ThreatQuotient

Flashpoint Connector Implementation Guide

Version 2.0.0

Monday, February 3, 2020

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: Monday, February 3, 2020

Contents

Versioning

- Current integration version: `2.0.0`
- 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

Perform the following steps to install the feed:

The same steps can be used to upgrade the feed to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **Flashpoint** feed file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed file on your local machine

ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

The feed will be added to the **Commercial** tab for Incoming Feeds. You will still need to configure and then enable the feed.

Configuration

ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other feed-related credentials.

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **Commercial** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameter:

Parameter	Description
API Key	The Bearer Token used for authentication.

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed name to enable the feed.

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 include:

- Reports
- Related Reports
- Related Indicators
- Orphaned Events
- IP Indicators

Reports

- **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 = 100
```

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/in-
telligence/reports/report/91YaRg_2RbeAjIxKHe7c7A",
```

```
                    "platform_url": "https://fp.tools/home/in-
telligence/reports/report/91YaRg_2RbeAjIxKHe7c7A#detail",
                    "source_id": "91YaRg_2RbeAjIxKHe7c7A",
                    "source": "/reports/91YaRg_
2RbeAjIxKHe7c7A",
                    "type": "Report",
                    "title": "Global Spotlight - Iran: Key
Developments This Week"
                },
                {
                    "original": "https://fp.tools/ap-
i/v4/indicators/event/FjPBIU9zRSOGS6PpJmP50Q?",
                    "platform_url":
"https://fp.tools/ap-
i/v4/indicators/event/FjPBIU9zRSOGS6PpJmP50Q#detail",
                    "source_id": "FjPBIU9zRSOGS6PpJmP50Q",
                    "source": "/re-
ports/FjPBIU9zRSOGS6PpJmP50Q",
                    "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/in-
telligence/reports/report/mKrYBtVbQBS69D3-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

- **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

- **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/ap-
i/v4/indicators/attribute/CJOaTCYLXsGhyfyKXyT_eg",
                    "timestamp": "1564088142",
                    "to_ids": true,
                    "type": "sha256",
                    "uuid": "5d3a174e-51d8-466e-b888-
05d00a640c05",
                    "value": {
                            "comment": "Hash for Phobos Mal-
ware, from Virus Total",
                            "sha256": "18637c278083785d8c5-
cafdcbf819407182fc554c90c75d02bd10d6a9c6feaff"
                    }
                }
            ],
            "Galaxy": [
                {
                    "GalaxyCluster": [
                        {
                            "type": "mitre-enterprise-attack-
attack-pattern",
                            "value": "Change Default File Asso-
ciation - 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/in-
telligence/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/ap-
i/v4/indicators/event/viArcNG0WR-eCjo2uhZUYg"
    }
}
```

Orphaned Events

- **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.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.data[].title	report.name		ISIS Releases Infographi...	
.data[].body	report.description		ISIS Releases...	The descriptions larger than 32766 chars will be rejected and the value will remain empty.
.data[].id	report.attribute	Report ID	https://fp.tools/home/intelligence/reports/report/mKrYBtVbQBS69D3-oMQyMQ	
.data[].tags[]	report.attribute	Tag	Communities & NGOs	
.data[].asset_ids[]	report.attribute	Assets	https://fp.tools/ui/v4/assets/lPzQsDD2SZ2zWYfqoQUn8Q?size=orig	
.data	report.attribute	Source	Report, Global Spotlight - Iran: Key Developments	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
[].sources[].title				
.data[].is_featured	report.attribute	Is Featured	True	
.data[].ingested_at	report.attribute	Ingested At	2019-07-29T20:33:55.409+00:00	
.data[].notified_at	report.attribute	Notified At	2019-07-29T20:33:55.409+00:00	
.data[].updated_at	report.attribute	Updated At	2019-07-29T20:33:55.409+00:00	
.data[].published_status	report.attribute	Published	published	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
		Status		
.data[].data-platform_url	report.attribute	Platform URL		
.data[].sources[].original	report.attribute	Events ids	FjPBIU9zRSOGS6PpJmP50Q	The id following https://fp.tools/api/v4/indicators/event
.Event.Attributes[].value.value	indicator.value	SHA-256	18637c278083785d8c5-cafdcbf819407182fc554c90c75d02bd10d6a9c6feaff	
.Event.Attributes[].timestamp	indicator.published_at		1564154421	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.Event.Attributes[].category	indicator.attribute	Category	Payload installation	
.Event.Attributes[].value.comment	indicator.attribute	Comment	Hash for Phobos Malware, from Virus Total	
.Event.Attributes[].href	indicator.attribute	Reference	https://fp.tools/api/v4/indicators/attribute/CJOaTCYLXsGhyfyKXyT_eg	
.Event.Attributes[].to_ids	indicator.attribute	To IDS	True	
.Event.Galaxy	attack_pattern.value		T1042 - Change Default File Association	if type = 'mitre-enterprise-attack-attack-pattern'

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
[].GalaxyCluster[].value				
Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.data[].title	report.name		ISIS Releases Infographi...	
.data[].body	report.description		ISIS Releases...	The descriptions larger than 32766 chars will be rejected and the value will remain empty.
.data[].id	report.attribute	Report ID	https://fp.tools/home/intelligence/reports/report/mKrYBtVbQBS69D3-oMQyMQ	

IP Indicators

- **IP Indicators** - GET/api/v4/indicators/attribute?types=ip-src

This endpoint is called only once and it retrieves IP Address and URL Indicators, as well as Events.

Example of response:


```
{
    "Event": {
      "Tag": [
        {
          "name": "vulnerability:cve:CVE-2018-2893"
        },
        {
          "name": "report:OJdEgLiLTvqjnn1cBMTuvg"
        }
      ],
      "attribute_count": "14",
      "date": "2018-07-27",
      "event_creator_email": "info@flashpoint-intel.com",
      "fpid": "cEJ6EZD_XZu3W0vw2wB4fg",
      "href": "https://fp.tools/ap-
i/v4/indicators/event/cEJ6EZD_XZu3W0vw2wB4fg",
      "info": "CVE-2018-2893",
      "publish_timestamp": "1540932685",
      "report": "https://fp.tools/home/in-
telligence/reports/report/OJdEgLiLTvqjnn1cBMTuvg",
      "timestamp": "1533152744",
```

```
      "uuid": "5b5aed3f-5220-4862-9611-64810a640c05"
    },
    "basetypes": [
      "indicator",
      "indicator_attribute"
    ],
    "category": "Network activity",
    "fpid": "Of_9va3-XjCFgho85TBYZg",
    "header_": {
      "indexed_at": 1560989346,
      "ingested_at": 1560935433,
      "is_visible": true,
      "observed_at": 1560935433,
      "source": "urn:fp:resource:qualified:indicator"
    },
    "href": "https://fp.tools/api/v4/indicators/attribute/Of_
9va3-XjCFgho85TBYZg",
    "timestamp": "1532685835",
    "to_ids": false,
    "type": "ip-src",
    "uuid": "5b5aee0b-0a20-4efc-b899-662d0a640c05",
    "value": {
      "comment": "payload hosting IP",
      "ip-src": "103.99.115.220"
    }
}
```

ThreatQ provides the following default mapping for the feed.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.Event.info	event.name	Flashpoint Event	"Winnti Burning Unbrella"	
.Event.Tag[].name	event.attribute	Tags	"source:OSINT"	
.Event.date	event.attribute	Date	"2018-05-21"	
.Event.event_creator_email	event.attribute	Event Creator Email	"info@flashpoint-intel.com"	
.Event.href	event.attribute	Href	"https://fp.tools/api/v4/indicators/event/t4v43lHPV1CV2-NEqUJSug"	
.Event.fpid	event.attribute	FPID	"t4v43lHPV1CV2-NEqUJSug"	
.Event.publish_timestamp	event.attribute	Publish Timestamp	"1540933386"	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.Event.timestamp	event.attribute	Timestamp	"1527187990"	
.Event.uuid	event.attribute	UUID	"5b02fb5e-8470-4971-babe-4b9f0a640c05"	
.value.ip-src	indicator.value	IP Address	"98.126.107.249"	Indicator of type IP Address, see attributes below
.value.comment	indicator.value	URL	"http://401trg.pw/burning-umbrella"	Indicator of type URL, see

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
				attrib-utes below
.href	indicator.attribute	HREF	"https://fp.tools/ap-i/v4/indicators/attribute/7uvMMqlmVkGrMWLsynUD1A"	
.to_ids	indicator.attribute	To IDS	"false"	
.timestamp	indic-ator.published_at		"1526927159"	
.uuid	indicator.attribute	UUID	"5b030e82-db88-4d85-9b1f-64810a640c05"	
.category	indicator.attribute	Category	"Network activity"	
.fpid	indicator.attribute	FPID	"7uvMMqlmVkGrMWLsynUD1A"	
.header_.indexed_at	indicator.attribute	Indexed At		

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.header_.ingested_at	indicator.attribute	Ingested At		
.header_.is_visible	indicator.attribute	Is Visible		
.header_.observed_at	indicator.attribute	Observed At		
.header_.source	indicator.attribute	FP Source	"urn:fp:resource:qualified:indicator"	

Indicator Type Mapping

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

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