

# ThreatQuotient

A Securonix Company



## ESET WeLiveSecurity CDF

Version 1.0.0

July 21, 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

    ESET WeLiveSecurity..... 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	>= 5.12.0
Support Tier	ThreatQ Supported

# Introduction

The ESET WeLiveSecurity CDF integration ingests blog posts from the WeLiveSecurity website, <https://www.welivesecurity.com/>, enabling analysts to stay up-to-date on advisories, bulletins, and analyses from the WeLiveSecurity team.

The integration provides the following feed:

- **ESET WeLiveSecurity** - ingests ESET articles as ThreatQ 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
<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.
<b>Parsed IOC Types</b>	Select the IOC types you would like to automatically parse from the content. The only option available at this time is CVE.
<b>Ingest CVEs As</b>	Select the entity type to ingest CVE IDs as into the ThreatQ platform. Options include: <ul style="list-style-type: none"> <li>◦ Vulnerabilities (default)</li> <li>◦ Indicators</li> </ul> <div>            This parameter is only accessible if the CVE option is selected for the <b>Parsed IOC Types</b> parameter.         </div>



< ESET WeLiveSecurity

Disabled ☐ Enabled ☒

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version: 1.0.0

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 ThreatQuarant.

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

## ESET WeLiveSecurity

The ESET WeLiveSecurity feed pulls blog posts from the WeLiveSecurity website and ingests them into ThreatQ as report objects.

GET <https://www.welivesecurity.com/en/eset-research/>

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.welivesecurity.com/{{ uri }}>



Only blog posts marked as ESET 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.Title	Report	Published At	The slow Tick-ing time bomb: Tick APT group compromise of a DLP software developer in East Asia	Parsed from HTML
N/A	Report.Attribute	Published At	Published At	N/A	Parsed from HTML
N/A	Report.Attribute	External Reference	Published At	<a href="https://www.welivesecurity.com/2023/03/14/slow-ticking-time-bomb-tick-apt-group-dlp-software-developer-east-asia/">https://www.welivesecurity.com/2023/03/14/slow-ticking-time-bomb-tick-apt-group-dlp-software-developer-east-asia/</a>	Parsed from HTML
N/A	Report.Description	N/A	Published At	<HTML content>	Parsed from HTML
N/A	Indicator/Vulnerability	CVE/Vulnerability	Published At	CVE-2023-41232	Parsed from HTML. 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	12
Report Attributes	24

## Known Issues / Limitations

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

# Change Log

- Version 1.0.0
  - Initial release