Migrate detection hiding rules

Published: 2021-08-28

You can migrate detection hiding rules from one ExtraHop system to another through the REST API. This can be useful if you have created a large number of detection hiding rules and do not want to manually recreate them. In this topic, we show methods for migrating a rule manually through the REST API Explorer and migrating all rules from a Command appliance to Reveal(x) 360 with a Python script.

Before you begin
Both ExtraHop systems must be running firmware version 8.4 or later.

Migrate a detection hiding rule through the REST API Explorer

Note: The REST API Explorer is not available on Reveal(x) 360.

1. Retrieve the detection hiding rule metadata from the source system.
   a) In a browser, navigate to the REST API Explorer.
      The URL is the hostname or IP address of your ExtraHop system, followed by `/api/v1/explore/`. For example, if your hostname is seattle-eda, the URL is `https://seattle-eda/api/v1/explore/`.
   b) Click **Enter API Key** and then paste or type your API key into the **API Key** field.
   c) Click **Authorize** and then click **Close**.
   d) Click **Detections**.
   e) Click **GET /detections/rules/hiding**.
   f) Click **Try it out**.
   g) Click **Send Request**.
   h) In the Response body field, copy the JSON object that represents the detection hiding rule you want to copy.
2. Recreate the detection hiding rule on the target system.
   a) In a browser, navigate to the REST API Explorer.
   b) Click **Enter API Key** and then paste or type your API key into the **API Key** field.
   c) Click **Authorize** and then click **Close**.
   d) Click **Detections**.
   e) Click **POST /detections/rules/hiding**.
   f) Click **Try it out**.
   g) In the body text box, paste the JSON object you copied from the source ExtraHop system.
      The entry should look similar to the following text:

```
{
    "id": 1,
    "enabled": false,
    "detection_type": "cifs_round_trip_time",
    "offender": {
      "object_type": "device",
      "object_id": 123
    },
    "victim": {
      "object_type": "device",
      "object_id": 321
    },
    "author": "example_user",
    "create_time": 1615588932838,
    "expiration": 1615675096000,
```

```
    "detections_hidden": 0,
    "description": null
}
```

h) Click **Send Request**.

3. Optional: Disable the detection rule on the target system.

   If the detection rule was disabled on the source system, indicated by the enabled field set to `false`, set the enabled field to false on the target system.

   a) In a browser, navigate to the REST API Explorer.
   b) Click **Enter API Key** and then paste or type your API key into the **API Key** field.
   c) Click **Authorize** and then click **Close**.
   d) Click **Detections**.
   e) Click **PATCH /detections/rules/hiding**.
   f) Click **Try it out**.
   g) In the body text box, paste the following JSON:

```
{
    "enabled": false
}
```

   h) Click **Send Request**.

Retrieve and run the example Python script

The ExtraHop GitHub repository contains an example Python script that migrates all detection hiding rules on a Command appliance to Reveal(x) 360.

Note: The script only migrates rules that are enabled.

1. Go to the ExtraHop code-examples GitHub repository and download the `migrate_detection_hiding/migrate_detection_hiding.py` file to your local machine.
2. In a text editor, open the `migrate_detection_hiding.py` file and replace the following configuration variables with information from your environment:

   • **SOURCE_HOST:** The hostname of the ExtraHop system you are migrating detection hiding rules from

   • **SOURCE_API_KEY:** The API KEY on the ExtraHop system you are migrating detection hiding rules from

   • **TARGET_HOST:** The hostname of the Reveal(x) 360 API you are migrating detection hiding rules to. This hostname is displayed in the Reveal(x) 360 API Access page under API Endpoint. The hostname does not include the `/oauth/token`.

   • **TARGET_ID:** The ID of the REST API credentials for Reveal(x) 360

   • **TARGET_SECRET:** The secret of the REST API credentials for Reveal(x) 360
3. Run the following command:

```
python3 migrate_detection_hiding.py
```

   If detection hiding rules specify participant devices or device groups by an ID, the script tries to find the IDs of equivalent participants on Reveal(x) 360 by searching for device IP addresses and device group names.

   If the script cannot find the IDs for equivalent participants on Reveal(x) 360, the script prompts you to migrate the other rules that equivalent participants were found for. To continue, type y and press ENTER.

Note: If the script returns an error message that the SSL certificate verification failed, make sure that a trusted certificate has been added to your ExtraHop system. Alternatively, you can add the `verify=False` option to bypass certificate verification. However, this method is not secure and is not recommended. The following code sends an HTTP GET request without certificate verification:

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