Integrieren Sie Reveal (x) Enterprise mit Splunk SOAR

Veröffentlicht: 2023-09-30

Diese Integration ermöglicht es Ihnen, Erkennungen von Netzwerkbedrohungen, Metriken und Paketdaten von Reveal (x) Enterprise nach Splunk SOAR zu exportieren.

Bevor Sie diese Integration konfigurieren können, müssen Sie Generieren Sie einen ExtraHop REST API-Schlüssel und füge dann den Schlüssel hinzu, wenn du die ExtraHop App für Splunk SOAR konfigurieren.

Anforderungen an das System

ExtraHop Reveal (x) Enterprise

- Ihr Benutzerkonto muss volle Schreibrechte oder höher auf Reveal (x) Enterprise.
- Ihr Reveal (x) Enterprise-System muss mit einem ExtraHop verbunden sein Sensor mit Firmware-Version 9.0 oder höher.
- Ihr Reveal (x) Enterprise-System muss verbunden mit ExtraHop Cloud Services.
- Ihr Reveal (x) Enterprise-System muss konfiguriert, um die Generierung von REST-API-Schlüsseln zu ermöglichen.

Splunk SOAR

- Sie benötigen Splunk SOAR Version 5.3 oder höher.

Generieren Sie einen REST-API-Schlüssel

Sie müssen einen ExtraHop-API-Schlüssel generieren, bevor Sie die ExtraHop-App für Splunk SOAR konfigurieren können. Mit dem API-Schlüssel können Sie auf die Integration zugreifen und Operationen von Splunk SOAR aus ausführen.

1. <extrahop-hostname-or-IP-address>Melden Sie sich über https://beim ExtraHop-System an.
2. Klicken Sie in der oberen rechten Ecke der Seite auf das Benutzersymbol und dann auf **API-Zugriff**.
3. In der Generieren Sie einen API-Schlüssel Abschnitt, geben Sie eine Beschreibung für den neuen Schlüssel ein, und klicken Sie dann auf **Generieren**.
4. Scrollen Sie nach unten zum API-Schlüssel Abschnitt und kopieren Sie den API-Schlüssel , der Ihrer Beschreibung entspricht.

Installieren und konfigurieren Sie die ExtraHop App für Splunk SOAR

1. Laden Sie das herunter und installieren Sie es ExtraHop App für Splunk SOAR von der Splunkbase-Site gemäß der Splunk-Add-Ons und -Apps Dokumentation.
2. Klicken Sie in der installierten App auf **Neues Asset konfigurieren**.
3. Aus dem Art des Vermögenswerts Drop-down-Liste, wählen **Enthülle (x) Enterprise**.
4. Geben Sie den **IP-Adresse oder Hostname** des Reveal (x) Enterprise-Systems, mit dem dieses Asset eine Verbindung herstellen wird.
5. Geben Sie den Schlüssel, den Sie von Ihrem Reveal (x) Enterprise-System generiert haben, in das **REST-API-Schlüssel** Feld.
6. Klicken Sie auf **Dokumentation** klicken Sie auf der Asset-Konfigurationsseite und schließen Sie die Konfiguration der ExtraHop App für Splunk SOAR gemäß der Dokumentation ab.