

Network Overview

Published: 2024-04-02

The Network Overview displays a map of the detections on your network and a list of offenders by detection count. The Network Overview refreshes the detection map and offender data every minute.

 **View** the related training: [Security, Network, and Perimeter Overview](#) 



Detection category toggle

You can toggle between views that show **All Attack Detections** or **All Performance Detections**, depending on enabled modules and your module access.

Offenders in detections

This list shows offenders, sorted by the number of detections where the device or endpoint acted as an offender.

Here are some ways you can interact with the offenders list:

- Click a device or endpoint in the list to highlight associated detections in the detection map and view device properties and access links to [endpoint lookup](#)  sites, detections, records, or packets.
- Depending on the selected detection category and your system module, click the **View All Attack Detections** or **View All Performance Detections** link to go to the Detections page, [filtered by detection category and grouped by source](#) .
- Select the **Show detections with no victims** checkbox to display detections that do not include a victim participant. For example SSL/TLS Scans and certain caution detections for suspicious activity only include an offender.


Detection map

The detection map displays the offender and victim for all detections selected in the detection category toggle.

Circles are highlighted in red if the device has appeared as an offender in at least one detection during the selected time interval and are highlighted in teal if the device is a victim.

The participants are connected by lines that are labeled with the detection type or number of detections associated with the connection, and device roles are represented by an icon.

Here are some ways you can interact with the detection map:

- Click a circle to view device properties and access links to [endpoint lookup](#)  sites, detections, records, or packets.
- Click a connection to view associated detections.
- Hover over a circle to see device labels and highlight device connections.

Learn more about [Detections](#) .

Site selector and executive report

You can specify the sites you want to view data from on this page. Users with NDR module access can generate an executive report to share results.

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 only available from a console.

(NDR module only) Executive Report

The Executive Report contains a summary of the top detections and risks to your network. Click **Generate Report** to create a PDF file on demand that contains a summary of the last week from the selected sites. Click **Schedule Report** to [create a scheduled Executive Report](#) that contains a detection summary from a specified time interval and is emailed to recipients according to a configured frequency.