Security dashboard

Published: 2020-12-02

Monitor general information about potential security threats on your network.

The Security dashboard is a built-in, system dashboard, and you cannot edit, delete, or add a system dashboard to a collection. However, you can copy a chart from a system dashboard and add it to a custom dashboard, or you can make a copy of the dashboard and edit it to monitor metrics that are relevant to you.

Each chart in the Security dashboard contains visualizations of protocol metric data, organized by region. The following information summarizes each region and its charts.

Security Overview

Click the links to visit the Security Overview page, which can help you evaluate the scope of a suspicious activity on your network. The Security Overview page dynamically displays high-risk detections, trending security metrics, and rotating activity maps that display network activity by protocol.

Note: Machine learning detections require a connection to ExtraHop Cloud Services.

Alerts

See which alerts were issued most recently in your environment. For more information about configuring and interpreting alerts, see Alerts.

Threat Intelligence

See the number of connections and transactions that contain suspicious hostnames, IP addresses, or URIs found in threat intelligence. Click a blue metric value or metric name in the legend to drill down on a suspicious metric. A detail page appears that displays a red camera icon next to the suspicious object. Click the red camera icon to learn about the threat intelligence source.

Note: Threat intelligence metrics display a zero value for one or more of the following reasons:

- Your Reveal(x) subscription does not include threat intelligence. Threat intelligence requires a Reveal(x) Premium or Ultra subscription.
- You have not enabled threat intelligence for your Reveal(x) system.
- You have not directly uploaded custom threat collections to your sensors (Discover appliances). Contact ExtraHop Support for help uploading a custom threat collection to you ExtraHop-managed sensors.
- No suspicious objects were found.

SSL - Weak Ciphers

See the number of active SSL sessions with weak cipher suites on your network. You can also see which clients and servers are participating in those sessions along with which cipher suites those sessions are encrypted with. DES, 3DES, MD5, RC4, null, anonymous, and export cipher suites are considered to be weak because they include an encryption algorithm that is known to be vulnerable. Data encrypted with a weak cipher suite is potentially insecure.

SSL - Certificates

See which SSL certificates in your network are self-signed, wildcard, expired, and expiring soon. Self-signed certificates are signed by the entity that issues the certificate, rather than a trusted certificate authority. Although self-signed certificates are cheaper than certificates issued by a certificate authority, they are also vulnerable to man-in-the-middle attacks.

A wildcard certificate applies to all first-level subdomains of a given domain name. For example, the wildcard certificate *.company.com secures www.company.com, docs.company.com, and customer.company.com. Although wildcard certificates are cheaper than individual certificates,

wildcard certificates create a greater risk if they are compromised because they can apply to any number of domains.

Vulnerability Scans

See which devices are scanning applications and systems on your network to search for weaknesses and potential targets, such as high-value devices. In the left chart, you can identify which devices are sending the most scan requests, which are HTTP requests associated with known scanner activity. In the right chart, you can see which user-agents are associated with the scan requests. The user-agent can help you determine if scan requests are associated with known vulnerability scanners such as Nessus and Qualys.

DNS

See which DNS servers are most active on your network and the total number of reverse DNS lookup failures those servers have encountered. A reverse DNS lookup failure occurs when a server issues an error in response to a client request for a pointer (PTR) record. Failures in reverse DNS lookups are normal, but a sudden or steady increase in failures on a specific host might indicate that an attacker is scanning your network.

Note: In the ExtraHop Command appliance, you can display the Security dashboard for each Discover appliance. The appliance name appears in the navigation bar; click the down arrow next to the appliance name to pivot the display to other Discover appliances.