Présentation du système ExtraHop

Publié: 2023-11-14

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

Les flux de travail de surveillance des performances du réseau vous permettent de surveiller la manière dont les services et les appareils interagissent les uns avec les autres et la manière dont les transactions circulent entre la couche de liaison de données (L2) et la couche d' application (L7) de votre réseau. Les flux de travail 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 vous permettent de savoir quels appareils ont participé aux tactiques, techniques et procédures (TTP) de MITRE ATT&CK associées à des campagnes d'attaque avancées en plusieurs étapes.

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 réseau (NDR) et la surveillance des performances réseau (NPM), avec des modules supplémentaires pour les systèmes de détection d'intrusion (IDS) et l'analyse des paquets.

Les administrateurs peuvent accorder aux utilisateurs un accès basé sur les rôles 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.
- Affichez, 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 le 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.

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

Criminalistique des paquets

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

© 2023ExtraHop Networks, Inc. Tous droits réservés.

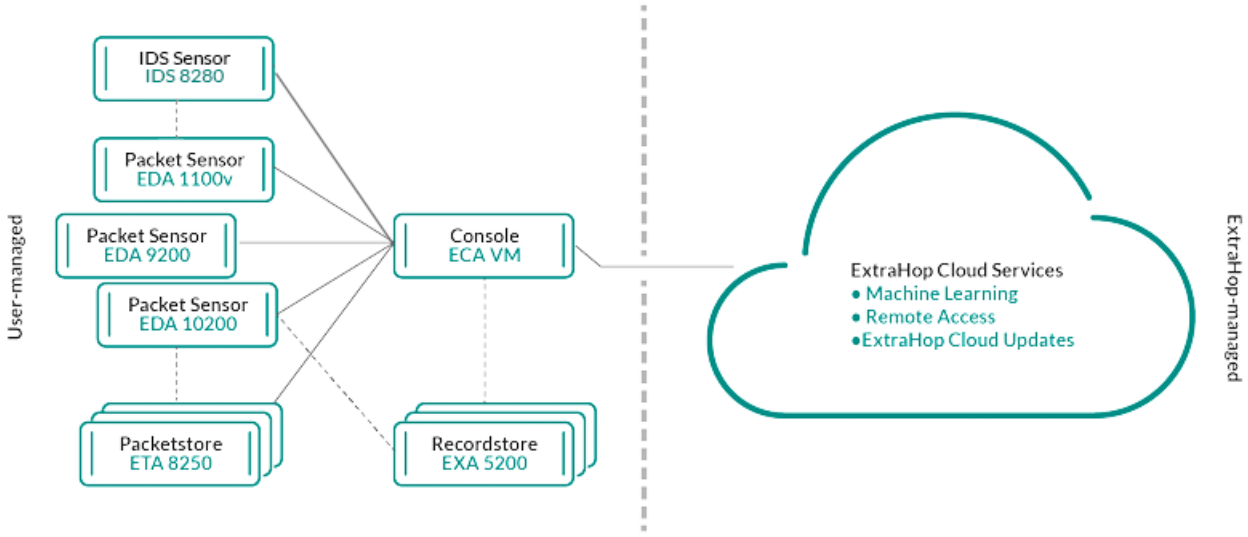
Systèmes de détection d'intrusion

Le module IDS doit être associé au module NDR et fournit des détections basées sur des signatures IDS conformes aux normes du secteur.

Des solutions

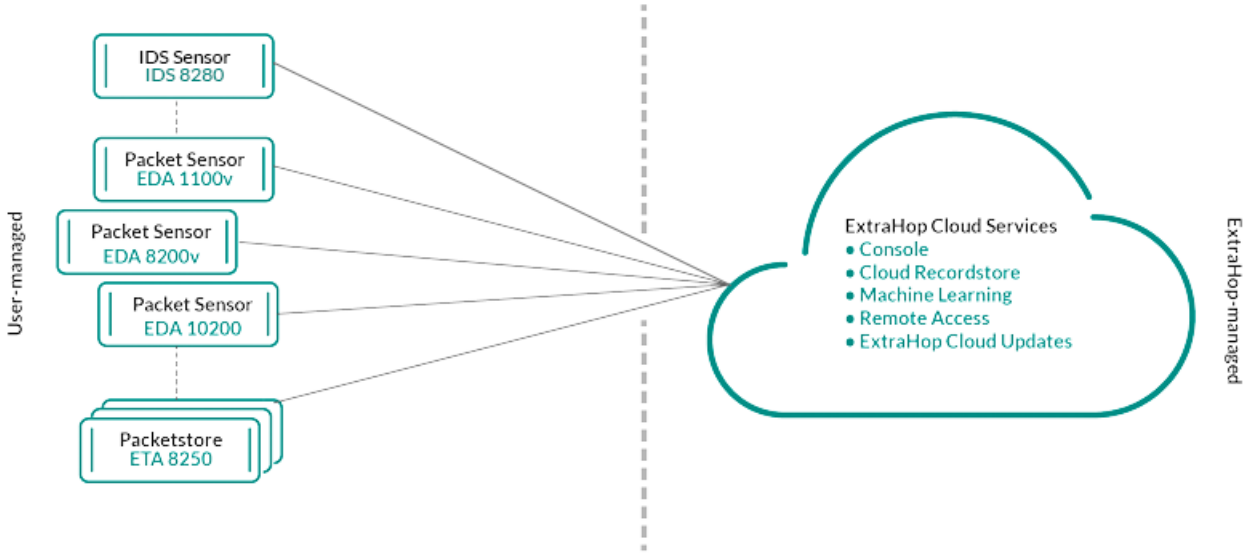
Révéler (x) Enterprise

Reveal (x) Enterprise est une solution autogérée qui comprend capteurs, consoles, des magasins de paquets, des magasins de disques et un accès aux services cloud ExtraHop.



Révéler (x) 360

Reveal (x) 360 est une solution logicielle en tant que service (SaaS) qui comprend capteurs et des stockages par paquets et comprend un espace de stockage des enregistrements basé sur le cloud, un console, et accès aux services cloud ExtraHop.



Composants

Chaque solution propose un ensemble de composants en fonction de vos besoins environnementaux : capteurs, magasins de paquets, magasins de disques et un 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 avec un capteur de paquets associé et sont disponibles pour les environnements Reveal (x) 360 ou Reveal (x) Enterprise.

Capteurs de débit

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

Magasins de disques

Les magasins de disques s'intègrent aux capteurs et consoles à enregistrer les transactions et les flux qui peuvent être interrogés depuis l'ensemble du système ExtraHop. Les recordstores peuvent être déployés en tant qu'options physiques ou virtuelles autonomes, pris en charge en tant que connexions tierces à Splunk ou BiqQuery depuis Reveal (x) Enterprise, et sont disponibles sous forme de packages avec des modules NPM et NDR.

Magasins de paquets

Les magasins de paquets s'intègrent aux capteurs et consoles pour fournir capture de paquets en continu et un espace de stockage suffisant pour les enquêtes approfondies et les besoins en 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 virtuelles autonomes ou basées sur le cloud pour Reveal (x) Enterprise et sont incluses dans Reveal (x) 360.

Le tableau suivant fournit une vue d'ensemble des options disponibles pour chaque solution.

	Révéler (x) Enterprise		**Révéler (x) 360**	
	Physique	Virtuel/Cloud	Physique	Virtuel/Cloud
sonde de paquets	EDA 1200 EDA 6200 EDA 820 EDA 9200 EDA 10200	EDA 1100 v AWS EDA 1100v Azure EDA 100 v GCP KVM Linux EDA 1100v VMWare EDA 1100v VMware EDA 6100v EDA 6100v AWS	EDA 1200 EDA 6200 EDA 820 EDA 9200 EDA 10200	EDA 1100 v AWS EDA 1100v Azure EDA 100 v GCP KVM Linux EDA 1100v VMWare EDA 1100v VMware EDA 6100v EDA 6100v AWS

	Révéler (x) Enterprise		Révéler (x) 360	
		EDA 6100v Azure EDA 8200v AWS Reveal (x) Ultra 1 Gbit/s et 10 Gbit/s AWS GCP Reveal (x) Ultra 1 Gbit/s		EDA 6100v Azure EDA 8200v AWS Reveal (x) Ultra 1 Gbit/s et 10 Gbit/s AWS GCP Reveal (x) Ultra 1 Gbit/s
sonde IDS	IDS 8280	N/A	IDS 8280	N/A
sonde de débit	N/A	N/A	N/A	EFC 1291v
Magasin de paquets	ETA 6150 ETA 8250	ETA 1150 v AWS ETA 1150v Azure ETA 1150 v GCP VMWare ETA 1150v VMWare ETA 6150v	ETA 6150 ETA 8250	ETA 1150 v AWS ETA 1150v Azure ETA 1150 v GCP VMWare ETA 1150v VMWare ETA 6150v Inclus dans les abonnements Ultra
Boutique de disques	EXA 5200	EXA 5100v AWS EXA 5100v Azure Hyper-V EXA 5100v KVM Linux EXA 5100v VMWare EXA 5100v	N/A	Inclus dans les abonnements Premium et Ultra
Console	N/A	LOIS DE LA CEA ECA Azure ECA GCP Hyper-V ECA Système KVM ECA Linux	N/A	Inclus dans tous les abonnements

Révéler (x) Enterprise	Révéler (x) 360
VMWare ECA	

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 par 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 de haut en bas et de personnaliser la façon dont vous collectez, consultez et partagez les données de votre réseau. Les utilisateurs expérimentés peuvent automatiser et écrire des scripts à la fois pour les tâches administratives et pour les utilisateurs par le biais du API REST ExtraHop et personnalisez la collecte de données par le biais du API de déclenchement ExtraHop, qui est un outil IDE JavaScript.

Au cœur du système ExtraHop se trouve un système intelligent 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. Capteurs sont dotés d'un stockage compatible avec 30 jours de rétrospective métrique. Notez que le rétrospective réel 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 agissent comme un 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 Reveal (x) 360 incluent une console ; Reveal (x) Enterprise peut déployer des variantes virtuelles ou cloud.

Les consoles fournissent des vues unifiées des données 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 façon dont ils fonctionnent ensemble.

Types de capteurs

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

Données de câblage
Les capteurs de paquets observent passivement les paquets non structurés par le biais d'un miroir de ports ou d'un tap et stockent les données dans la banque de données locale. Les données des paquets passent par un traitement de flux en temps réel qui transforme les paquets en données filaires structurées selon les étapes suivantes :

1. Les machines d'état 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, puis les données métriques sont 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 conformément au 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 points de terminaison. Débit capteurs sont disponibles pour Reveal (x) 360 et offrent une visibilité continue du réseau basée sur les 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 à destination et en provenance 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 grâce à des 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 les adresses MAC) demandées par les 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.

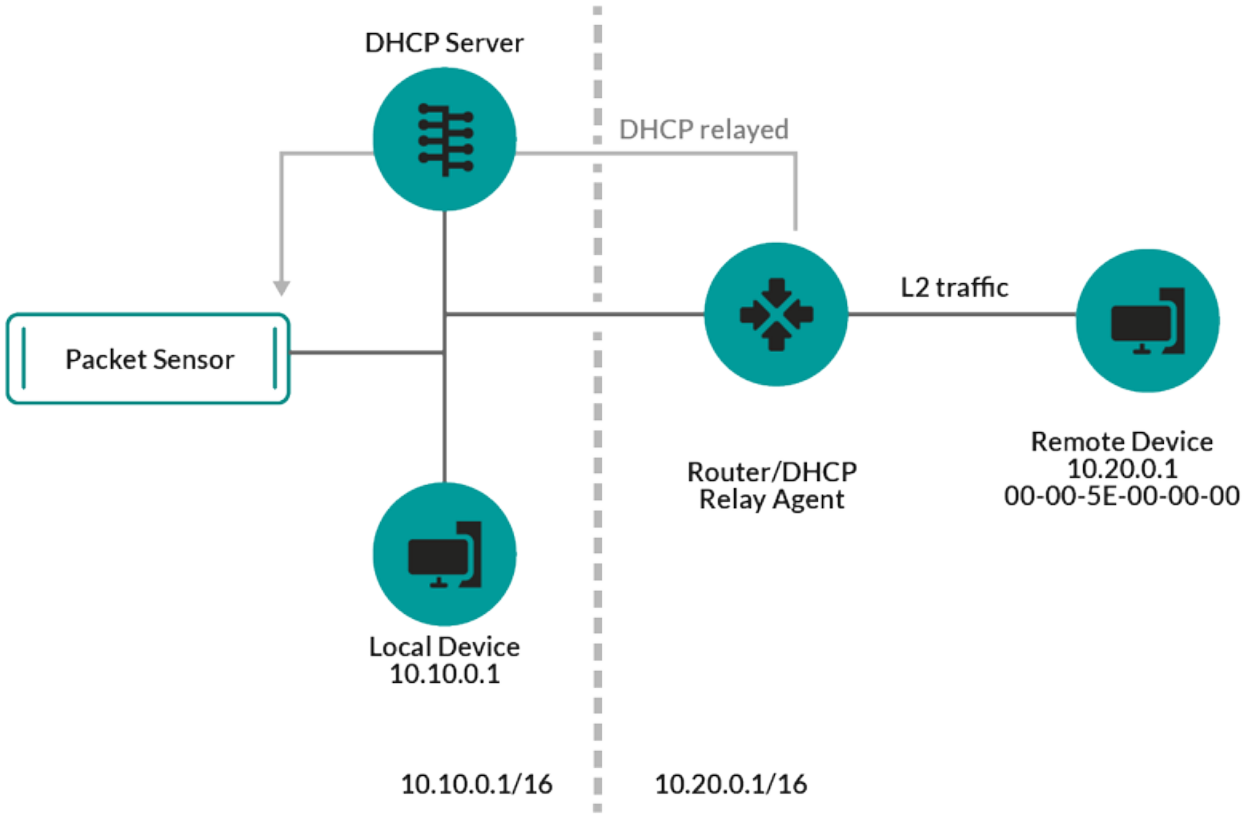


Figure 1: L'adresse MAC et l'adresse IP de l'équipement distant sont découvertes.

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.)

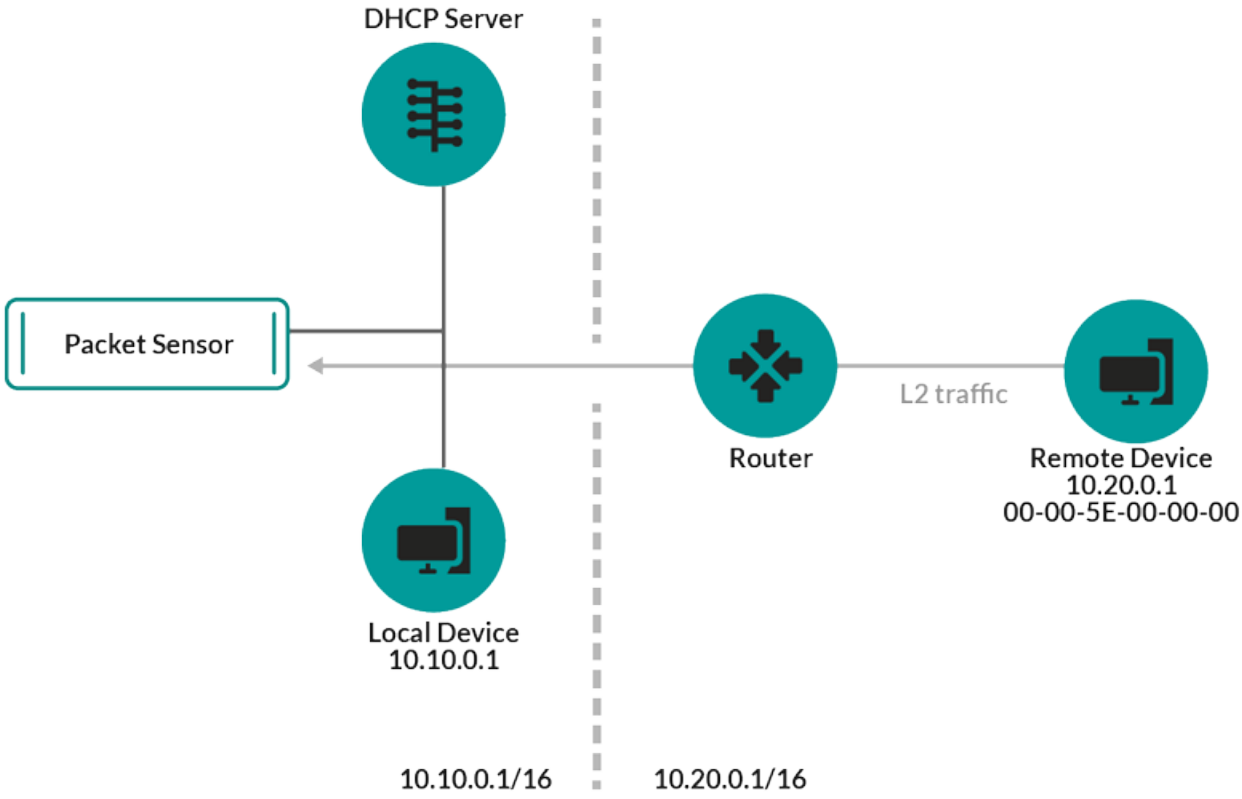


Figure 2: Seule l'adresse IP de l'équipement distant est découverte.

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.)

Détection des menaces

Le système ExtraHop propose à la fois un apprentissage automatique et un système basé 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.

De plus, graphiques, visualisations, et cartes d'activité de l'équipement permettre une chasse proactive aux menaces.

Réglage de la détection
Réduisez le bruit et repérez uniquement 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 vulnérabilité.

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

Localité du réseau
Par défaut, tout équipement possédant 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 qu'équipement interne.

Toutefois, étant donné que certains environnements réseau incluent des adresses IP non conformes à la norme 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 un renseignement sur les menaces fil 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 ou par l'intermédiaire d'un partenaire intégrations avec ExtraHop Reveal (x) 360.

Briefings sur les menaces
Briefings 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 enquête. Vous pouvez y accéder depuis le Aperçu de la sécurité page.

Intégrations
Reveal (x) 360 propose plusieurs intégrations tierces qui peuvent améliorer la gestion de la détection et des réponses et offrir 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.

CrowdStrike

Importez des renseignements sur les menaces depuis CrowdStrike FalconX, consultez les informations sur les appareils CrowdStrike et empêchez ces appareils du système ExtraHop.

Échelle CrowdStrike FalconLogScale

Spécifiez les critères de filtrage pour les détections de sécurité ExtraHop et exportez les résultats vers CrowdStrike Falco LogScale.

Microsoft 365

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

Déchiffrement du protocole Microsoft

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

QRadar

Exportez et visualisez les détections ExtraHop dans votre QRadar SIEM.

Splunk

Exportez et visualisez les détections ExtraHop dans votre SIEM Splunk.

Splunk SOAR

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