Datensätze von ExtraHop an Splunk senden

Veröffentlicht: 2024-08-09

Sie können das ExtraHop-System so konfigurieren, dass Datensätze auf Transaktionsebene zur Langzeitspeicherung an einen Splunk-Server gesendet werden, und diese Datensätze dann vom ExtraHop-System und der ExtraHop-REST-API abfragen.

Hier sind einige Überlegungen zum Senden von Datensätzen von ExtraHop an Splunk:

- Alle Trigger, die für das Senden von Datensätzen konfiguriert sind `commitRecord` zu einem Recordstore werden automatisch zum Splunk-Server umgeleitet. Es ist keine weitere Konfiguration erforderlich.
- Wenn Sie von einem verbundenen ExtraHop-Recordstore zu Splunk migrieren, können Sie nicht mehr auf die im Recordstore gespeicherten Datensätze zugreifen.
- Wenn Sie ExtraHop-Daten wie Metriken und Erkennungen in einer Splunk-Oberfläche anzeigen und analysieren möchten, konfigurieren Sie eine Splunk oder Splunk SOAR Integration.

Splunk als Recordstore aktivieren

Führen Sie dieses Verfahren auf allen angeschlossenen ExtraHop-Systemen durch.

Wichtig: Wenn Ihr ExtraHop-System eine Konsole oder RevealX 360 enthält, konfigurieren Sie alle Sensoren mit denselben Recordstore-Einstellungen oder Übertragungsmanagement, um die Einstellungen von der Konsole oder RevealX 360 aus zu verwalten.

Bevor Sie beginnen

- Auf jeder Konsole und allen angeschlossenen Sensoren muss dieselbe ExtraHop-Firmware-Version ausgeführt werden.
- Sie benötigen Version 7.0.3 oder höher von Splunk Enterprise und ein Benutzerkonto mit Administratorrechte.
- Sie müssen den Splunk HTTP Event Collector konfigurieren, bevor Ihr Splunk-Server ExtraHop-Datensätze empfangen kann. Sehen Sie die Splunk HTTP-Event-Collector Dokumentation für Anweisungen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken **Plattenladen**.
3. Wählen **Splunk als Recordstore aktivieren**.
4. In der Aufnahmeziel aufzeichnen Abschnitt, füllen Sie die folgenden Felder aus:
   - **Splunk Ingest Host:** Der Hostname oder die IP-Adresse Ihres Splunk-Servers.
   - **Port für HTTP-Event-Collector:** Der Port, über den der HTTP Event Collector Datensätze senden soll.
   - **HTTP-Event-Collector-Token:** Das Authentifizierungstoken, das Sie erstellt in Splunk für den HTTP Event Collector.
5. In der Ziel der Datensatzabfrage Abschnitt, füllen Sie die folgenden Felder aus:
   - **Splunk-Abfragehost:** Der Hostname oder die IP-Adresse Ihres Splunk-Servers.
   - **REST-API-Port:** Der Port, über den Datensatzabfragen gesendet werden sollen.
   - **Methode der Authentifizierung:** Die Authentifizierungsmethode, die von Ihrer Splunk-Version abhängt.

© 2024ExtraHop Networks, Inc. Alle Rechte vorbehalten.

Für Splunk-Versionen nach 7.3.0 wählen Sie **Authentifizieren Sie sich mit einem Token**, und fügen Sie dann Ihr Splunk-Authentifizierungstoken ein. Anweisungen zum Erstellen eines Authentifizierungstokens finden Sie in der Splunk-Dokumentation.

Für Splunk-Versionen vor 7.3.0 wählen Sie **Authentifizieren Sie sich mit Benutzername und Passwort**, und geben Sie dann Ihre Splunk-Anmeldeinformationen Anmeldedaten.

6. Löschen Sie das **Zertifikatsüberprüfung erforderlich** Kontrollkästchen, wenn für Ihre Verbindung kein gültiges SSL/TLS-Zertifikat erforderlich ist.

   Hinweis: Sichere Verbindungen zum Splunk-Server können verifiziert werden durch vertrauenswürdige Zertifikate die Sie in das ExtraHop-System hochladen.

7. In der Name des Indexes Feld, geben Sie den Namen des Splunk-Indexes ein , in dem Sie Datensätze speichern möchten.

   Der Standardindex auf Splunk heißt `main`Wir empfehlen jedoch, dass Sie einen separaten Index für Ihre ExtraHop-Datensätze erstellen und den Namen dieses Indexes eingeben. Anweisungen zum Erstellen eines Indexes finden Sie in der Splunk-Dokumentation.

8. (ExtraHop Sensor (nur) Klicken **Verbindung testen** um zu überprüfen , ob das ExtraHop-System Ihren Splunk-Server erreichen kann.
9. Klicken Sie **Speichern**.

Nachdem Ihre Konfiguration abgeschlossen ist, können Sie im ExtraHop-System nach gespeicherten Datensätzen abfragen, indem Sie auf **Rekorde** aus dem oberen Menü.

Recordstore-Einstellungen übertragen

Wenn du einen ExtraHop hast Konsole Wenn Sie an Ihre ExtraHop-Sensoren angeschlossen sind, können Sie die Recordstore-Einstellungen auf dem Sensor konfigurieren und verwalten oder die Verwaltung der Einstellungen an den Konsole. Durch die Übertragung und Verwaltung der Recordstore-Einstellungen auf der Konsole können Sie die Recordstore-Einstellungen für mehrere Sensoren auf dem neuesten Stand halten.

Die Recordstore-Einstellungen werden für verbundene Recordstores von Drittanbietern konfiguriert und gelten nicht für den ExtraHop-Recordstore.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken **Plattenladen**.
3. Aus dem **Recordstore-Einstellungen** Dropdownliste, wählen Sie die Konsole aus und klicken Sie dann auf **Inhaberschaft übertragen**.

   Wenn Sie sich später dazu entschließen, die Einstellungen auf der Sensor, wählen **dieser Sensor** aus der Dropdownliste Recordstore-Einstellungen und klicken Sie dann auf **Inhaberschaft übertragen**.