ThreatQuotient

A Securonix Company

Zscaler Security Research Blog CDF

Version 1.0.0

December 01, 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 Zscaler Security Research Blog CDF automatically ingests ThreatLabz's in-depth analyses of emerging threats, malware campaigns, and newly discovered vulnerabilities into ThreatQ as Report objects, enabling analysts to stay current on critical threat activity and enhance their intelligence workflows.

The integration provides the following feed:

- **Zscaler Security Research Blog –** retrieves the most recent security research articles and related metadata.

The integration ingests the following object types:

- Attack Patterns
- Indicators
- Reports
    - Report Attributes
- Vulnerabilities

Installation

Perform the following steps to install the integration:

> The same steps apply when upgrading to a newer version.

1. Log into https://marketplace.threatq.com/.
2. Download the integration YAML file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click 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(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:

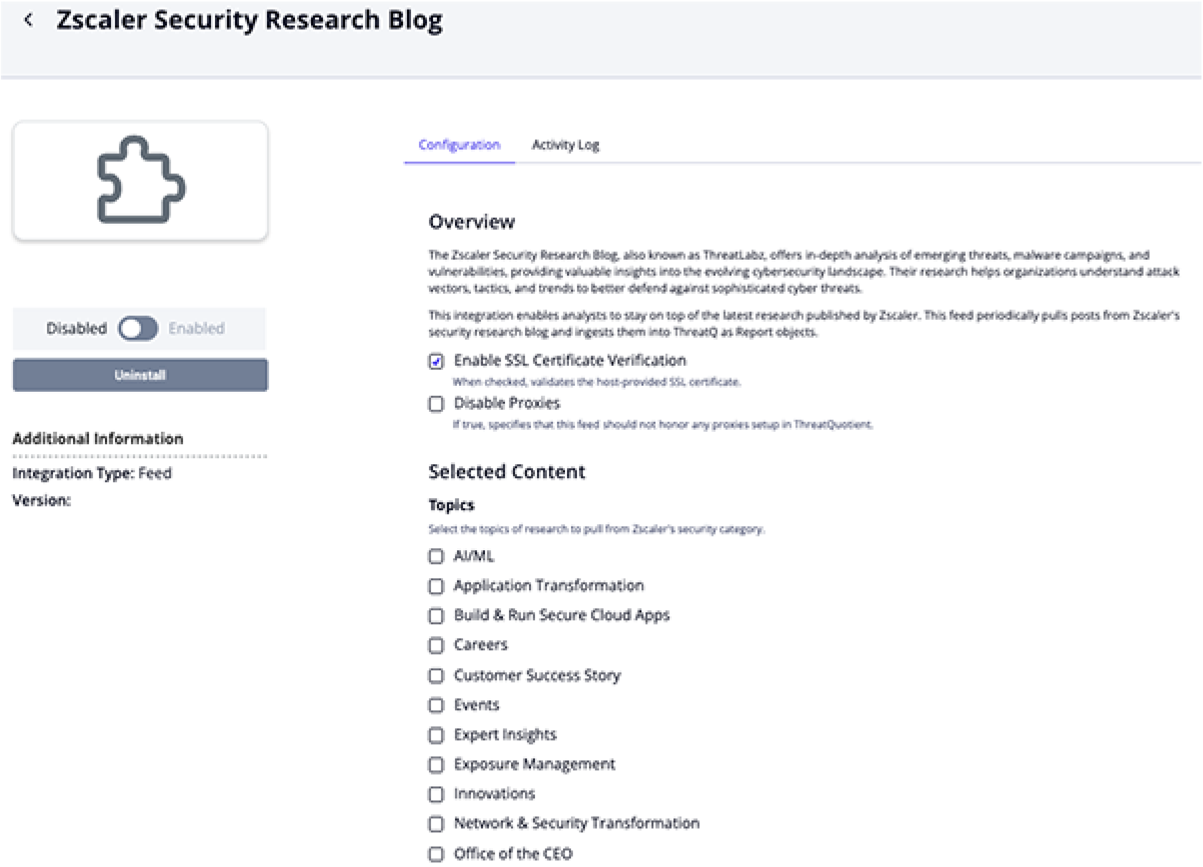
1. Navigate to the ThreatQ integrations management page.
2. Select the **OSINT** category (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Open the integration entry.
4. Enter the following configuration 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.
Topics	Select Zscaler blog categories to ingest. Options include: ◦ AI/ML ◦ Application Transformation ◦ Build & Run Secure Cloud Apps ◦ Careers ◦ Customer Success Story ◦ Events ◦ Expert Insights ◦ Exposure Management ◦ Innovations ◦ Security Insights *(default)* ◦ Stop Cyberattacks ◦ Third-Party Access ◦ Threat Detection & Response ◦ Threat Research *(default)* ◦ Zero Trust ◦ Zero Trust App Access ◦ Zero Trust Architecture

PARAMETER	DESCRIPTION
	◦ Network & Security Transformation ◦ Office of the CEO ◦ Optimize Digital Experiences ◦ Partners ◦ People & Culture ◦ Public Sector ◦ Ransomware *(default)* ◦ Risk Management ◦ SASE & SSE ◦ SecOps & Endpoint Security ◦ Secure IoT & OT ◦ Secure Remote Access ◦ Zero Trust Branch & Cloud ◦ Zero Trust SD-WAN ◦ Zero Trust Segmentation ◦ Zscaler Internet Access (ZIA) ◦ Zscaler Private Access (ZPA) ◦ Zscaler Zero Trust Exchange (ZTE) ◦ Accelerate M&A and Divestitures ◦ Data Security ◦ Resilience ◦ VDI Alternative ◦ Zscaler Digital Experience (ZDX)
Parse for MITRE ATT&CK Techniques	Parses and ingests ATT&CK techniques found in article content. This parameter is enabled by default.
Parsed IOC Types	Select indicator types to extract. Options include: ◦ CIDR Blocks ◦ CVEs *(default)* ◦ Email Addresses ◦ Filenames ◦ File Paths ◦ FQDNs ◦ IP Addresses ◦ MD5 *(default)* ◦ SHA-1 *(default)* ◦ SHA-256 *(default)* ◦ SHA-384 ◦ SHA-512 *(default)* ◦ URLs
Ingest CVEs as	Choose whether CVE values are ingested as Vulnerabilities (default) or as Indicators (type CVE).



Zscaler Security Research Blog

Additional Information

Integration Type: Feed

Version:

Overview

The Zscaler Security Research Blog, also known as ThreatLabz, offers in-depth analysis of emerging threats, malware campaigns, and vulnerabilities, providing valuable insights into the evolving cybersecurity landscape. Their research helps organizations understand attack vectors, tactics, and trends to better defend against sophisticated cyber threats.

This integration enables analysts to stay on top of the latest research published by Zscaler. This feed periodically pulls posts from Zscaler's security research blog and ingests them into ThreatQ as Report objects.

☑ 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.

Selected Content

Topics

Select the topics of research to pull from Zscaler's security category.

□ AI/ML
□ Application Transformation
□ Build & Run Secure Cloud Apps
□ Careers
□ Customer Success Story
□ Events
□ Expert Insights
□ Exposure Management
□ Innovations
□ Network & Security Transformation
□ Office of the CEO

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

Zscaler Security Research Blog

The Zscaler Security Research Blog feed retrieves security-research blog posts from Zscaler, parses metadata and full article content, and ingests results into ThreatQ as Report objects, along with indicators, vulnerabilities, and attack patterns.

`POST https://www.zscaler.com/api/search`

This request returns JSON data, which is parsed for `tags`, `editors`, `categories`, and the `link` to the underlying article. The full article content is then fetched.

`GET https://zscaler.com/{{ uri }}`

Sample Response:

```
{
  "results": [
    {
      "title": { "raw": ["Example Threat Research Post"] },
      "published_at": "2025-04-05",
      "topics": { "raw": ["Ransomware"] },
      "blog_category": { "raw": ["Threat Research"] },
      "author": { "raw": [{"name": "ThreatLabz"}] },
      "uri": "path/to/article"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed based on the `.results[]` array in the JSON data, as well as information parsed out of the article's HTML content.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.title.raw[].0	Report.Title	N/A	.published_at	New “Crypto Drainer” Phishing Pages Siphon Cryptocurrency	N/A
N/A	Report.Description	N/A	N/A	N/A	Parsed from HTML content
.published_at	Report.Attribute	Published At	.published_at	April 05, 2025	N/A
.topics.raw[]	Report.Attribute	Topic	.published_at	Ransomware	N/A
.topics.raw[]	Report.Tag	N/A	N/A	Ransomware	N/A
.blog_category.raw[]	Report.Attribute	Category	.published_at	Threat Research	N/A
.blog_category.raw[]	Report.Tag	N/A	N/A	Threat Research	N/A
.author.raw[].name	Report.Attribute	Author	N/A	ThreatLabz	N/A
N/A	Report.Indicator.Value	Various Types	N/A	N/A	User-configurable extraction from HTML content
N/A	Report.Attack-Pattern.Value	N/A	N/A	T1087 – Account Discovery	User-configurable extraction
N/A	Report.Vulnerability.Value / Report.Indicator.Value	CVE	N/A	CVE-2023-41232	User-configurable extraction

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	15
Report Attributes	45
Attack Patterns	25
Indicators	117
Vulnerabilities	4

Known Issues / Limitations

- ThreatQuotient recommends running this integration every 2 days based on the publication pace of the site.
- ThreatQ may extract hostnames or IPs from URLs even when only "URLs" is selected as a parsed IOC type, due to internal indicator expansion logic.
- 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