

Créer une investigation

Publié: 2025-01-05

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.