Laden Sie die IDS-Regeln über die REST-API in das ExtraHop-System hoch

Veröffentlicht: 2024-11-03

Sie können einen Satz kuratierter IDS-Regeln vom ExtraHop Kundenportal herunterladen und die Regeln manuell auf IDS-Sensoren hochladen. Wenn Ihr ExtraHop-System mit ExtraHop Cloud Services verbunden ist, wird der neueste Regelsatz automatisch auf das System heruntergeladen, sobald eine aktualisierte Version verfügbar ist. In diesem Handbuch zeigen wir Methoden zum Hochladen von IDS-Regeln sowohl über den cURL-Befehl als auch über ein Python-Skript.

Wichtig: Das ExtraHop Kundenportal bietet Downloads sowohl für IDS-Regelsatzdateien als auch für IDS-Ressourcendateien. Wenn Sie eine IDS-Regelsatzdatei auf einen Sensor hochladen, müssen Sie auch die entsprechende IDS-Ressourcendatei auf die Konsole hochladen, mit der der Sensor verbunden ist.

Laden Sie IDS-Regeln mit dem cURL-Befehl hoch

1. Laden Sie die neuesten IDS-Regeln von der Extrahop-Website herunter.
2. Gehe zum ExtraHop Kundenportal, und klicken Sie auf **IDS-Regeln**.
3. Öffnen Sie ein Terminal und führen Sie den folgenden Befehl aus, wobei Sie die Variablen durch Informationen aus Ihrer Umgebung ersetzen:

   • **GASTGEBER:** Die IP-Adresse oder der Hostname des IDS-Sensors oder der IDS-Sonde.

   • **API-SCHLÜSSEL:** Der API-Schlüssel.

   • **IDS_DATEI:** Der Dateipfad der IDS-Datei. Wenn der Host ein Sensor ist, geben Sie den Pfad der IDS-Regelsatzdatei an. Wenn der Host eine Konsole ist, geben Sie den Pfad der IDS-Ressourcendatei an.

   ```
   curl -X POST "https://<HOST>/api/v1/extrahop/cloudresources" -H "accept:
    application/json" -H "Authorization: ExtraHop apikey=<API_KEY>" --data-
   binary @IDS_FILE -w "%{http_code}\n"
   ```

   Der Befehl gibt den HTTP-Statuscode der Antwort zurück. Wenn der Befehl erfolgreich ist, lautet der Statuscode 202.

   Hinweis: Wenn der Befehl keine Ergebnisse zurückgibt, stellen Sie sicher, dass Ihrem ExtraHop-System wurde ein vertrauenswürdiges Zertifikat hinzugefügt. Alternativ können Sie das hinzufügen `--insecure` Option zum Abrufen der Geräteliste von einem ExtraHop-System ohne vertrauenswürdiges Zertifikat; diese Methode ist jedoch nicht sicher und wird nicht empfohlen.
4. Wiederholen Sie den vorherigen Schritt für jeden IDS-Sensor und jede Konsole, die Sie aktualisieren möchten.

Rufen Sie das Python-Beispielskript ab und führen Sie es aus

Das ExtraHop GitHub-Repository enthält ein Python-Beispielskript, das eine Liste von ExtraHop-Sensoren und -Konsolen aus einer CSV-Datei liest und IDS-Regeln programmgesteuert in jede einzelne hochlädt.

1. Gehe zum GitHub-Repository mit ExtraHop-Codebeispielen und laden Sie den Inhalt des `upload_ids_rules` Verzeichnis zu Ihrem lokalen Computer.
2. Laden Sie die neuesten IDS-Regeln von der Extrahop-Website herunter.
   a) Gehe zum ExtraHop Kundenportal, und klicken **IDS-Regeln**.
   b) klicken **Herunterladen** neben dem IDS-Regelsatz und den IDS-Ressourcen.

c) Kopieren Sie die Dateien in den `upload_ids_rules` Verzeichnis auf Ihrem lokalen Computer.

3. Öffnen Sie in einem Texteditor den `ids.csv` archivieren und ersetzen Sie die Beispielwerte durch die Hostnamen, API-Schlüssel und den IDS-Dateipfad für jeden Sensor oder jede Konsole. Geben Sie den Pfad der IDS-Regelsatzdateien für Sensoren und der IDS-Ressourcendateien für Konsolen an.

   Wichtig: Löschen oder ändern Sie die Kopfzeile nicht.

4. Führen Sie den folgenden Befehl aus:

```
python3 upload_ids_rules.py
```

Hinweis: Wenn das Skript eine Fehlermeldung zurückgibt, dass die TLS-Zertifikatsüberprüfung fehlgeschlagen ist, stellen Sie sicher, dass Ihrem Sensor oder Ihrer Konsole wurde ein vertrauenswürdiges Zertifikat hinzugefügt. Alternativ können Sie das hinzufügen `verify=False` Option zur Umgehung der Zertifikatsüberprüfung. Diese Methode ist jedoch nicht sicher und wird nicht empfohlen. Der folgende Code sendet eine HTTP GET-Anfrage ohne Zertifikatsüberprüfung:

```
requests.get(url, headers=headers, verify=False)
```