Security Overview

Published: 2021-08-27

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 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 Command appliances and Reveal(x) 360 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.

Attack Detections

This count chart shows you the number of attack category detections that occurred during the selected time interval. By changing the time interval, you can see how many detections occurred during that time. Click the number to open the Detections page. Learn more about detections.

Detections by Attack Category

This chart provides a quick way to see the types of attacks your network might be at risk for. Click any number to open a filtered view of detections that match the selected attack category, and continue your investigation.

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.

Detections by Risk Score

This chart shows you a gradient view of how many detections are in each risk level.

Top Detections

This chart shows you a list of detections, sorted by highest risk. Click the number to open a filtered view of the selected detection. Each detection summarizes what caused the detection; click the detection name to open all detections of that type and begin your investigation.

Learn more about network security with the Security dashboard.

Threat Briefings

Threat briefings provide guidance about industry-wide security events. These briefings are cloud-updated as details emerge about indicators of compromise (IOC), potential attack vectors, and known risks.

Threat briefings contain detections of scans, exploits, and indicators of compromise that are related to the threat. The information in each briefing can vary depending on the type of attack.