

Integrieren Sie Reveal (x) Enterprise mit QRadar

Veröffentlicht: 2023-09-30

Diese Integration ermöglicht es Ihnen, Metriken von Reveal (x) Enterprise in IBM Security QRadar anzuzeigen, um Erkenntnisse über das Verhalten Ihrer Umgebung zu gewinnen.

Bevor Sie diese Integration konfigurieren können, müssen Sie [Generieren Sie einen ExtraHop REST API-Schlüssel](#) und füge dann den Schlüssel hinzu, wenn du [konfigurierst die ExtraHop App für QRadar](#).

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](#).

QRadar

- Sie benötigen IBM Security QRadar Version 7.4.1 FP2 oder höher.

Generieren Sie einen REST-API-Schlüssel

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

1. Laden Sie das herunter und installieren Sie es [ExtraHop App für QRadar](#) von der IBM Exchange-Website.
2. Klicken Sie im rechten Bereich der Download-Seite auf **Ansicht** neben Dokumentation um ein PDF des Benutzerhandbuchs herunterzuladen.
3. Klicken Sie in der installierten App auf **ExtraHop-System hinzufügen**.
4. Aus dem Instanztyp Drop-down-Liste, wählen **On-Prem-Instanz**.
5. In der **ExtraHop-System** Feld, geben Sie den Hostnamen des Reveal (x) Enterprise-Systems ein, zu dem diese App 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 der ExtraHop App für QRadar gemäß der heruntergeladenen Dokumentation.