# ThreatQuotient

**A Securonix Company**



## Cybereason Blog CDF

**Version 1.0.0**

January 06, 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

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 Cybereason Research Blog provides in-depth analysis of emerging cyber threats, including malware campaigns and advanced persistent threats (APTs), with a focus on attack techniques, adversary tactics, reverse engineering insights, and detection strategies. The Cybereason Blog CDF integration periodically ingests this research into ThreatQ as Report objects, enabling analysts to centrally track and operationalize the latest Cybereason threat intelligence alongside other sources within the ThreatQ platform.

The integration provides the following feed:

- **Cybereason Research Blog** - ingests Cybereason blog posts as ThreatQ reports.

The integration ingests reports and report attributes.

# 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

## Cybereason Research Blog

The Cybereason Research Blog feed pulls blog posts from Cybereason's Research blog posts and ingests them into ThreatQ as report objects.

> The feed will only pull blog posts under the **Research** category.

```
GET https://www.cybereason.com/blog/category/research
```

The output of this request is HTML. The HTML is parsed for the `title`, `author`, `date`, `links`, etc. The blog itself is then fetched.

```
GET https://www.cybereason Blog.com/{{ 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 | `Phorpiex - Downloader Delivering Ransomware` | Parsed from the HTML |
| N/A | Report.Description | N/A | N/A | N/A | Parsed from the HTML |
| N/A | Report.Attribute | Published At | N/A | `September 05, 2024` | Parsed from the HTML |
| N/A | Report.Attribute | Author | N/A | `Cybereason Security Services Team` | Parsed from the HTML |
| N/A | Report.Attribute | External URL | N/A | `https://www.Cybereason Blog.com...` | 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 | 2 |
| Report Attributes | 4 |

# 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.
- ThreatQuotient recommends running this integration every 2 days based on the publication pace of the site.

# Change Log

- **Version 1.0.0**
  - Initial release