

Investigations

Published: 2025-04-04

(NDR module only) Investigations enable you to add and view multiple detections in a single timeline and map. Viewing a summary of connected detections can help you determine whether suspicious behavior is a valid threat and if a threat is from a single attack, or part of a larger attack campaign.

You can create and add to investigations from a detection detail page, the **Actions** menu on an **individual detection card** [🔗](#), or the **Bulk Actions** menu on a **detection summary** [🔗](#). Your ExtraHop system will also create **recommended investigations** through Smart Investigations, which are investigations automatically created in response to potentially malicious activity.

Each investigation page includes the following tools:

Investigation Timeline

The investigation timeline appears on the left side of the page and lists the added detections, beginning with the most recent detection. New detections that are added to the investigation appear in the timeline according to the time and date the detection occurred. Detection participants are displayed under the detection title and detection tracking information, such as assignee and status, is displayed next to the participants.

Attack Categories

The categories of the added detections are displayed across the top of the investigation page.

The attack category chain displays the number of detections in each category, not the order in which the detections occurred. Refer to the investigation timeline for an accurate view of how the detections occurred over time.

Viewing investigations

At the top of the investigation page, there are two options for viewing the investigation: Summary and Attack Map. Both options provide a unique view of your investigation.

Summary

By default, investigations open in **Summary** view, which includes the detection timeline, an aggregated list of participants, and a panel for tracking the status and response actions for the investigation.

You can click a detection in the investigation timeline to view **detection details** [🔗](#), then click the x icon to close the detection details and return to the investigation summary. You can also click the go to [🔗](#) icon in the upper right corner to view the detection details page in a new tab.

In the Participants panel, participants in the investigation are grouped by external endpoints, high value devices, and recurring participants, which are participants that appear in multiple detections in the investigation. Click on a participant to view details and access links.

Investigation title

View attack map

Detection count for each category

Investigation timeline

Participants

Click detections to view detection details

Authoring information

Update investigation tracking, add or remove detections

Investigation tracking

In the Status and Response Actions panel, click **Edit Investigation** to change the investigation name, set the status or final assessment of the investigation, specify an assignee, or add notes.

You can continue to [track individual detections](#) after you add them to an investigation.

Attack Map

In **Attack Map** view, the offender and victim from every detection in the investigation are displayed in an interactive map next to the investigation timeline.

View summary

Investigation timeline

Selected detection

Highlighted detection participants

The participants are connected by lines that are labeled with the detection type, and device roles are represented by an icon.

- Click a detection in the investigation timeline to highlight participants. Circles are highlighted in red if the device has appeared as an offender in at least one detection in the investigation and

are highlighted in teal if the device is a victim. Highlights are updated when you click a different detection to help you identify when a participant changes from victim to offender.

- Click a circle to view details such as the device hostname, IP address, or MAC address, or to navigate to associated detections or the [Device Overview page](#).
- Hover over any circle or line to display the label.

Recommended investigations

The ExtraHop Machine Learning Service monitors network activity for combinations of attack techniques that might indicate malicious behavior. When a combination is identified, the ExtraHop system will create a recommended investigation, enabling your security teams to assess the situation and respond quickly if malicious behavior is confirmed.

For example, if a device is the victim in a detection in the Command-and-Control category, but becomes the offender in an Exfiltration detection, the ExtraHop system will recommend a C&C with Exfiltration investigation.

The screenshot displays the 'C&C with Exfiltration' investigation page. At the top, it states 'Recommended Investigation' and provides a summary: 'A device on your network was the victim in a command-and-control (C&C) detection, then became the offender in an exfiltration detection.' The page is divided into three main sections: 'Attack Progression', 'Participants', and 'Status and Response Actions'.

Attack Progression: Shows a sequence of steps: Command & Control (1), Reconnaissance (0), Exploitation (0), Lateral Movement (0), and Actions on C (0).

Detections: Lists two detections linked in this investigation:

- Meterpreter C&C Session (COMMAND & CONTROL):** Occurred on Apr 2 10:03, 3 hours ago. Severity 50. Involved IP 125.67.28.39 and host webserver.east.example.
- Data Exfiltration (ACTIONS ON OBJECTIVE, EXFILTRATION):** Occurred on Apr 2 10:03, 3 hours ago. Severity 50. Involved host webserver.east.example and IP 151.92.230.221.

Participants: Lists two participants linked in this investigation:

- External Endpoints:** IP 62.144.181.162 (test.example.com), labeled as an External Endpoint.
- Recurring Participants:** webserver.east.example (192.168.16.42), labeled as Site: East.

Status and Response Actions: Shows the investigation status as 'IN PROGRESS' (yellow button) and 'Undecided' (grey button). The assignee is 'garyp'. A note indicates: 'Reviewed with team. Gary to take lead here. - Sean'.

You can interact with recommended investigations in the same way as user-created investigations, such as adding or removing detections, specifying an assignee, and setting a status and assessment.

Recommended investigations can be found in the [investigations table](#). You can sort the Created By column to find investigations that were created by ExtraHop.

Navigating investigations

After a detection is added to an investigation, a link to the investigation appears at the bottom of the detection card and on the detection detail page.

Click the name to open the investigation and then click the name of the detection on the investigation page to return to the detection detail page.

98

RISK

Data Exfiltration to S3 Bucket


EXFILTRATION


Jan 29 00:00
lasting 3 hours


`workstation10-south` performed an unusual upload to an Amazon S3 (Simple Storage Service) bucket. This behavior is unusual based on the amount of transferred data and the time of the transfer. `workstation10-south` might be compromised and an attacker is attempting to exfiltrate data.

The risk score is higher than normal because one of the participants is a critical device.

OFFENDER

 `workstation14-south`
Site: south5

S3 Bytes Out by S3 Bucket Metric	6h Snapshot	1hr Peak Value	Expected Range	Deviation
168438423658-example		571 MB	0 B - 1 B	57,058,367,900%

 S3 Data Watcher

Investigation contains this detection.

Learn how to [create an investigation](#).