Filter and Tune Hardening Detections

Published: 2024-03-26

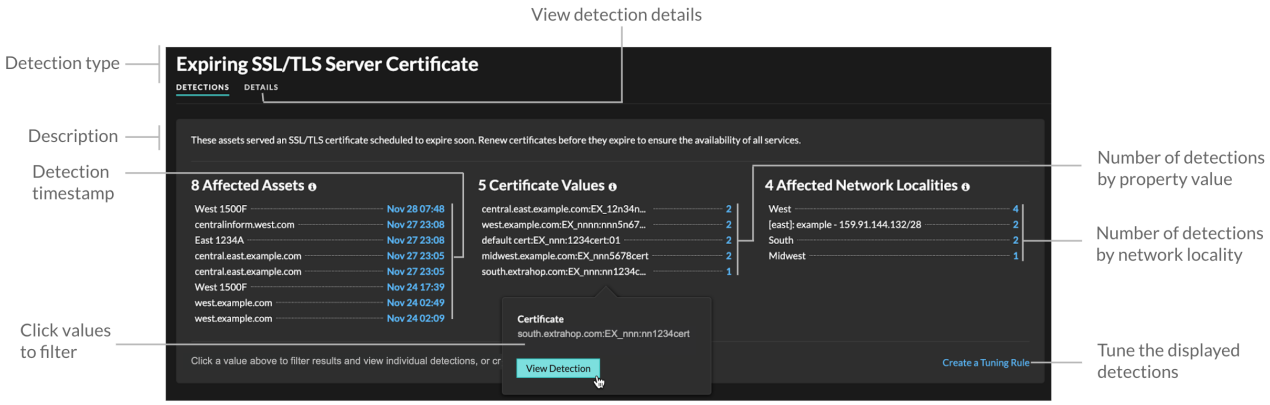
Detections in the Hardening category help mitigate the risk of exploitation. You can triage a large number of hardening detections by filtering and tuning the Detections page.

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.



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.