ThreatQuotient

A Securonix Company

Trellix Research Blog CDF

Version 1.0.0

July 29, 2025

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	>= 5.5.0
Support Tier	ThreatQ Supported

Introduction

The Trellix Research Blog CDF integration enables analysts to ingest blog posts from the Trellix blog, www.trellix.com/blogs/research/, allowing analysts to stay up-to-date on advisories, bulletins, and analyses from the Trellix team.

The integration provides the following feed:

- **Trellix Research Blog** - ingests Trellix articles as ThreatQ report objects.

The integration ingests the following system object types:

- Indicators
- Reports
- 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 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

> 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 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.

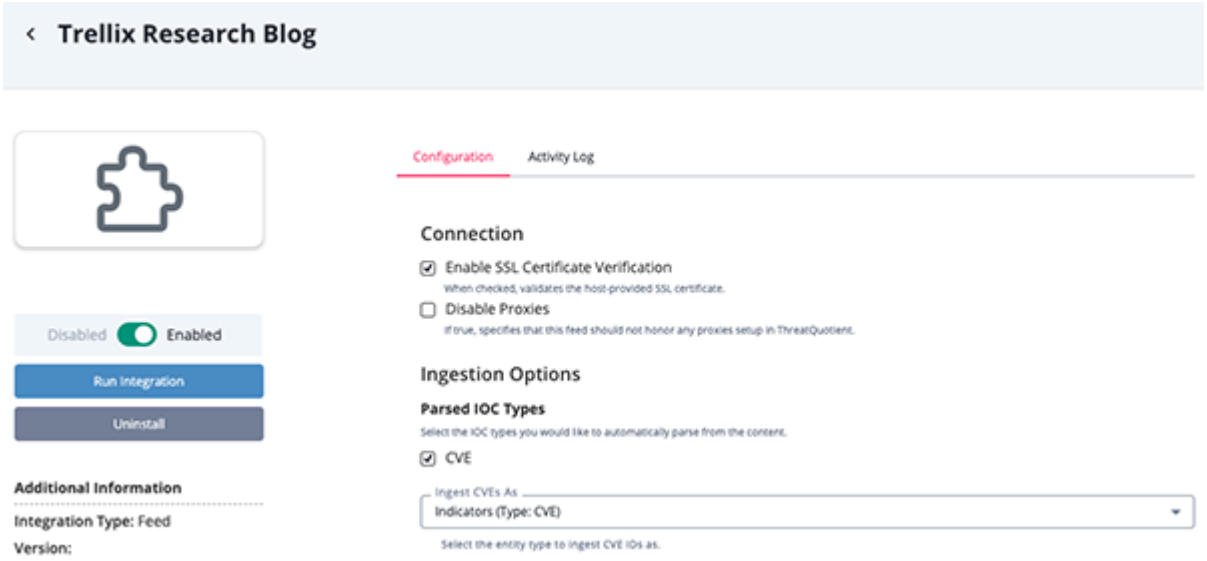
To configure the integration:

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
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Parsed IOC Types	Select the IOC types you would like to automatically parse from the content. The only option available at this time is `CVE`.
Ingest CVEs As	Select the entity type to ingest CVE IDs as into the ThreatQ platform. Options include: ◦ Vulnerabilities (default) ◦ Indicators > This parameter is only accessible if the `CVE` option is selected for the **Parsed IOC Types** parameter.



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

Trellix Research Blog

The Trellix Research Blog feed pulls blog posts from the Trellix website and ingests them into ThreatQ as report objects. .

`GET https://www.trellix.com/corpcomsvc/topicslisting?newsPagePath=/content/mainsite/en-us/about/newsroom/stories/research`

Sample Response


```
{
  "topics": [
    {
      "title": "ChatGPT: A tool for offensive cyber operations?! Not so fast!
",
      "summary": "Artificial intelligence is not a new concept; what is new is
that ChatGPT is easily accessible to millions of people around the world and
does not require a large fee to use. Yet, it has been hailed as something novel
that may be an immediate threat as it may be utilized by cyberthreat actors to
facilitate attacks.",
      "thumbnail": "/en-us/img/thumbnails/chatgpt-offensive-cyber-
operations.jpg",
      "url": "/content/mainsite/en-us/about/newsroom/stories/research/chatgpt-
a-tool-for-offensive-cyber-operations-not-so-fast.html",
      "target": "_self"
    },
    {
      "title": "Qakbot Evolves to OneNote Malware Distribution",
      "summary": "Since the end of January 2023, there has been an upsurge in
the number of Qakbot campaigns using a novel delivery technique: OneNote
documents for malware distribution. Moreover, the Trellix Advanced Research
Center has detected various campaigns that used OneNote documents to distribute
other malware such as AsyncRAT, Icedid, XWorm etc.",
      "thumbnail": "/en-us/img/thumbnails/qakbot-evolves.jpg",
      "url": "/content/mainsite/en-us/about/newsroom/stories/research/qakbot-
evolves-to-onenote-malware-distribution.html",
      "target": "_self"
    },
    {
      "title": "The Bug Report - February 2023 Edition",
      "summary": "Love and RCE payloads were in the air this February. So sit
back, grab your leftover conversation hearts, and let's dive into last month's
top CVEs.",
      "thumbnail": "/en-us/img/thumbnails/the-bug-report-february-2023-
edition.jpg",
      "url": "/content/mainsite/en-us/about/newsroom/stories/research/the-bug-
```

```
report-february-2023-edition.html",
      "target": "_self"
    }
  ]
}
```

The response data will give you links to the actual blog posts in order to fetch their content using the following request:

```
GET https://www.trellix.com/{{ url }}
```

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	Report	parsed date from HTML	`Qakbot Evolves to OneNote Malware Distribution`	From the API request
`.url`	Report.Attribute	External Reference	parsed date from HTML	`https://www.trellix.com/content/mainsite/en-us/about/newsroom/stories/research/qakbot-evolves-to-onenote-malware-distribution.html`	From the API request
N/A	Report.Attribute	Published At	parsed date from HTML	`February 21, 2023`	Parsed from the HTML
N/A	Report.Description	N/A	N/A	`<HTML content>`	Parsed from the HTML
N/A	Report.Vulnerability/ Indicator	CVE	parsed date from HTML	`CVE-2023-41232`	User-Configurable. 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	2
Report Attributes	4
Vulnerabilities	4

Known Issues / Limitations

- ThreatQuotient recommends running this integration every 7 days based on the publication pace of the site.
- The feed utilizes **since** and **until** dates to make sure entries are not re-ingested if they haven't been updated.
- If you need to ingest historical blog posts, run the feed manually by setting the **since** date back.

Change Log

- **Version 1.0.0**
  - Initial release