ThreatQuotient

Mandiant Blog CDF

Version 1.0.0

June 24, 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	>= 5.24.1
Support Tier	ThreatQ Supported

Introduction

The Mandiant Blog CDF enables analysts to automatically ingest blog posts from the Mandiant website. This allows analysts to stay up-to-date on advisories, bulletins, and analyses from the Mandiant team.

The integration provides the following feed:

- **Mandiant Blog -** pulls blog posts from the Mandiant website and ingests them into ThreatQ as Report Objects.

The integration ingests report and indicator type system 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.

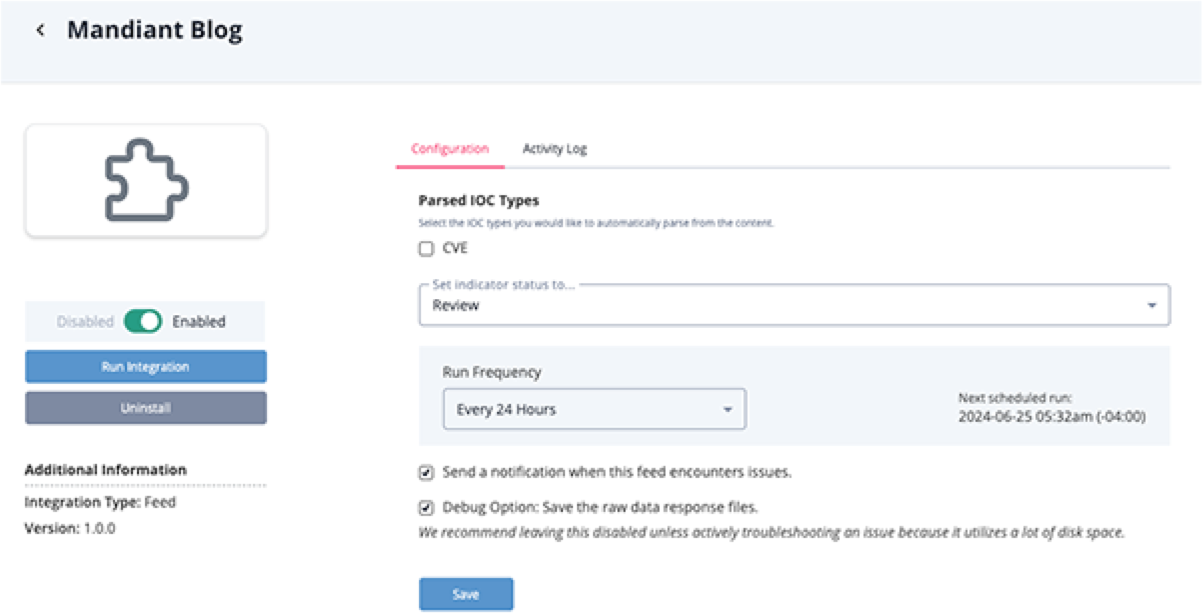
To configure the integration:

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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Parsed IOC Types	Select the IOC type to parse from the content ingested. Currently, the only type available is CVE.



Mandiant Blog

Configuration | Activity Log

Parsed IOC Types

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

□ CVE

Set indicator status to...: Review

Run Frequency: Every 24 Hours

Next scheduled run:
2024-06-25 05:32am (-04:00)

☑ 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.

Additional Information

Integration Type: Feed

Version: 1.0.0

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

Mandiant Blog

The Mandiant Blog feed pulls blog posts from the Mandiant website and ingests them into ThreatQ as Report Objects.

```
GET https://www.mandiant.com/views/ajax?_wrapper_format=drupal_ajax
```

The output of this request is JSON which contains a field with the HTML for the page of blogs. The HTML is parsed for blog links and the links are fetched.

```
GET https://www.mandiant.com/resources/blog/{{ 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
N/A	Report.Title	N/A	N/A	`Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government`	Parsed from the HTML
N/A	Report.Published_At	N/A	N/A	N/A	Parsed from the HTML
N/A	Report.Attribute	External Reference	N/A	`https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government`	Parsed from HTML
N/A	Report.Attribute	Published At	N/A	`DEC 15, 2022`	Parsed from the HTML
N/A	Report.Tag	N/A	N/A	`Ransomware`	Parsed from the HTML
N/A	Report.Description	N/A	N/A	`<HTML content>`	Parsed from the HTML
N/A	Report.Indicator	CVE	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	27
Report Attributes	54
Indicators	3

Known Issues / Limitations

- In order to avoid re-ingesting data, the feed uses the `since` and `until` dates.
- If you'd like to fetch historical data, you can run the feed manually, setting the `since` date to the desired date.
- The max number of pages of posts the feed will fetch is 3.

Change Log

- **Version 1.0.0**
  - Initial release