ThreatQuotient

A Securonix Company

Sekoia Blog CDF

Version 1.0.1

February 02, 2026

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**
Sekoia Blog 10
Average Feed Run **12**
Sekoia Blog 12
Known Issues / Limitations **13**
Change Log **14**

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	1.0.1
Compatible with ThreatQ Versions	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

The Sekoia Blog CDF enables analysts to automatically ingest blog posts from the Sekoia website. This allows analysts to stay up-to-date on advisories, bulletins, and analyses from the Sekoia team. Considering the pace of new articles, we recommend running this CDF every week.

The integration provides the following feed:

- **Sekoia Blog** - pulls blogs posts from the Sekoia website.

The integration ingests the following system 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
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.

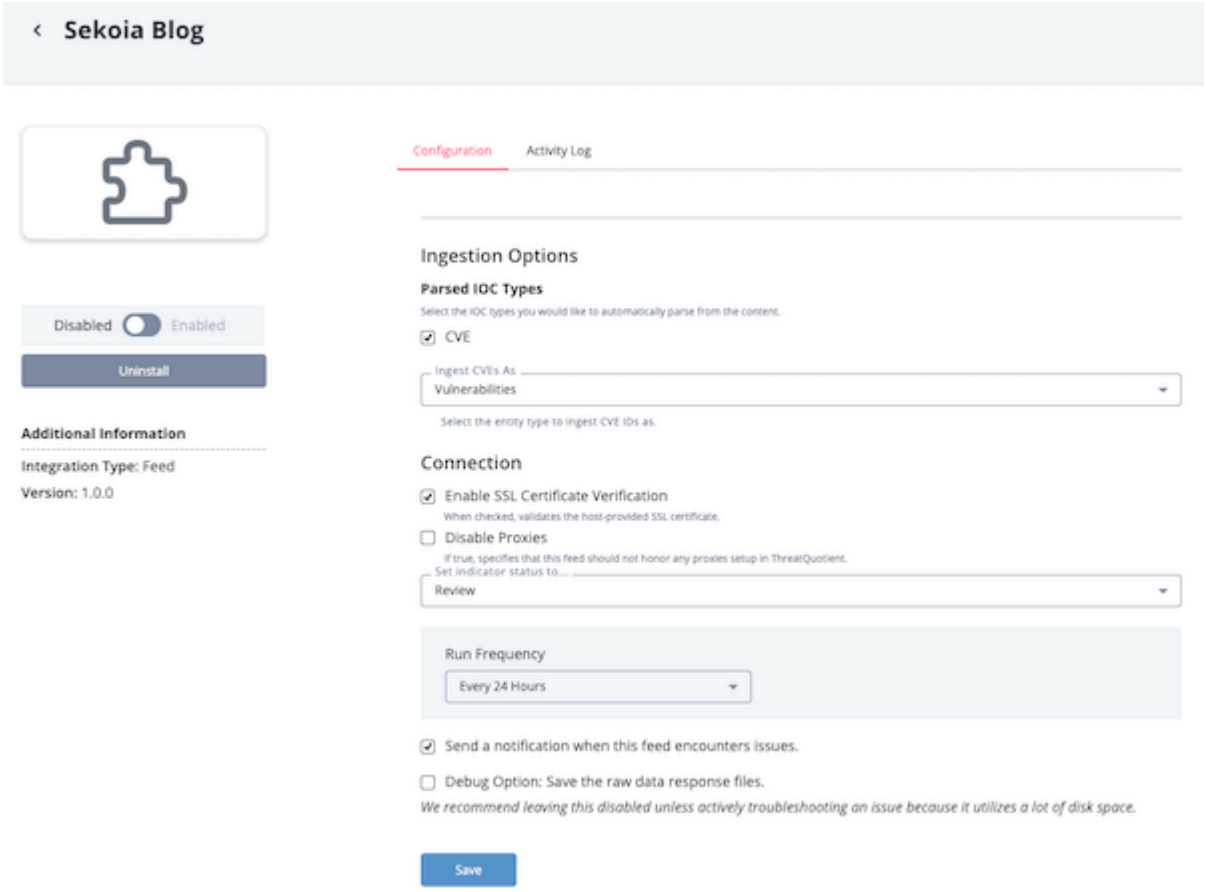
To configure the integration:

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
Parsed IOC Types	Select the IOC types you would like to automatically parse from the content: • CVE (default)
Ingest CVEs As	Select the entity type to ingest CVE IDs as: • Vulnerabilities (default) • Indicators > This field is displayed if you select CVE in the Parsed IOC Types field.
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

Sekoia Blog

This feed periodically pulls blog posts from the Sekoia website, and ingests them into ThreatQ as report objects.

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

The output of this request is HTML, which is parsed for links to the actual blog posts In addition, the HTML content for each blog is also fetched and imported as the description for the report object

```
GET https://blog.sekoia.io/{{ url_path }}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
{HTML}	Report.Title	N/A	{HTML}	Global analysis of Adversary-in-the-Middle phishing threats - Sekoia.io Blog	Parsed from HTML.
{HTML}	Report.Description	N/A	{HTML}	In recent years, organisations have increasingly...	Parsed from HTML.
{HTML}	Report.Attribute	External Reference	{HTML}	https://blog.sekoia.io/global-analysis-of-adversary-in-the-middle-phishing-threats/	Parsed from HTML.
{HTML}	Report.Attribute	Published At	{HTML}	June 11 2025	Parsed from title.
{HTML}	Report.Indicator/ Vulnerability.Value	CVE/Vulnerability	{HTML}	CVE-2023-41232	Parsed from HTML. Ingested according to Ingest CVEs As.

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.

Sekoia Blog

METRIC	RESULT
Run Time	1 minute
Reports	1
Report Attributes	2

Known Issues / Limitations

- This feed uses "since" and "until" dates to make sure entries are not re-ingested if they have not been updated.
- If you would like to ingest historical blog posts, run the feed manually, setting the since date back.
- The maximum number of posts this feed will return is the most recent 25.

Change Log

- **Version 1.0.1**
  - Resolved an ingestion issue related to regular expressions.
- **Version 1.0.0**
  - Initial release