

Filtrer et régler les détections de durcissement

Publié: 2025-02-04

Les détections de la catégorie Renforcement contribuent à atténuer le risque d'exploitation. Vous pouvez trier un grand nombre de détections de durcissement en filtrant et en ajustant la page Détections.

Avant de commencer

Les utilisateurs doivent être autorisés [privilèges](#) pour afficher les détections et doit disposer de privilèges d'écriture complets ou supérieurs pour créer une règle de réglage.

En savoir plus sur [détections de réglage](#).

En savoir plus sur [bonnes pratiques de réglage](#).

Cliquez sur une détection de durcissement dans [Détections](#) page pour consulter le résumé. Les résumés de détection renforcés identifient le type de détection, les actifs qui participent aux détections de ce type, les propriétés de détection et les localités du réseau qui contiennent les actifs concernés.

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

- Description:** These assets served an SSL/TLS certificate scheduled to expire soon. Renew certificates before they expire to ensure the availability of all services.
- 8 Affected Assets:** A list of assets and their detection timestamps.

Asset	Timestamp
West 1500F	Nov 28 07:48
centralinfrom.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
- 5 Certificate Values:** A list of certificate values and their counts.

Certificate Value	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
- 4 Affected Network Localities:** A list of network localities and their counts.

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

Annotations on the screenshot:

- View detection details:** Points to the top of the page.
- Detection type:** Points to the title 'Expiring SSL/TLS Server Certificate'.
- Description:** Points to the text block.
- Detection timestamp:** Points to the timestamp column in the affected assets table.
- Click values to filter:** Points to the certificate values table.
- Number of detections by property value:** Points to the counts in the certificate values table.
- Number of detections by network locality:** Points to the counts in the network localities table.
- Tune the displayed detections:** Points to the 'View Detection' and 'Create a Tuning Rule' buttons.

Cliquez sur n'importe quelle valeur d'actif, de propriété ou de localité de réseau pour afficher les détections individuelles associées à cette valeur.

Actifs concernés

Liste des actifs participant au renforcement des détections du type sélectionné. La liste des actifs concernés est triée selon l'heure la plus récente à laquelle la détection a eu lieu.

Valeurs des propriétés

Liste des valeurs de propriétés clés associées au type de détection. Par exemple, le type de détection Weak Cipher Suite répertorie les suites de chiffrement référencées dans les détections, et la détection des certificats de serveur TLS expirant répertorie les certificats dont l'expiration est programmée. La liste des valeurs de propriété est triée en fonction du nombre de détections contenant la valeur de propriété.

Localités du réseau touchées

Liste des localités du réseau contenant des détections de durcissement du type sélectionné. La liste des localités du réseau concernées est triée en fonction du nombre de détections dans la localité du réseau.

En filtrant les résultats sur un actif, une propriété ou une localité unique, vous pouvez identifier les détections qui affectent des systèmes critiques ou [créer une règle de réglage](#) qui masque les détections de faible valeur similaires aux résultats filtrés.