ThreatQuotient

Flashpoint Connector Implementation Guide

Version 1.0.1

Wednesday, November 6, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Last Updated: Wednesday, November 6, 2019

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions: `4.21.1` or higher

Introduction

The Flashpoint feed retrieves reports and indicators data.

Prerequisites

ThreatQ version 4.25 included the full STIX 2.0 object set. If you have not upgraded your ThreatQ instance to version 4.25 or later, Report objects (STIX 2.0 custom object) must be installed prior to running the feed.

The commands to install the custom objects are as follows:

1. `cd /var/www/api`
2. `sudo php artisan threatq:create-custom-objects`
3. `sudo php artisan threatq:make-object-set --file=/var/www/api/database/seeds/data/custom_objects/stix2_0.json`
4. `sudo php artisan up`

Installation

Complete the following steps to install the connector:

1. Log into https://marketplace.threatq.com/.
2. Download the **flashpoint.yaml** file.
3. From the ThreatQ user interface, select the **Settings icon > Incoming Feeds**.
4. Click **Add New Feed**.
5. In the Add New Feed dialog box, complete one of the following actions:
   - Drag and drop the yaml file into the dialog box.
   - **Click to browse** to the yaml file and select it.

   The connector installs as a feed on **Commercial** tab.
6. Under Flashpoint, click **Feed Settings**.
7. Enter the Flashpoint account API key.
8. Click the toggle button next to Flashpoint to enable the feed.
9. Click **Save Changes**.

ThreatQ Mapping

Flashpoint provides an API that users can use to programmatically extract data in JSON format. The response contains a list of reports and indicators.

The API uses HTTP and requires a Bearer token for authentication.

Endpoints:

- **Reports** - GET /api/v4/reports/

  Parameters:

```
* since (string) - Only include reports published on or after
the specified date and time. Must be either a datetime or a
relative time period. A datetime must have the format
"YYYY-MM-DDThh:mm:ss.sssZ", where decimal seconds are
```

```
optional.
* until (string) - Only include reports published on or before
the specified date and time. Must be either a datetime or a
relative time period. A datetime must have the format
"YYYY-MM-DDThh:mm:ss.sssZ", where decimal seconds are
optional.
* Pagination Limit = 10
```

Example of the response:

```
{
    "total": 11934,
    "limit": 10,
    "count": 10,
    "skip": 0,
    "data": [
        {
            "id": "mKrYBtVbQBS69D3-oMQyMQ",
            "title": "ISIS Releases Infographic Illustrating
            its Attacks Throughout First Half of 2019",
            "summary": "This weekly report highlights ...",
            "tags": [
                "Communities & NGOs",
                "Government & Policymakers",
            ],
            "title_asset": "/assets/BTnrNdemRXCd2snXQaQT_Q",
            "body": "ISIS Releases...",
            "title_asset_id": "BTnrNdemRXCd2snXQaQT_Q",
            "assets": [
                "/assets/lPzQsDD2SZ2zWYfqoQUn8Q"
            ],
```

```
            "asset_ids": [
                "lPzQsDD2SZ2zWYfqoQUn8Q"
            ],
            "sources": [
                {
                    "original": "https://fp.tools/home/
                    intelligence/reports/report/
                    91YaRg_2RbeAjIxKHe7c7A",
                    "platform_url": "https://fp.tools/
                    home/intelligence/reports/report/
                    91YaRg_2RbeAjIxKHe7c7A#detail",
                    "source_id": "91YaRg_2RbeAjIxKHe7c7A",
                    "source": "/reports/91YaRg_2RbeAjIxKH
                    e7c7A",
                    "type": "Report",
                    "title": "Global Spotlight - Iran: Key
                    Developments This Week"
                },
                {
                    "original": "https://fp.tools/
                    api/v4/indicators/event/FjPBIU
                    9zRSOGS6PpJmP50Q?",
                    "platform_url": "https://fp.tools/
                    api/v4/indicators/event/FjPBIU
                    9zRSOGS6PpJmP50Q#detail",
                    "source_id": "FjPBIU9zRSOGS6PpJmP50Q",
                    "source": "/reports/FjPBIU9zRSOGS6Pp
                    JmP50Q",
                    "type": "Report",
```

```
                    "title": "ISIS Issues First Claim of
                    Responsibility for Activities in
                    Mozambique Amid Expanding Africa
                    Presence"
                }
            ],
            "is_featured": false,
            "ingested_at": "2019-07-29T20:33:55.409+00:00",
            "posted_at": "2019-07-29T20:33:55.409+00:00",
            "platform_url": "https://fp.tools/home/
            intelligence/reports/report/mKrYBtVbQBS69
            D3-oMQyMQ#detail",
            "notified_at": "2019-07-29T20:33:55.409+00:00",
            "updated_at": "2019-07-29T20:33:55.409+00:00",
            "version_posted_at": "2019-07-29T20:33:55.409+
            00:00",
            "published_status": "published"
        }
    ]
}
```


- **Related Reports** - GET/api/v4/reports/{report_id}/related

  For each report, the related reports are being retrieved, each of them having related indicators, as described for the previous endpoint.

  The format is the same as the above.

- **Related Indicators** - GET/api/v4/indicators/event/{event_id}

For each report, we call this endpoint in order to get information about the related indicators. The id of the indicator is taken from "sources[].original", as being the id following the url "https://fp.tools/home/intelligence/reports/report/"

Example of the response:


```
[
        {
         "Event": {
             "Attribute": [
                 {
                     "category": "Payload installation",
                     "comment": "Hash for Phobos Malware, from
                     Virus Total",
                     "fpid": "CJOaTCYLXsGhyfyKXyT_eg",
                     "href": "https://fp.tools/
                     api/v4/indicators/attribute/
                     CJOaTCYLXsGhyfyKXyT_eg",
                     "timestamp": "1564088142",
                     "to_ids": true,
                     "type": "sha256",
                     "uuid": "5d3a174e-51d8-466e-b888-
                     05d00a640c05",
                     "value": {
                             "comment": "Hash for Phobos
                             Malware, from Virus Total",
                             "sha256": "18637c278083785d8c5
                             cafdcbf819407182fc554c90c
                             75d02bd10d6a9c6feaff"
                     }
                 }
```

```
        ],
        "Galaxy": [
            {
                "GalaxyCluster": [
                    {
                        "type": "mitre-enterprise-attack-
                        attack-pattern",
                        "value": "Change Default File
                        Association - T1042",
                        ...
                    }
                ],
                ...
            }
        ],
        "Tag": [
            {
                "name": "malware:Phobos",
                "numerical_value": null
            }
        ],
        "attribute_count": "5",
        "date": "2019-07-23",
        "event_creator_email":
        "info@flashpoint-intel.com",
        "info": "Phobos Ransomware",
        "publish_timestamp": "1564154422",
        "report": "https://fp.tools/home/
        intelligence/reports/report/
        VU-GBMoDR-SoHWxWRSPLvQ",
```

```
            "timestamp": "1564154421",
            "uuid": "5d3757e5-3bbc-4a31-9be3-56550a640c05"
        },
        "basetypes": [
            "misp",
            "indicator"
        ],
        "fpid": "viArcNG0WR-eCjo2uhZUYg",
        "header_": {
            "indexed_at": 1564154470,
            "ingested_at": 1564154467,
            "is_visible": true,
            "observed_at": 1564154467,
            "source": "urn:fp:component:misp-exporter"
        },
        "href": "https://fp.tools/api/v4/indicators/event/
        viArcNG0WR-eCjo2uhZUYg"
    }
}
```


- **Orphaned Events** - GET/api/v4/indicators/event

  This endpoint is called only once and it retrieves indicators that are not related to any report.

  The format is the same as the above.

  ThreatQ provides the following default mapping for the feed.

Flashpoint Key	ThreatQ Entity	ThreatQ Name	Examples	Notes
Report				
title	report .name		ISIS Releases Infographi...	
body	report .de-scription		ISIS Releases...	The descrip-tions larger than 32766 char-acters will be rejected and the value will remain empty.
id	report .attribute	Report ID	https://fp.tools/home/intelligence/reports/report/mKrYBtVbQBS69D3-oMQyMQ	
tags[]	report .attribute	Tag	Communities & NGOs	

Flashpoint Key	ThreatQ Entity	ThreatQ Name	Examples	Notes
asset_ids[]	report.attribute	Assets	https://fp.tools/ui/v-4/asset-s/lPzQDD2SZ2zWYfqoQUn8Q?size=orig	
sources[].type, sources[].title	report.attribute	Source	Report, Global Spotlight - Iran: Key Developments	
is_featured	report.attribute	Is Featured	True	
ingested_at	report.attribute	Ingested At	2019-07-29T20:33:55.409+00:00	
notified_at	report.attribute	Notified At	2019-07-29T20:33:55.409+00:00	
updated_at	report.attribute	Updated At	2019-07-29T20:33:55.409+00:00	
published_status	report.attribute	Published Status	published	
platform_	report	Platform		

Flashpoint Key	ThreatQ Entity	ThreatQ Name	Examples	Notes
url	.attribute	URL		
sources[].original	report.attribute	Events ids	FjPBIU9zRSOGS6PpJmP50Q	The id following https://fp.tools/api/v4/indicators/event
Indicator				
Event.Attributes[].value.value	indicator.value		18637c278083785d8c5cafdcbf819407182fc554c90c75-d02bd10d6a9c6feaf-f	
Event.Attributes[].type	indicator.type		SHA-256	see mapping below
Event.Attributes[].timestamp	indicator.published_at		1564154421	
Event	indicator	Category	Payload install-	

Flashpoint Key	ThreatQ Entity	ThreatQ Name	Examples	Notes
.Attributes []. category	.attribute		ation	
Event .Attributes []. value .comment	indicator .attribute	Comment	Hash for Phobos Malware, from Virus Total	
Event .Attributes []. href	indicator .attribute	Refer- ence	https://fp.tools/ api/v4/indicators/ attribute/CJOaTC YLXsGhyfyKXyT_ eg	
Event .Attributes []. to_ids	indicator .attribute	To IDS	True	
Attack pattern				
Event .Galaxy []. Galaxy Cluster []. value	attack_ pattern .value		T1042 - Change Default File Association	if type = 'mitre- enterprise- attack- attack-pattern'

The mapping between the indicator types in Flashpoint and ThreatQ is:

Flashpoint	ThreatQ
md5	MD5
sha1	SHA-1
sha256	SHA-256
sha512	SHA-512

Change Log

Version 1.0.1:

We have fixed an issue where the Flashpoint feed failed to perform historic feed pulls.