Enquêtes

Publié: 2025-03-28

(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 et compléter des enquêtes à partir d'une page détaillée de détection, la **Actions** menu sur un carte de détection individuelle, ou le **Actions groupées** menu sur un résumé de la 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

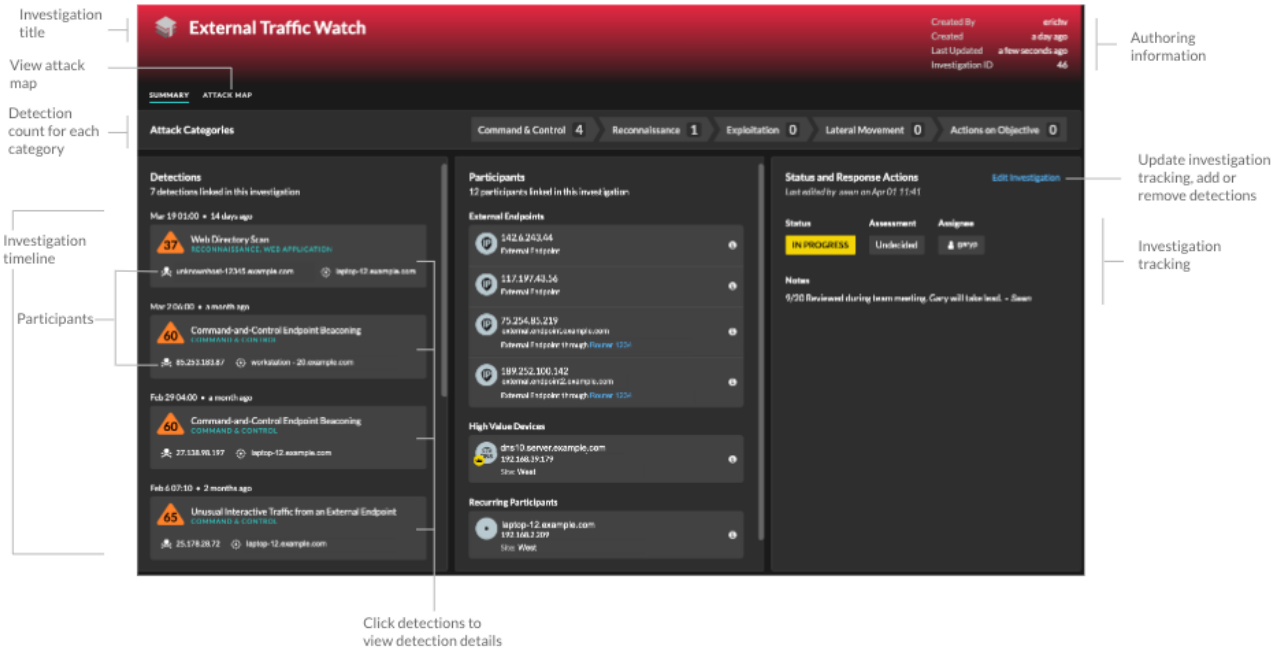
En haut de la page d'enquête, deux options permettent de visualiser l' enquête : Résumé et Carte des attaques. Les deux options offrent une vision unique de votre enquête.

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.

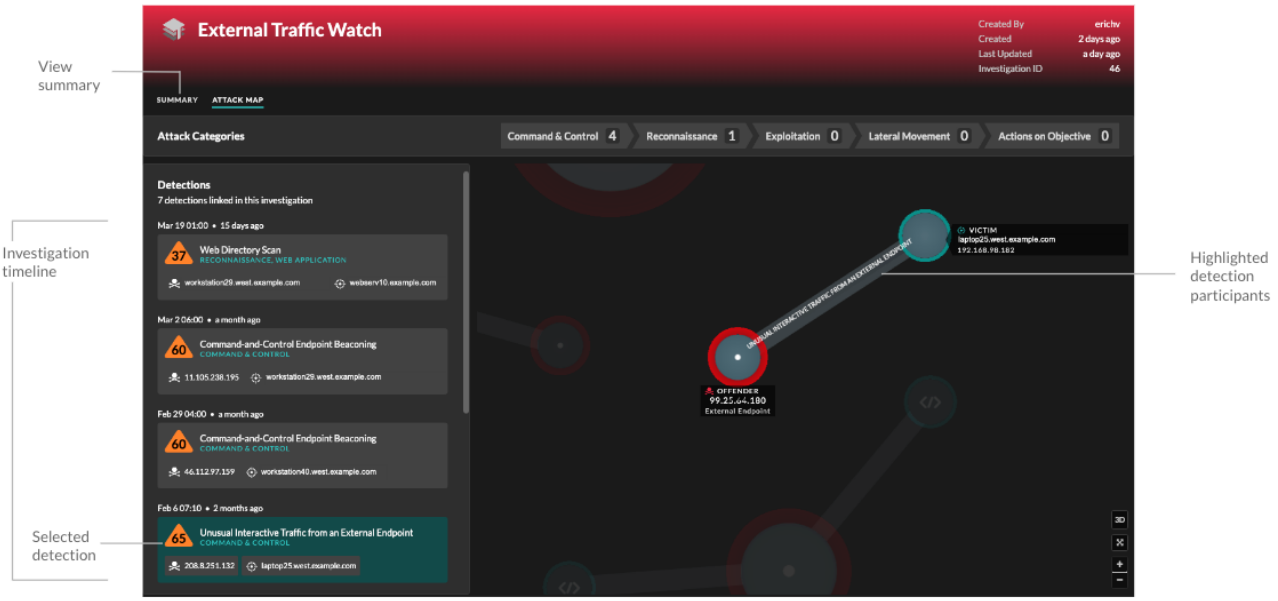


Dans le État et mesures de réponse panneau, cliquez sur **Modifier l'enquête** pour modifier le nom de l'enquête, définir le statut ou l'évaluation finale de l'enquête, spécifier un cessionnaire ou ajouter des notes.

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.



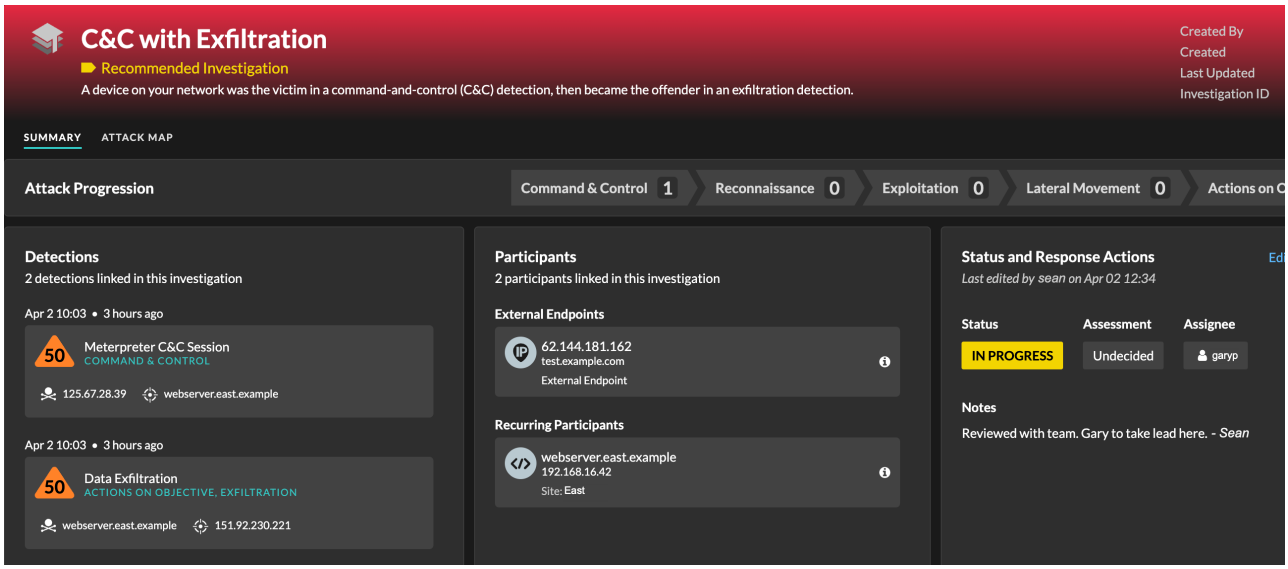
Les participants sont connectés par des lignes étiquetées selon le type de détection et les rôles des équipements sont représentés par une icône.

- 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.



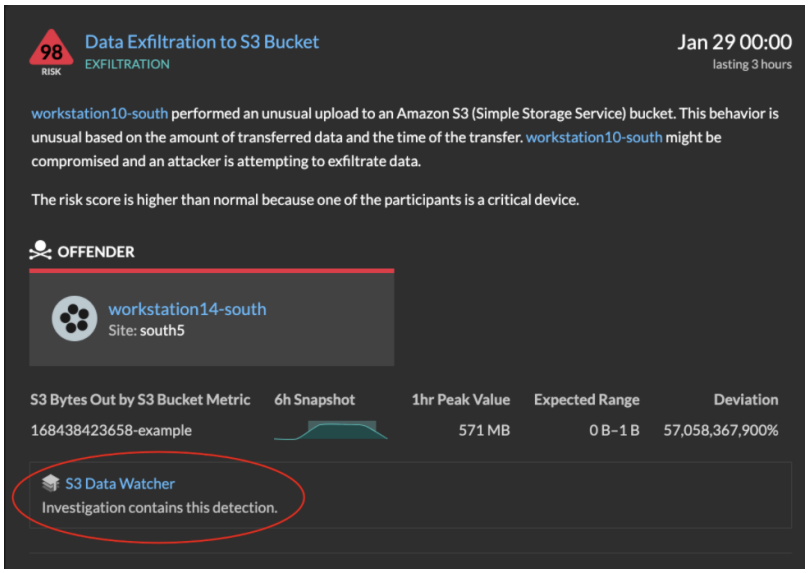
Vous pouvez interagir avec les enquêtes recommandées de la même manière que les enquêtes créées par les utilisateurs, par exemple en ajoutant ou en supprimant des détections, en spécifiant un destinataire et en définissant un statut et une évaluation.

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.