Spécifiez les appareils à valeur élevée via l'API REST

Publié: 2024-03-20

L'API REST ExtraHop vous permet de spécifier qu'un équipement a une valeur élevée. Vous pouvez spécifier l'équipement via l'explorateur d'API REST ou automatiser la procédure en lisant les critères de l'équipement à partir d'un fichier CSV ou similaire via un script d'API REST.

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).

Spécifiez un équipement à valeur élevée via l'explorateur d'API REST

Récupérez l'identifiant de l'équipement

Avant de pouvoir spécifier un équipement à valeur élevée, vous devez récupérer l'ID de l'API REST de l' appareil.

1. Dans un navigateur, accédez à l'explorateur d'API REST.

   L'URL est le nom d'hôte ou l'adresse IP de votre sonde ou console, suivi de `/api/v1/explore/`. Par exemple, si votre nom d'hôte est seattle-eda, l'URL est `https://seattle-eda/api/v1/explore/`.
2. Cliquez **Entrez la clé d'API** puis collez ou saisissez votre clé d'API dans **Clé d'API** champ.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **POST /appareils/recherche**.
5. Cliquez **Essayez-le**.

   Le schéma JSON est automatiquement ajouté à la zone de texte des paramètres du corps.
6. Dans le corps de la zone de texte, saisissez les critères de recherche qui sélectionnent l'équipement. Les critères de recherche suivants renvoient un équipement dont l'adresse IP est 10.10.10.200 :

   ```
   {
     "filter": {
       "field": "ipaddr",
       "operand": "10.10.10.200",
       "operator": "="
     }
   }
   ```

   Pour plus d'informations sur les filtres de recherche d'équipements, voir Valeurs d'opérande pour la recherche d'équipements.
7. Cliquez **Envoyer une demande**.

   Dans la section Corps de la réponse, notez `id` champ de l' équipement.

Spécifiez un équipement de valeur élevée

1. Cliquez **PATCH /appareils/ {id}**.
2. Cliquez **Essayez-le**.

3. Dans le **corps** dans le champ, saisissez l'objet JSON suivant :

```
{
    "custom_criticality": "critical"
}
```

4. Dans le **identifiant** dans ce champ, saisissez l'ID de l'équipement qui que vous avez récupéré lors de la procédure précédente.
5. Cliquez **Envoyer une demande**.
   Si la demande aboutit, un code de réponse 204 apparaît dans la section Réponse du serveur.

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub ExtraHop contient un exemple de script Python qui lit une liste d'adresses IP à partir d'un fichier CSV et spécifie tous les appareils dont ces adresses ont une valeur élevée .

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le contenu du `specify_high_value` répertoire sur votre machine locale.
2. Dans un éditeur de texte, ouvrez `ip_list.csv` archivez et remplacez les adresses IP par les adresses IP des appareils que vous souhaitez spécifier comme valeur élevée.
3. Dans un éditeur de texte, ouvrez `specify_high_value.py` archivez et remplacez les variables de configuration par des informations provenant de votre environnement.
   - Pour les capteurs et les machines virtuelles ECA, spécifiez les variables de configuration suivantes :
     - **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la machine virtuelle ECA.
     - **CLÉ_API:** La clé API.
   - Pour Reveal (x) 360, spécifiez les variables de configuration suivantes :
     - **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.
4. Exécutez la commande suivante :

```
python3 specify_high_value.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)
```