Threat briefings

Published: 2024-04-02

Threat briefings provide guidance about potential threats to your network.

Threat briefings cover the following occurrences:

- Industry-wide security events, where the ExtraHop system surfaces detections related to known compromises.
- Security Analysis Briefings, which provide machine-learning analysis that is specific to your network.
- (Reveal(x) 360 only.) Retrospective Threat Analysis Briefings, which detect new indicators of compromise in updated ExtraHop-curated threat intelligence collections.

Threat briefings contain detections of scans, exploits, and indicators of compromise (IOC) that are related to the threat. The information in each briefing varies depending on the type of threat. Information related to the briefing is cloud-updated as details emerge about IOC, potential attack vectors, and known risks.

Threat briefings are available from the top-left corner of the Security Overview page. Click any title to go to the detail page for that briefing. The detail page is updated as more information is discovered.

Here are some ways you can keep track of threat briefings:

- Create a threat briefing notification rule to receive emails when a new threat briefing appears.
- Click **Create Investigation** from the detail page to add the detections associated with the briefing to an investigation.
- Click **Archive Briefing** from the detail page when you no longer want to monitor the briefing; the briefing is automatically restored and a notification email is sent if the briefing is updated. You can view older briefings in the Archived section on the Threat Briefing page. Click **Restore Briefing** on the detail page to move the briefing back to the Active section of the Threat Briefing page.