ThreatQuotient

Flashpoint Ignite CDF

Version 3.3.2

September 17, 2024

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

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.

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	3.3.2
Compatible with ThreatQ Versions	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

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

The integration ingests threat intelligence data from the following feeds:

- **Flashpoint Ignite** - ingests compromised Reports and any related Events, Indicators, Adversaries, Malware, Vulnerabilities and Attack Patterns.
- **Flashpoint Ignite Community Ransomware** - requests article and conversation data gathered by Flashpoint Ignite regarding Ransomware.
- **Flashpoint Ignite Events** - ingests related Events.
- **Flashpoint Ignite Related Events (Supplemental)** - called once per each `.data[].id` returned by the Flashpoint feed.
- **Flashpoint Ignite Media Sources** - ingests media data that has been analyzed by Flashpoint Ignite Optical Character Recognition (OCR) process.
- **Flashpoint Ignite Fraud Mitigation** - ingests compromised credit cards from illicit communities and data breaches.

The integration ingests the following system object types:

- Adversaries
  - Adversary Attributes
- Attack Patterns
- Compromised Card (custom object)
- Events
  - Event Attributes
- Identity
- Indicators
  - Indicator Attributes
- Malware
- Reports
- Vulnerabilities

Prerequisites

The Flashpoint Ignite CFD requires the following:

- Flashpoint Ignite API Key.
- Compromised Card custom object.

Compromised Card Custom Object

The integration requires the Compromised Card custom object.

Use the steps provided to install the custom object.

> When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

ThreatQ V6 Steps

Use the following steps to install the custom object in ThreatQ v6:

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.

   > The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Navigate to the tmp folder:

   ```
   cd /var/lib/threatq/misc/
   ```

5. Upload the custom object files, including the images folder.

   The directory structure should be as the following:

   - misc
     - install.sh
     - <custom_object_name>.json
     - images (directory)
       - <custom_object_name>.svg

6. Run the following command:

   ```
   kubectl exec -it deployment/api-schedule-run -n threatq -- sh /var/
   lib/threatq/misc/install.sh /var/lib/threatq/misc
   ```

> The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

7. Delete the install.sh, definition json file, and images directory from the `misc` directory after the object has been installed as these files are no longer needed.

ThreatQ v5 Steps

Use the following steps to install the custom objects in ThreatQ v5:

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   cd /tmp/
   ```

4. Create a new directory:

   ```
   mkdir ignite_cdf
   ```

5. Upload the **compromised_card.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the ignite_cdf directory.

   ```
   mkdir images
   ```

7. Upload the compromised_card.svg.
8. Navigate to the **/tmp/ignite_cdf**.

   The directory should resemble the following:

   - tmp
     - **ignite_cdf**
       - **compromised_card.json**
       - **install.sh**
       - **images**
         - **compromised_card.svg**

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
chmod +x install.sh
```

10. Run the following command:

```
sudo ./install.sh
```

> You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf ignite_cdf
```

Installation

> The CDF requires the installation of the Compromised Card custom object before installing the actual CDF. See the Prerequisites chapter for more details. The custom object must be installed prior to installing the CDF. Attempting to install the CDF without the custom object will cause the CDF install process to fail.

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 zip file.
3. Extract the contents of the zip and install the required Compromised Card custom object.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration on your local machine
7. Select the individual feeds to install, when prompted, and click **Install**.

   > 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.

8. The feed(s) 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 Ignite Parameters

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.
Enable SSL Verification	When checked, validates the host-provided SSL certificate. This option is enabled by default.

PARAMETER	DESCRIPTION
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.

Flashpoint Ignite Community Ransomware Parameters

PARAMETER	DESCRIPTION
API Key	Your Flashpoint API Key.
Related IoCs Filter	Select the IoCs to ingest into the ThreatQ platform. Options include: ◦ Email Address ◦ IP Address ◦ FQDN
Append Translation to the Description	If a translation is available, it will added to the description.
Search Query	Optional - This query allows you to specify additional keywords that the returned result must contain.
Enable SSL Verification	When checked, validates the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.

Flashpoint Ignite Events Parameters

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
Enable SSL Verification	When checked, validates the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.

Flashpoint Ignite Media Sources Parameters

PARAMETER	DESCRIPTION
API Key	Your Flashpoint API Key.
Search Query	Optional - This query allows to specify additional keywords that the returned media must contain.
Enable SSL Verification	When checked, validates the host-provided SSL certificate. This option is enabled by default.

PARAMETER	DESCRIPTION
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.

Flashpoint Ignite Card Fraud Mitigation Parameters

PARAMETER	DESCRIPTION
API Key	Your Flashpoint API Key.
BIN FIlter	Optional - The BINs that you want to ingest compromised credit cards for.
Context Filter	Select which pieces of context to bring into ThreatQ with each compromised card. Options include: ◦ Account Number ◦ BIN ◦ CVV ◦ Last 4 Digits ◦ Site ◦ Release Name ◦ Owner First Name ◦ Owner Full Name ◦ Sale Price ◦ Source Type ◦ Source ◦ Data Type ◦ Last Observed At ◦ First Observed At ◦ Expiration ◦ Owner City ◦ Owner Region ◦ Owner Country ◦ Owner Zip Code ◦ Site Uri
Enable SSL Verification	When checked, validates the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.

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 Ignite

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

> 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://api.flashpoint.io/technical-intelligence/v1/event/5e7a40ba-e198-4e44-90f5-007b0a212811`, the `<event_id>` will be equal to `5e7a40ba-e198-4e44-90f5-007b0a212811`).

`GET https://api.flashpoint.io/finished-intelligence/v1/reports`

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/9vXqarKJRPubHLa8UUntAA",
        "title_asset_id": "9vXqarKJRPubHLa8UUntAA",
        "assets": [
          "/assets/agEIfiLjSe6e7FXcuPiaLg",
          "/assets/2c2At8cZTT--JcGvqYUKOw",
          "/assets/6ofKfKcER5aqROXTtSEZsA"
        ],
        "asset_ids": [
          "agEIfiLjSe6e7FXcuPiaLg",
          "2c2At8cZTT--JcGvqYUKOw"
        ],
```

```
        "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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.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)
.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/agEIfiLjSe6e7FXcuPiaLg?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/XWnZwZYsS1WzljFH2SqIeA#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	6473dac67b75194deeaef37103bba17936f6c16ffcd2a7345a5a46756996fad748a97f36f8fd4be4e1f264ece313773cc5596099d68e71344d8135f50e5d8971	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 to ThreatQ Indicator 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 FORMATTING	EXAMPLE
md5	FQDN	None	`c4ca4238a0b923820dcc509a6f75849b`
sha1	URL	None	`356A192B7913B04C54574D18C28D46E6395428AB`
sha256	URL	None	`f1013d882f4507c08976debd09f202e4b2c1a0939` `ea136ede34a78ad8b2ef069`
sha512	FQDN	None	`4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579C` `CB851F8DB9DFE84C58B2B37B89903A740E1EE172DA` `793A6E79D560E5F7F9BD058A12A280433ED6FA46510A`
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`

FLASHPOINT INDICATOR TYPE	THREATQ INDICATOR TYPE	STRING FORMATTING	EXAMPLE
email-src	Email Address	None	`me@toliku.com`

Flashpoint Ignite Community Ransomware

The Flashpoint Ignite Community Ransomware feed requests article and conversation data gathered by Flashpoint Ignite regarding Ransomware.

`POST https://api.flashpoint.io/sources/v2/communities`

Sample Body:

```
{
  "query": "communication",
  "page": 0,
  "size": 100,
  "include": {
    "type": [
      "ransomware"
    ],
    "date": {
      "start": "2024-04-01T00:00:00Z",
      "end": "2024-04-25T00:00:00Z"
    }
  }
}
```

Sample Response:

```
{
  "items": [
    {
      "id": "hN2MrDM8VtGvSv0Q48ReZQ",
      "author": "CiphBit",
      "date": "2024-04-06T00:00:00Z",
      "enrichments": {
        "location": [
          {
            "country_code": "EG",
            "name": "Arab Republic of Egypt",
            "lat": 27.0,
            "long": 30.0
          }
        ],
        "url_domains": [
          "vietnamnet.vn"
        ],
        "ip_addresses": [
          "179.61.12.162"
        ],
        "email_addresses": [
          "cyberoutlaw@cock.li"
        ],
        "translation": {
```

```
          "language": "english",
          "message": "TermoPlastic S.R.L \n  post date, Apr 6, 2024 \n It's a
company.."
        }
      },
      "first_observed_at": "2024-04-06T05:00:10Z",
      "last_observed_at": "2024-05-07T01:03:47Z",
      "message": "TermoPlastic S.R.L \n  post date, Apr 6, 2024 \n Est una
compania...",
      "message_id": "TermoPlastic S.R.L",
      "native_id": "TermoPlastic S.R.L",
      "site": "CiphBit Ransomware Blog",
      "site_actor_handle": "CiphBit",
      "site_source_uri":
"ciphbitqyg26jor7eeo6xieyq7reouctefrompp6ogvhqjba7uo4xdid.onion",
      "site_title": "CiphBit Ransomware Blog",
      "sort_date": "2024-04-06T00:00:00Z",
      "title": "TermoPlastic S.R.L",
      "type": "ransomware"
    }
  ],
  "size": 1,
  "total": {
    "value": 1,
    "relation": "="
  }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].type, .items[].title	Report.Value	N/A	.items[].date	Flashpoint Ignite Ransomware: TermoPlastic S.R.L	Format: `Flashpoint Ignite <type>: <title>`
.data[].message	Report.Description	N/A	N/A	`TermoPlastic S.R.L \n post date, Apr 6, 2024 \n Est una compania...`	Formatted.
.data[].enrichments.translation.message	Report.Description	N/A	N/A	`TermoPlastic S.R.L \n post date, Apr 6, 2024 \n It's a company...`	Formatted. Added only if Append `translation` to the `description` is enabled.
.data[].site	Report.Attribute	Source	.items[].date	CiphBit Ransomware Blog	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data[].enrichments.location.country_code	Report.Attribute	Country Code	.items[].date	EG	N/A
.data[].enrichments.location.name	Report.Attribute	Location	.items[].date	Arab Republic of Egypt	N/A
.data[].enrichments.url_domains	Related Indicator.Value	FQDN	.items[].date	vietnamnet.vn	If enabled in `Related IoCs Filter`
.data[].enrichments.ip_addresses	Related Indicator.Value	IP Address	.items[].date	179.61.12.162	If enabled in `Related IoCs Filter`
.data[].enrichments.email_addresses	Related Indicator.Value	Email Address	.items[].date	cyberoutlaw@cock.li	If enabled in `Related IoCs Filter`
.data[].author	Related Identity.Value	N/A	.items[].date	CiphBit	N/A

Flashpoint Ignite Events and Related Events

The Flashpoint Ignite Events feed and Related Events Supplemental feed use the same endpoint and share the same mapping.

Flashpoint Ignite Events

`GET https://api.flashpoint.io/technical-intelligence/v1/event`

Flashpoint Ignite Related Events

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

`GET https://api.flashpoint.io/technical-intelligence/v1/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": "kajq3e5OW4uEs4G6wZam4Q",
      "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/kajq3e5OW4uEs4G6wZam4Q"
    }
  ]
```


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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					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 MITRE Attack Patterns in TQ if the value is valid
[].Event.Tag[].name	Event.attribute, Indicator.Attribute	Tag	[].Event.publish_timestamp	'XWnZwZYsS1WzljFH2SqIeA'	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.Intrussion.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`

Flashpoint Ignite Media Sources

The Flashpoint Ignite Media Sources feed ingests media data that has been analyzed by Flashpoint Ignite Optical Character Recognition (OCR) process. The OCR process returns any text, classifications, or logos found within the media that are available for search. The output of the OCR process is ingested as a ThreatQ Report.

`POST https://api.flashpoint.io/sources/v2/media`

Sample Body:

```
{
  "query": "checks",
  "page": 0,
  "size": 50,
  "include": {
    "date": {
      "start": "2024-04-25T00:00:00Z",
      "end": "2024-04-27T00:00:00Z"
    }
  }
}
```

Sample Response


```
{
  "items": [
    {
      "author": "TollaG",
      "author_id": "7093587118",
      "id": "YB3lxHk5XUa9Wa_WmDGMbQ",
      "date": "2024-04-21T03:52:54Z",
      "media_id": "3NoHlK5CVt2ah7EabvQ1lw",
      "media_type": "image",
      "phash": "9037b7c06a8dcd2e",
      "site": "Telegram",
      "sort_date": "2024-04-21T03:52:54Z",
      "safe_search": "moderate",
      "size": 80719,
      "storage_uri": "gs://kraken-datalake-media/artifacts/a9/
a9cd128156c43f24f20cf67c58f36535d66d50708b5357a5ff124453c4f5b00d",
      "title": "Loaders and Carders(worldwide)",
      "title_id": "1454251053",
      "extracted_classifications": [
        "Communication Device",
        "Font",
        "Portable communications device"
      ],
      "extracted_text": [
        "MARKET\nDDARKNET MARKET\nDARKNET MARKET\nDOPIETAT\nDARKNET
MARKET\nC\nRegistered Email\nDARKNET\nEnter password here\nDARKNET
MARKET\nLogin to Logsnow.world\nFast and Easy\nDARK DARKNET
MARKET\nLOGIN\nForgot your password?\nDEWAN LHKKNE:\nDon't have an account?
```

```
Sign Up",
        "MARKET",
        "DDARKNET",
        "MARKET",
        "DARKNET",
        "MARKET",
        "DOPIETAT",
        "DARKNET",
        "MARKET",
        "C",
        "Registered",
        "Email",
        "DARKNET",
        "Enter",
        "password",
        "here",
        "DARKNET",
        "MARKET",
        "Login",
        "to",
        "Logsnow.world",
        "Fast",
        "and",
        "Easy",
        "DARK",
        "DARKNET",
        "MARKET",
        "LOGIN",
        "Forgot",
        "your",
        "password",
        "?",
        "DEWAN",
        "LHKKNE",
        ":",
        "Don't",
        "have",
        "an",
        "account",
        "?",
        "Sign",
        "Up"
      ],
      "image_uri": "gs://kraken-datalake-media/artifacts/a9/
a9cd128156c43f24f20cf67c58f36535d66d50708b5357a5ff124453c4f5b00d",
      "image_sha": "129bff58f43bef754584edeba1a5fcb5922a5b25",
      "type": "chat"
    },
    {
      "author": "Caesarin0",
      "id": "odQGJdatWLKef78bmwUFUA",
```

```
      "date": "2024-04-20T19:51:41Z",
      "file_name": "/hy4t7009vovc1.png",
      "media_id": "ITDg001BU_yuyZfsPrftPA",
      "media_type": "image",
      "phash": "95330fbc7a8c620f",
      "parent_container_name": "bleach",
      "site": "Reddit",
      "sort_date": "2024-04-20T19:51:41Z",
      "safe_search": "moderate",
      "section": "bleach",
      "section_id": "bleach",
      "size": 102860,
      "storage_uri": "gs://kraken-datalake-media/artifacts/3c/
3cb4835991439191d99e4762d149fc8f73e645ae1df0e3a3d787b76a6b821e24",
      "title": "Theory: Aizen doesn't have a bankai",
      "title_id": "1c8wtu1",
      "extracted_classifications": [
        "Joint",
        "Shoulder",
        "Human"
      ],
      "extracted_text": [
        "...KYÔKA\nSUIGETSU.\nSHATTER\n\"\nSEE.",
        "...",
        "KYÔKA",
        "SUIGETSU",
        ".",
        "SHATTER",
        "\"",
        "SEE",
        "."
      ],
      "image_uri": "gs://kraken-datalake-media/artifacts/3c/
3cb4835991439191d99e4762d149fc8f73e645ae1df0e3a3d787b76a6b821e24",
      "image_sha": "3db5dfc1050d2a444874bc094bd3ce85becbbb5a",
      "type": "reddit"
    }
  ],
  "size": 50,
  "total": {
    "value": 5000,
    "relation": ">"
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].site, .items[].title	Report.Value	N/A	.items[].date	Flashpoint Ignite Media: Telegram - Loaders and Carders(worldwide)	Values are concatenate and prepended with `Flashpoint Ignite Media`
.data[].extracted_text[0]	Report.Description	N/A	N/A	`MARKET\nDDARKNET MARKET\nDARKNET MARKET\nDOPIETAT\nDARKNET MARKET\nC\nRegistered Email...`	Formatted.
.data[].extracted_ classifications[]	Report.Tag	Tag	N/A	['Communication Device', 'Font', 'Portable communications device']	N/A
.data[].site	Report.Attribute	Source	.data[].date	Telegram	N/A
.data[].storage_uri	Report.Attribute	Storage URI	.data[].date	gs://kraken-datalake-media/artifacts/a9/a9cd128156c43f24f20cf67c58f36535d66d50708b5357a5ff124453c4f5b00d	N/A
.data[].type	Report.Attribute	Source Type	.data[].date	Chat	N/A
.data[].author	Related Identity.Value	N/A	.data[].date	TollaG	N/A

Flashpoint Ignite Card Fraud Mitigation

The Flashpoint Ignite Card Fraud Mitigation feed detects and ingests compromised credit cards from illicit communities and data breaches.

`POST https://api.flashpoint.io/sources/v2/fraud`

Sample Request Body:

```
{
        "page": 0,
        "size": 10000,
        "include": {
            "date": {
                "after": "2023-01-10T00:00:00Z"
            }
        }
    }
```

Sample Response:

```
{
  "size": 7,
  "total": {
    "value": 5000,
    "relation": ">"
  },
  "items": [
    {
      "author": "fernando_club",
      "bin": 517800,
      "card": {
        "expiration": "01/26"
      },
      "cardholder": {
        "location": {
          "city": "LIVERMORE",
          "country": "US",
          "region": "CA",
          "zip_code": "94550"
        }
      },
      "date": "2024-03-19T19:29:41Z",
      "first_observed_at": "2024-03-19T19:29:41Z",
      "last_observed_at": "2024-03-19T19:29:41Z",
      "prices": [
        24
      ],
      "release": {
        "name": "March, 2024",
        "id": "6brA7geGXBehI1uON0iMFg"
```

```
      },
      "site": "Fernando Club",
      "author_alias": [
        "fernando_club"
      ],
      "site_source_uri": "fernandogoods.biz",
      "id": "rdPOB562X6-BywkMhVHy0g",
      "source_type": "shop",
      "type": "partial_card_cvv"
    },
    {
        "author": "CC CHEAPLUXURY SCRAPE",
        "bin": 470881,
        "card": {
            "cvv": 614,
            "expiration": "08/2024",
            "number": 4708810311302243
        },
        "created_at": "2024-07-11T05:24:46Z",
        "date": "2024-07-11T05:24:46Z",
        "first_observed_at": "2024-07-11T05:24:47.297485Z",
        "last4": 2243,
        "last_observed_at": "2024-07-11T05:24:47.297485Z",
        "site": "Telegram",
        "account_number": "031130224",
        "author_alias": [
            "CC CHEAPLUXURY SCRAPE"
        ],
        "site_source_uri": "web.telegram.org",
        "id": "yPYaOyqHWLSBYAiHi5_qYQ",
        "source_type": "chat",
        "type": "full_card"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].card.number	Card.Value	N/A	.items[].date	`4708810311302243`	If `items[].card.number` is available.
.items[].bin, .items[].last4, items[].card.expiration, items[].card.cvv	Card.Value	N/A	.items[].date	`517800|26|01`	If `items[].card.number` is not available.
.items[].account_number	Card.Attribute	Account Number	.items[].date	`031130224`	If value exists and `Account Number` checked in `Context Filter`.
.items[].bin	Card.Attribute	BIN	.items[].date	`470881`	If value exists and `BIN` checked in `Context Filter`.
.items[].card.cvv	Card.Attribute	CVV	.items[].date	`614`	If value exists and `CVV` checked in `Context Filter`.
.items[].last4	Card.Attribute	Last 4 Digits	.items[].date	`2243`	If value exists and `Last 4 Digits` checked in `Context Filter`.
.items[].site	Card.Attribute	Site	.items[].date	`Telegram`	If value exists and `Site` checked in `Context Filter`.
.items[].release.name	Card.Attribute	Release Name	.items[].date	`March, 2024`	If value exists and `Release Name` checked in `Context Filter`.
.items[].prices[]	Card.Attribute	Sale Price	.items[].date	`24`	If value exists and `Sale Price` checked in `Context Filter`.
.items[].source_type	Card.Attribute	Source Type	.items[].date	`chat`	If value exists and `Source Type` checked in `Context Filter`.
.items[].author	Card.Attribute	Source	.items[].date	`CC CHEAPLUXURY SCRAPE`	If value exists and `Source` checked in `Context Filter`.
.items[].type	Card.Attribute	Data Type	.items[].date	`full_card`	If value exists and `Data Type` checked in `Context Filter`.
.items[].last_observed_at	Card.Attribute	Last Observed At	.items[].date	`2024-07-11 05:24:47.297485`	Timestamp. If value exists and `Last Observed At` checked in `Context Filter`. Updatable.
.items[].first_observed_at	Card.Attribute	First Observed At	.items[].date	`2024-07-11 05:24:47.297485`	Timestamp. If value exists and `First Observed At` checked in `Context Filter`.
.items[].card.expiration	Card.Attribute	Expiration	.items[].date	`08/2024`	If value exists and `Expiration` checked in `Context Filter`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].cardholder.name.first	Card.Attribute	Owner First Name	.items[].date	N/A	If value exists and `Owner First Name` checked in `Context Filter`.
.items[].cardholder.name.full_name	Card.Attribute	Owner Full Name	.items[].date	N/A	If value exists and `Owner Full Name` checked in `Context Filter`.
.items[].cardholder.location.city	Card.Attribute	Owner City	.items[].date	`LIVERMORE`	If value exists and `Owner City` checked in `Context Filter`.
.items[].cardholder.location.region	Card.Attribute	Owner Region	.items[].date	`CA`	If value exists and `Owner Region` checked in `Context Filter`.
.items[].cardholder.location.country	Card.Attribute	Owner Country	.items[].date	`US`	If value exists and `Owner Country` checked in `Context Filter`.
.items[].cardholder.location.zip_code	Card.Attribute	Owner Zip code	.items[].date	`94550`	If value exists and `Owner Zip code` checked in `Context Filter`.
.items[].site_source_uri	Card.Attribute	Flashpoint Link	.items[].date	`web.telegram.org`	If value exists and `Flashpoint Link` checked in `Context Filter`.

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 Ignite

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

Flashpoint Ignite Community Ransomware

METRIC	RESULT
Run Time	8 minutes
Reports	856
Report Attributes	1,980
Identity	46
Indicators	3,921

Flashpoint Ignite Events, Related 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

METRIC	RESULT
Vulnerabilities	0

Flashpoint Ignite Media Sources

METRIC	RESULT
Run Time	2 minutes
Reports	647
Report Attributes	2,394
Identity	818

Flashpoint Ignite Card Fraud Mitigation

METRIC	RESULT
Run Time	8 minutes
Compromised Cards	4,571
Card Attributes	51,599

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
- The API used by `Flashpoint Ignite Media Sources` only returns the latest 10000 records.

Change Log

- **Version 3.3.2**
  - Added a new feed: **Flashpoint Ignite Card Fraud Mitigation**. This new feed ingests compromised card objects and requires the Compromised Card custom object.
  - Added the following parameters to all feeds:
    - Disable Proxies
    - Enable SSL Verification
- **Version 3.3.1**
  - Added a new feed: **Flashpoint Ignite Community Ransomware**.
- **Version 3.3.0**
  - Migrated the feeds to the Flashpoint Ignite API.
  - Added new feed: **Flashpoint Ignite Media Sources**.
  - Added a new Known Issue - the API used by `Flashpoint Ignite Media Sources` only returns the latest 10000 records.
  - Updated minimum ThreatQ version to 5.12.0
  - Updated integration name from **Flashpoint CDF** to **Flashpoint Ignite CDF**.
- **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