Security Hardening dashboard

Published: 2024-02-05

The Security Hardening dashboard enables you to monitor general information about potential security threats on your network.

Each chart in the Security Hardening dashboard contains visualizations of security data that have been generated over the selected time interval, organized by region.

Note: From a console, you can display the Security Hardening dashboard for each packet sensor. Click down arrow next to the name of the sensor in the navigation bar to display the Security Hardening dashboard for other sensors.

The Security Hardening dashboard is a built-in, system dashboard that you cannot edit, delete, or add to a shared collection. However, you can copy a chart from the Security Hardening 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.

The following information summarizes each region and its charts.

Threat Intelligence

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

SSL - Sessions

Observe the number of active SSL sessions with weak cipher suites on your network. You can 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.

You can also observe the number of SSL sessions established with TLS v1.0 and which clients are participating in those sessions. Known vulnerabilities are associated with TLS v1.0. If you have a high number of TLS v1.0 sessions, consider configuring servers to support the latest version of TLS.

SSL - Certificates

Observe 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.

© 2024ExtraHop Networks, Inc. All rights reserved.

Vulnerability Scans

Observe 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

Observe 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.

You can also observe the number of address mapping and text record queries on your network. A large or sudden increase in these types of queries can be an indicator of a potential DNS tunnel.