Integrieren Sie RevealX 360 mit CrowdStrike Falcon LogScale

Veröffentlicht: 2024-07-02

Diese Integration ermöglicht es Ihnen, Sicherheitserkennungen von RevealX 360 nach LogScale zu exportieren, um Erkennungsdaten in einem zentralen System anzuzeigen, wodurch der Kontext rund um Erkennungen verbessert und die Zeit zur Bestätigung von Bedrohungen verkürzt wird.

Anforderungen an das System

ExtraShop RevealX 360

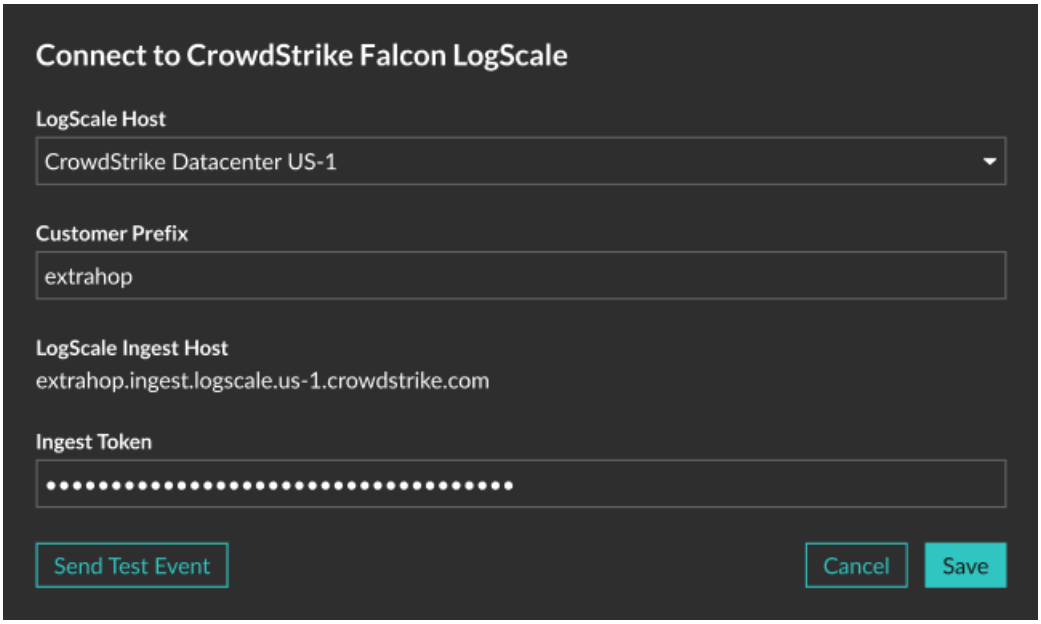
- Ihr Benutzerkonto muss über Rechte auf RevealX 360 für die System- und Zugriffsverwaltung oder das Cloud-Setup verfügen.
- Ihr RevealX 360-System muss mit einem ExtraHop verbunden sein Sensor mit Firmware-Version 9.3 oder höher.
- Ihr RevealX 360-System muss verbunden mit ExtraHop Cloud Services.

CrowdStrike Falcon LogScale

- Sie benötigen CrowdStrike Falcon LogScale Version 1.92.0 oder höher.
- Sie müssen das konfigurieren LogScale HTTP Event Collector-API für die Datenaufnahme.

Konfigurieren Sie die CrowdStrike Falcon LogScale-Integration

1. Loggen Sie sich in das RevealX 360-System ein.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Integrationen**.
3. Klicken Sie auf **CrowdStrike Falcon LogScale** Kachel.
4. Aus dem **LogScale-Host** Wählen Sie in der Dropdownliste den Hostnamen Ihres LogScale-Endpunkts aus.
5. Optional: Wenn Sie ein CrowdStrike Datacenter als Host ausgewählt haben, geben Sie Ihre Kunden-Subdomain in das **Kundenpräfix** Feld. Das Präfix wird dem Hostnamen hinzugefügt und im LogScale Ingest-Host Feld, ähnlich dem folgenden Beispiel:



6. In der **Token aufnehmen** Geben Sie in dieses Feld das Ingest-Token ein, das Sie für den LogScale HTTP Event Collector konfiguriert haben.
7. Klicken Sie **Testevent senden**, und überprüfen Sie dann, ob das Ereignis von Ihrem LogScale-Endpunkt empfangen wurde. Es kann mehrere Minuten dauern, bis das Testereignis eintrifft.
8. Optional: Konfigurieren Sie die folgenden Integrationsoptionen:
   a) Klicken Sie **RevealX 360-Sicherheitserkennungen exportieren** .
   b) Klicken Sie **Kriterien hinzufügen** um den Filter zu konfigurieren, der bestimmt, welche Sicherheitserkennungen auf Ihren LogScale-Endpunkt exportiert werden.
9. Optional: Klicken Sie **Anmeldeinformationen ändern** um den LogScale-Hostnamen oder das HEC-Token zu aktualisieren.
10. Optional: Klicken Sie **Integration deaktivieren** um die aktuellen Anmeldedaten und Optionen beizubehalten, aber die LogScale-Integration zu deaktivieren.
11. Klicken Sie **Speichern**.