Téléchargez des fichiers STIX via l'API REST

Publié: 2024-03-20

Publié: 2024-03-20

Les collectes de menaces permettent à votre système ExtraHop d'identifier les adresses IP, les noms d'hôte et les URI suspects détectés dans le cadre de votre activité réseau. Bien que les collectes de menaces organisées par ExtraHop soient activées par défaut, vous pouvez également télécharger une collecte de menaces personnalisée à partir de sources gratuites ou commerciales.

Avant de commencer

- Pour les capteurs et les machines virtuelles ECA, vous devez disposer d'une clé API valide pour apporter des modifications via l' API REST et suivre les procédures ci-dessous. (Voir Génération d'une clé d'API).
- Pour Reveal (x) 360, vous devez disposer d'informations d'identification d'API REST valides pour apporter des modifications via l' API REST et suivre les procédures ci-dessous. (Voir Création d'informations d'identification pour l'API REST).
- Familiarisez-vous avec renseignement sur les menaces.

Les collections de menaces doivent être ajoutées et mises à jour pour tous les utilisateurs connectés capteurs et consoles. Et comme ces sources sont souvent mises à jour fréquemment, l'API REST permet d' automatiser les mises à jour des collections de menaces destinées à tous capteurs et consoles.

Les collections de menaces personnalisées doivent être formatées dans STIX (Structured Threat Information Expression) sous forme de fichiers TAR compressés, tels que .TGZ ou TAR.GZ. Les systèmes ExtraHop prennent actuellement en charge les versions STIX 1.0 à 1.2.

Récupérez et exécutez l'exemple de script Python

Le dépôt GitHub d'ExtraHop contient un exemple de script Python qui télécharge tous les fichiers STIX d'un répertoire donné vers une liste de capteurs et consoles. Tout d'abord, le script lit un fichier CSV contenant les URL et les clés d'API de chaque système. Pour chaque système, le script obtient une liste de toutes les collections de menaces déjà présentes sur le système. Le script traite ensuite chaque fichier STIX du répertoire de chaque système.

Si le nom du fichier correspond au nom d'une collection de menaces sur le système, le script remplace la collecte de menaces par le contenu du fichier. Si aucun nom de collecte des menaces ne correspond au nom du fichier, le script télécharge le fichier pour créer une nouvelle collection de menaces.

Note: La procédure suivante n'est pas compatible avec l' API REST Reveal (x) 360. Pour télécharger des fichiers STIX vers Reveal (x) 360, voir Récupérez et exécutez l'exemple de script Python pour Reveal (x) 360.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `upload_stix/upload_stix.py` fichier sur votre machine locale.
2. Créez un fichier CSV avec des lignes contenant les colonnes suivantes dans l' ordre indiqué :

Nom d'hôte du système	Clé d'API

   Conseil: Le `upload_stix` répertoire contient un exemple de fichier CSV nommé `systems.csv`.
3. Dans un éditeur de texte, ouvrez `upload_stix.py` archivez et remplacez les variables de configuration suivantes par des informations provenant de votre environnement :
   - **LISTE_SYSTÈME:** Le chemin du fichier CSV contenant les URL HTTPS et les clés API des systèmes
   - **STIX_DIR:** Le chemin du répertoire contenant les fichiers STIX

4. Exécutez la commande suivante :

```
python3 upload_stix.py
```

Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat SSL a échoué, assurez-vous que un certificat fiable a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter le `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)
```

Récupérez et exécutez l'exemple de script Python pour Reveal (x) 360

Le référentiel GitHub ExtraHop contient un exemple de script Python qui télécharge tous les fichiers STIX d'un répertoire donné vers Reveal (x) 360.

Si le nom du fichier correspond au nom d'une collection de menaces sur Reveal (x) 360, le script remplace la collecte des menaces par le contenu du fichier. Si aucun nom de collecte des menaces ne correspond au nom du fichier, le script télécharge le fichier pour créer une nouvelle collection de menaces.

Note: La procédure suivante est uniquement compatible avec l'API REST Reveal (x) 360. Pour télécharger des fichiers STIX vers des capteurs et des machines virtuelles ECA, voir Récupérez et exécutez l'exemple de script Python.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `upload_stix/upload_stix_rx360.py` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez `create_device_groups.py` archivez et remplacez les variables de configuration suivantes par des informations provenant de votre environnement :

   • **HÔTE:** Le nom d'hôte de l'API Reveal (x) 360. Ce nom d'hôte est affiché sur la page d'accès à l'API Reveal (x) 360 sous API Endpoint. Le nom d'hôte n'inclut pas `/oauth2/token`.

   • **IDENTIFIANT:** L'ID des informations d'identification de l'API REST Reveal (x) 360.

   • **SECRET:** Le secret des informations d'identification de l'API REST Reveal (x) 360.

   • **STIX_DIR:** Le chemin du répertoire contenant les fichiers STIX
3. Exécutez la commande suivante :

```
python3 upload_stix_rx360.py
```