Créer une investigation

Publié: 2025-02-12

Créez une investigation pour visualiser plusieurs détections sur une seule chronologie et une seule carte.

Vous pouvez accéder à la liste des enquêtes créées dans le vue des enquêtes sur 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 d'une 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. Vous pouvez également définir le statut de l'investigation et l'attribuer à un utilisateur d'ExtraHop.
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 investigation à partir d'un résumé des détections

Publié: 2025-02-12

Vous pouvez ajouter plusieurs détections à une investigation 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 Résumé de la page Détections.

Pour ajouter un groupe de détections à une investigation 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 Résumé avec les détections regroupées par type. Si la page n'est pas en mode Résumé, cliquez sur Vue récapitulative puis 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, localités du réseau ou utilisateurs.
5. Dans le coin inférieur gauche du panneau récapitulatif, cliquez sur le **Actions groupées** menu déroulant, puis sélectionnez **Ajouter toutes les détections à une enquête**.
6. Spécifiez l'endroit où vous souhaitez ajouter les détections.
   - Cliquez **Ajouter des détections à une nouvelle investigation** pour créer une nouvelle enquête.
   - Cliquez **Ajouter des détections à une enquête existante** puis sélectionnez l'investigation à laquelle vous souhaitez ajouter les détections.
7. Cliquez **Suivant**.

Prochaines étapes
Si vous avez créé une nouvelle investigation, saisissez un nom et ajoutez des notes. Vous pouvez également définir le statut et attribuer l'investigation à un utilisateur d'ExtraHop. Si vous avez ajouté les détections à une enquête existante, vérifiez le nom, le statut, le destinataire et les notes pour vous assurer qu'ils reflètent vos modifications.