

ExtraHop 7.5

Upload STIX files through the REST API to Reveal(x)

Published: 2019-01-08


Published: 2019-01-08

Published: 2019-01-08

By uploading a Structured Threat Information Expression (STIX) file, you can add a threat collection to your ExtraHop Discover and Command appliances. Threat collections enable you to find suspicious hosts, IP addresses, and URIs on your network.

Before you begin

- You must have unlimited [privileges](#) to generate an API key.
- You must have a valid API key to make changes through the REST API and complete the procedures below. (See [Generate an API key](#).)
- Familiarize yourself with [Threat intelligence - Reveal\(x\) only](#).
- Familiarize yourself with the [ExtraHop REST API Guide](#) to learn how to navigate the ExtraHop REST API Explorer.

 **Note:** This topic applies only to ExtraHop Reveal(x) Premium and Ultra.

STIX files must be uploaded to all connected Command and Discover appliances before you can see threat intelligence metrics in the ExtraHop Web UI. Because threat intelligence data is updated frequently (sometimes daily), the REST API offers a way to automate these updates across all appliances.

Here are some important considerations about adding threat collections:

- ExtraHop currently supports STIX versions 1.0 - 1.2.
- The maximum number of observables that a threat collection can contain depends on your platform and license. Contact your ExtraHop representative for more information.

Python script example

The following Python script shows you how to upload all STIX files in a given directory to a list of ExtraHop appliances. First, the script reads through a CSV file that contains the URLs and API keys for each appliance. For each appliance, the script gets a list of all threat collections that are already on the appliance. The script then processes each STIX file in the directory for each appliance.

If the name of the file matches the name of a threat collection on the appliance, 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.

Each row of the CSV file must contain the following columns in the specified order:

HTTPS URL	API key
-----------	---------

 **Note:** The script does not accept a header row in the CSV file.

The script includes the following configuration variables:

- **APPLIANCE_LIST:** The path of the CSV file with the HTTPS URLs and API keys of the appliances

- **STIX_DIR:** The path of the directory that contains the STIX files

```
#!/usr/bin/env python2

import ssl
import json
import os
import requests
import sys
import csv

APPLIANCE_LIST = 'appliances.csv'
STIX_DIR = 'stix_dir'

# Get appliance hostnames and Read through appliance URL and API key list
appliances = []
with open(APPLIANCE_LIST, 'rb') as f:
    reader = csv.reader(f)
    for row in reader:
        appliance = {
            'host': row[0],
            'api_key': row[1]
        }
        appliances.append(appliance)

# Get a json object of every threat collection on the appliance
def getCollections():
    url = host + 'api/v1/threatcollections'
    r = requests.get(url, headers=headers, verify=False)
    return r.json()

# Check which STIX files have already been uploaded
def check_files(collections):
    update_list = []
    skip_list = []
    # Get a list of all stix files in the STIX_DIR directory
    names = []
    for dir, subdirs, files in os.walk(STIX_DIR):
        for file in files:
            if file.endswith(('.tar', '.tar.gz', '.tgz')):
                name = file.split('.')[0]
                names.append(name)
    # Check each threat collection for names that match the STIX file names
    for c in collections:
        c_name = c['name']
        if c_name in names:
            update_list.append(c)
            skip_list.append(c_name)
    return update_list, skip_list

# Process each file in the STIX_DIR directory
# If it is for a new threat collection, add the threat collection
# If there is already a threat collection for the file, update the threat
collection
def process_files(update_files, skip_list):
    for dir, subdirs, files in os.walk(STIX_DIR):
        for file in files:
            name = file.split('.')[0]
            if file.endswith(('.tar', '.tar.gz', '.tgz')) and name not in
skip_list:
                upload_new(file, dir)
            else:
                for c in update_files:
```

```
        if c['name'] == name:
            update_old(file, dir, c)

# Upload a new threat collection
def upload_new(file, dir):
    print 'Uploading ' + file + ' on ' + host
    url = host + 'api/v1/threatcollections'
    file_path = os.path.join(dir, file)
    name = file.split('.')[0]
    files = {'file': open(file_path, 'rb')}
    values = {'name': name}
    r = requests.post(url, data=values, files=files, headers=headers,
verify=False)
    print r.status_code
    print r.text

# Update an existing threat collection
def update_old(file, dir, c):
    print 'Updating ' + file + ' on ' + host
    url = host + 'api/v1/threatcollections/~' + str(c['user_key'])
    file_path = os.path.join(dir, file)
    files = {'file': open(file_path, 'rb')}
    r = requests.put(url, files=files, headers=headers, verify=False)
    print r.status_code
    print r.text

# Process STIX files for each appliance
for appliance in appliances:
    host = appliance['host']
    api_key = appliance['api_key']
    context = ssl.SSLContext(ssl.PROTOCOL_TLSv1_2)
    headers = {'Authorization': 'ExtraHop apikey=%s' % api_key}
    collections = getCollections()
    update_files, skip_list = check_files(collections)
    process_files(update_files, skip_list)
```