Filtrer et régler les détections de durcissement

Publié: 2025-02-04

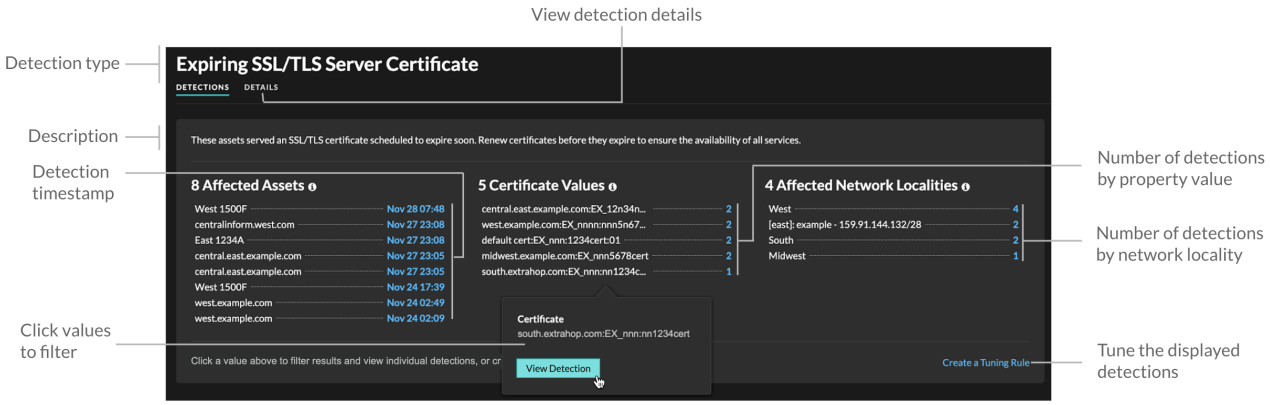
Les détections de la catégorie Renforcement contribuent à atténuer le risque d'exploitation. Vous pouvez trier un grand nombre de détections de durcissement en filtrant et en ajustant la page Détections.

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.



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.