Create an investigation

Published: 2024-04-02

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

You can access the list of created investigations from the **Investigations** icon in the upper right corner of the Detections page.

Before you begin

- Users must be granted NDR module access and have limited-write privileges IP 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 the 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.
- 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.