ThreatQuotient

Flashpoint Ignite Compromised Accounts CDF

Version 1.1.1

October 21, 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	1.1.1
Compatible with ThreatQ Versions	>= 5.10.0
Support Tier	ThreatQ Supported

Introduction

The Flashpoint Ignite Compromised Accounts feed for ThreatQ enables the automatic ingestion of an organization's compromised credentials into ThreatQ. Ultimately, tracking the accounts to link them to internal incidents as well as mitigating potential future breaches.

The integration provides the following feed:

- **Flashpoint Ignite Compromised Accounts** - ingests Compromised Accounts as the main object and Events as related objects.

The integration ingests the following system objects:

- Events
- Compromised Account

Prerequisites

Review the requirements below before attempting to install the CDF.

Compromised Account Custom Object

The integration requires the Compromised Account custom object.

> For export purposes, the system name for Compromised Account objects is `account`.

> 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 following location:

   ```
   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 flashpoint_cdf
   ```

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

   ```
   mkdir images
   ```

7. Upload the account.svg.
8. Navigate to the **/tmp/flashpoint_cdf**.

   The directory should resemble the following:

   - tmp
     - **flashpoint_cdf**
       - **account.json**
       - **install.sh**
       - **images**
         - **account.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 flashpoint_cdf
```

Installation

The CDF requires the installation of the Compromised Account 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 files and install the Compromised Account custom object.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the 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.
7. 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:

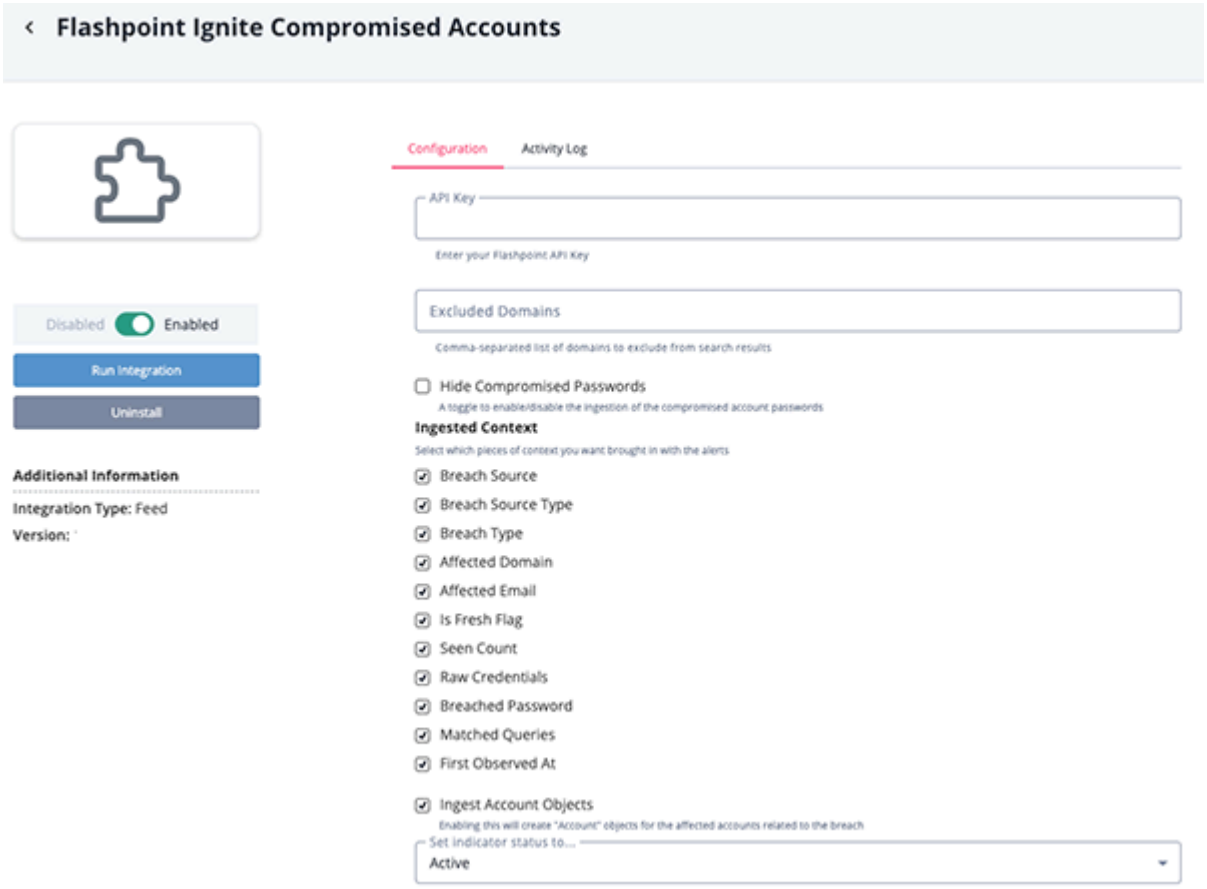
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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:

PARAMETER	DESCRIPTION
API Key	Your Flashpoint API Key
Excluded Domains	A comma-separated list of domains to exclude from search results.
Hide Compromised Passwords	Enable/disable the ingestion of the compromised account passwords.
Ingested Context	Select which pieces of context you want brought in with the alerts. Options include: ◦ Breach Source ◦ Breach Source Type ◦ Breach Type ◦ Affected Domain ◦ Affected Email ◦ Is Fresh Flag ◦ Seen Count ◦ Raw Credentials ◦ Breached Password ◦ Matched Queries ◦ First Observed At
Ingest Account Objects	Enable/disable the creation of Compromised Account objects for the affected accounts related to the breach.

PARAMETER	DESCRIPTION
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 Compromised Accounts

The Flashpoint Ignite Compromised Accounts feed for ThreatQ enables the automatic ingestion of an organization's compromised credentials into ThreatQ.

`GET https://api.flashpoint.io/sources/v1/noncommunities/search`

Sample Response:


```
{
    "hits": {
        "hits": [
            {
                "_id": "EMX6QiiPW-ay8-5d732GqB",
                "_source": {
                    "basetypes": [
                        "credential-sighting"
                    ],
                    "body": {
                        "raw": "someone@threatq.com:<some password>"
                    },
                    "breach": {
                        "_header": {},
                        "basetypes": [
                            "breach"
                        ],
                        "breach_type": "credential",
                        "created_at": {
                            "date-time": "2021-06-25T23:57:31Z",
                            "timestamp": 1624665451
                        },
                        "first_observed_at": {
                            "date-time": "2021-06-25T23:57:31Z",
                            "timestamp": 1624665451
                        },
                        "fpid": "ESiczBZVW0Kx3Fxpybfd4B",
                        "published_at_ts": "2021-06-25 23:57:31",
                        "source": "https://www.virustotal.com/gui/file/
bd5e65fecff172bce63fb054c85953f93e63baf863456e571df4dfe52da85d3b/details",
                        "source_type": "VirusTotal",
                        "title": "Compromised Users from VirusTotal: Compressed
File \"bd5e65fecff172bce63fb054c85953f93e63baf863456e571df4dfe52da85d3b\"
Jun252021"
                    },
                    "credential_record_fpid": "iCb5b0mfXvqk0QVJnL6jTw",
                    "customer_id": "0013l00002MH03tAAD",
```

```
                    "domain": "threatq.com",
                    "email": "someone@threatq.com",
                    "extraction_id": "DxEdSTXwWR6ouuZc3e7veA",
                    "extraction_record_id": "zEv0ARXyVVuMUEUkDcLzTA",
                    "fpid": "EMX6QiiPW-ay8-5d732GqA",
                    "header_": {
                        "indexed_at": 1625842497,
                        "pipeline_duration": 63793061697
                    },
                    "is_fresh": false,
                    "last_observed_at": {
                        "date-time": "2021-06-25T23:57:31Z",
                        "timestamp": 1624665451
                    },
                    "last_observed_at_ts": "2021-06-25 23:57:31",
                    "password": "<some password>",
                    "password_complexity": {
                        "has_lowercase": true,
                        "has_number": true,
                        "has_symbol": false,
                        "has_uppercase": false,
                        "length": 6
                    },
                    "published_at_ts": "2021-06-25 23:57:31",
                    "times_seen": 1
                },
                "_type": "_doc",
                "matched_queries": [
                    "dat.edm.org.r"
                ]
            }
        ],
        "max_score": null,
        "total": 1
    },
    "timed_out": false,
    "took": 18
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`._source.breach.title`	Related Event.Value	Alert	`._source.breach.created_at`	N/A	N/A
`._source.breach.victim`	Related Event.Attribute	Victim	`._source.breach.created_at`	someone@threatq.com	N/A
`._source.breach.source`	Related Event.Attribute	Source	`._source.breach.created_at`	https://www.virustotal.com/gui/file/xxxx	Will be ingested if the user field is checked
`._source.breach.source_type`	Related Event.Attribute	Source Type	`._source.breach.created_at`	VirusTotal	Will be ingested if the user field is checked
`._source.breach.breach_type`	Related Event.Attribute	Breach Type	`._source.breach.created_at`	credential	Will be ingested if the user field is checked
`._source.domain`	Related Event.Attribute	Affected Domain	`._source.breach.created_at`	threatq.com	Will be ingested if the user field is checked
`._source.email`	Related Event.Attribute	Affected Email	`._source.breach.created_at`	someone@threatq.com	Will be ingested if the user field is checked
`._source.is_fresh`	Related Event.Attribute	Is Fresh	`._source.breach.created_at`	false	Will be ingested if the user field is checked
`._source.times_seen`	Related Event.Attribute	Seen Count	`._source.breach.created_at`	1	Will be ingested if the user field is checked
`._source.body.raw`	Related Event.Attribute	Raw Credentials	`._source.breach.created_at`	someone@threatq.com:<some password>	Will be ingested if the user field is checked
`.matched_queries`	Related Event.Attribute	Matched Query	`._source.breach.created_at`	dat.edm.org.r	Will be ingested if the user field is checked
`._source.breach.first_observed_at.date-time`	Related Event.Attribute	First Observed At	`._source.breach.created_at`	2021-06-25T23:57:31Z	Will be ingested if the user field is checked
`._source.email`	Account.Value	Account	`._source.last_observed_at`	someone@threatq.com	The custom object must be installed
`._source.password`	Account.Attribute	Password	`._source.last_observed_at`	Hunter2	N/A
`._source.affected_domain`	Account.Attribute	Affected Domain	`._source.last_observed_at`	threatq.com	N/A
`._source.credential_record_fpid + _source.fpid`	Account.Attribute	Flashpoint URL	`._source.last_observed_at`	https://app.flashpoint.io/cti/ato/credential/iCb5b0mfXvqk0QVJnL6jTw::EMX6QiiPW-ay8-5d732GqA	Constructed as https://app.flashpoint.io/cti/ato/credential/{{_source.credential_record_fpid}}::{{_source.fpid}}

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.

METRIC	RESULT
Run Time	1 minute
Events	162
Event Attributes	2,156
Compromised Accounts	93
Compromised Account Attributes	889

Known Issues / Limitations

- Due to "lag time" between when a breach is first observed and when the entry appears on the Flashpoint API, we now back-date the feed's last run time by 12 hours. This is to account for that "lag time". It may cause some alerts to be re-ingested, but they will be de-duplicated, so there shouldn't be any concerns.
- For consecutive runs at an interval of 1 minute, we can receive 429 and we recommend waiting 3 or 5 minutes and then repeating.

Change Log

- **Version 1.1.1**
  - The feed now correctly ingests the `Affected Domain` attribute from Flashpoint.
  - Added a rule to update `Is Fresh` and `Is Fresh` attributes if it already exists in the ThreatQ platform.
  - Added new configuration parameters: **Enable SSL Verification** and **Disable Proxies**.
  - Added two new known limitation entries regarding lag times and consecutive runs.
  - Updated the text for the **Exclude Domains** configuration parameter field.
- **Version 1.1.0**
  - The integration now uses the Flashpoint Ignite Compromised Accounts endpoint.
  - Updated the name of integration to Flashpoint Ignite Compromised Accounts.
  - Updated the minimum ThreatQ version to 5.10.0
- **Version 1.0.1**
  - Fixed an issue with lag time between when a breach was first observed and when the entry appeared in the Flashpoint API.
  - Updated the support tier for the integration from Not Actively Supported to ThreatQ Supported.
- **Version 1.0.0**
  - Initial release