Track a detection

Published: 2024-04-01

Detection tracking enables you to assign users, set a status, and add notes to a detection card.

You can also filter your view of detections by specific status or assignee.

Before you begin
Users must have limited write privileges or higher to complete the tasks in this guide.

Here are important considerations about tracking detections:

- The Acknowledged or Closed status does not hide the detection.
- The detection status can be updated by any privileged user.
- Optionally, you can configure detection tracking with a third-party system.
- If you are currently tracking detections with a third-party system, you will not see ExtraHop detection tracking until you change the setting in the Administration settings.

To track a detection, 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**.
3. Click **Actions** from the lower-left corner of the detection card.
4. Optional: Click a detection status to add it to the detection.

Option	Description
Acknowledge	The detection has been seen and should be prioritized for follow-up.
In Progress	The detection has been assigned to a team member and is being reviewed.
Closed - Action Taken	The detection was reviewed and action was taken to address the potential risk.
Closed - No Action Taken	The detection was reviewed and required no action.

5. Click **Update Status...** to set the detection status, assign the detection to a user, and add notes to the detection card.

From the **Actions** dropdown, select **Update Status...** and then **None** to remove the status from the detection; the assignee and notes remain visible.