

ThreatQuotient

A Securonix Company



Fortinet Threat Research CDF

Version 1.0.0

July 15, 2025

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 **ThreatQ Supported**

Support

Email: support@threatq.com

Web: 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

 Fortinet Threat Research 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

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 Fortinet Threat Research CDF enables analysts to automatically ingest blog posts from the Fortinet website, <https://www.fortinet.com/blog/threat-research>, allowing them to stay up-to-date on advisories, bulletins, and analyses from the FortiGuard Labs team.

The integration provides the following feed:

- **Fortinet Threat Research Data** - pulls blog posts from the Fortinet Threat Research website and ingests them into ThreatQ as report objects.

The integration ingests the following system object types:

- Indicators
- Reports
- 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



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.
Parsed IOC Types	Select the IOC types you would like to automatically parse from the content. The only option available at this time is CVE.
Ingest CVEs As	Select the entity type to ingest CVE IDs as into the ThreatQ platform. Options include: ◦ Vulnerabilities (default) ◦ Indicators
	 This parameter is only accessible if the CVE option is selected for the Parsed IOC Types parameter.

< Fortinet Threat Research

Disabled ☐ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

Connection

☒ Enable SSL Certificate Verification
When checked, validates the host-provided SSL certificate.

☒ Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Ingestion Options

Parsed IOC Types

Select the iOC types you would like to automatically parse from the content.

☒ CVE

Ingest CVEs As Indicators (Type: CVE)

Select the entity type to ingest CVE IDs as.

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

Fortinet Threat Research

The Fortinet Threat Research feed pulls blog posts from the Fortinet Threat Research website and ingests them into ThreatQ as report objects.

```
GET https://www.fortinet.com/content/fortinet-blog/us/en/threat-research/jcr:content/root/bloglist.0.html
```

The output of this request is HTML which is parsed for links to the actual blog posts. These links will be fetched to get the content of each blog post.

```
GET https://www.fortinet.com/{{ uri }}
```



Only blog posts marked as Threat Research will be ingested.

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	Report	Parsed from HTML	Ransomware Roundup – HardBit 2.0	Parsed from HTML
N/A	Report.Attribute	External Reference	Parsed from HTML	https://www.fortinet.com/blog/threat-research/fortiguards-labs-ransomware-roundup	Parsed from HTML
N/A	Report.Attribute	Published At	Parsed from HTML	March 16, 2023	Parsed from HTML
N/A	Report.Description	N/A	N/A	<HTML content>	Parsed from HTML
N/A	Indicator/Vulnerability.Value	CVE/Vulnerability	N/A	CVE-2023-41232	Parsed from HTML. Ingested according to Ingest CVEs As



This mapping does not include feed data paths as there is no structured data.

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
Indicators	2
Reports	6
Report Attributes	12

Known Issues / Limitations

- ThreatQuotient recommends running this integration every 2 days based on the publication pace of the Fortinet site.
- 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 integration can fetch a maximum of 4 blog posts.

Change Log

- Version 1.0.0
 - Initial release