ThreatQuotient

A Securonix Company
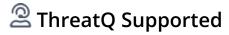
SentinelOne Labs Blog CDF

Version 1.0.0

September 09, 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 SentinelOne Labs Blog CDF enables analysts to automatically ingest content from the SentinelOne Labs blog: `https://www.sentinelone.com/labs`. This ensures analysts remain current on malware, threat actors, vulnerabilities, and other threat research articles.

The integration provides the following feed:

- **SentinelOne Labs Blog** - ingests blog posts as reports filtered by published time.

The integration ingests Report object types.

Installation

Perform the following steps to install the integration:

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

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** category 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. Review 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

SentinelOne Labs Blog

The SentinelOne Labs Blog feed periodically pulls threat research posts from the SentinelOne Labs blog and ingests them into ThreatQ as report objects.

`GET https://www.sentinelone.com/labs/`

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

`GET https://www.sentinelone.com/labs/{{ uri }}`

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Report.Value	N/A	N/A	`AcidPour | New Embedded Wiper Variant of AcidRain Appears in Ukraine`	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://www.sentinelone.com/labs/ acidpour-new-embedded-wiper-variant-of- acidrain-appears-in-ukraine/`	Parsed from the HTML
N/A	Report.Attribute	Published At	N/A	`2024-02-20`	Parsed from the HTML
N/A	Report.Tag	N/A	N/A	`Security & Intelligence`	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	5
Report Attributes	10

Known Issues / Limitations

- The feed utilizes **since** and **until** dates to make sure entries are not re-ingested if they haven't been updated.
- The first run of this feed will only pull the blog posts from the last 24 hours. To ingest historical blog posts, run the feed manually by setting the **since** date back.
- This feed will only pull a maximum of the latest 2 pages of the blog.

Change Log

- **Version 1.0.0**
  - Initial release