîne de format qui indique quand commencer à mettre en mémoire tampon les données du serveur. Vous pouvez spécifier la chaîne sous forme de texte ou de nombres hexadécimaux. Par exemple, les deux `ExtraHop` et `\x45\x78\x74\x72\x61\x48\x6F\x70` sont équivalents. Les nombres hexadécimaux ne font pas la distinction entre majuscules et minuscules. Toute valeur spécifiée pour cette option est ignorée si **Par tour** ou **Exécuter le déclencheur sur tous**	• SSL_PAYLOAD • TCP_PAYLOAD • UDP_PAYLOAD

Option	Descriptif	Événements pris en charge
	les protocoles UDP l'option est activée.	
Exécuter le déclencheur sur tous les paquets UDP	Permet la capture de tous les datagrammes UDP.	• `UDP_PAYLOAD`
Exécutez FLOW_CLASSIFY sur des flux non classés expirant	Permet de lancer l'événement à son expiration afin de cumuler des métriques pour flux qui n'étaient pas classés avant leur expiration.	• `FLOW_CLASSIFY`
Types externes	Spécifie les types de données externes que le déclencheur traite. Le déclencheur ne s'exécute que si la charge utile contient un champ de type avec l'une des valeurs spécifiées. Spécifiez plusieurs types dans une liste séparée par des virgules.	1. `EXTERNAL_DATA`

Surveillez les performances du déclencheur

Après avoir créé un déclencheur, assurez-vous qu'il fonctionne comme prévu , sans erreur ni consommation inutile de ressources. Si votre script de déclencheur inclut une instruction de débogage, consultez le journal de débogage pour les résultats de débogage. Vous pouvez également consulter le journal de débogage pour détecter les erreurs et les exceptions. Vous pouvez consulter les informations de performance d'un déclencheur individuel et vous pouvez consulter plusieurs graphiques de santé du système qui indiquent l'impact collectif de tous vos déclencheurs sur le système.

Pour en savoir plus sur les étapes à suivre pour créer un déclencheur, voir Créez un déclencheur.

Vérifiez le résultat du déclencheur dans le journal de débogage

Après avoir créé ou modifié un déclencheur, vous pouvez consulter Journal de débogage onglet pour vérifier que le déclencheur fonctionne comme prévu, sans problème. Le journal de débogage affiche les résultats de débogage, les erreurs et les exceptions. Cet onglet n'apparaît qu'une fois le déclencheur enregistré.

Si un déclencheur inclut une instruction de débogage, le résultat de cette instruction est affiché dans le journal de débogage du déclencheur. Assurez-vous que la sortie enregistrée est attendue. Si aucun résultat ne s'affiche, vérifiez que le débogage est activé sur Configuration onglet.

Notez que la sortie de débogage commence à être enregistrée dès que le déclencheur est attribué et enregistré ; toutefois, le journal ne peut pas afficher les données antérieures à l'attribution et à l'enregistrement du déclencheur.

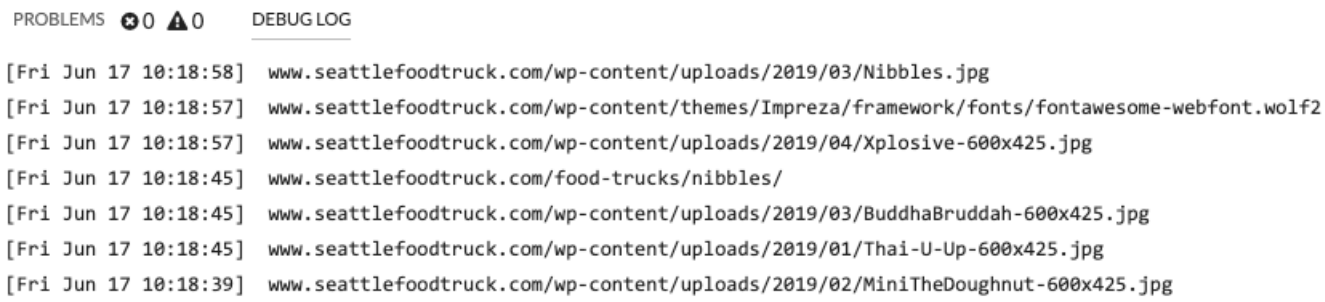
Les étapes suivantes vous indiquent comment accéder au journal de débogage :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système, puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez sur le nom du déclencheur que vous souhaitez afficher.
4. Cliquez **Modifier le script de déclenchement**.
5. Cliquez sur le **Journal de débogage** onglet.

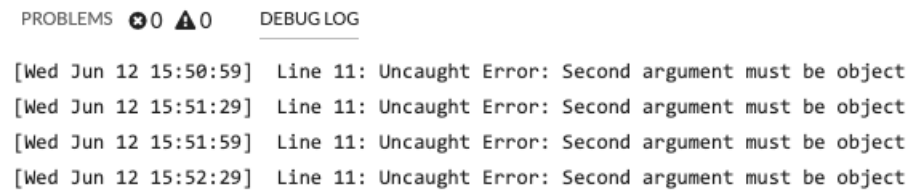
Dans l'exemple suivant, le déclencheur surveille les connexions HTTP sur des appareils sélectionnés et renvoie des URI contenant « seattle ».

```
if (HTTP.uri.match("seattle")){
    Application("Seattle App").commit();
    debug(HTTP.uri);
}
```

Lorsqu' une correspondance se produit, l'URI qui contient la correspondance est écrite dans le journal de débogage, comme illustré dans la figure suivante :



Le journal de débogage affiche également les erreurs d'exécution ou les exceptions qui se produisent, que le débogage soit activé ou non dans l'onglet Configuration. Vous devez corriger les exceptions lorsqu'elles se produisent afin de minimiser l'impact sur les performances de votre système.

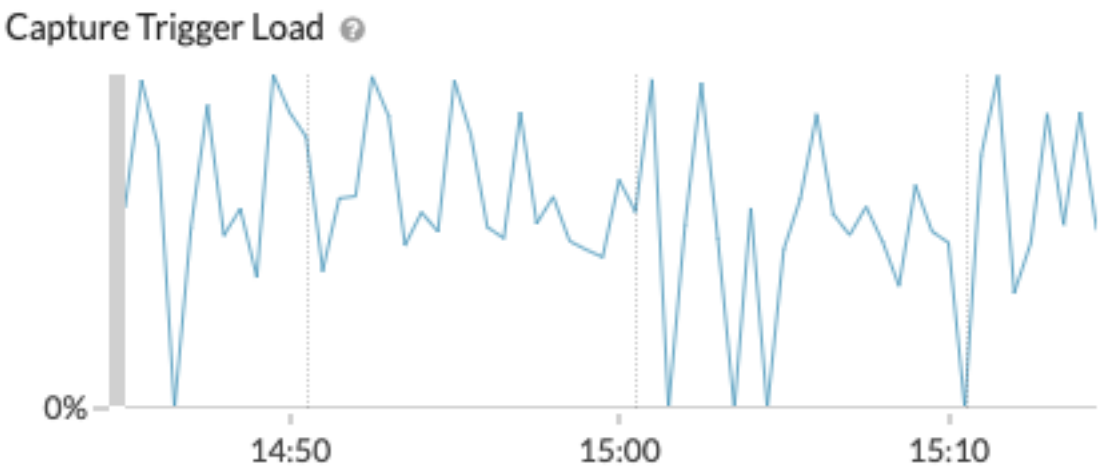


Afficher les performances d'un déclencheur individuel

Après avoir créé ou modifié un déclencheur, vous pouvez consulter le Rendement onglet pour afficher une représentation graphique de l'impact du déclencheur sur les performances de votre environnement. Cet onglet n'apparaît qu'une fois le déclencheur enregistré.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système, puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez sur le déclencheur que vous souhaitez afficher.
4. Dans le volet Modifier le déclencheur, faites défiler la page vers le bas jusqu'au graphique de charge du déclencheur de capture.

L'onglet affiche un graphique des performances du déclencheur qui suit le nombre de cycles consommés par le déclencheur au cours d'un intervalle de temps donné.



Prochaines étapes
Si l'impact du déclencheur est élevé, réévaluez l'objectif du déclencheur et envisagez les options suivantes :

- Assurez-vous que le déclencheur exécute uniquement les tâches nécessaires et s'exécute uniquement sur les appareils ou réseaux requis.
- Vérifiez les exceptions dans le tableau ci-dessous Capture Trigger Load, visitez le État du système page, qui fournit des mesures supplémentaires sur les performances des déclencheurs, telles que le nombre de déclencheurs en cours d'exécution, la charge du déclencheur et les exceptions relatives aux déclencheurs .
- Évaluez l'efficacité du script de déclenchement et recherchez des conseils d' optimisation des déclencheurs dans le Guide des meilleures pratiques en matière de déclencheurs.

Afficher les performances de tous les déclencheurs du système

Après avoir créé un déclencheur, consultez plusieurs graphiques d'état du système qui indiquent l'impact collectif de tous vos déclencheurs sur le système. Vous pouvez surveiller ces graphiques pour détecter les problèmes susceptibles d'affecter les performances du système ou d'entraîner des données incorrectes.

Le État du système Cette page contient plusieurs graphiques qui fournissent une vue d'ensemble des déclencheurs exécutés sur le système ExtraHop.

1. Cliquez sur l'icône des paramètres système, puis cliquez sur **État du système**.
2. Consultez les graphiques suivants :

Option	Description
Le déclencheur s'exécute par déclencheur	Affiche tous les déclencheurs en cours d'exécution sur le système. Si le déclencheur que vous venez de créer ou de modifier n'est pas répertorié, il se peut que le script du déclencheur présente un problème.
Le déclencheur s'exécute	Affiche des pics d'activité susceptibles d'indiquer le comportement inefficace d'un ou de plusieurs déclencheurs. Si des pics d'activité sont affichés, consultez le graphique Trigger Executes by Trigger pour localiser tout déclencheur consommant plus de ressources que la moyenne, ce qui peut indiquer que le script du déclencheur est mal optimisé et affecte les performances.
Déclenchez des exceptions par déclencheur	Affiche toutes les exceptions provoquées par des déclencheurs. Les exceptions contribuent

Option	Description
	largement aux problèmes de performance du système et doivent être corrigées immédiatement.
Gâchez Drops	Affiche le nombre de déclencheurs qui ont été supprimés de la file d'attente des déclencheurs. L'une des causes fréquentes d'abandon des déclencheurs est un déclencheur de longue durée qui domine la consommation de ressources. Un système sain ne doit contenir aucune goutte à tout moment.
Charge du déclencheur	Suit l'utilisation de toutes les ressources disponibles par déclencheurs. Une charge élevée est d'environ 50 %. Recherchez les pics de consommation qui peuvent indiquer qu'un nouveau déclencheur a été introduit ou qu'un déclencheur existant présente des problèmes.

Vous pouvez vérifier si les déclencheurs de votre banque de données, également appelés déclencheurs de pont, fonctionnent correctement à l'aide des graphiques suivants :

- Le déclencheur de la banque de données s'exécute
- Exceptions de déclencheur de banque de données par déclencheur
- Le déclencheur de la banque de données s'arrête

Lots

Un bundle est un ensemble personnalisé de configurations système qui peuvent être enregistrées et téléchargé vers un système ExtraHop.

Vidéo: Consultez la formation associée : Lots

Les personnalisations système suivantes peuvent être enregistrées dans le cadre d'un bundle :

- Alertes
- Demandes
- Tableaux de bord
- Détections personnalisées
- Groupes de périphériques dynamiques
- Requêtes d'enregistrement
- Formats d'enregistrement
- éléments déclencheurs

En savoir plus sur la création et le partage de packs avec Guide des meilleures pratiques relatives aux offres groupées.

Installer un bundle

Les offres groupées ExtraHop vous permettent d'ajouter des personnalisations préconfigurées au système ExtraHop.

Avant de commencer

- Vous devez avoir une écriture complète ou supérieure privilèges pour télécharger un bundle.
- Vous devez avoir une écriture personnelle ou supérieure privilèges pour télécharger et installer un bundle.
- Vous devez disposer d'un fichier JSON du bundle. Vous pouvez télécharger un bundle depuis le système ExtraHop en accédant à **Paramètres système > Bundles**, en sélectionnant le bundle, puis en cliquant sur **Télécharger le bundle** depuis le volet droit.

Après avoir téléchargé un bundle, vous pouvez le charger et l' installer sur votre système.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système.
3. Cliquez **Lots**.
4. Cliquez **Télécharger le bundle**.
5. Dans le Télécharger le bundle volet, cliquez sur **Choisissez un fichier**, puis sélectionnez le fichier JSON du bundle que vous souhaitez charger.

   Les détails concernant le contenu du bundle apparaissent, y compris la version minimale du firmware requise.
6. Dans la section Options d'installation, cochez les cases suivantes :
   a) (Console uniquement) Sélectionnez le site sur lequel vous souhaitez installer le bundle.

      Note: Des personnalisations groupées telles que des alertes et des déclencheurs sont ajoutées aux sites sélectionnés. Cependant, vous ne pouvez afficher, activer et configurer les personnalisations qu'à partir du système ExtraHop sur lequel le bundle a été installé.
   b) Sélectionnez le **Appliquer les devoirs inclus** case à cocher.

Cette option affecte le bundle aux sources métriques incluses dans le bundle. Dans la plupart des cas, il est préférable d'appliquer les affectations par défaut.

c) Sélectionnez le **Remplacer le contenu existant** case à cocher.

Cette option remplace tous les objets portant le même nom que les objets du bundle. Si vous souhaitez conserver des objets système portant le même nom , vous devez les renommer pour éviter de les remplacer par les objets du bundle.

7. Cliquez **Installer**.

Prochaines étapes

- Activez n'importe quel déclencheurs inclus dans le bundle.
- Configurez n'importe alertes dans le bundle pour notifier les adresses e-mail pertinentes.

Créez un bundle

Vous pouvez enregistrer les configurations système dans un fichier bundle, puis télécharger ce fichier vers d'autres systèmes ExtraHop.

Avant de commencer
Vous devez avoir une écriture complète ou supérieure privilèges pour créer un bundle.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Lots**.
3. Sur le Lots page, cliquez sur **Créez**.
4. Complétez les informations suivantes :

Nom

Attribuez un nom au bundle.

Auteur

Spécifiez le créateur du bundle. Ce nom est appliqué au champ auteur de tous les objets du bundle. Si vous ne spécifiez pas d' auteur, chaque objet du bundle conserve son paramètre d'auteur.

Version ExtraHop minimale

Spécifiez la version la plus ancienne du microprogramme ExtraHop sur laquelle le bundle peut être exécuté. Nous vous recommandons de spécifier la version actuelle du firmware ExtraHop. La spécification de la version actuelle empêche l'installation accidentelle de votre bundle sur un système qui ne prend pas en charge le bundle.

Note: Si vous essayez d'installer un bundle qui nécessite une version plus récente du firmware, un message d'avertissement s'affiche. Toutefois, cet avertissement ne vous empêche pas de télécharger et d'appliquer le bundle.

Description (facultatif)

Entrez une description du bundle.

Ajouter au pack

Dans le menu déroulant, sélectionnez les configurations système que vous souhaitez ajouter au bundle, telles que les déclencheurs, les tableaux de bord et les alertes. Vous pouvez sélectionner plusieurs articles à ajouter au bundle.

Note: Vous pouvez sélectionner rapidement plusieurs configurations de bundle à l'aide des touches de raccourci suivantes :

OPTION + clic (Mac), Alt + clic (Windows)

Sélectionnez tous les éléments sauf celui sur lequel vous avez cliqué.

SHIFT + Cliquez

Désélectionnez tous les éléments sauf celui sur lequel vous avez cliqué.

5. Cliquez **Enregistrer**.

   Vous pouvez télécharger le fichier JSON du bundle que vous avez créé en le sélectionnant dans la liste, puis en cliquant **Télécharger le bundle** depuis le volet droit.

Prochaines étapes

- Installez votre bundle sur un autre système ExtraHop

Annexe

Modules de protocole

Le système ExtraHop fournit des métriques via les types de modules de protocole suivants :

Type de module	Protocoles
L2-L3 Métriques	• Multicast • IP • IPv6 • ICMP • ICMPv6
Métriques L4	• TCP • UDP
Dénomination	DNS
Services d'annuaire	LDAP
Web	• HTTP/HTTPS • AMF • TLS
Intergiciel	• MS-RPC • Memcache • IBMMQ
Base de données	• IBM DB2 • IBM Informix • Microsoft SQL Server • MongoDB • MySQL • Oracle • PostgreSQL • Sybase ASE • Sybase IQ
Rangement	• iSCSI • SMB • NFS
Transfert de fichiers	FTP
Courrier	SMTP
Citrix VDI	• ICA • CGP
Protocoles spécifiques à l'industrie	• Diamètre • FIX

Type de module	Protocoles
	• HL7 • RAYON • SMPP • Telnet
Décryptage	N'importe lequel protocole chiffré sur un canal TLS de bout en bout, peut être déchiffré à l'aide du module de décryptage TLS.

Pour plus d'informations sur les modules du protocole ExtraHop, visitez extrahop.com.

Navigateurs pris en charge

Les navigateurs suivants sont compatibles avec tous les systèmes ExtraHop. Appliquez les fonctionnalités d'accessibilité et de compatibilité fournies par votre navigateur pour accéder au contenu par le biais d'outils technologiques d'assistance.

- Firefox
- Google Chrome
- Microsoft Edge
- Safari

Important: Internet Explorer 11 n'est plus pris en charge. Nous vous recommandons d' installer la dernière version de tout navigateur compatible.

Acronymes courants

Les acronymes courants des protocoles informatiques et réseau suivants sont utilisés dans ce guide.

Sigle	Nom complet
AAA	Authentification, autorisation et comptabilité
AMF	Format du message d'action
CIFS	Système de fichiers Internet commun
CLI	Interface de ligne de commande
CPU	Unité centrale de traitement
DB	Base de données
DHCP	Protocole de configuration dynamique de l'hôte
DNS	Système de noms de domaine
ERSPAN	Analyseur encapsulé de ports commutés à distance
FIX	Échange d'informations financières
FTP	FTP
HTTP	Protocole de transfert Hyper Text
IBMMQ	Intergiciel orienté messages IBM
ICA	Architecture informatique indépendante

Sigle	Nom complet
IP	Protocole Internet
iSCSI	Interface Internet pour petits systèmes informatiques
L2	Couche 2
L3	Couche 3
L7	Couche 7
LDAP	Protocole d'accès aux annuaires léger
MAC	Contrôle d'accès aux médias
MIB	Base d'informations de gestion
NFS	NFS
NVRAM	Mémoire à accès aléatoire non volatile
RAYON	Service utilisateur d'authentification à distance par ligne commutée
RPC	Appel de procédure à distance
RPCAP	Capture de paquets à distance
RSS	Taille de l'ensemble pour résidents
SMPP	Protocole peer-to-peer à messages courts
SMTP	Protocole de transport de messages simple
SNMP	Protocole de gestion de réseau simple
SPAN	Analyseur de ports commutés
SSD	Disque SSD
SSH	Coque sécurisée
SLL	Secure Socket Layer
TACACS+	Contrôleur d'accès au terminal Access-Control System Plus
TCP	TCP
TLS	Sécurité de la couche de transport
UI	Interface utilisateur
VLAN	VLAN
VM	Machine virtuelle