

Track a detection

Published: 2022-01-05

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 system 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.

60 Rare SSH Port
RISK 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	VICTIM
 nat.west.example.com 192.168.210.185 Site: West 5	 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 **Update Status...** to set the detection status, assign the detection to a user, and add notes to the detection card.

The screenshot shows a detection card for 'Rare SSH Port' with a risk level of 60 (RISK) and a category of 'COMMAND & CONTROL'. The detection occurred on May 26 at 12:21, lasting a minute. The description states: '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.'

The card is divided into two sections: OFFENDER and VICTIM.

- 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

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

The status is **IN PROGRESS**, assigned to user shawnk, and last edited by garyp on Jun 02 12:15. A note reads: 'Let's talk to Samantha's team about this activity. Assigning to Shawn to follow up.'

Actions dropdown is visible at the bottom left, and 'Investigate This Detection' link is at the bottom right.

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