Geben Sie hoher Wert Geräte über die REST-API an

Veröffentlicht: 2024-02-12

Mit der ExtraHop REST-API können Sie angeben, dass ein Gerät einen hoher Wert. Sie können das Gerät über den REST API Explorer angeben oder das Verfahren automatisieren, indem Sie Gerätekriterien aus einer CSV- oder ähnlichen Datei über ein REST-API-Skript lesen.

Bevor Sie beginnen

- Für Sensoren und ECA-VMs benötigen Sie einen gültigen API-Schlüssel, um Änderungen über die REST-API vorzunehmen und die folgenden Verfahren durchzuführen. (siehe Generieren Sie einen API-Schlüssel.)
- Für Reveal (x) 360 benötigen Sie gültige REST-API-Anmeldeinformationen, um Änderungen über die REST-API vorzunehmen und die folgenden Verfahren durchzuführen. (siehe REST-API-Anmeldeinformationen erstellen.)

Geben Sie ein hoher Wert Gerät über den REST API Explorer an

Wichtig: Der REST-API-Explorer ist auf Reveal (x) 360 nicht verfügbar.

Rufen Sie die ID des Gerät ab

Bevor Sie ein hoher Wert Gerät angeben können, müssen Sie die REST-API-ID des Gerät abrufen.

1. Navigieren Sie in einem Browser zum REST API Explorer.
   Die URL ist der Hostname oder die IP-Adresse Ihres Sensor oder Konsole, gefolgt von `/api/v1/explore/`. Wenn Ihr Hostname beispielsweise seattle-eda ist, lautet die URL `https://seattle-eda/api/v1/explore/`.
2. klicken **Geben Sie den API-Schlüssel ein** und fügen Sie dann Ihren API-Schlüssel ein oder geben Sie ihn in das **API-Schlüssel** Feld.
3. klicken **Autorisieren** und dann klicken **Schliessen**.
4. klicken **POST /Geräte/Suche**.
5. klicken **Probiere es aus**.
   Das JSON-Schema wird automatisch dem Textfeld für den Body-Parameter hinzugefügt.
6. Geben Sie in das Textfeld die Suchkriterien ein, mit denen das Gerät ausgewählt wird.
   Die folgenden Suchkriterien geben ein Gerät mit der IP-Adresse 10.10.10.200 zurück:

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

   Weitere Informationen zu Gerätesuchfiltern finden Sie unter Operandenwerte für die Gerätesuche.
7. klicken **Anfrage senden**.
   Beachten Sie im Abschnitt Antworttext den `id` Feld des Gerät.

Geben Sie ein hoher Wert Gerät an

1. klicken **PATCH /Geräte/ {id}**.

2. klicken **Probiere es aus**.
3. In der **Körper** Feld, geben Sie das folgende JSON-Objekt ein:

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

4. In der **id** Feld, geben Sie die ID des Gerät, das Sie haben im vorherigen Verfahren abgerufen.
5. klicken **Anfrage senden**.
   Wenn die Anfrage erfolgreich ist, wird im Abschnitt Serverantwort der Antwortcode 204 angezeigt.

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

Das ExtraHop GitHub-Repository enthält ein Python-Skript, das eine Liste von IP-Adressen aus einer CSV-Datei liest und alle Geräte mit diesen Adressen als hohen Wert angibt.

1. Gehe zum ExtraHop Codebeispiele GitHub-Repository und laden Sie den Inhalt des `specify_high_value` Verzeichnis auf Ihrem lokalen Computer.
2. Öffnen Sie in einem Texteditor den `ip_list.csv` speichern und ersetzen Sie die IP-Adressen durch die IP-Adressen der Geräte, die Sie als hohen Wert angeben möchten.
3. Öffnen Sie in einem Texteditor den `specify_high_value.py` archivieren und ersetzen Sie die Konfigurationsvariablen durch Informationen aus Ihrer Umgebung.
   - Geben Sie für Sensoren und ECA-VMs die folgenden Konfigurationsvariablen an:
     - **GASTGEBER:** Die IP-Adresse oder der Hostname des Sensor oder der ECA-VM.
     - **API-SCHLÜSSEL:** Der API-Schlüssel.
   - Geben Sie für Reveal (x) 360 die folgenden Konfigurationsvariablen an:
     - **GASTGEBER:** Der Hostname der Reveal (x) 360-API. Dieser Hostname wird auf der Reveal (x) 360 API Access-Seite unter API-Endpunkt angezeigt. Der Hostname enthält nicht die `/oauth2/token`.
     - **ID:** Die ID der Reveal (x) 360-REST-API-Anmeldeinformationen.
     - **GEHEIM:** Das Geheimnis der Reveal (x) 360 REST-API-Anmeldeinformationen.
4. Führen Sie den folgenden Befehl aus:

```
python3 specify_high_value.py
```

Hinweis: Wenn das Skript eine Fehlermeldung zurückgibt, dass die Überprüfung des SSL-Zertifikats 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)
```