ThreatQuotient

Proofpoint Threat Insights CDF

Version 1.0.0

September 03, 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	1.0.0
Compatible with ThreatQ Versions	>= 5.6.0
Support Tier	ThreatQ Supported

Introduction

The Proofpoint Threat Insights CDF enables analysts to automatically ingest blog posts from the Proofpoint website in order to stay up-to-date on advisories, bulletins, and analyses from the Proofpoint team.

The integration provides the following feed:

- **Proofpoint Threat Insights** - ingests blog posts into ThreatQ.

The integration ingests Reports and Indicator type objects.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. 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 file on your local machine
6. 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.

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.

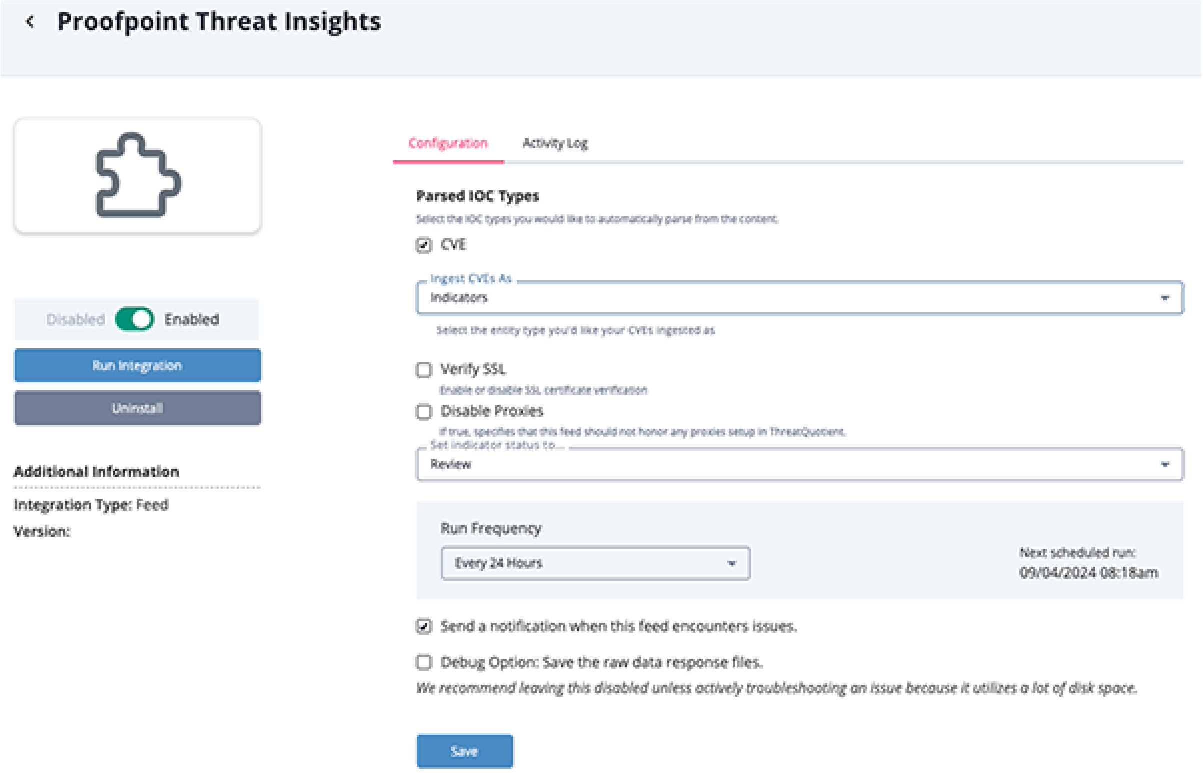
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** 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
Parsed IOC Types	Select the IOC types to automatically parse from the content. As of this publication, the only available option is **CVE**.
Ingest CVEs As	Set how to ingest CVEs as. Options include: Indicators and Vulnerabilities. This field is only displayed if you have selected CVE for the Parse IOC Type.
Verify SSL	Enable or disable SSlL certificate verification.
Disable Proxies	Enable this option to have the feed ignore proxies set in the ThreatQ UI.



Proofpoint Threat Insights

Additional Information

Integration Type: Feed

Version:

Parsed IOC Types

Select the IOC types you would like to automatically parse from the content.

☑ CVE

Ingest CVEs As: Indicators

Select the entity type you'd like your CVEs ingested as

☐ Verify SSL

Enable or disable SSL certificate verification

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Set indicator status to...: Review

Run Frequency: Every 24 Hours

Next scheduled run: 09/04/2024 08:18am

☑ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

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

Proofpoint Threat Insights

The Proofpoint Threat Insights feed periodically pulls blog posts from the Proofpoint website, and ingests them into ThreatQ as Report Objects.

`GET https://www.proofpoint.com/us/blog/threat-insight`

> The output of this request is HTML, which is parsed for links to the actual API containing information on the blog posts.

Once we get the links to the actual API, we need to fetch the blog post metadata from it.

`POST https://{{ app_id }}-dsn.algolia.net/1/indexes/*/queries`

Sample Body:

```
{"requests": [{"indexName": "blog","params":
"filters=search_api_language%3Aen%20AND%20category%3A10346distinct=truefaceting
AfterDistinct=truehitsPerPage=25"}]}
```

The response data will give us links to the actual blog posts so we can fetch their content using the following request

`GET https://www.proofpoint.com/{{ uri }}`

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Report.Title	N/A	N/A	`TA444: The APT Startup Aimed at Acquisition (of Your Funds)`	From the API request
`.date`	Report.Published_At	N/A	N/A	N/A	From the API Request
`.url`	Report.Attribute	External Reference	N/A	`https://www.proofpoint.com//us/blog/threat-insight/ta444-apt-startup-aimed-at-your-funds`	Parsed from HTML
`.date_formatted`	Report.Attribute	Published At	N/A	`February 21, 2023`	From the API Request
`.author`	Report.Attribute	Author	N/A	`Greg Lesnewich and the Proofpoint Threat Research Team`	From the API Request
N/A	Report.Description	N/A	N/A	`<HTML content>`	Parsed from the HTML
N/A	Related.Indicator	CVE	N/A	`CVE-2023-41232`	Parsed from HTML
N/A	Related.Vulnerability	N/A	N/A	`CVE-2023-41232`	Parsed from HTML

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
Reports	14
Report Attributes	42
Indicators	2

Known Issues / Limitations

- In order to avoid reingesting the same IPs, the feed will request IPs based on the `since` date of the last run. At a minimum, the feed will fetch the last day's worth of data.
- If you'd like to fetch more data, you can run the feed manually, setting the `since` date to the desired date. The feed will then fetch data from that date until the current date.
- The max posts the feed will return is 25.

Change Log

- **Version 1.0.0**
  - Initial release