

# ThreatQuotient



## Outpost24 Research Blog CDF

Version 1.0.0

May 12, 2025

### ThreatQuotient

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 ThreatQ Supported

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

Warning and Disclaimer ..... 3

Support ..... 4

Integration Details..... 5

Introduction ..... 6

Installation..... 7

Configuration ..... 8

ThreatQ Mapping..... 10

    Outpost24 Research Blog ..... 10

Average Feed Run..... 11

Known Issues / Limitations ..... 12

Change Log ..... 13

# 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:** [support@threatq.com](mailto:support@threatq.com)

**Support Web:** <https://support.threatq.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 Outpost24 Research Blog CDF integration enables analysts to stay on top of the latest posts published by the [Outpost24 team](#). The Outpost24 Research and Threat Intel blog delivers in-depth cybersecurity research and analysis, providing current insights into emerging threats and vulnerabilities and helps security professionals stay informed with actionable intelligence on the latest cyber risks.

The integration provides the following feed:

- **Outpost24 Research Blog** - ingest news posts from Outpost24 Research Blog's security category as 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
<b>Enable SSL Certificate Verification</b>	Enable this parameter if the feed should validate the host-provided SSL certificate.
<b>Disable Proxies</b>	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



## < Outpost24 Research Blog



Disabled ☒ Enabled

Run Integration

Uninstall

### Additional Information

Integration Type: Feed

Version:

Configuration **Activity Log**

### Overview

The Outpost24 Research & Threat Intel blog delivers in-depth cybersecurity research and analysis, providing current insights into emerging threats and vulnerabilities. It helps security professionals stay informed with actionable intelligence on the latest cyber risks.

This integration enables analysts to stay on top of the latest posts published by the Outpost24 team. This feed periodically pulls posts from Outpost24's Research & Threat Intelligence Blog and ingests them into ThreatQ as Report objects.

### Request Options

☐ Enable SSL Certificate Verification

When checked, validates the host-provided SSL certificate. Checked by default.

☒ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient

Set indicator status to...

Review

Run Frequency

Every 24 Hours

Next scheduled run:  
05/13/2025 09:33am

☒ Send a notification when this feed encounters issues.

☒ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

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

## Outpost24 Research Blog

The Outpost24 Research Blog feed periodically pulls news posts from Outpost24 Research Blog's security category and ingests them into ThreatQ as Report objects.

GET `https://outpost24.com/blog/category/research-and-threat-intel/page/{{ page }}`

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

GET `https://outpost24.com/blog/{{ path }}`

The mapping for this feed is 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	Black Basta & M_A_G_A: Threat intelligence briefing Feb 2025	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	February 24, 2025	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	6
Report Attributes	6

---

## 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 pull a maximum of the first 3 pages of news posts from Outpost24 Research Blog.

# Change Log

- Version 1.0.0
  - Initial release