

Härteerkennungen filtern und abstimmen

Veröffentlicht: 2024-04-13

Erkennungen in der Kategorie Härtung tragen dazu bei, das Risiko einer Ausnutzung zu verringern. Sie können eine große Anzahl von Härteerkennungen sortieren, indem Sie die Seite „Erkennungen“ filtern und Abstimmung.

Bevor Sie beginnen

Benutzern muss Folgendes gewährt werden [Privilegien](#) um Erkennungen anzuzeigen und müssen über vollständige Schreibrechte oder höhere Rechte verfügen, um eine Optimierungsregel zu erstellen.

Erfahre mehr über [Abstimmung von Erkennungen](#).

Erfahre mehr über [Abstimmung von Best Practices](#).

Klicken Sie auf eine Härteerkennung aus dem [Erkennungen](#) Seite, um die Zusammenfassung anzusehen. In den Zusammenfassungen der Hardening-Erkennung werden der Entdeckungstyp, die Ressourcen, die an Erkennungen dieses Typs beteiligt sind, die Erkennungseigenschaften und die Netzwerkstandorte, an denen sich die betroffenen Geräte befinden, identifiziert.

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
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
- 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

Additional features shown include a 'View Detection' button and a 'Create a Tuning Rule' button. The page also includes a 'Click values to filter' instruction and a 'View detection details' link.

Klicken Sie auf einen Asset-, Objekt- oder Netzwerkstandortwert, um einzelne Erkennungen anzuzeigen, die diesem Wert zugeordnet sind.

Betroffene Vermögenswerte

Eine Liste von Assets, die an Hardening-Erkennungen des ausgewählten Typs beteiligt sind. Die Liste der betroffenen Ressourcen ist nach dem letzten Zeitpunkt der Erkennung sortiert.

Immobilienwerte

Eine Liste der wichtigsten Eigenschaftswerte, die dem Erkennungstyp zugeordnet sind. Beispielsweise listet der Erkennungstyp Weak Cipher Suite die Verschlüsselungssammlungen auf, auf die bei Erkennungen verwiesen wird, und der Erkennungstyp Auslaufendes SSL/TLS-Serverzertifikat listet Zertifikate auf, deren Ablauf geplant ist. Die Liste der Eigenschaftswerte ist nach der Anzahl der Funde sortiert, die den Eigenschaftswert enthalten.

Betroffene Netzwerkstandorte

Eine Liste von Netzwerkstandorten, die Hardening-Erkennungen des ausgewählten Typs enthalten. Die Liste der betroffenen Netzwerkstandorte ist nach der Anzahl der Funde in der Netzwerklokalität sortiert.

Durch Filtern der Ergebnisse für eine einzelne Asset, Immobilie oder Lokalität können Sie Erkennungen identifizieren, die sich auf kritische Systeme auswirken oder [eine Tuning-Regel erstellen](#). Dadurch werden Erkennungen mit niedrigen Werten ausgeblendet, die den gefilterten Ergebnissen ähneln.