Create an investigation

Published: 2025-01-14

Create an investigation to view multiple detections in a single timeline and map.

You can access the list of created investigations in the investigations view on the Detections page.

Before you begin

- Users must be granted NDR module access and have limited-write privileges or higher to complete the tasks in this guide.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. At the top of the page, click **Detections**.
3. Click **Actions** from the lower-left corner of a detection card.
4. Click **Add to an Investigation...**.
5. Select **Add detection to a new investigation**.
6. Click **Next**.
7. Type a name and add notes to the new investigation. You can also set the status of the investigation and assign it to an ExtraHop user.
8. Click **Create**.

After the investigation name appears at the bottom of the detection card, you can click the investigation name to view the timeline and map.

- To add a detection to the investigation, click **Actions**, and then click **Add to an Investigation...**.
- To delete a detection from an investigation, click the delete icon (X) on the detection in the investigation timeline.

Create an investigation from a detection summary

Published: 2025-01-14

You can add multiple detections to an investigation at the same time from a summary panel on the Detections page.

A summary panel appears when detections are grouped by Type in Summary view on the Detections page.

To add a group of detections to an investigation from a detection summary, complete the following steps:

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. At the top of the page, click **Detections**.

   By default, the page should be in Summary view with detections grouped by Type. If the page is not in Summary view, click Summary view ↗ and then group by Type ↗.
3. Click a detection type in your detections list.
4. Click the criteria you want to filter by: participants, properties, network localities, or users.
5. In the lower left corner of the summary panel, click the **Bulk Actions** drop-down menu, and select **Add All Detections to an Investigation**.
6. Specify where you want to add the detections.

   - Click **Add detections to a new investigation** to create a new investigation.
   - Click **Add detections to an existing investigation** then select the investigation where you want to add the detections.
7. Click **Next**.

Next steps
If you created a new investigation, type a name, and add notes. You can also set the status and assign the investigation to an ExtraHop user. If you added the detections to an existing investigation, review the name, status, assignee, and notes to make sure they reflect your changes.