ThreatQuotient

A Securonix Company

Foresiet Blog CDF

Version 1.0.0

October 10, 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 Foresiet Blog CDF integration provides analysts with direct access to the latest cybersecurity research and insights from Foresiet, including analyses of threat actors, malware investigations, and vulnerability trend reports. The integration ensures ThreatQ analysts remain informed about emerging threats and up-to-date with Foresiet's latest research publications.

The integration provides the following feed:

- **Foresiet Blog -** ingests reports parsed directly from published blog posts on the Foresiet website.

The integration ingests reports and report attributes.

Prerequisites

No special prerequisites are required to install and run this integration.

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. This integration requires no external credentials.

To configure the integration:

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

   > If installing 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
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.

5. Review any additional settings, make changes if needed, and click **Save**.
6. Click the toggle switch located above the *Additional Information* section to enable the feed.

ThreatQ Mapping

Foresiet Blog

The Foresiet Blog feed periodically retrieves cybersecurity research posts from the Foresiet Blog. Posts are ingested into ThreatQ as Report objects, with full post content included in the Report description.

```
GET https://foresiet.com/resources/blog/
```

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

```
GET https://foresiet.com/blog/{{ url-path }}
```

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	EXAMPLES	NOTES
N/A	Report.Title	N/A	Military ID Deepfakes: How North Korean Hackers Target the South with AI	Parsed from the HTML
N/A	Report.Description	N/A	N/A	Parsed from the HTML
N/A	Report.Attribute	Published At	September 17, 2025	Parsed from the HTML
N/A	Report.Attribute	Category	APT / Cyber Espionage	Parsed from the HTML
N/A	Report.Attribute	External URL	https://foresiet.com/blog/military-id-deepfakes-north-korean-hackers/	Parsed from the HTML

Average Feed Run

> Object counts and Feed runtime are supplied as generalities only. Actual results may vary depending on provider configurations and system performance.

METRIC	RESULT
Run Time	1 minute
Reports	5
Report Attributes	5

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 pull, at maximum, the first 2 pages of posts from the Foresiet Blog.
- ThreatQuotient recommends running this integration every 7 days based on the publication pace of the site.

Change Log

- **Version 1.0.0**
    - Initial release