Security Overview

Published: 2022-12-29

The Security Overview displays several charts that highlight data from different perspectives about detections. These charts can help you evaluate the scope of security risks, launch investigations into unusual activity, and mitigate security threats. Detections are analyzed every 30 seconds or every hour, depending on the metric.

Site Selector

Click the site selector at the top of the page to view data for one or more sites in your environment. View combined traffic across your networks or focus on a single site to help you quickly find device data.

The site selector indicates which sites are flow sensors and when all or some sites are offline. Because data is not available from offline sites, the charts and device pages associated with offline sites might not show data or might only show limited data. The site selector is available from consoles only.

Executive Report

Click **Generate Executive Report** to create a PDF file. The Executive Report provides a summary of the top detections and risks to your network from the last week. The Executive Report only includes information for the selected sites.

Open Detections

This chart shows you a list of detections with a status other than Closed, sorted by highest risk. Click a detection to view open detections of the selected detection type. Each detection card summarizes what caused the detection; click the detection name to open the detection detail page.

Detection Types

This chart shows you the number of distinct detection types that occurred in the Attack, Hardening, and Operations categories during the selected time interval. By changing the time interval, you can see how many detection types occurred during that time. Click a number to open the Detections page filtered to show detections for each type in the selected detection category.

Detections by Attack Category

This chart provides a quick way to see the types of attacks your network might be at risk for and displays the number of detections that occurred in each category during the selected time interval. Actions on Objective detections are listed by type to help you prioritize the most severe detections. Click any number to open a filtered view of detections that match the selected attack category.

Top Offenders

This chart shows the top 20 devices or endpoints that acted as offenders in one or more detections. The ExtraHop system considers the number of distinct attack categories and detection types and the risk scores of the detections associated with each device to determine which devices are considered top offenders.

The size of the device role icon indicates the number of distinct detection types and the position of the icon indicates the number of distinct attack categories. Click a role icon to view more information about the attack categories and detection types associated with the device. Click the device name to view device properties.

Learn more about network security with the Security Hardening dashboard.

Threat briefings

Threat briefings provide cloud-updated guidance about industry-wide security events. Learn more about threat briefings.