ThreatQuotient

A Securonix Company

Trend Micro Research Blog CDF

Version 1.0.0

September 15, 2025

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	>= 5.5.0
Support Tier	ThreatQ Supported

Introduction

The Trend Micro Research Blog CDF for ThreatQ ingests blog posts from the Trend Micro Research Blog, a site that provides insights into the latest cybersecurity threats, including malware, vulnerabilities, and cybercriminal activities, along with analysis of attack techniques and mitigation strategies. These blog posts are ingested into ThreatQ as Report objects, ensuring analysts remain up to date on threat research, vulnerabilities, and other security-related articles that are published.

The integration provides the following feed:

- **Trend Micro Research Blog -** pulls blog posts from the Trend Micro Research Blog.

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
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.

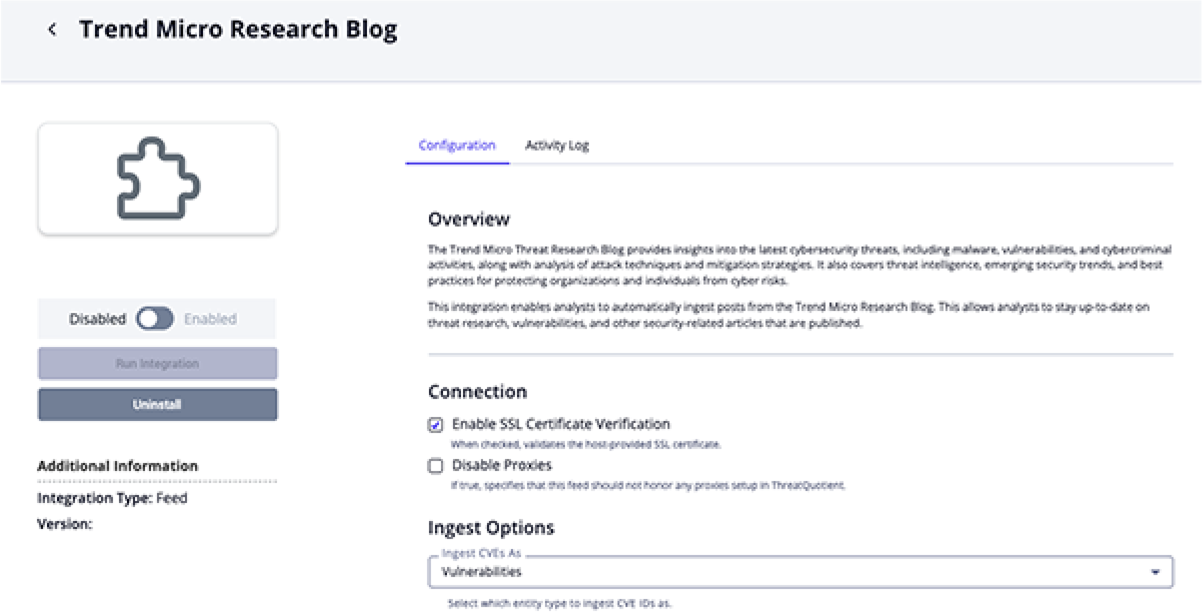
To configure the integration:

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
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.
Ingest CVEs As	Select the entity type to ingest CVE IDs as: • Vulnerabilities *(default)* • Indicators (CVE type)



Additional Information

Integration Type: Feed

Version:

Overview

The Trend Micro Threat Research Blog provides insights into the latest cybersecurity threats, including malware, vulnerabilities, and cybercriminal activities, along with analysis of attack techniques and mitigation strategies. It also covers threat intelligence, emerging security trends, and best practices for protecting organizations and individuals from cyber risks.

This integration enables analysts to automatically ingest posts from the Trend Micro Research Blog. This allows analysts to stay up-to-date on threat research, vulnerabilities, and other security-related articles that are published.

Connection

☑ Enable SSL Certificate Verification

When checked, validates the host-provided SSL certificate.

☐ Disable Proxies

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

Ingest Options

Ingest CVEs As: Vulnerabilities

Select which entity type to ingest CVE IDs as.

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

Trend Micro Research Blog

The Trend Micro Research Blog feed periodically pulls blog posts from the Trend Micro Research Blog and ingests them into ThreatQ as report objects.

Relevant indicators of compromise will be parsed and ingested into ThreatQ, related to each report.

`GET https://www.trendmicro.com/en_us/research.tagSearch.json`

Sample Response:

```
{
  "articles": [
    {
      "adaptiveImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/
SEO-manipulation-thumbnail:Medium?qlt=80",
      "articleType": "Research",
      "authors": [
        {
          "author": "Ted Lee",
          "title": "Threat Researcher"
        },
        {
          "author": "Lenart Bermejo",
          "title": "Threats Analyst"
        }
      ],
      "description": "This blog post details our analysis of an SEO
manipulation campaign targeting Asia. We also share recommendations that can
help enterprises proactively secure their environment.",
      "isoDate": "2025-02-07",
      "largeImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/SEO-
manipulation-thumbnail:Large?qlt=80",
      "linkMode": "default",
      "medium": "Articles, News, Reports",
      "mediumImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/
SEO-manipulation-thumbnail:Medium?qlt=80",
      "pageId": "110968239",
      "path": "https://www.trendmicro.com/en_us/research/25/b/chinese-speaking-
group-manipulates-seo-with-badiis.html",
      "primaryTag": "Malware",
      "publishDate": "Feb 07, 2025",
      "smallImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/SEO-
manipulation-thumbnail:Small?qlt=80",
      "tagNamespace": "trend-micro-research:",
      "tags": [
        "Trend Micro Research : Malware",
        "Trend Micro Research : Web",
        "Trend Micro Research : Research",
        "Trend Micro Research : Articles, News, Reports"
      ],
      "title": "Chinese-Speaking Group Manipulates SEO with BadIIS"
    },
    {
      "adaptiveImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/
cve-2025-0411-cover:Medium?qlt=80",
      "articleType": "Research",
      "authors": [
        {
          "author": "Peter Girnus",
          "title": "Sr. Threat Researcher"
        }
      ],
      "description": "The Trend ZDI team offers an analysis on how
CVE-2025-0411, a zero-day vulnerability in 7-Zip, was actively exploited to
target Ukrainian organizations in a SmokeLoader campaign involving homoglyph
attacks.",
      "isoDate": "2025-02-04",
      "largeImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/
cve-2025-0411-cover:Large?qlt=80",
      "linkMode": "default",
      "medium": "Articles, News, Reports",
      "mediumImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/
cve-2025-0411-cover:Medium?qlt=80",
      "pageId": "1298308672",
      "path": "https://www.trendmicro.com/en_us/research/25/a/cve-2025-0411-
ukrainian-organizations-targeted.html",
      "primaryTag": "Exploits  Vulnerabilities",
      "publishDate": "Feb 04, 2025",
      "smallImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/
cve-2025-0411-cover:Small?qlt=80",
      "tagNamespace": "trend-micro-research:",
      "tags": [
        "Trend Micro Research : APT  Targeted Attacks",
        "Trend Micro Research : Endpoints",
        "Trend Micro Research : Exploits Vulnerabilities",
        "Trend Micro Research : Research",
        "Trend Micro Research : Articles, News, Reports"
      ],
      "title": "CVE-2025-0411: Ukrainian Organizations Targeted in Zero-Day
Campaign and Homoglyph Attacks"
    },
    {
      "adaptiveImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/
native-sensors-vs-integrations-tn:Large?qlt=80",
      "articleType": "Expert Perspective",
      "authors": [
        {
          "author": "Chris LaFleur",
          "title": "Sr. Global Incident Response Program Manager"
        }
      ],
      "description": "Native sensors vs. integrations in XDR: Native sensors
offer faster deployment, real-time detection, and deeper visibility, while
integrations may add complexity and delays. Learn how to optimize your XDR
strategy for improved security.",
      "isoDate": "2025-02-03",
      "largeImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/
native-sensors-vs-integrations-tn:Large?qlt=80",
      "linkMode": "default",
      "medium": "Articles, News, Reports",
      "mediumImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/
native-sensors-vs-integrations-tn:Medium?qlt=80",
      "pageId": "412057230",
      "path": "https://www.trendmicro.com/en_us/research/25/b/native-sensors-
integrations-xdr-platform.html",
      "primaryTag": "Endpoints",
      "publishDate": "Feb 03, 2025",
      "smallImagePath": "https://trendmicro.scene7.com/is/image/trendmicro/
native-sensors-vs-integrations-tn:Small?qlt=80",
      "tagNamespace": "trend-micro-research:",
      "tags": [
        "Trend Micro Research : Endpoints",
        "Trend Micro Research : Articles, News, Reports",
        "Trend Micro Research : Expert Perspective"
      ],
      "title": "Native Sensors vs. Integrations for XDR Platforms?"
    }
  ]
}
```

The full blog content will be fetched for each of the entries in the `articles` list.

```
GET https://www.trendmicro.com/en_us/research/{{ uri }}
```

ThreatQuotient provides the following default mapping for this feed 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
`.title`	Report.Value	Report	`.isoDate`	`Attackers in Profile: menuPass and ALPHV/ BlackCat	N/A
N/A	Report.Description	N/A	`.isoDate`	N/A	Parsed from the HTML
`.publishDate`	Report.Attribute	Published At	`.isoDate`	`January 15, 2025`	N/A
`.path`	Report.Attribute	External Reference	`.isoDate`	`https://www.trendmicro.com/en_us/research/25/b/native-sensors-integrations-xdr-platform.html`	N/A
`.tags`	Report.Tag	N/A	`.isoDate`	`Exploits & Vulnerabilities`	N/A
`.authors .author`	Report.Attribute	Author	`.isoDate`	`Peter Girnus`	N/A
N/A	Indicator.Value	*	`.isoDate`	N/A	Indicators are fetched and parsed from the provided .txt files
N/A	Indicator/ Vulnerability.Value	CVE	`.isoDate`	N/A	CVE are fetched and parsed from the 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	2 minutes
Indicators	945
Indicator Attributes	31
Reports	22
Report Attributes	22

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.
- ThreatQuotient recommends running this integration every 2 days based on the publication pace of the site.

Change Log

- **Version 1.0.0**
    - Initial release