Upload STIX files through the REST API

Published: 2024-05-03

Published: 2024-05-03

Threat collections enable your ExtraHop system to identify suspicious IP addresses, hostnames, and URIs found in your network activity. While ExtraHop-curated threat collections are enabled by default, you can also upload a custom threat collection from free or commercial sources.

Before you begin

- For sensors and ECA VMs, you must have a valid API key to make changes through the REST API and complete the procedures below. (See Generate an API key.)
- For Reveal(x) 360, you must have valid REST API credentials to make changes through the REST API and complete the procedures below. (See Create REST API credentials.)
- Familiarize yourself with threat intelligence.

Threat collections must be added and updated to all connected sensors and consoles. And because these sources are often updated frequently, the REST API provides the opportunity to automate updates for threat collections to all sensors and consoles.

Custom threat collections must be formatted in Structured Threat Information Expression (STIX) as compressed TAR files, such as .TGZ or TAR.GZ. ExtraHop systems currently support uploads of STIX file versions 1.0 - 1.2.

Retrieve and run the example Python script

The ExtraHop GitHub repository contains an example Python script that uploads all STIX files in a given directory to a list of sensors and consoles. First, the script reads through a CSV file that contains the URLs and API keys for each system. For each system, the script gets a list of all threat collections that are already on the system. The script then processes each STIX file in the directory for each system.

If the name of the file matches the name of a threat collection on the system, the script overwrites the threat collection with the file contents. If there are no threat collection names that match the file name, the script uploads the file to create a new threat collection.

Note: The following procedure is not compatible with the Reveal(x) 360 REST API. To uploads STIX files to Reveal(x) 360, see Retrieve and run the example Python script for Reveal(x) 360.

1. Go to the ExtraHop code-examples GitHub repository and download the `upload_stix/upload_stix.py` file to your local machine.
2. Create a CSV file with rows that contain the following columns in the specified order:

System hostname	API key

   Tip: The `upload_stix` directory contains an example CSV file named `systems.csv`.

3. In a text editor, open the `upload_stix.py` file and replace the following configuration variables with information from your environment:
   - **SYSTEM_LIST:** The path of the CSV file with the HTTPS URLs and API keys of the systems
   - **STIX_DIR:** The path of the directory that contains the STIX files
4. Run the following command:

```
python3 upload_stix.py
```

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 sensor or console. Alternatively, you can add the `verify=False` option to bypass certificate verification. However, this method is not secure and not recommended. The following code sends an HTTP GET request without certificate verification:

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

Retrieve and run the example Python script for Reveal(x) 360

The ExtraHop GitHub repository contains an example Python script that uploads all STIX files in a given directory to Reveal(x) 360.

If the name of the file matches the name of a threat collection on Reveal(x) 360, the script overwrites the threat collection with the file contents. If there are no threat collection names that match the file name, the script uploads the file to create a new threat collection.

Note: The following procedure is only compatible with the Reveal(x) 360 REST API. To uploads STIX files to sensors and ECA VMs, see Retrieve and run the example Python script.

1. Go to the ExtraHop code-examples GitHub repository and download the `upload_stix/upload_stix_rx360.py` file to your local machine.
2. In a text editor, open the `create_device_groups.py` file and replace the following configuration variables with information from your environment:

   • **HOST:** The hostname of the Reveal(x) 360 API. This hostname is displayed in the Reveal(x) 360 API Access page under API Endpoint. The hostname does not include the `/oauth2/token`.

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

   • **SECRET:** The secret of the Reveal(x) 360 REST API credentials.

   • **STIX_DIR:** The path of the directory that contains the STIX files
3. Run the following command:

   ```
   python3 upload_stix_rx360.py
   ```