Track a detection investigation

Published: 2021-08-31

Investigation tracking enables you to track how a detection is reviewed and resolved with the ExtraHop system.

You can set an investigation status for a detection, assign the investigation to yourself or another ExtraHop user, and add notes about the investigation. You can also filter your view of detections to show detections with a specific investigation status or assignee.

Before you begin
Users must have limited write privileges or higher to set a detection status, assign a detection, or leave investigation notes.

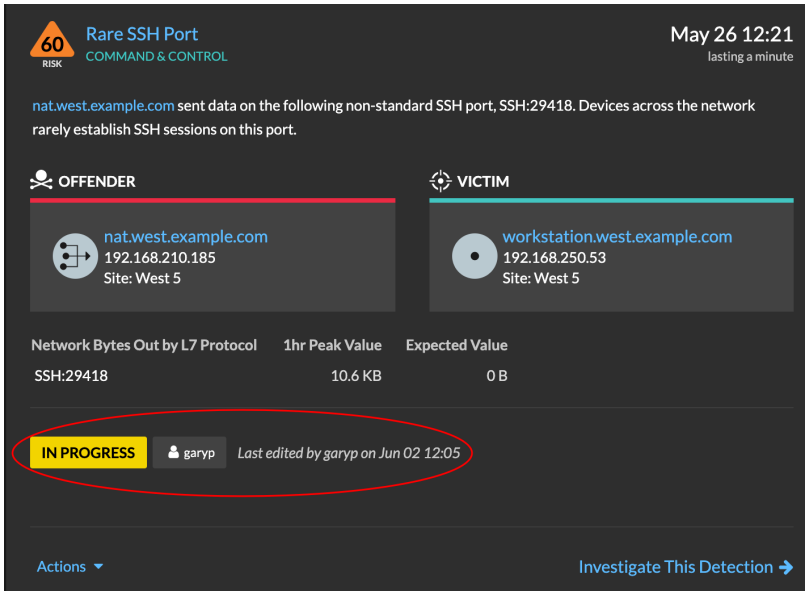
Here are important considerations about tracking detection investigations:

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

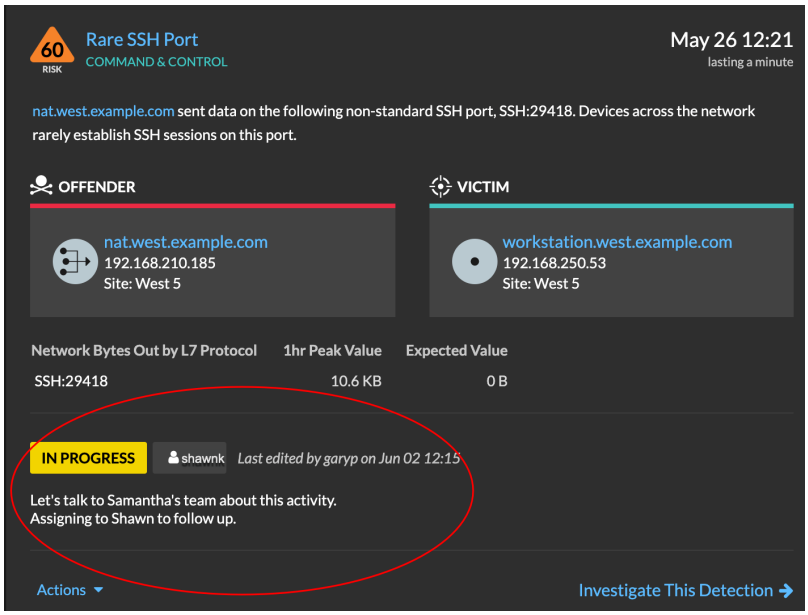
To track an investigation, complete the following steps:

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 an investigation 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 investigated and action was taken to address the potential risk.
Closed - No Action Taken	The detection was investigated and required no response.



5. Click **Track Investigation...** to set the investigation status, assign the investigation to a user, and add notes that are displayed on the detection.



Selecting **None** in the Track Investigation dialog box removes the status from the detection, but the previously added assignee and investigation notes remain visible.