Détections

Publié: 2024-01-31

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

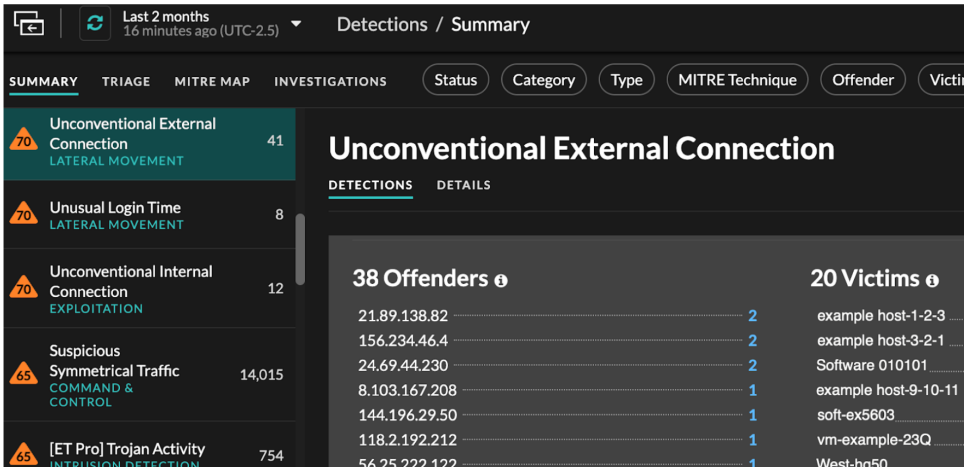
Affichage des détections

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

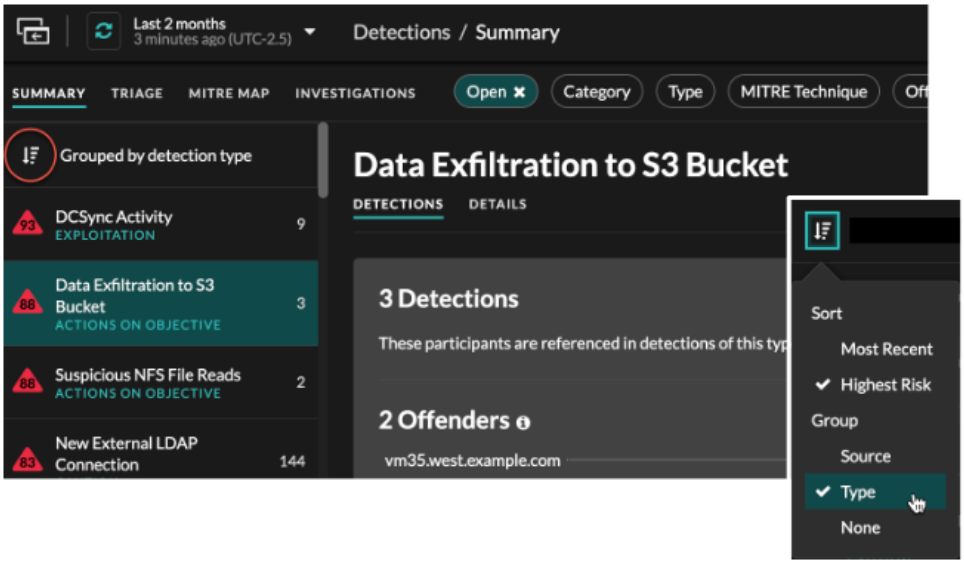
Vous pouvez trier les détections en fonction de l'indice de risque le plus élevé ou de l'événement le plus récent.

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

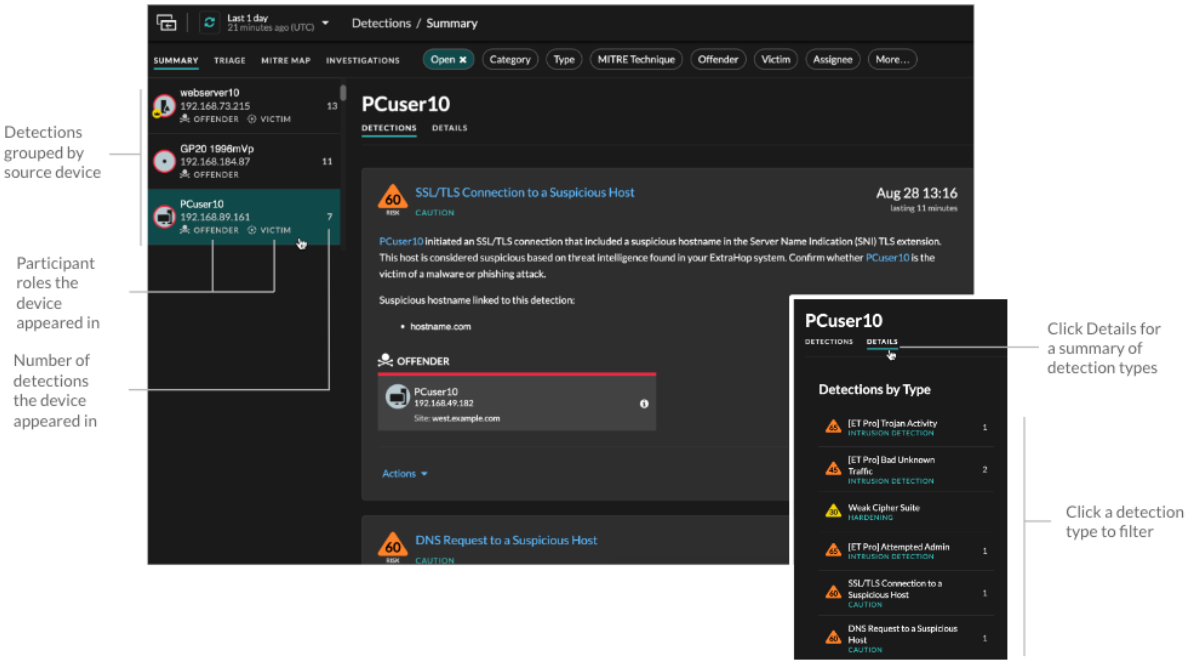
Répertorie les localités du réseau qui contiennent des détections du type sélectionné . La liste des localités du réseau est ordonnée en fonction du nombre de détections dans la localité du réseau.

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 recommandées par ExtraHop pour le triage sur la base d'une analyse contextuelle des facteurs de votre environnement.

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.

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.

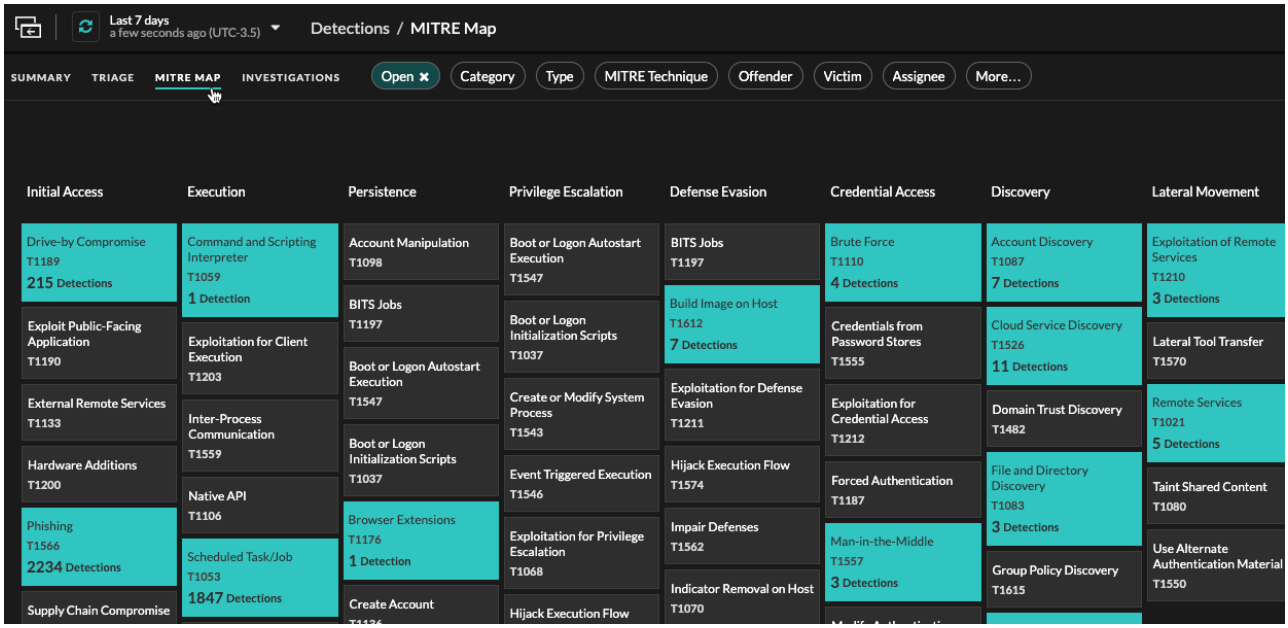


Tableau des enquêtes

La vue Investigations affiche toutes les enquêtes créées.

Cliquez sur le nom d'une enquête pour ouvrir l'enquête. En savoir plus sur Enquêtes.

Filtrer les détections

Vous pouvez filtrer la page Détections pour n'afficher que les détections correspondant aux critères que vous avez 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 Accusé, En cours ou Fermé. Par défaut, le **Ouvert** le filtre d'état est appliqué au Détections page. Cliquez sur **Ouvert** filtre pour accéder à d'autres options de filtrage.

Vous pouvez sélectionner **Caché** statut pour afficher uniquement les détections qui sont actuellement masqué par règles de réglage.

Catégorie

Vous pouvez filtrer par détections d'attaques ou d'opérations, ou vous pouvez sélectionner une catégorie plus spécifique pour affiner votre affichage de la page des détections. Lorsque vous cliquez sur le filtre Catégorie, la plupart des catégories répertoriées sous le **Toutes les catégories d'attaques** et **Toutes les catégories d'opérations** les options sont triées en fonction du nombre de détections dans la catégorie. Les détections de renforcement 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 une connexion à un équipement compromis sur votre réseau. Les serveurs C&C peuvent envoyer des programmes malveillants, des commandes et des charges utiles pour soutenir l'attaque. Ces détections identifient le moment où 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 points faibles à exploiter. Ces détections identifient les scans et les techniques d'énumération.

Note: Les détections peuvent identifier un scanner de vulnérabilités connu tel que Nessus et Qualys. Cliquez sur le nom de l'équipement pour confirmer si un rôle de scanner de vulnérabilités a déjà été attribué à celui-ci 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 identifient les comportements inhabituels et suspects associés aux techniques d'exploitation.

Mouvement latéral

Un attaquant s'est infiltré dans votre réseau et passe 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 dans le corridor est-ouest.

Actions relatives 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.

Prudence

Mettez en évidence les activités qui ne présentent pas de menace imminente pour les opérations, mais qui doivent être prises en compte 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.

Fonctionnement 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 mettent au jour les appareils aux ressources limitées.

Base de données

Mettez en évidence les problèmes d'accès pour les applications ou les 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 les transactions.

Virtualisation des postes de travail et des applications

Mettez en évidence 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 fenêtres Zero, ce qui indique qu'un serveur Citrix est surchargé.

Infrastructure réseau

Mettez en évidence les événements inhabituels liés aux protocoles TCP, DNS et DHCP. Ces détections peuvent indiquer 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

Mettez en évidence 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 e-mail. Ces détections peuvent indiquer des dégradations de service liées à l'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

Mettez en évidence 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 aux fichiers sur les serveurs Windows en raison de problèmes SMB/CIFS, ou que les serveurs de stockage en réseau (NAS) n'ont pas pu être atteints en raison d'erreurs NFS.

Application Web

Mettez en évidence 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 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'amélioration de votre posture de sécurité.

Durcissement

Mettez en évidence les meilleures pratiques en matière de renforcement de la sécurité qui devraient être appliquées pour atténuer le risque d'exploitation. Ces détections identifient les opportunités d' améliorer le niveau de sécurité de votre réseau, par exemple en empêchant la divulgation des informations d'identification et en supprimant les certificats SSL/TLS expirés des serveurs. Après avoir cliqué sur une détection de renforcement, vous pouvez appliquer des filtres supplémentaires pour afficher des détections spécifiques au sein de ce type de détection de renforcement. En savoir plus sur filtrage et réglage des détections de durcissement.

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 aux signatures connues de pratiques dangereuses, de tentatives d'exploitation et aux indicateurs de compromission liés aux programmes malveillants et aux 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.

Type

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 technique 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 dispositifs de passerelle ou d'équilibrage de charge associés à des participants externes au point de terminaison peuvent également être spécifiés dans ces filtres.

Cessionnaire

Filtrez les détections par l'utilisateur affecté à la détection.

Plus de filtres

Vous pouvez également filtrer vos détections selon les critères suivants :

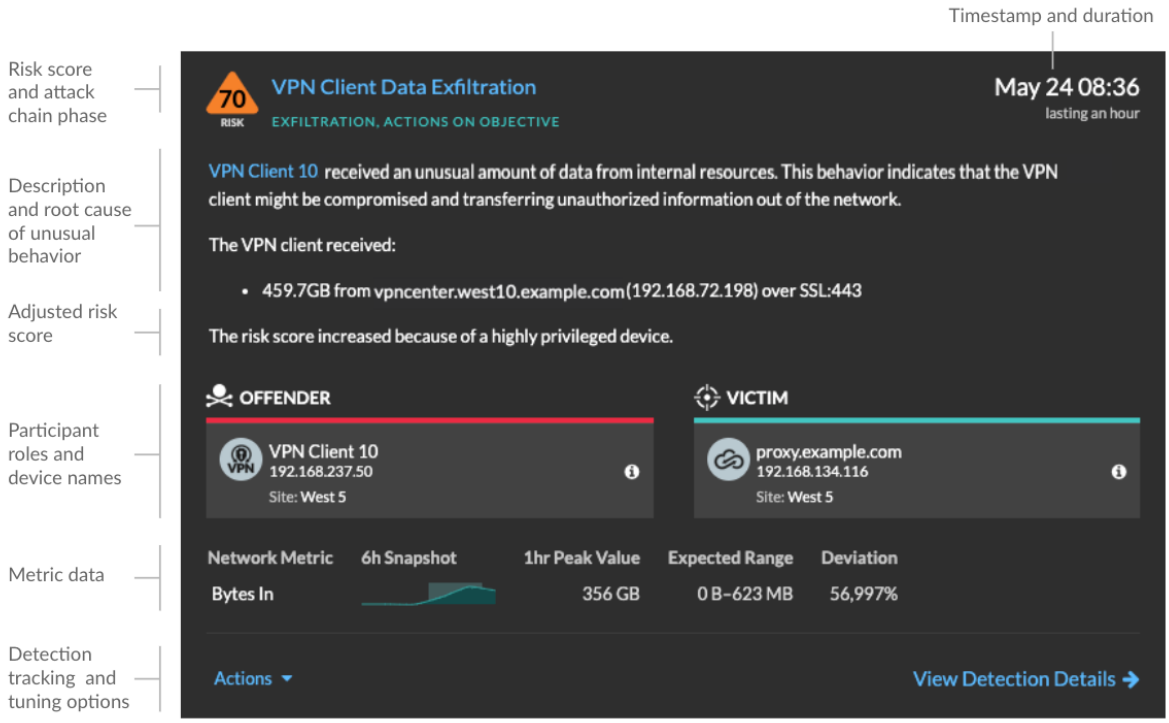
- Recommandé pour le triage
- Rôles des appareils
- La source
- Site (console uniquement)
- Filtre d'identification du ticket (Systèmes de billetterie tiers uniquement)
- Note de risque minimale

Navigation dans les détections

Après avoir sélectionné le mode d'affichage, de regroupement et de filtrage de 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, le moment où la détection s'est produite, ainsi que la victime et le délinquant participants. Les détections de sécurité incluent un indice de risque.



Score de risque

Mesure le 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 aux niveaux de compétence nécessaires à un pirate informatique potentiel et aux conséquences d'une attaque réussie. L'icône est codée par couleur par gravité en 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 voir les informations de base et les liens d'accès. Les points de terminaison internes affichent un lien vers la page de présentation de l'appareil ; les points de terminaison externes affichent la géolocalisation de l'adresse IP, liens de recherche de point de terminaison tels que le Whois ARIN 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 tous deux affichés sur la carte de participant, mais seul le point de terminaison d'origine est considéré comme un participant .

Note: Le déchiffrement SSL/TLS est nécessaire pour afficher les points de terminaison d'origine si le protocole HTTPS est activé. En savoir plus sur Déchiffrement SSL/TLS.

Lorsque vous regroupez par **Type**, un panneau récapitulatif apparaît sous le type de détection. Il ventile les détections par délinquant et par victime et vous permet de appliquer des filtres pour les participants.

Lorsque vous regroupez par **La source**, les icônes de rôle internes de l'équipement sont surlignées en rouge si l' appareil était un délinquant lors d'une détection et en bleu sarcelle si l'équipement était une victime. Vous pouvez cliquer **Détails** sous le nom de la source pour afficher un résumé des détections auxquelles cette source était un participant. Les détails de ces équipements sont affichés à côté de la carte de détection sur les écrans larges (1900 pixels ou plus).

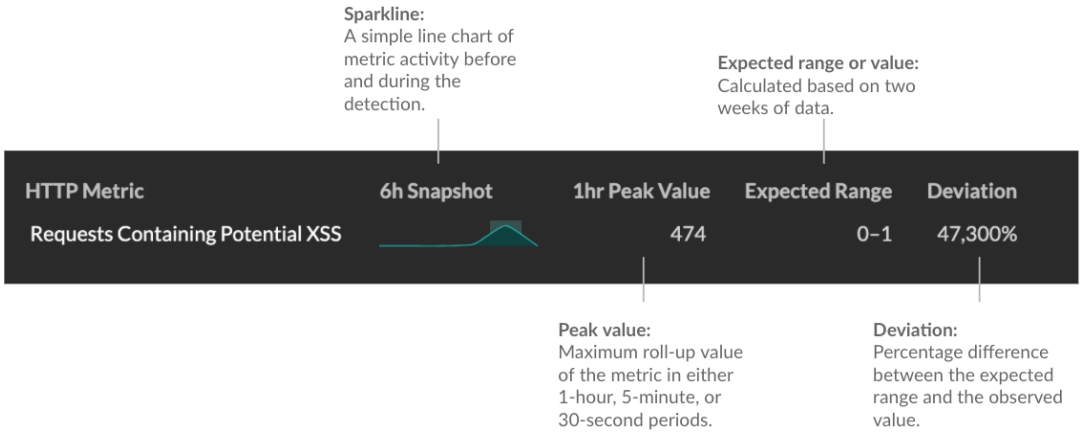
Durée

Identifie la durée pendant laquelle le comportement inhabituel a été détecté ou affiche EN COURS si le comportement se produit actuellement.

Les détections qui mettent en évidence les meilleures pratiques en matière de renforcement de la sécurité affichent deux dates : la première et la dernière fois que la violation a été identifiée.

Données métriques

Identifie les 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 depuis la liste déroulante Actions, ou cliquez sur **Afficher les détails de la détection** pour accéder à la page détaillée de la détection.

Page détaillée de la 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.

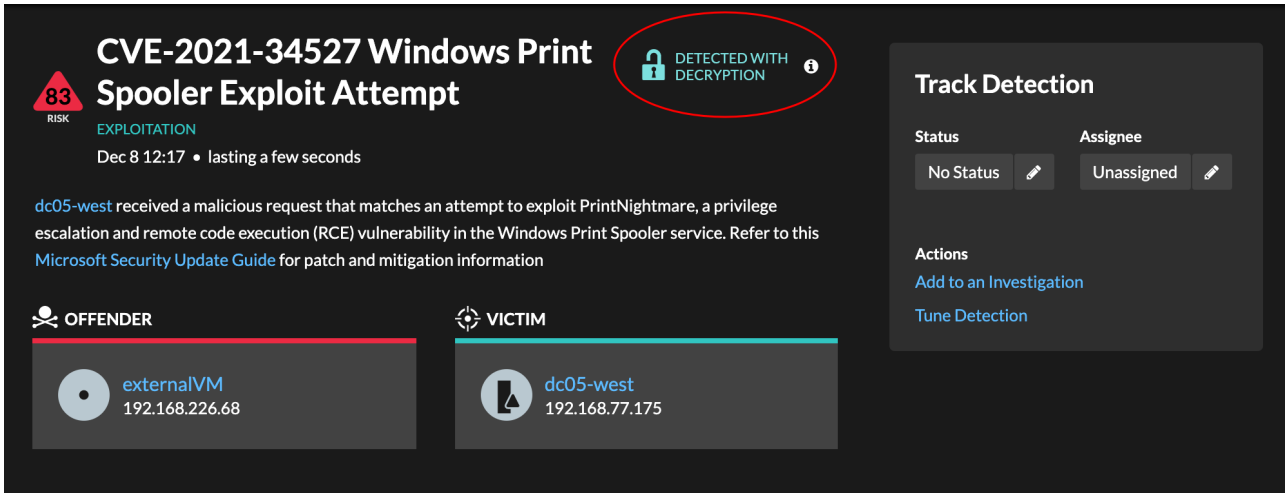
Détection de pistes

Tu peux piste ou syntoniser la détection, ou cliquez **Ajouter à une enquête** pour inclure la détection dans un nouveau ou un 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. (Reveal (x) 360 uniquement.)

Badge de déchiffrement

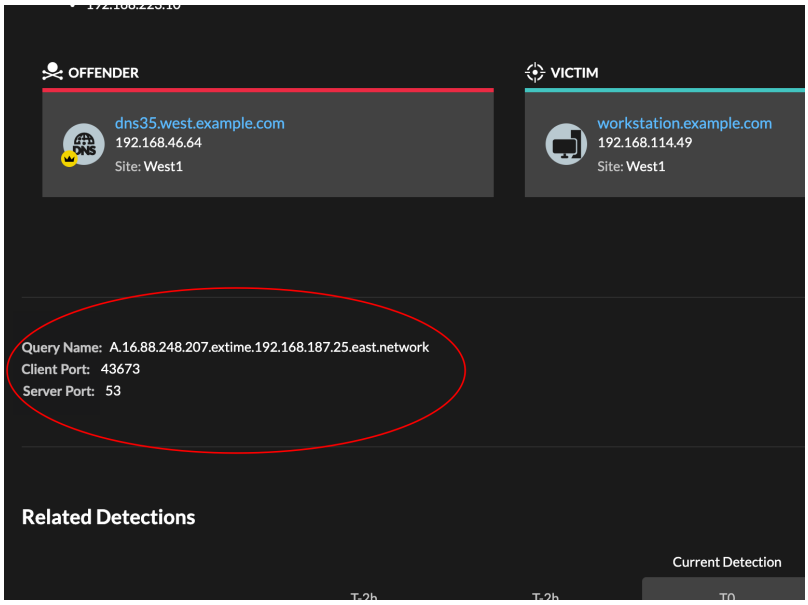
Lorsque le système ExtraHop identifie un comportement suspect ou une attaque potentielle dans les enregistrements de trafic déchiffrés, la page détaillée de la détection affiche un badge de déchiffrement à droite du nom de détection.



En savoir plus sur Déchiffrement SSL/TLS et déchiffrement du trafic avec un contrôleur de domaine Windows.

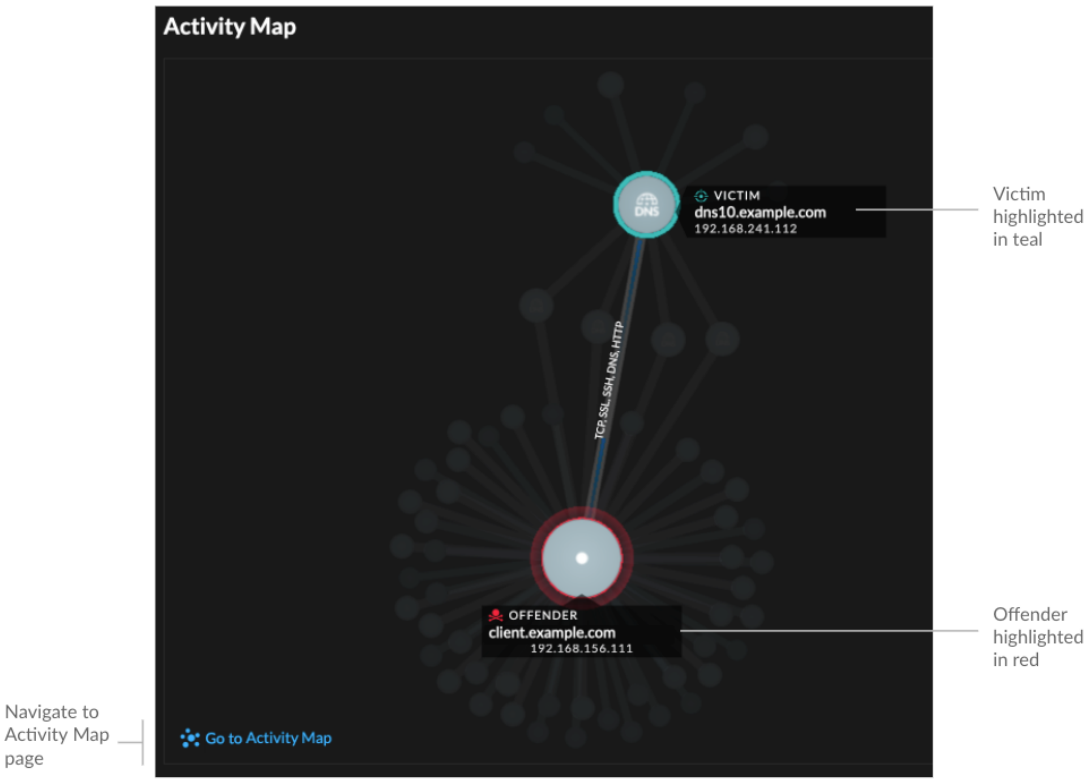
Propriétés de détection

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 essentiel à la détection.



Carte des activités

Fournit un 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 pour 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 vers 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 relatives aux transactions et un lien vers un 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 une table d'enregistrements, cliquez sur l'icône pour afficher la requête de paquet associée à une transaction.

Note: UN espace de stockage des enregistrements doit être configuré pour afficher les transactions et continuer 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 de détection. Le graphique apparaît pour les détections liées à une activité non conventionnelle d'un équipement et met en évidence les comportements inattendus en les affichant à côté du comportement des appareils du réseau présentant des propriétés similaires.

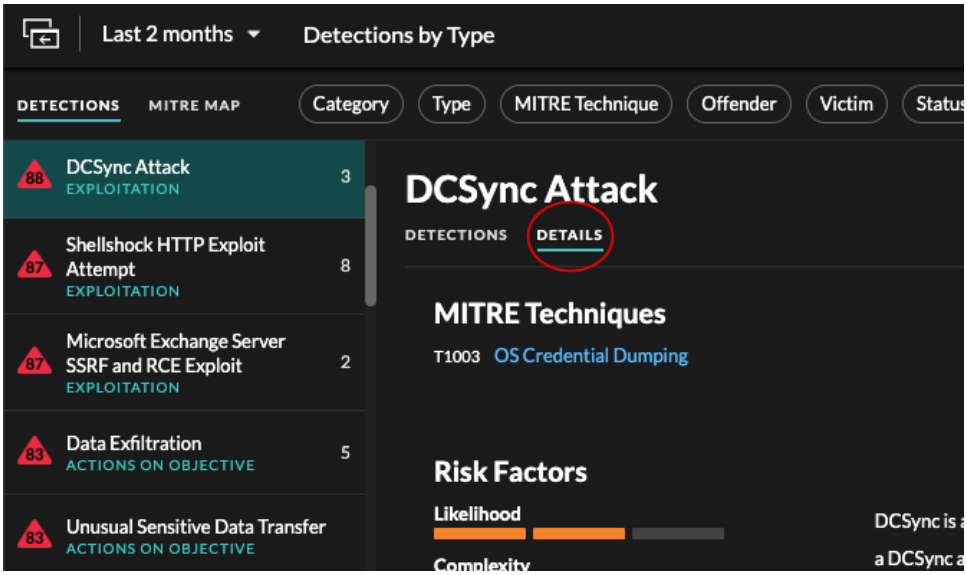
Détections associées

Fournit une chronologie des détections liées à la détection en cours qui peut vous aider à identifier une campagne d'attaque de plus grande envergure. 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 de détails de cette détection.

Détails de la 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, ainsi que des liens de référence vers des organisations de sécurité telles que MITRE.

Ces informations sont affichées à côté de la carte de détection sur des écrans larges (1900 pixels ou plus), ou vous pouvez y accéder en cliquant **Détails** sous le titre de la détection lorsque vous regroupez la page de détection par **Types**.

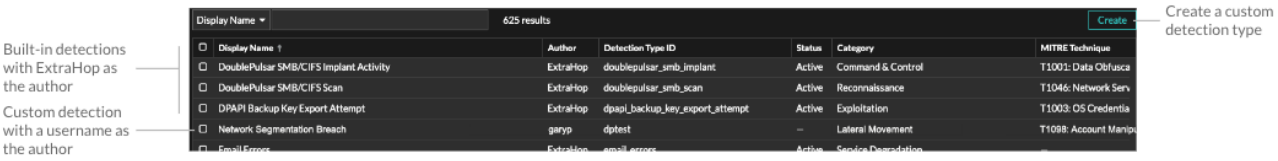


Conseil Vous pouvez détection des partages pages de détails avec d'autres utilisateurs d'ExtraHop.

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 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 (Reveal (x) 360 uniquement).
- Les systèmes Reveal (x) 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.

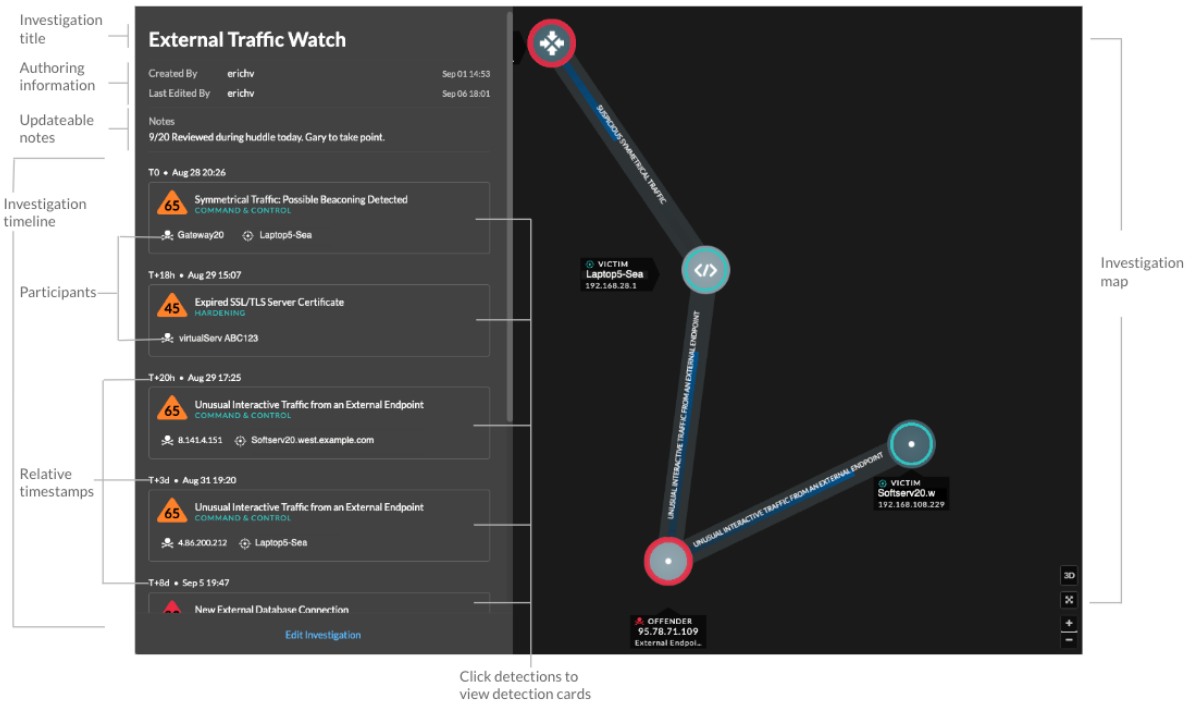
Détections personnalisées

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 dans une chronologie et une carte uniques. L'affichage d'une carte des détections connectées peut vous aider à déterminer si un comportement suspect constitue une menace valide et si une menace provient d'une attaque unique ou s'inscrit dans le cadre d'une campagne d'attaque plus vaste.



Vous pouvez créer et ajouter des enquêtes à partir de la page détaillée de la détection ou du menu Actions de chaque fiche de détection.

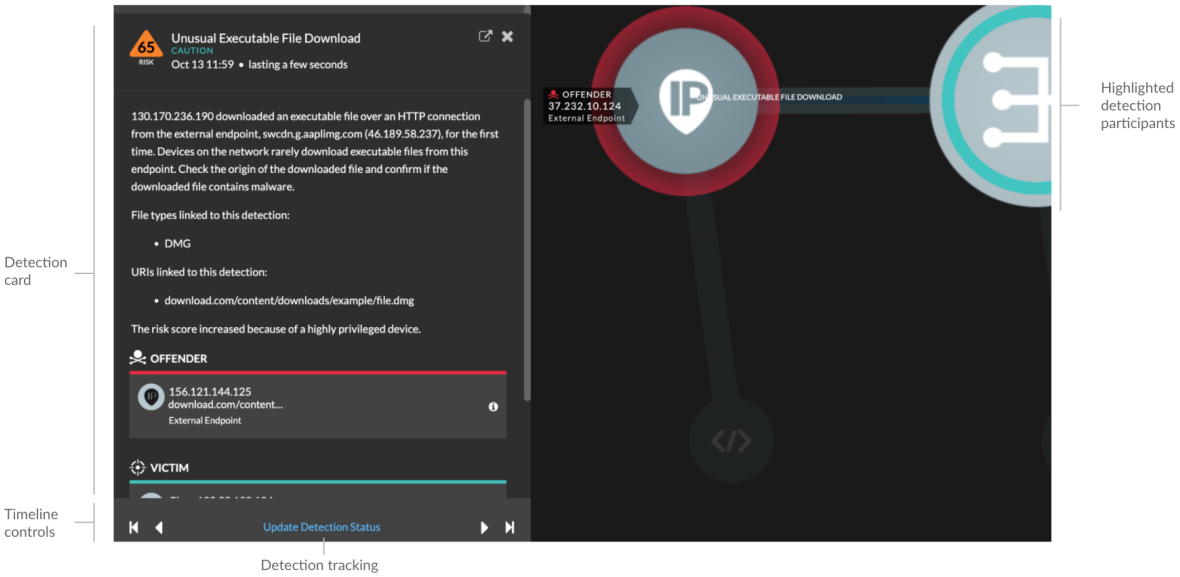
Chaque page d'investigation inclut les outils suivants :

Chronologie de l'enquête

La chronologie apparaît sur le côté gauche de la page et répertorie les détections ajoutées par ordre chronologique. Les nouvelles détections ajoutées apparaissent dans la chronologie en fonction de l'heure et de la date de la détection et par rapport à la détection la plus ancienne, qui est étiquetée T0. Les participants à la détection sont affichés sous le titre de la détection et les informations de suivi de la détection, telles que le responsable et le statut, sont affichées à côté des participants.

Cliquez sur une détection dans la chronologie pour afficher carte de détection et mettez en évidence les participants à la détection sur la carte d'investigation. Cliquez sur un participant sur la carte ou sur la carte d' investigation pour afficher les informations de base et les liens vers la page de présentation de l'appareil et d'autres détections impliquant l'équipement.

Dans le coin supérieur droit de la carte de détection, cliquez sur le bouton Accéder à icône pour afficher le page détaillée de détection, ou **x** icône pour fermer la détection et revenir à la chronologie de l'investigation.



Sous la carte de détection, cliquez sur **Détection de pistes** pour modifier suivi des détections informations. Vous pouvez cliquer sur les commandes de chronologie pour voir les autres détections au cours de l'investigation.

Carte d'enquête

La carte d'investigation affiche le délinquant et la victime à chaque détection au cours de l'enquête. Les participants sont connectés par des lignes étiquetées avec le type de détection, et les rôles des équipements sont représentés par une icône.

- Cliquez sur une détection dans la chronologie de l'investigation pour mettre en évidence les participants. Les cercles sont surlignés en rouge si l'équipement est l' auteur de l'infraction et en bleu sarcelle s'il est la victime. Les points saillants sont mis à jour lorsque vous cliquez sur une autre détection pour vous aider à identifier lorsqu'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 de l'équipement, l'adresse IP ou l'adresse MAC, ou pour accéder aux détections associées ou à Page de présentation de l'appareil.
- Passez le pointeur de la souris sur un cercle ou une ligne pour afficher l'étiquette.

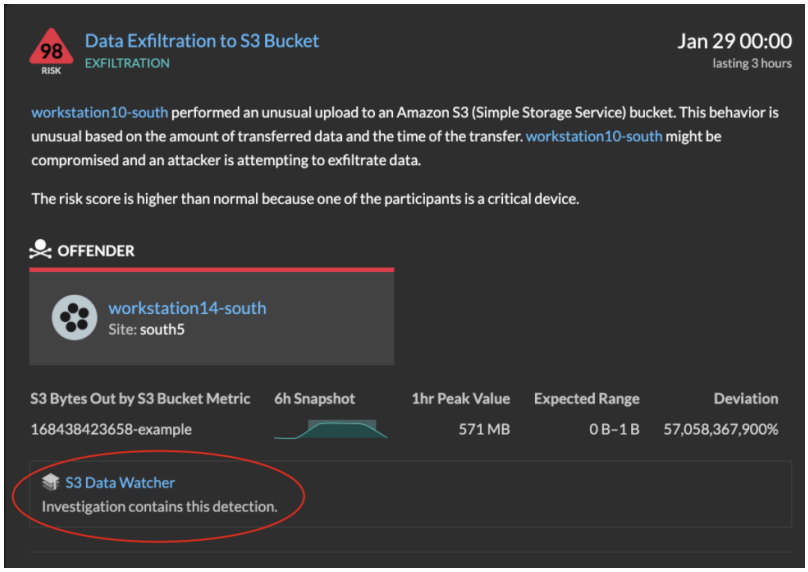
Remarques

Cliquez **Modifier l'enquête** pour ajouter des notes ou modifier le nom de l'investigation. Vous pouvez continuer à suivre les détections individuelles après les avoir ajoutés à une investigation.

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.

Trouver des 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 le système ExtraHop.

Note: Les détections restent dans le système en fonction de votre capacité de rétrospective du système pour les métriques d'une heure, avec une durée de stockage minimale de cinq semaines. Les détections resteront dans le système sans mesures prises en compte si la capacité rétrospective de votre système est inférieure à cinq semaines.

- Sur la page de présentation de l'appareil, 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 du groupe dequipment en tant que source.
- Sur la page de protocole d'un équipement ou d'un groupe d'équipements, cliquez sur le lien Détections pour accéder à la page Détections. La liste des détections est filtrée en fonction de la source et du protocole.
- Sur une carte dlai d'activités, cliquez sur un équipement qui affiche des pulsations 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.