Track a detection

Published: 2025-02-11

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.

Video the related training: Detection Tracking

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

You can change the assignee to any user in the system, add notes, and set the status on a detection to one of the following:

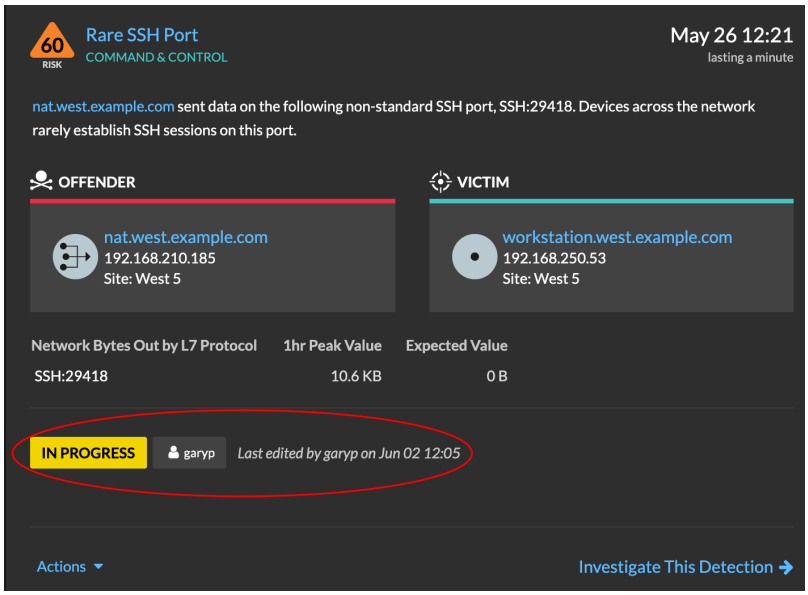
Open
The detection has not been reviewed.

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.



Here are important considerations about tracking detections:

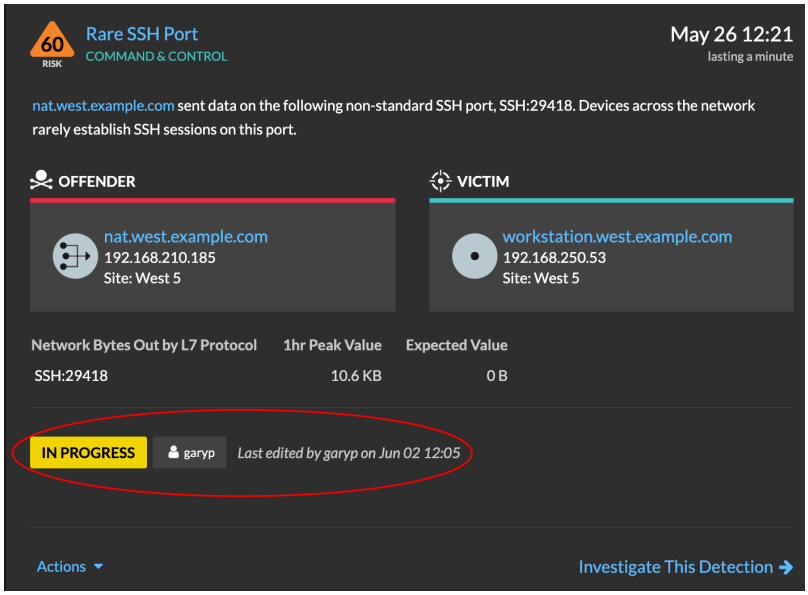
- The Acknowledged or Closed status does not hide the detection.
- The detection status can be updated by any privileged user.
- You can add detection tracking with ExtraHop and third-party systems in the Administration settings.

To track a detection, complete the following steps:

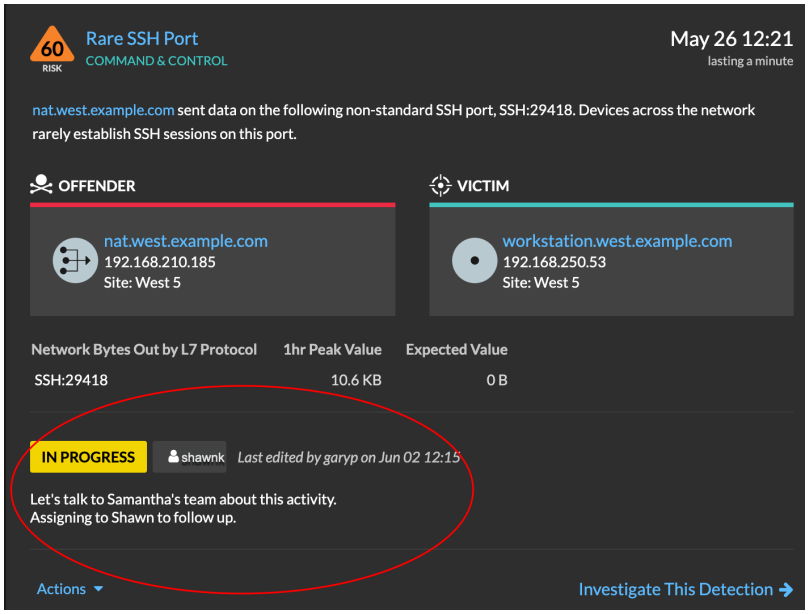
1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. At the top of the page, click **Detections**.

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 **Track Detection...** to set the detection status, assign the detection to a user, and add notes to the detection card.



From the **Actions** drop-down menu, select **Track Detection...** and then **Open** to remove the status from the detection; the assignee and notes remain visible.

Track a detection from a detection card

You can track a detection by adding an assignee, status, and notes from a detection card.

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

   From the **Actions** dropdown, select **Track Detection...** and then **Open** to remove the status from the detection; the assignee and notes remain visible.

Track a group of detections from a detection summary

You can apply a status, assignee, or note to multiple detections 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 track a group of detections 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 they are not, click the 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 **Track All Detections**.
6. Optional: Select the status you want to apply to all selected detections.
7. Optional: Select the assignee you want to apply to all selected detections.
8. Optional: Select whether you want to add a new note to the existing notes of the selected detections, or overwrite all existing notes.

   When adding your note to existing notes, the new note is added above existing notes.
9. Click **Save**.