Integrieren Sie RevealX 360 mit CrowdStrike Falcon SIEM der nächsten Generation

Veröffentlicht: 2025-03-28

Diese Integration ermöglicht es CrowdStrike Falcon Next-Gen SIEM, Gerät- und Erkennungsdaten mithilfe von Regeln für Erkennungsbenachrichtigungen aus dem ExtraHop-System zu exportieren. Sie können exportierte Daten im SIEM anzeigen, um einen Einblick in die Kommunikation Ihrer Geräte in Ihrer Umgebung zu erhalten und um erkannte Netzwerkbedrohungen anzuzeigen.

Für diese Integration müssen Sie zwei Aufgaben ausführen. Ein ExtraHop-Administrator muss die Verbindung zwischen dem SIEM und dem ExtraHop-System konfigurieren. Nachdem die Verbindung hergestellt wurde, können Sie Regeln für Erkennungsbenachrichtigungen erstellen das sendet Webhook-Daten an das SIEM.

Bevor Sie beginnen

Sie müssen die folgenden Systemanforderungen erfüllen:

- ExtraHop RevealX 360
  - Ihr Benutzerkonto muss Privilegien auf RevealX 360 für System- und Zugriffsadministration.
  - Ihr RevealX 360-System muss mit einem ExtraHop verbunden sein Sensor mit Firmware-Version 9.8 oder höher.
  - Ihr RevealX 360-System muss verbunden mit ExtraHop Cloud Services.
- Crowdstrike
  - Sie benötigen CrowdStrike Falcon Next-Gen SIEM Version 1.0 oder höher.
  - Sie müssen ein CrowdStrike Falcon Next-Gen SIEM konfigurieren HEC-Stecker für die Datenaufnahme und Festlegung der folgenden Feldwerte:
    - Datentyp: JSON
    - Parser: json-for-action
  - Sie müssen eine API-URL und einen API-Schlüssel aus dem HEC-Connector generieren und kopieren.
  - Ihr SIEM muss Webhook-Daten empfangen können. Du kannst Fügen Sie statische Quell-IP-Adressen zu Ihren Sicherheitskontrollen hinzu um Anfragen von RevealX 360 zu ermöglichen.

1. Loggen Sie sich in RevealX 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Integrationen**.
3. Klicken Sie auf **CrowdStrike Falcon SIEM der nächsten Generation** Kachel.
4. Geben Sie die folgenden Informationen ein, die Sie vom CrowdStrike HEC-Connector generiert und kopiert haben:
   a) In der **API-URL** Feld, geben Sie die URL ein, die Webhook-Daten empfangen soll.
   b) In der **API-Schlüssel** Feld, geben Sie den Schlüssel ein, der die Verbindung zur URL authentifiziert.
5. Wählen Sie eine der folgenden Verbindungsoptionen:

Option	Description
Direkte Verbindung	Wählen Sie diese Option, um eine direkte Verbindung von dieser RevealX 360-Konsole zur angegebenen URL zu konfigurieren.
Proxy über einen angeschlossenen Sensor	Wählen Sie diese Option, wenn Ihr SIEM aufgrund von Firewalls oder anderen Sicherheitskontrollen keine direkte Verbindung von dieser RevealX 360-Konsole aus unterstützt.

Option	Description
	1. Wählen Sie im Drop-down-Menü einen verbundenen Sensor aus, der als Proxy fungiert. 2. (Optional): Wählen Sie **Stellen Sie eine Verbindung über den globalen Proxyserver her, der für den ausgewählten Sensor konfiguriert ist** um Daten über einen globalen Proxy zu senden. (Nur verfügbar, wenn auf dem ausgewählten Sensor RevealX Enterprise läuft.

6. Klicken Sie **Testevent senden** um eine Verbindung zwischen dem ExtraHop-System und dem SIEM-Server herzustellen und eine Testnachricht an den Server zu senden.

   Es wird eine Meldung angezeigt, die angibt, ob die Verbindung erfolgreich war oder fehlgeschlagen ist. Wenn der Test fehlschlägt, bearbeiten Sie die Konfiguration und testen Sie die Verbindung erneut.
7. Optional: Wählen Sie **Serverzertifikatsüberprüfung überspringen** um die Überprüfung des SIEM-Serverzertifikats zu umgehen.
8. klicken **Speichern**.

Erstellen Sie eine Regel für Erkennungsbenachrichtigungen für eine SIEM-Integration

Bevor Sie beginnen

- Ihr Benutzerkonto muss über Zugriff auf das NDR-Modul verfügen, um Benachrichtigungsregeln für Sicherheitserkennung zu erstellen.
- Ihr Benutzerkonto muss über NPM-Modulzugriff verfügen, um Benachrichtigungsregeln zur Leistungserkennung zu erstellen.
- Sie können in den Systemeinstellungen auch Regeln für Erkennungsbenachrichtigungen erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Regel für Erkennungsbenachrichtigungen.

1. Loggen Sie sich in RevealX 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Integrationen**.
3. Klicken Sie auf die Kachel für das SIEM, das das Ziel der Regel für Erkennungsbenachrichtigungen sein soll.
4. klicken **Benachrichtigungsregel hinzufügen**.
   Das Benachrichtigungsregel erstellen Das Fenster wird in einer neuen Registerkarte geöffnet und die folgenden Felder sind auf Standardwerte gesetzt.
   - Das **Name** Das Feld ist auf den Namen des SIEM gesetzt.
   - Das **Art der Veranstaltung** Feld ist gesetzt auf **Sicherheitserkennung**.
   - Das **Ziel** Das Feld ist auf die SIEM-Integration gesetzt.
5. In der Beschreibung Feld, fügen Sie Informationen zur Benachrichtigungsregel hinzu.
6. In der Kriterien Abschnitt, klicken **Kriterien hinzufügen** um Kriterien anzugeben, die eine Benachrichtigung generieren.
   - **Für Triage empfohlen**
   - **Mindestrisikobewertung**
   - **Typ**
   - **Kategorie**
   - **MITRE-Technik** (nur NDR)
   - **Täter**

- **Opfer**
- **Rolle des Geräts**
- **Teilnehmer**
- **Standort**

Die Kriterienoptionen entsprechen den Filteroptionen auf der Seite „Erkennungen“.

7. Unter Payload-Optionen, wählen Sie aus, ob Sie die senden möchten Standard-Nutzlast oder geben Sie eine benutzerdefinierte JSON-Nutzlast ein.

   - **Standard-Nutzlast**

     Füllen Sie die Webhook-Nutzlast mit einem Kernsatz von Erkennungsfeldern.

     Im Dropdownmenü Payload-Felder hinzufügen können Sie auf zusätzliche Felder klicken, die Sie in die Payload aufnehmen möchten.
   - **Benutzerdefinierte Nutzlast**

     Füllen Sie die Webhook-Nutzlast mit benutzerdefiniertem JSON auf.

     Sie können die vorgeschlagene benutzerdefinierte Nutzlast in der **Nutzlast bearbeiten** Fenster.
8. klicken **Verbindung testen**.
   Eine Nachricht mit dem Titel Testbenachrichtigung wird gesendet, um die Verbindung zu bestätigen.
9. In der Optionen Abschnitt, der **Benachrichtigungsregel aktivieren** Das Kontrollkästchen ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Benachrichtigungsregel zu deaktivieren.
10. klicken **Speichern**.

Nächste Schritte

- Gehen Sie zurück zur Integrationskonfigurationsseite, um zu überprüfen, ob Ihre Regel erstellt und der Tabelle hinzugefügt wurde.
- klicken **Bearbeiten** um eine Regel zu ändern oder zu löschen.