Add observations through the REST API

Published: 2021-09-04

Observations enable you to associate two or more IP addresses. For example, you can add an observation that tracks the activity of a VPN user by reading VPN logs and then associating the IP address of the VPN client on your network with the external IP address assigned to the user on the internet. This guide provides instructions for adding an observation through the ExtraHop REST API Explorer and through a Python script.

Before you begin

- You must log in to the ExtraHop system with an account that has full write 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 the ExtraHop REST API Guide to learn how to navigate the ExtraHop REST API Explorer.

Add observations through the REST API Explorer

1. 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/`.
2. Click **Enter API Key** and then paste or type your API key into the **API Key** field.
3. Click **Authorize** and then click **Close**.
4. Click **Observations** and then click **POST /observations/associatedipaddrs**.
5. Click **Try it out**.

   The JSON schema is automatically added to the body parameter text box.
6. In the body text box, specify the observations you want to add.

   For example, the following fields associate 10.8.0.0 with 108.162.0.0:

```
{
    "observations": [
        {
            "associated_ipaddr": "108.162.0.0",
            "ipaddr": "10.8.0.0",
            "timestamp": 1257935231
        }
    ],
    "source": "OpenVPN"
}
```

7. Click **Send Request**.

Python script example

The following Python script creates associations on the ExtraHop system based on a CSV log file from OpenVPN. You can configure the script to read other CSV files by modifying the `IPADDR`, `ASSOCIATED_IPADDR`, and `TIMESTAMP` variables, which specify the names of the CSV columns that the script reads.

The script includes the following configuration variables that you must replace with information from your environment:

© 2021 ExtraHop Networks, Inc. All rights reserved.

- **HOST:** The IP address or hostname of the ExtraHop system.
- **API_KEY:** The API key.
- **CSV_FILE:** The name of the CSV file.
- **SOURCE:** The source of the observations.
- **IPADDR:** The name of the column in the CSV file that specifies the IP addresses of the VPN clients on your internal network.
- **ASSOCIATED_IPADDR:** The name of the column in the CSV file that specifies the external IP addresses assigned to the users on the public internet.
- **TIMESTAMP:** The name of the column in the CSV file that specifies the time that the observation was created by the source. By default, the timestamp must be in the format: `Month/Day/Year Hour:Minute:Second`. However, you can change the format by modifying the `pattern` variable in the `translateTime()` function.

Tip: If the log file distributes timestamp values over multiple columns, you can modify the `timestamp` field in the `readCSV()` function to concatenate the values. For example, assume that the first four columns of the CSV file are organized as shown in the following table:

01	01	01	10:10:10
Month	**Day**	**Year**	**Time**

The following code reads those first four columns into the default `translateTime()` function:

```
'timestamp': translateTime(row[0] + '/' + row[1] + '/' + row[2] + ' ' +

 row[3])
```

```
#!/usr/bin/python3

import json
import csv
import time
import requests

HOST = 'https://extrahop.example.com'
API_KEY = '123456789abcdefghijklmnop'
CSV_FILE = 'log.csv'
SOURCE = 'OpenVPN'

ASSOCIATED_IPADDR = 'Real IP'
IPADDR = 'VPN IP'
TIMESTAMP = 'Start Time'

# Function that extracts observations from CSV file
def readCSV(associated_ipaddr, ipaddr, timestamp):
    observations = []
    with open(CSV_FILE, 'rt', encoding='ascii') as f:
        reader = csv.reader(f)
        header = next(reader, None)
        for row in reader:
            observations.append({
                'associated_ipaddr': row[header.index(associated_ipaddr)],
                'ipaddr': row[header.index(ipaddr)],
                'timestamp': translateTime(row[header.index(timestamp)])
            })
    return observations

# Function that translates formatted timestamp into epoch time
def translateTime(t):
```

```
    pattern = '%m/%d/%y %H:%M:%S'
    return int(time.mktime(time.strptime(t, pattern)))

# Function that sends observations to the ExtraHop system
def makeObservations(observations):
    url = HOST + '/api/v1/observations/associatedipaddrs'
    headers = {
        'Content-Type': 'application/json',
        'Accept': 'application/json',
        'Authorization': 'ExtraHop apikey=%s' % API_KEY
    }
    data = {
        'observations': observations,
        'source': SOURCE
    }
    r = requests.post(url, headers=headers, data=json.dumps(data))
    if r.status_code == 202:
        print(r.text)
    else:
        print('Observation upload failed')
        print(r.text)

observations = readCSV(ASSOCIATED_IPADDR, IPADDR, TIMESTAMP)
makeObservations(observations)
```

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)
```