

Filter and Tune Hardening Detections

Published: 2024-03-26

Detections in the Hardening category help mitigate the risk of exploitation. You can triage a large number of hardening detections by filtering and tuning the Detections page.

Before you begin

Users must be granted [privileges](#) to view detections and must have full write or higher privileges to create a tuning rule.

Learn more about [tuning detections](#).

Learn about [tuning best practices](#).

Click a hardening detection from the [Detections](#) page to view the summary. Hardening detection summaries identify the detection type, the assets that are participants in detections of that type, the detection properties, and the network localities that contain affected assets.

The screenshot shows the 'Expiring SSL/TLS Server Certificate' detection details page. The page is divided into several sections:

- Detection type:** Expiring SSL/TLS Server Certificate
- Description:** These assets served an SSL/TLS certificate scheduled to expire soon. Renew certificates before they expire to ensure the availability of all services.
- Detection timestamp:** 8 Affected Assets

Asset	Timestamp
West 1500F	Nov 28 07:48
centralinformat.west.com	Nov 27 23:08
East 1234A	Nov 27 23:08
central.east.example.com	Nov 27 23:05
central.east.example.com	Nov 27 23:05
West 1500F	Nov 24 17:39
west.example.com	Nov 24 02:49
west.example.com	Nov 24 02:09
- Property values:** 5 Certificate Values

Certificate	Count
central.east.example.com:EX_12n34n...	2
west.example.com:EX_nnnnnnn5n67...	2
default cert:EX_nnn1234cert:01	2
midwest.example.com:EX_nnn5678cert	2
south.extrahop.com:EX_nnnnn1234c...	1
- Network localities:** 4 Affected Network Localities

Locality	Count
West	4
[east]: example - 159.91.144.132/28	2
South	2
Midwest	1

At the bottom, there is a 'View Detection' button and a 'Create a Tuning Rule' button. A callout box indicates that clicking a value above filters results and allows viewing individual detections.

Click any asset, property, or network locality value to view individual detections associated with that value.

Affected Assets

A list of assets that are participants in hardening detections of the selected type. The Affected Assets list is ordered by the most recent time that the detection occurred.

Property Values

A list of the key property values associated with the detection type. For example, the Weak Cipher Suite detection type lists the cipher suites referenced in detections, and the Expiring SSL/TLS Server Certificate detection lists certificates that are scheduled to expire. The Property Values list is ordered by the number of detections that contain the property value.

Affected Network Localities

A list of network localities that contain hardening detections of the selected type. The Affected Network Localities list is ordered by the number of detections in the network locality.

By filtering results on a single asset, property, or locality, you can identify detections that affect critical systems or [create a tuning rule](#) that hides low-value detections similar to the filtered results.