Integrieren Sie RevealX 360 mit Splunk Enterprise Security SIEM

Veröffentlicht: 2025-03-28

Diese Integration ermöglicht es dem Splunk Enterprise Security SIEM, Erkennungsdaten mithilfe von Regeln für Erkennungsbenachrichtigungen aus dem ExtraHop-System zu exportieren. Sie können exportierte Daten im SIEM anzeigen, um Einblicke in Sicherheitsbedrohungen in Ihrer Umgebung zu erhalten und die Reaktionszeiten zu verkürzen.

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.

Nachdem die Verbindung hergestellt und die Benachrichtigungsregeln konfiguriert sind, können Sie installiere die ExtraHop RevealX App für Splunk auf Ihrem Splunk SIEM. Die App bietet ein Dashboard mit Erkennungsdaten und Korrelationsregeln, die Erkennungswarnungen in Splunk generieren.

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.
- Splunk
  - Sie müssen Splunk Enterprise Version 9.1 oder höher haben
  - Sie müssen ein Splunk Enterprise 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
	keine direkte Verbindung von dieser RevealX 360-Konsole aus unterstützt. 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 Sie **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.

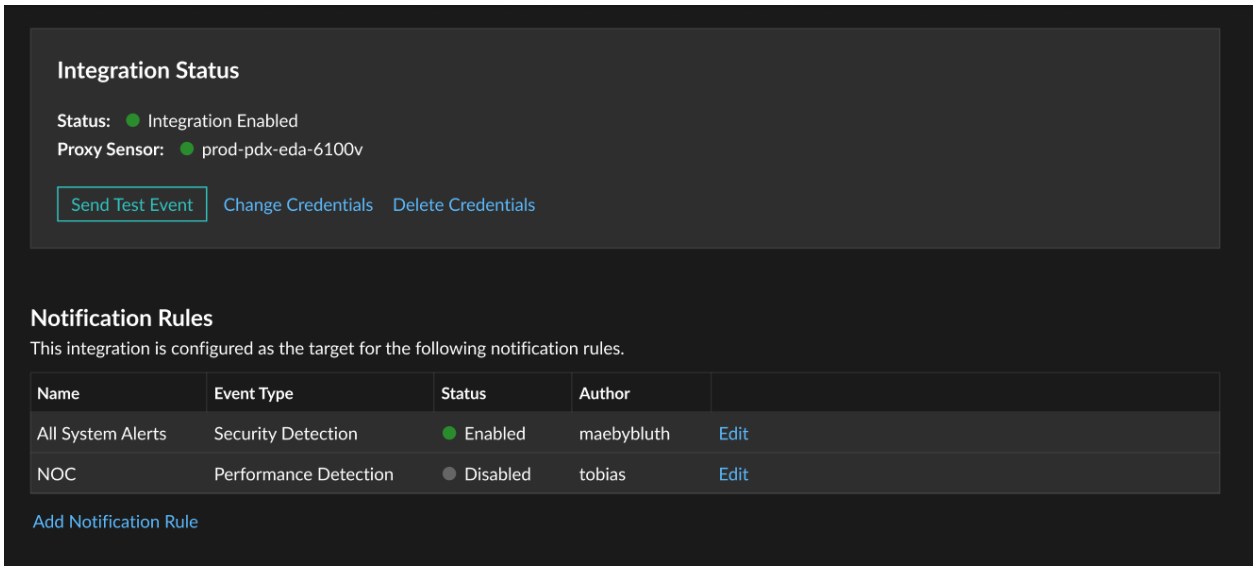
     Im Dropdownmenü Payload-Felder hinzufügen können Sie auf zusätzliche Felder klicken, die Sie in die Payload aufnehmen möchten.
   - **Benutzerdefinierte Nutzlast**

     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.



Installieren Sie die ExtraHop RevealX App für Splunk

Die ExtraHop RevealX App für Splunk erhält ExtraHop RevealX-Erkennungsdaten vom Splunk Ereignis Collector, um ein Erkennungs-Dashboard zu erstellen und Warnmeldungen zu Erkennungsereignissen in Splunk auf der Grundlage von Korrelationsregeln zu generieren.

1. Laden Sie das herunter ExtraHop RevealX App für Splunk von Splunkbase.
2. Loggen Sie sich in Ihr Splunk SIEM ein.
3. Aus dem **Apps** Dropdownliste, klicken Sie **Apps verwalten** .
4. Klicken Sie in der oberen rechten Ecke auf **Installieren Sie die App aus einer Datei**.
5. Klicken Sie **Wählen Sie Datei**, und wählen Sie dann die heruntergeladene App aus.
6. Klicken Sie **Upload** und folge den Anweisungen.
7. Aus dem **Apps** Dropdownliste, klicken Sie **ExtraHop RevealX App für Splunk** um die App in Ihrem Splunk SIEM zu öffnen.
   Das ExtraHop Detections Overview-Dashboard wird standardmäßig angezeigt und enthält die folgenden Diagramme:

Diagramm	Beschreibung
Empfohlene Erkennungen	Zeigt die Gesamtzahl der empfohlenen Erkennungen an, die während des ausgewählten Zeitraums generiert wurden.
Gesamtzahl der Erkennungen	Zeigt die Anzahl der Erkennungen an, die während des ausgewählten Zeitraums generiert wurden.
Maximaler Risikowert	Zeigt die höchste Risikoscore Erkennungen an, die während des ausgewählten Zeitraums generiert wurden.
Die am häufigsten empfohlenen Erkennungen	Zeigt die 10 empfohlenen Erkennungen an, die während des ausgewählten Zeitraums generiert wurden, sowie die Häufigkeit, mit der jede Erkennung aufgetreten ist.
Die häufigsten Erkennungskategorien	Zeigt die zehn wichtigsten Erkennungskategorien an, die den während des ausgewählten Zeitraums generierten Entdeckungen zugeordnet sind, sowie den Prozentsatz und die Anzahl der Funde für jede Kategorie.
Die besten MITRE-Techniken	Zeigt die 10 wichtigsten MITRE-Techniken an, die mit Erkennungen verknüpft sind, die während des ausgewählten Zeitraums generiert wurden, sowie die Anzahl der Erkennungen für jede Technik.
Top-Quellen	Zeigt die zehn wichtigsten Quellhosts an, die den während des ausgewählten Zeitraums generierten Entdeckungen zugeordnet sind, sowie die Anzahl der Funde für jede Quelle.
Top-Destinationen	Zeigt die zehn wichtigsten Zielhosts an, die den während des ausgewählten Zeitraums generierten Entdeckungen zugeordnet sind, sowie die Anzahl der Funde für jedes Ziel.

Diagramm	Beschreibung
Quellen und Ziele	Zeigt den Fluss der Quellen und Ziele an, die mit Funden verknüpft sind, die während des ausgewählten Zeitraums generiert wurden.
Aktuelle Erkennungen	Zeigt die neuesten Erkennungen an, die während des ausgewählten Zeitraums generiert wurden, sowie Erkennungsdetails wie Risikobewertung, Kategorie und URL

8. Gehen Sie wie folgt vor, um die in der App bereitgestellten Korrelationsregeln anzuzeigen:
   a) Aus dem **Einstellungen** Dropdownliste, klicken Sie **Suchanfragen, Berichte und Benachrichtigungen**.
   b) Aus dem **Besitzer** Dropdownliste, klicken Sie **Alle**

      In der Tabelle werden die folgenden Korrelationsregeln angezeigt, die standardmäßig aktiviert sind:

      - Warnmeldungen mit niedrigem Schweregrad werden für Erkennungen mit einer Risikobewertung von 1 bis 30 generiert.
      - Warnmeldungen mit mittlerem Schweregrad werden für Erkennungen mit einer Risikobewertung zwischen 31 und 79 generiert.
      - Warnmeldungen mit hohem Schweregrad werden für Erkennungen mit einer Risikobewertung zwischen 80 und 99 generiert.
9. Aus dem **Aktivität** Dropdownliste, klicken Sie **Ausgelöste Alarme** um Warnungen anzuzeigen, die anhand der Korrelationsregeln generiert wurden.