

Integrieren Sie Reveal (x) Enterprise mit Splunk

Veröffentlicht: 2023-10-31

Diese Integration ermöglicht es Ihnen, Erkennungen von Netzwerkbedrohungen und Verhaltensinformationen von Reveal (x) Enterprise in Splunk einzusehen.

Bevor Sie diese Integration konfigurieren können, müssen Sie [Generieren Sie einen ExtraHop REST API-Schlüssel](#) und füge dann den Schlüssel hinzu, wenn du [das ExtraHop Add-on für Splunk 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 8.8 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

- Sie müssen Splunk Version 8.1 oder höher haben.

Generieren Sie einen REST-API-Schlüssel

Sie müssen einen ExtraHop-API-Schlüssel generieren, bevor Sie das ExtraHop-Add-on für Splunk konfigurieren können. Mit dem API-Schlüssel können Sie auf die Integration zugreifen und Operationen von Splunk 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 das ExtraHop Add-on für Splunk

1. Downloaden und installieren Sie das [ExtraHop-Add-on für Splunk](#) von der SplunkBase-Site gemäß [Splunk-Add-Ons und -Apps](#) Dokumentation.
2. Klicken Sie in der installierten App auf **Konfiguration**, und klicken Sie dann **Hinzufügen** von der Konto Registerkarte.
3. Geben Sie ein Unikat ein **Kontoname**.
4. Aus dem Instanztyp Drop-down-Liste, wählen **On-Prem-Instanz**.
5. Geben Sie den **Hostname** des Reveal (x) Enterprise-Systems , mit dem dieses Konto eine Verbindung herstellen wird.
6. Geben Sie den Schlüssel, den Sie von Ihrem Reveal (x) Enterprise-System generiert haben, in das **API-Schlüssel** Feld.

7. Vervollständigen Sie die Konfiguration des Kontos gemäß [Dokumentation zum ExtraHop-Add-on für Splunk](#) erhältlich bei Einzelheiten Tab auf der Download-Seite.