ThreatQuotient

A Securonix Company



abuse.ch CDF

Version 2.0.0

November 03, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **3**
Support **4**
Integration Details **5**
Introduction **6**
Installation **7**
Configuration **8**
All Feeds 8
ThreatQ Mapping **10**
Feodo Tracker Botnet C2 IP Blocklist 10
SSLBL SSL Blacklist 11
URLhaus Database Dump 12
URLhaus Plain-Text URL List 13
URLhaus Response Policy Zones 14
Average Feed Run **15**
Feodo Tracker Botnet C2 IP Blocklist 15
SSLBL SSL Blacklist 15
URLhaus Database Dump 15
URLhaus Plain-Text URL List 16
URLhaus Response Policy Zones 16
Known Issues / Limitations **17**
Change Log **18**

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 © 2026 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@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	2.0.0
Compatible with ThreatQ Versions	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The abuse.ch CDF imports community-sourced threat indicators into ThreatQ from Feodo Tracker, SSLBL, and URLhaus. These feeds include botnet command-and-control IPs, URLs associated with malicious SSL activity, recent malware URLs, and URLhaus Response Policy Zone data, helping security teams use this intelligence in threat investigations and detection.

The integration provides the following feeds:

- **abuse.ch Feodo Tracker Botnet C2 IP Blocklis**t - Ingests botnet C&C servers associated with the Feodo malware family
- **abuse.ch SSLBL SSL Blacklist** - ingests URLs associated with malicious SSL connections
- **abuse.ch URLhaus Database Dump** - ingests recent URLs from the authenticated URLhaus Database Dump export
- **abuse.ch URLhaus Plain-Text URL List** - ingests recent malware URLs from the authenticated URLhaus export
- **abuse.ch URLhaus Response Policy Zones** - ingests URLS from URLhaus DNS Response Policy Zone

The integration ingests indicators and indicator Attribute types into the ThreatQ Platform.

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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration 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.
6. If prompted, select the individual feeds to install and click **Install**. 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).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

All Feeds

PARAMETER	DESCRIPTION
Auth Key	Enter your abuse.ch authentication key.
Enable SSL Certificate Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.
Only Ingest New Indicators *(Database Dump Feed Only)*	Enabling this parameter will filter out indicators that are not new since the last time the feed ran.
Only Ingest Online Indicators *(Database Dump Feed Only)*	Enabling this parameter will filter out indicators that have a status of **offline**.

Context Selection *(Database Dump Feed Only)*	Select which pieces of context to ingest into ThreatQ with each indicator. Options include: ◦ URL Haus ID *(default)* ◦ URL Status *(default)* ◦ Threat Type *(default)* ◦ URLHaus Tag *(default)* ◦ URLHaus Link *(default)*

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

Feodo Tracker Botnet C2 IP Blocklist

The Feodo Tracker Botnet C2 IP Blocklist feed ingests botnet C&C servers associated with the Feodo malware family.

```
GET https://feodotracker.abuse.ch/downloads/ipblocklist.csv
```

Sample Response:

```
"2021-01-17
07:30:05","67.213.75.205","443","offline","2021-02-04","Dridex"
"2021-01-17
07:44:46","192.73.238.101","443","online","2021-02-04","Dridex
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
1 (second token)	Indicator.Value	IP Address	0 (first token)	74.58.188.22	N/A
2 (third token)	Indicator.Attribute	Destination Port	0 (first token)	8080	N/A
3 (fourth token)	Indicator.Attribute	C2 Status	0 (first token)	online	N/A
4 (sixth token)	Indicator.Attribute	Malware Type	0 (first token)	Dridex	N/A

SSLBL SSL Blacklist

The SSLBL SSL Blacklist feed is a project of `abuse.ch` with the goal of detecting malicious SSL connections, by identifying and blacklisting SSL certificates used by botnet C&C servers. In addition, SSLBL identifies JA3 fingerprints that helps you to detect & block malware botnet C&C communication on the TCP layer.

```
GET https://sslbl.abuse.ch/blacklist/sslblacklist.csv
```

Sample Response:

```
2019-01-21 10:08:50,b8e3ed1bb59bac1a0d18725e751a7b43b462df59,Malware C&C
2019-01-21 09:21:38,f10c6f69a0252454792fc3cbcdd7f0e7bab3bb2b,Malware C&C
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
1 (second token)	Indicator.Value	SHA-1	0 (first token)	b8e3ed1bb59bac1a0d18725e751a7b43b462df59	N/A
2 (third token)	Indicator.Attribute	Malware Family	0 (first token)	Malware C&C	N/A

URLhaus Database Dump

The URLhaus Database Dump feed ingests the URLhaus recent database dump.

```
GET https://urlhaus-api.abuse.ch/v2/files/exports/<AUTH_KEY>/recent.csv
```

Sample Response:

```
#
id,dateadded,url,url_status,last_online,threat,tags,urlhaus_link,reporter
"4041559","2026-10-28 12:18:42","http://105.96.242.68:43747/bin.sh","online","2026-10-28 12:18:42","malware_download","None","https://urlhaus.abuse.ch/url/4041559/","adliwahid"
"4041558","2026-10-28 12:18:29","https://github.com/example/sample.zip","offline","","malware_download","github,example","https://urlhaus.abuse.ch/url/4041558/","anonymous"
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
id	Indicator.Attribute	URL Haus ID	dateadded	4041559	User-configurable.
url	Indicator.Value	URL	dateadded	http://105.96.242.68:43747/bin.sh	N/A
url_status	Indicator.Attribute	URL Status	dateadded	online	User-configurable. Updatable.
threat	Indicator.Attribute	Threat Type	dateadded	malware_download	User-configurable.
tags	Indicator.Attribute	URLHaus Tag	dateadded	github, example	Comma-separated values. None values are skipped.
urlhaus_link	Indicator.Attribute	URLHaus Link	dateadded	https://urlhaus.abuse.ch/url/4041559/	User-configurable.

URLhaus Plain-Text URL List

The URLhaus Plain-Text URL List feed ingests recent malware URLs from the authenticated URLhaus export.

```
GET https://urlhaus-api.abuse.ch/v2/files/exports/<AUTH_KEY>/urls_recent.txt
```

Sample Response:

```
https://winbitbrowser.com/telegram_mess.apk
https://github.com/teceduoswaldo3000/github-slideshow/raw/main/node_modules/reveal.js/lib/font/github-slideshow_v2.0.zip
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
Line value	Indicator.Value	URL	N/A	https://winbitbrowser.com/telegram_mess.apk	Includes HTTP(S) and FTP URLs.

URLhaus Response Policy Zones

The URLhaus Response Policy Zones feed ingests FQDNs from the authenticated URLhaus DNS Response Policy Zone and adds the related URL as context.

```
GET https://urlhaus-api.abuse.ch/v2/files/exports/<AUTH_KEY>/rpz.txt
```

> The Auth Key is included in the export URL path. Keep the key confidential because it can appear in request logs.

Sample Response:

```
0qixri.thule.su CNAME . ; Malware download (2019-01-17), see https://
urlhaus.abuse.ch/host/0qixri.thule.su/
188mbnews.com CNAME . ; Malware download (2018-12-30), see https://
urlhaus.abuse.ch/host/188mbnews.com/
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator	FQDN	1 (second token)	0qixri.thule.su	Text " CNAME . ; Malware download (" is stripped from the FQDN
2 (third token)	Indicator.Attribute	URL	1 (second token)	https://urlhaus.abuse.ch/host/0qixri.thule.su	Text "), see " is stripped from the URL

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.

Feodo Tracker Botnet C2 IP Blocklist

METRIC	RESULT
Run Time	1 minutes
Indicators	326
Indicator Attributes	987

SSLBL SSL Blacklist

METRIC	RESULT
Run Time	4 minutes
Indicators	3,737
Indicator Attributes	3,737

URLhaus Database Dump

METRIC	RESULT
Run Time	26 min

METRIC	RESULT
Indicators	10,477
Indicator Attributes	82,548

URLhaus Plain-Text URL List

METRIC	RESULT
Run Time	50 min
Indicators	93,573
Indicator Attributes	154,759

URLhaus Response Policy Zones

METRIC	RESULT
Run Time	1 minute
Indicators	1,050
Indicator Attributes	1,050

Known Issues / Limitations

URLhaus Database Dump

- The authenticated `recent.csv` export can contain a substantial number of URLs. Feed runtime and output volume depend on the current URLhaus data volume and selected ingestion filters.

URLhaus Plain-Text URL List

- The authenticated `urls_recent.txt` export can contain a substantial number of URLs. Feed runtime and output volume depend on the current URLhaus data volume.

Change Log

- **Version 2.0.0**
  - Updated the URLhaus Database Dump, Plain-Text URL List, and Response Policy Zones feeds to use authenticated exports from the URLhaus v2 API.
  - Removed the obsolete **Dump Type** configuration option from the Plain-Text URL List feed.
- **Version 1.7.0**
  - Added support for authenticating with the API.
  - Removed deprecated feeds: abuse.ch SSLBL Response Policy Zones (RPZ) and abuse.ch SSLBL IP Blacklist
  - Changed Minimum ThreatQ version to 5.29.
  - Introduced a new design for user fields.
  - Added the option to to enable SSL certificate verification and/or disable proxies.
  - Added a **Context Selection** configuration option for abuse.ch URLhaus Database Dump.
- **Version 1.6.0**
  - Added the following new configuration parameters:
    - **Only Ingest New Indicators** - filter out indicators that are not new since the last time the feed ran.
    - **Only Ingest Online Indicators** - filter out indicators that have a status of offline.
  - Updated the **URLHAUS Tags** attribute name to **URLHAUS Tag**.
- **Version 1.5.1**
  - Updated the URLhaus Plain-Text URL List feed default behavior to fetch recent data.
- **Version 1.5.0**
  - Added new parameter for the URLhaus Plain-Text URL List. You can now select to bring in **All Data** or **Recent Data** (last 30 days).
- **Version 1.4.0**
  - Fixed a bug with abuse.ch Feodo Tracker Botnet C2 IP Blocklist that caused an "Error creating objects from threat data" exception to be raised

- Added a new C2 Status attribute to abuse.ch Feodo Tracker Botnet C2 IP Blocklist
- Removed the now defunct abuse.ch Feodo Tracker Malware Hashes feed
- Updated abuse.ch SSLBL Response Policy Zones (RPZ) in order to support `.rpz-ip` indicators in addition to the previously supported `.sslbl-rpz` indicators. Also, added logic to reverse the reverse IP-lookup format supplied by Abuse.