

Integrieren Sie RevealX 360 mit Splunk Enterprise Security SIEM

Veröffentlicht: 2024-10-26

Diese Integration ermöglicht es dem Splunk Enterprise Security 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 einzusehen.


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.

Die Regeln für Erkennungsbenachrichtigungen, die mit dieser Integration verknüpft sind, sind auf der Integrationskonfigurationsseite sowie auf der [Regeln für Benachrichtigungen](#) [Tabelle](#), auf die Sie über die Systemeinstellungen zugreifen können.

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 Splunk Enterprise Security Version 8.2 oder höher
 - Sie müssen Splunk Enterprise Security konfigurieren [HEC-Stecker](#) für die Datenaufnahme.
 - 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 **Splunk Unternehmenssicherheit (SIEM)** Kachel.
4. Gehen Sie wie folgt vor, um die Verbindung zwischen dem Splunk Enterprise Security SIEM und dem ExtraHop-System zu konfigurieren:
 - a) In der **Host aufnehmen** Feld, geben Sie die URL oder den Hostnamen des SIEM-Servers ein, der Webhook-Daten empfangen soll.
 - b) In der **Port aufnehmen** In diesem Feld geben Sie die Portnummer ein , die Webhook-Daten empfangen soll.
 - c) In der **Index** Feld, geben Sie den Namen des Indexes ein, der die Webhook-Daten speichern soll.
 - d) In der **HEC-Token** Feld, geben Sie das Token ein, das die Verbindung zum Ingest-Host 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

Option	Description
<p>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.</p> <p>7. Optional: Wählen Sie Serverzertifikatsüberprüfung überspringen um die Überprüfung des SIEM-Serverzertifikats zu umgehen.</p> <p>8. Klicken Sie Speichern.</p>	<p>keine direkte Verbindung von dieser RevealX 360-Konsole aus unterstützt.</p> <ol style="list-style-type: none"> 1. Wählen Sie im Dropdownmenü 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.

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 Sie **Kriterien hinzufügen** um Kriterien anzugeben, nach denen eine Benachrichtigung generiert wird.
 - **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“](#).

- Wählen Sie unter Payload-Optionen 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.

In der Dropdownliste Payload-Felder hinzufügen können Sie auf zusätzliche Felder klicken, die Sie in die Payload aufnehmen möchten.

- **Benutzerdefinierte Nutzlast**

Geben Sie Ihre eigene Payload direkt in das Fenster Payload (JSON) -Vorschau ein.



Hinweis: Um eine Standard-Payload anzupassen, kopieren Sie die Payload aus dem Vorschaufenster und wechseln Sie zu **Benutzerdefinierte Nutzlast** und fügen Sie dann die Payload zur Bearbeitung in das Vorschaufenster ein.

Sie können auch Beispiel-Payloads aus dem [Referenz zur Webhook-Benachrichtigung](#).

- klicken **Verbindung testen**.
Eine Nachricht mit dem Titel Testbenachrichtigung wird gesendet, um die Verbindung zu bestätigen.
- In der Optionen Abschnitt, der **Benachrichtigungsregel aktivieren** Das Kontrollkästchen ist standardmäßig aktiviert. Deaktivieren Sie das Kontrollkästchen, um die Benachrichtigungsregel zu deaktivieren.
- 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.

Integration Status

Status: ● Integration Enabled
 Proxy Sensor: ● prod-pdx-eda-6100v

[Send Test Event](#) [Change Credentials](#) [Delete Credentials](#)

Notification Rules

This integration is configured as the target for the following notification rules.

Name	Event Type	Status	Author	
All System Alerts	Security Detection	● Enabled	maebybluth	Edit
NOC	Performance Detection	● Disabled	tobias	Edit

[Add Notification Rule](#)