

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.

▶ **View** 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.

The screenshot shows a detection card for 'Rare SSH Port' with a risk level of 60. The card includes the following information:

- Title:** Rare SSH Port (COMMAND & CONTROL)
- Time:** May 26 12:21 (lasting a minute)
- Description:** nat.west.example.com sent data on the following non-standard SSH port, SSH:29418. Devices across the network rarely establish SSH sessions on this port.
- Offender:** nat.west.example.com (192.168.210.185, Site: West 5)
- Victim:** workstation.west.example.com (192.168.250.53, Site: West 5)
- Network Bytes Out by L7 Protocol:** SSH:29418
- 1hr Peak Value:** 10.6 KB
- Expected Value:** 0 B
- Status:** IN PROGRESS (highlighted with a red circle)
- Assignee:** garyp
- Last Edited:** Last edited by garyp on Jun 02 12:05
- Actions:** Investigate This Detection

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**.

- Click **Actions** from the lower-left corner of the detection card.
- 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.

The screenshot shows a detection card for 'Rare SSH Port' with a risk level of 60 (Command & Control). The detection occurred on May 26 at 12:21, lasting a minute. The description states that nat.west.example.com sent data on a non-standard SSH port (SSH:29418). The card identifies an offender (nat.west.example.com) and a victim (workstation.west.example.com). A table shows network bytes out by L7 protocol for SSH:29418, with a 1hr peak value of 10.6 KB and an expected value of 0 B. The status is 'IN PROGRESS', assigned to user garyp, and last edited on Jun 02 at 12:05. An 'Actions' dropdown and an 'Investigate This Detection' link are visible at the bottom.

60 RISK
Rare SSH Port
COMMAND & CONTROL

May 26 12:21
lasting a minute

nat.west.example.com sent data on the following non-standard SSH port, SSH:29418. Devices across the network rarely establish SSH sessions on this port.

OFFENDER

nat.west.example.com
192.168.210.185
Site: West 5

VICTIM

workstation.west.example.com
192.168.250.53
Site: West 5

Network Bytes Out by L7 Protocol	1hr Peak Value	Expected Value
SSH:29418	10.6 KB	0 B

IN PROGRESS garyp Last edited by garyp on Jun 02 12:05

Actions ▾ Investigate This Detection →

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

60 RISK
Rare SSH Port
COMMAND & CONTROL

May 26 12:21
lasting a minute

nat.west.example.com sent data on the following non-standard SSH port, SSH:29418. Devices across the network rarely establish SSH sessions on this port.

OFFENDER

nat.west.example.com
192.168.210.185
Site: West 5

VICTIM

workstation.west.example.com
192.168.250.53
Site: West 5

Network Bytes Out by L7 Protocol	1hr Peak Value	Expected Value
SSH:29418	10.6 KB	0 B

IN PROGRESS shawnk Last edited by garyp on Jun 02 12:15

Let's talk to Samantha's team about this activity.
Assigning to Shawn to follow up.

Actions ▾ Investigate This Detection →

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**.