ThreatQuotient

A Securonix Company

Volexity Blog CDF

Version 1.0.0

February 24, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

The Volexity Blog CDF enables organizations to automatically ingest threat intelligence blog posts from Volexity's Threat Intelligence category directly into ThreatQ. This integration ensures analysts remain informed on the latest advisories, technical analyses, and incident response research published by the Volexity team.

The integration provides the following feed:

- **Volexity Blog** - fetches reports from the Volexity blog.

The integration ingests Report 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 yaml file into the dialog box
   - Select **Click to Browse** to locate the integration yaml 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.

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.

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

Volexity Blog

The Volexity Blog feed pulls threat intel blog posts from the Volexity blog and ingests them into ThreatQ as Report Objects.

`GET https://www.volexity.com/blog/?_categories=threat-intelligence`

The following request returns HTML. The HTML is parsed for blog content. The HTML content for each blog is also fetched and imported as the description for the Report Object.

`GET ttps://www.volexity.com/blog/{{ url_path }}`

The mapping for this feed is based on the information parsed out of the blog's HTML content:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Report.Title	N/A	{HTML}	Dangerous Invitations: Russian Threat Actor Spoofs European Security Events in Targeted Phishing Attacks	Parsed from HTML
N/A	Report.Description	N/A	{HTML}	In early 2025, Volexity published two blog posts detailing...	Parsed from HTML
N/A	Report.Attribute	External Reference	{HTML}	https://www.volexity.com/blog/2025/12/04/dangerous-invitations-russian-threat-actor-spoofs-european-security-events-in-targeted-phishing-attacks/	Parsed from HTML
N/A	Report.Attribute	Published At	{HTML}	December 4, 2025	Parsed from HTML
N/A	Report.Attribute	Author	{HTML}	Matthew Meltzer, Steven Adair, and Tom Lancaster	Parsed from HTML

This mapping does not include feed data paths, as the data is not provided in a structured format.

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	5
Report Attributes	15

Known Issues / Limitations

- 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.
- This feed only brings in blog posts from the `threat intelligence` category.
- ThreatQuotient recommends running this integration every 30 days based on the publication pace of the site.

Change Log

- **Version 1.0.0**
  - Initial release