

ThreatQuotient

A Securonix Company



SOC Prime Blog CDF

Version 1.0.0

December 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	3
Support	4
Integration Details.....	5
Introduction	6
Installation.....	7
Configuration	8
ThreatQ Mapping.....	9
SOC Prime Blog	9
Average Feed Run.....	10
Known Issues / Limitations	11
Change Log	12

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 $\geq 5.12.1$

Support Tier ThreatQ Supported

Introduction

The SOC Prime Blog CDF integration enables analysts to automatically ingest blog content published on the SOC Prime website, ensuring timely access to expert research and insights. By streamlining the delivery of updates on emerging threats, vulnerabilities, and broader cybersecurity developments, this integration helps security teams stay informed and maintain situational awareness within their operational workflows.

The integration provides the following feed:

- **SOC Prime Blog** - ingests posts under the *Latest Threats* category of the SOC Prime blog as ThreatQ reports.

The integration ingests reports and report attributes into the ThreatQ platform.

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.

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

SOC Prime Blog

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

GET `https://socprime.com/wp-admin/admin-ajax.php`

This request returns JSON with an html key that contains raw HTML. The HTML is parsed for the title, author, date, links, etc. The blog itself is then fetched.

GET `https://socprime.com/blog/cve-2024-6670-and-cve-2024-6671-detection/`

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	CVE-2024-6670 and CVE-2024-6671 Detection: RCE Attacks Exploiting Critical SQL Injection Vulnerabilities in WhatsUp Gold	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://socprime.com/blog/cve-2024-6670-and-cve-2024-6671-detection/	Parsed from HTML
N/A	Report.Attribute	Published At	N/A	Sep 17/2024	Parsed from the HTML
N/A	Report.Attribute	Author	N/A	Veronika Telychko	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	1 minute
Reports	8
Report Attributes	16

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.
- The feed will only return at maximum, the most recent 23 posts.
- ThreatQuotient recommends running this integration every 7 days based on the publication pace of the site.

Change Log

- **Version 1.0.0**
 - Initial release