

ThreatQuotient

A Securonix Company



Permiso Research Blog CDF

Version 1.0.0

November 12, 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	3
Support	4
Integration Details.....	5
Introduction	6
Installation.....	7
Configuration	8
ThreatQ Mapping.....	10
Permisos Research Blog	10
Average Feed Run.....	11
Known Issues / Limitations	12
Change Log	13

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.

Copyright © 2025 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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 $\geq 5.6.0$

Support Tier ThreatQ Supported

Introduction

The Permiso Research Blog CDF allows analysts to automatically ingest blog posts directly from the Permiso Research Blog, ensuring timely access to the latest cybersecurity updates. This integration enables teams to stay informed on emerging threats, trends, and research insights across the cybersecurity landscape.

The integration provides the following feed:

- **Permiso Research Blog** - pulls blogs posts from the Permiso Blog's Research category and ingests them into ThreatQ as Report objects.

The integration ingests the following object types:

- Indicators
- Reports
 - Report Attributes
- 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
Parsed IOC Types	Select the IOC types to automatically parse from the content.  At this time, the only option available for this parameter is CVE .
Ingest CVEs As	Select the entity type to ingest CVE IDs as in ThreatQ. Options include: <ul style="list-style-type: none">◦ Vulnerabilities (<i>default</i>)◦ Indicators  This parameter is only accessible if you have selected the CVE option for the Parsed IOC Types parameter.
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.

[Permiso Research Blog](#)

Configuration Activity Log

Overview
This feed pulls the posts from Permiso's Security Blog. Just note, this feed will only pull the recent posts from the blog, nothing historical. This feed does not pull the private threat briefings published by Permiso, only the public blog posts.

Ingestion Options
Parsed IOC Types
Select the IOC types you would like to automatically parse from the content.
 CVE
Ingest CVEs As Select the entity type to ingest CVE IDs as.

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.

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

Permiso Research Blog

The Permiso Research Blog feed periodically pulls blog posts from the Permiso Blog's Research category and ingests them into ThreatQ as Report objects.

GET `https://permiso.io/blog`

This request returns HTML. The HTML is parsed for the title, author, date, links, etc. The blog itself is then fetched.

GET `https://permiso.io/blog/{{ 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
N/A	Report.Title	N/A	N/A	LUCR-3: Scattered Spider Getting SaaS-y in the Cloud	Parsed from the HTML
N/A	Report.Description	N/A	N/A	N/A	Parsed from the HTML
N/A	Report.Attribute	External Reference	N/A	https://permiso.io/blog/lucr-3-scattered-spider-getting-saas-y-in-the-cloud	Parsed from HTML
N/A	Report.Attribute	Published At	N/A	2023-09-20	Parsed from the HTML
N/A	Report.Attribute	Author	N/A	Ian Ahl	Parsed from the HTML
N/A	Related Indicator/Vulnerability	CVE/Vulnerability	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	14
Report Attributes	32
Indicators	1

Known Issues / Limitations

- The Permisos Research Blog feed only pulls in blog posts from the Research Category.
- 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 weeks based on the publication pace of the site.

Change Log

- **Version 1.0.0**
 - Initial release