Téléchargez les règles IDS dans le système ExtraHop via l'API REST

Publié: 2024-11-04

Vous pouvez télécharger un ensemble de règles IDS sélectionnées depuis le portail client ExtraHop et télécharger manuellement les règles sur les capteurs IDS. Si votre système ExtraHop est connecté à ExtraHop Cloud Services, le dernier ensemble de règles est automatiquement téléchargé sur le système chaque fois qu'une version mise à jour est disponible. Dans ce guide, nous présentons des méthodes permettant de télécharger des règles IDS à la fois par le biais de la commande cURL et d'un script Python.

Important: Le portail client ExtraHop permet de télécharger à la fois les fichiers IDS Ruleset et les fichiers IDS Resource. Si vous chargez un fichier d'ensemble de règles IDS vers une sonde, vous devez également télécharger le fichier de ressources IDS correspondant sur la console à laquelle la sonde est connectée.

Téléchargez des règles IDS à l'aide de la commande cURL

1. Téléchargez les dernières règles IDS sur le site Web d'Extrahop.
2. Accédez au Portail client ExtraHop, et cliquez sur **Règles IDS**.
3. Ouvrez un terminal et exécutez la commande suivante, en remplaçant les variables par des informations provenant de votre environnement :

   • **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la console IDS.

   • **CLÉ_API:** La clé API.

   • **IDS_FILE:** Le chemin du fichier IDS. Si l'hôte est une sonde, spécifiez le chemin du fichier IDS Ruleset. Si l'hôte est une console, indiquez le chemin du fichier de ressources IDS.

   ```
   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"
   ```

   La commande renvoie le code dquo HTTP de la réponse. Si la commande aboutit, le code dquo est 202.

   Note: Si la commande ne renvoie aucun résultat, assurez-vous que un certificat fiable a été ajouté à votre système ExtraHop. Vous pouvez également ajouter `--insecure` option permettant de récupérer la liste des équipements à partir d'un système ExtraHop sans certificat fiable ; cependant, cette méthode n'est pas sécurisée et n'est pas recommandée.
4. Répétez l'étape précédente pour chaque sonde IDS et chaque console que vous souhaitez mettre à jour.

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub d'ExtraHop contient un exemple de script Python qui lit une liste de capteurs et de consoles ExtraHop à partir d'un fichier CSV et télécharge les règles IDS dans chacun d'eux par programmation.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le contenu du `upload_ids_rules` répertoire vers votre machine locale.
2. Téléchargez les dernières règles IDS sur le site Web d'Extrahop.
   a) Accédez au Portail client ExtraHop, puis cliquez **Règles IDS**.
   b) Cliquez **Télécharger** à côté de l'IDS Ruleset et de l'IDS Resources.

c) Copiez les fichiers dans `upload_ids_rules` répertoire sur votre machine locale.

3. Dans un éditeur de texte, ouvrez le `ids.csv` archivez et remplacez les valeurs d' exemple par les noms d'hôte, les clés d'API et le chemin du fichier IDS pour chaque sonde ou console. Spécifiez le chemin des fichiers IDS Ruleset pour les capteurs et des fichiers de ressources IDS pour les consoles.

   Important: Ne supprimez ni ne modifiez la ligne d'en-tête.

4. Exécutez la commande suivante :

```
python3 upload_ids_rules.py
```

Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat TLS a échoué, assurez-vous que un certificat fiable a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter `verify=False` option permettant de contourner la vérification des certificats. Cependant, cette méthode n'est pas sûre et n'est pas recommandée. Le code suivant envoie une requête HTTP GET sans vérification du certificat :

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