

ThreatQuotient



Flashpoint CDF Guide

Version 3.2.0

July 25, 2022

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147



ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

- Integration Details..... 5
- Introduction 6
- Installation..... 7
- Configuration 8
- ThreatQ Mapping 10
 - Flashpoint (Feed), Flashpoint Events..... 10
 - Flashpoint Related Events (Supplemental)..... 13
 - Type Mapping..... 17
- Average Feed Run..... 18
 - Flashpoint Feed, Flashpoint Events..... 18
 - Flashpoint Related Events (Supplemental)..... 19
- Known Issues / Limitations 20
- Change Log..... 21

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.

Copyright © 2022 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com

Support Web: <https://support.threatq.com>

Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	3.2.0
Compatible with ThreatQ Versions	>= 4.28.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https:// marketplace.threatq.com/ details/flashpoint

Introduction

The Flashpoint CDF delivers actionable threat intelligence in the form of compromised Adversaries, Attack Patterns, Events, Indicators, Malware, Reports and Vulnerabilities.

The integration ingests threat intelligence data from the following feeds:

- **Flashpoint Feed** - ingests compromised Reports and any related Events, Indicators, Adversaries, Malware, Vulnerabilities and Attack Patterns.
- **Flashpoint Events** - ingests related Events.
- **Flashpoint Related Events (Supplemental)** - called once per each `.data[].id` returned by the Flashpoint feed.

The integration ingests the following system object types:

- Adversaries
 - Adversary Attributes
- Events
 - Event Attributes
- Indicators
 - Indicator Attributes
- Malware
- Vulnerabilities

Installation

Perform the following steps to install the integration:



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

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration 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.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

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 integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

Flashpoint Feed

PARAMETER	DESCRIPTION
API Key	Your Flashpoint API Key.
Parse for Selected Indicators	Select the types of indicators to parse out of the report body. Options include: ◦ CVEs ◦ MD5 Hashes ◦ SHA-1 Hashes ◦ SHA-256 Hashes ◦ SHA-512 Hashes ◦ IP Addresses
Save Actor Profile As	Determines whether a Report containing a Tag with an 'Actor Profile' value should be ingested as an Adversary or as an Intrusion Set.

Flashpoint Events Feed

PARAMETER	DESCRIPTION
API Key	Your Flashpoint API Key.
Indicator Type Filter	Select the types of indicators to parse out of the report body. Options include: ◦ MD5 Hashes ◦ SHA-1 Hashes ◦ SHA-256 Hashes ◦ SHA-512 Hashes ◦ URLs ◦ Domains ◦ Source IPs ◦ Destination IPs ◦ Email Addresses

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Flashpoint (Feed), Flashpoint Events

The Flashpoint feed ingests compromised Reports and any related Events, Indicators, Adversaries, Malware, Vulnerabilities and Attack Patterns.

Flashpoint Feed - GET <https://fp.tools/api/v4/reports>

Flashpoint Events - <https://fp.tools/api/v4/indicators/event>



In order to fetch related events, `.data[].sources[].original` is used as the `<event_id>` parameter for the Related Events endpoint. The `<event_id>` is extracted from the URL (e.g., in <https://fp.tools/api/v4/indicators/event/5e7a40ba-e198-4e44-90f5-007b0a212811>, the `<event_id>` will be equal to `5e7a40ba-e198-4e44-90f5-007b0a212811`).

Sample Response:

```
{
  "total": 20,
  "limit": 1,
  "count": 1,
  "skip": 0,
  "data": [
    {
      "id": "XWnZwZYsS1WzljFH2SqIeA",
      "title": "Coronavirus (COVID-19) Threats (Analyst Knowledge Page)",
      "summary": "Risks concerning the coronavirus (COVID-19) began in early January 2020, shortly after the virus began to receive media attention.",
      "tags": [
        "Cybercrime",
        "Knowledge Base",
        "Malware",
        "Events"
      ],
      "body": "<html><head></head><body class=\"c47 c60\"><div><p class=\"c51 c10 c55\"><span class=....",
      "title_asset": "/assets/9vXqarKJRPuHLA8UUntAA",
      "title_asset_id": "9vXqarKJRPuHLA8UUntAA",
      "assets": [
        "/assets/agEIfiLjSe6e7FXcuPiaLg",
        "/assets/2c2At8cZTT--JcGvqYUK0w",
        "/assets/6ofKfKcER5aqR0XTtSEZsA"
      ],
      "asset_ids": [
        "agEIfiLjSe6e7FXcuPiaLg",
        "2c2At8cZTT--JcGvqYUK0w"
      ],
      "sources": [
```

```
{
  "original": "https://fp.tools/api/v4/indicators/event/5e7a40ba-e198-4e44-90f5-007b0a212811",
  "platform_url": null,
  "source": null,
  "source_id": null,
  "type": "External",
  "title": "https://fp.tools/api/v4/indicators/event/5e7a40ba-e198-4e44-90f5-007b0a212811"
},
{
  "original": "https://fp.tools/api/v4/indicators/event/5e7a471c-6f7c-4097-a4d0-061c0a212913",
  "platform_url": null,
  "source": null,
  "source_id": null,
  "type": "External",
  "title": "https://fp.tools/api/v4/indicators/event/5e7a471c-6f7c-4097-a4d0-061c0a212913"
}
],
"is_featured": false,
"ingested_at": "2020-07-31T19:44:52.090+00:00",
"posted_at": "2020-07-31T19:44:52.090+00:00",
"platform_url": "https://fp.tools/home/intelligence/reports/report/XwnZwZysS1WzljFH2SqIeA#detail",
"notified_at": null,
"updated_at": "2020-07-31T19:44:52.090+00:00",
"version_posted_at": "2020-07-31T19:40:01.041+00:00",
"published_status": "published"
}
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].title	Report.Value	N/A	.data[].ingested_at	'Coronavirus (COVID-19) Threats (Analyst Knowledge Page)'	Extracted value between " if " is available else trimmed Actor Profile: / Actor Profile Update: from the value, only applicable if .tags[] contains Actor Profile as an item
.data[].body	Report.Description	N/A	N/A	<html><head></head><body class=\"c47 c60\"><div><p class=\"c51 c10 c55\"><span class=....	Formatted and trimmed
.data[].summary	Report.Attribute	Summary	.data[].ingested_at	'Risks concerning the coronavirus (COVID-19) began in early January 2020, shortly after...'	Stripped HTML tags
.data[].tags	Report.Tag	Tag	N/A	['Cybercrime', 'Knowledge Base', 'Malware', 'Events']	If .tags[] contains Actor Profile as an item, the report will be ingested as selected by the user (see Save Actor Profile As user field)

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].sources[].title	Report.Attribute	Source	.data[].ingested_at	['External, https://fp.tools/api/v4/indicators/event/5e7a40ba-e198-4e44-90f5-007b0a212811', ...]	Converted to '.type', '.title', added only if title is present
.data[].asset_ids[]	Report.Attribute	Asset	.data[].ingested_at	['https://fp.tools/ui/v4/assets/agElfiLjSe6e7FXcuPiaLg?size=orig', 'https://fp.tools/ui/v4/assets/2c2At8cZTT--JcGvqYUKOw?size=orig']	Converted to https://fp.tools/ui/v4/assets/<asset_id>?size=orig
.data[].published_status	Report.Attribute	Published Status	.data[].ingested_at	'published'	N/A
.data[].platform_url	Report.Attribute	Platform URL	.data[].ingested_at	'https://fp.tools/home/intelligence/reports/report/XWnZwZYsS1WzljFH2SqeA#detail'	N/A
.data[].is_featured	Report.Attribute	Is Featured	.data[].ingested_at	false	N/A
.data[].body	Indicator.Value	MD5	.data[].ingested_at	492c423824351ff8dc1ed4bba761d200	Extracted using regex
.data[].body	Indicator.Value	SHA1	.data[].ingested_at	2dab955dab3fbf895047d74b5d232ab444e9d0d2	Extracted using regex
.data[].body	Indicator.Value	SHA256	.data[].ingested_at	d028e64bf4ec97dfd655ccd1157a5b96515d461a710231ac8a529d7bdb936ff3	Extracted using regex
.data[].body	Indicator.Value	SHA512	.data[].ingested_at	6473dac67b75194deaeaf37103bba17936f6c16ffcd2a7345a5a46756996fad748a97f36f8fd4be4e1f264ece313773cc5596099d68e71344d8135f50e5d8971	Extracted using regex
.data[].body	Indicator.Value	IP Address	.data[].ingested_at	167.114.242.226	Extracted using regex
.data[].body	Indicator.Value	CVE	.data[].ingested_at	CVE-2022-26143	Extracted using regex

Flashpoint Related Events (Supplemental)

The Flashpoint Related Events Supplemental feed is called once per each `.data[].id` returned by the Flashpoint feed.

GET `https://fp.tools/api/v4/indicators/event/<event_id>`

Sample Response:

```
[
  {
    "Event": {
      "Attribute": [
        {
          "category": "Network activity",
          "comment": "URLhaus database for malware",
          "first_seen": null,
          "fpid": "voX150-rw4exr1YKF2Gc_A",
          "href": "https://fp.tools/api/v4/indicators/attribute/voX150-rw4exr1YKF2Gc_A",
          "last_seen": null,
          "timestamp": "1588173544",
          "type": "url",
          "uuid": "5ea99ae8-6564-491c-86b4-46550a212b08",
          "value": {
            "comment": "",
            "url": "http://toliku.com/"
          }
        }
      ],
    },
    {
      "category": "Payload delivery",
      "comment": "",
      "first_seen": null,
      "fpid": "mZsbBwsowE-ykhS6oXyE9A",
      "href": "https://fp.tools/api/v4/indicators/attribute/mZsbBwsowE-ykhS6oXyE9A",
      "last_seen": null,
      "timestamp": "1588173393",
      "type": "sha256",
      "uuid": "5ea99a51-6e90-49cd-85ef-473b0a212921",
      "value": {
        "comment": "",
        "sha256": "f1013d882f4507c08976debd09f202e4b2c1a0939ea136ede34a78ad8b2ef069"
      }
    }
  ],
  "Galaxy": [
    "<Trimmed data, not used in TQ mapping>"
  ],
  "Tag": [
    {
      "local": 0,
      "name": "Banker: Dridex",
      "numerical_value": null
    },
    {
      "local": 0,
      "name": "COVID-19",
    }
  ]
}
```

```
        "numerical_value": null
    },
    {
        "local": 0,
        "name": "CoronaVirus",
        "numerical_value": null
    },
    {
        "local": 0,
        "name": "malware:Dridex",
        "numerical_value": null
    },
    {
        "local": 0,
        "name": "misp-galaxy:mitre-enterprise-attack-attack-pattern=\"Account Discovery - T1087\"",
        "numerical_value": null
    },
    {
        "local": 0,
        "name": "misp-galaxy:mitre-enterprise-attack-attack-pattern=\"Automated Collection - T1119\"",
        "numerical_value": null
    },
    {
        "local": 0,
        "name": "report:XWnZwZYsS1WzljFH2SqIeA",
        "numerical_value": null
    }
],
"attribute_count": "20",
"date": "2020-04-29",
"event_creator_email": "info@flashpoint-intel.com",
"info": "[COVID-19 04/29/2020] - Dridex",
"publish_timestamp": "1588183253",
"report": "https://fp.tools/home/intelligence/reports/report/XWnZwZYsS1WzljFH2SqIeA",
"timestamp": "1588183250",
"uuid": "5ea99719-f978-44a4-b0d3-4b7e0a212921"
},
"attack_ids": [
    "T1087",
    "T1119"
],
"basetypes": [
    "misp",
    "indicator"
],
"fpid": "kajq3e50W4uEs4G6wZam4Q",
"header_": {
    "indexed_at": 1588183277,
    "ingested_at": 1588183276,
    "is_visible": true,
    "observed_at": 1588183276,
    "source": "urn:fp:component:misp-exporter"
},
"href": "https://fp.tools/api/v4/indicators/event/kajq3e50W4uEs4G6wZam4Q"
}
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].Event.info	Event.Title	N/A	[].Event.publish_timestamp	'[COVID-19 04/29/2020] - Dridex'	In case .info starts with 'CVE-' besides the Event, a Vulnerability will be ingested with the same attributes as the Event
[].Event.date	Event.Happened_at	N/A	N/A	2020-04-29	Formatted timestamp
[].href	Event.Attribute	Reference	[].Event.publish_timestamp	'https://fp.tools/api/v4/indicators/event/kajq3e5OW4uEs4G6wZam4Q'	N/A
[].Event.Attribute[].type	Indicator.Type	N/A	N/A	'URL'	Mapped by using the table below
[].Event.Attribute[].value[[]].Event.Attribute[].type]	Indicator.Value	N/A	[].Event.Attribute[].timestamp	'http://toliku.com/'	N/A
[].Event.Attribute[].value[[]].Event.Attribute[].type]	Indicator.Attribute	Port	[].Event.Attribute[].timestamp	<port_number>	Added only when .type is 'ip-dst port' by splitting the actual value by and extracting the indicator value and port value
[].Event.Attribute[].href	Indicator.Attribute	Reference	[].Event.Attribute[].timestamp	'https://fp.tools/api/v4/indicators/attribute/voX150-rW4exr1YKF2Gc_A'	N/A
[].Event.Attribute[].comment	Indicator.Attribute	Comment	[].Event.Attribute[].timestamp	'URLhaus database for malware'	N/A
[].Event.Attribute[].category	Indicator.Attribute	Category	[].Event.Attribute[].timestamp	'Network activity'	N/A
[].basetypes[]	Event.Attribute, Indicator.Attribute	Base Type	[].Event.publish_timestamp	['misp', 'indicator']	N/A
[].attack_ids[]	Event.Attribute, Indicator.Attribute	Attack ID	[].Event.publish_timestamp	['T1087', 'T1119']	N/A
[].attack_ids[]	Attack_pattern.Value	N/A	N/A	'T1087 - Account Discovery'	Mapped to the already ingested

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					MITRE Attack Patterns in TQ if the value is valid
[].Event.Tag[].name	Event.attribute, Indicator.Attribute	Tag	[].Event.publish_timestamp	'XWnZwZYsS1WzljFH2SqleA'	Formatted, removed leading unnecessary data in case the .tag value starts with actor, malware, vulnerability, report or misp-galaxy
[].Event.Tag[].name	Related.Adversary.Value, Related.Intrusion.Value	N/A	N/A	'cobalt'	Ingested only if the .tag value starts with actor
[].Event.Tag[].name	Related.Malware.Value	N/A	N/A	'emotet'	Ingested only if the .tag value starts with malware
[].Event.Tag[].name	Related.Vulnerability.Value	N/A	N/A	'CVE-2018-2893'	Ingested only if the .tag value starts with vulnerability

Type Mapping

The Flashpoint Type, as found in `[].Event.Attribute[].type`, to ThreatQ Type mapping is as follows:

FLASHPOINT INDICATOR TYPE	THREATQ INDICATOR TYPE	STRING FORMAT	EXAMPLE
md5	FQDN	None	c4ca4238a0b923820dcc509a6f75849b
sha1	URL	None	356A192B7913B04C54574D18C28D46E6395428AB
sha256	URL	None	f1013d882f4507c08976debd09f202e4b2c 1a0939ea136ede34a78ad8b2ef069
sha512	FQDN	None	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
url	URL	None	http://toliku.com/
domain	FQDN	None	toliku.com
ip-src	IP Address	None	156.231.421.443
ip-dst port	IP Address	Split up by	156.231.421.443 8000 -> 156.231.421.19
email-src	Email Address	None	me@toliku.com

Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Flashpoint Feed, Flashpoint Events

METRIC	RESULT
Run Time	120 minutes
Events	107
Event Attributes	868
Indicators	42,759
Indicator Attributes	334,244
Malware	28
Attack Patterns	28
Adversaries	0
Vulnerabilities	0

Flashpoint Related Events (Supplemental)

METRIC	RESULT
Run Time	4 minutes
Reports	71
Report Attributes	1,413
Adversaries	1
Adversary Attributes	0
Events	15
Event Attributes	290
Indicators	1,101
Indicator Attributes	27,453
Malware	16
Attack Patterns	0
Vulnerabilities	0

Known Issues / Limitations

- MITRE ATT&CK attack patterns must have already been ingested by a previous run of the MITRE ATT&CK feeds in order for MITRE ATT&CK attack patterns to be extracted and related. MITRE ATT&CK attack patterns are ingested from the following feeds:
 - MITRE Enterprise ATT&CK
 - MITRE Mobile ATT&CK
 - MITRE PRE-ATT&CK

Change Log

- **Version 3.2.0**
 - Fixed a pagination issue.
 - Updated maximum number of skipped items to 10,000.
 - Added IOC Type filtering support for Flashpoint Events. See the [Configuration](#) chapter for more details.
- **Version 3.1.0**
 - Fixed an issue with blank descriptions.
 - Added indicator parsing for the report body (hashes, CVEs, and IPs). See the [ThreatQ Mapping](#) and [Configuration](#) chapters for further details.
 - Tags are now ingested as Tags within ThreatQ. Previously, these tags were ingested as attributes into the ThreatQ platform.
- **Version 3.0.1**
 - Fixes KeyError for `Attribute`
- **Version 3.0.0**
 - Mapping Changed
 - CDF Rewritten
 - Removed the Ingest Related Reports user field
- **Version 2.1.0**
 - Ingest data as Adversaries or Intrusion Set
 - Add the Ingest Related Reports user field
 - Removed the attribute 'Notified At'
 - Add `published_at` to Reports and Report Attributes
 - Filter the `<div>` and `<img>` from the `.body` JSON key
- **Version 2.0.2**
 - Header Enhancements
- **Version 2.0.1**
 - Fix the error with the JSON Parsing
- **Version 2.0.0**
 - Ingest IPs from new endpoint

- **Version 1.0.0**
 - Initial release