ThreatQuotient

Spamhaus CDF

Version 2.0.1

April 01, 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

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: 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	2.0.1
Compatible with ThreatQ Versions	>= 5.6.0
Support Tier	ThreatQ Supported

Introduction

The Spamhaus CDF for ThreatQ enables users to ingest CIDR Block indicators, along with attributes and tags, allocated from compromised or known cyber-crime operations.

The integration provides the following feeds:

- **Spamhaus DROP List -** ingests CIDR Block indicators from netblocks allocated directly by an established Regional Internet Registry (RIR) or National Internet Registry (NIR) that are "hijacked" or leased by professional spam or cyber-crime operations (used for dissemination of malware, trojan downloaders, botnet controllers).
- **Spamhaus eXBL -** enables the automatic ingestion of the eXBL dataset that Spamhaus offers (downloaded using the REST API).

The integration ingests the following system objects:

- Indicators
    - Indicator 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 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
6. Select the individual feeds to install, when prompted, and click **Install**.

    > 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.

7. The feed(s) will be added to the integrations page. You will still need to configure and then enable the feed(s).

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:

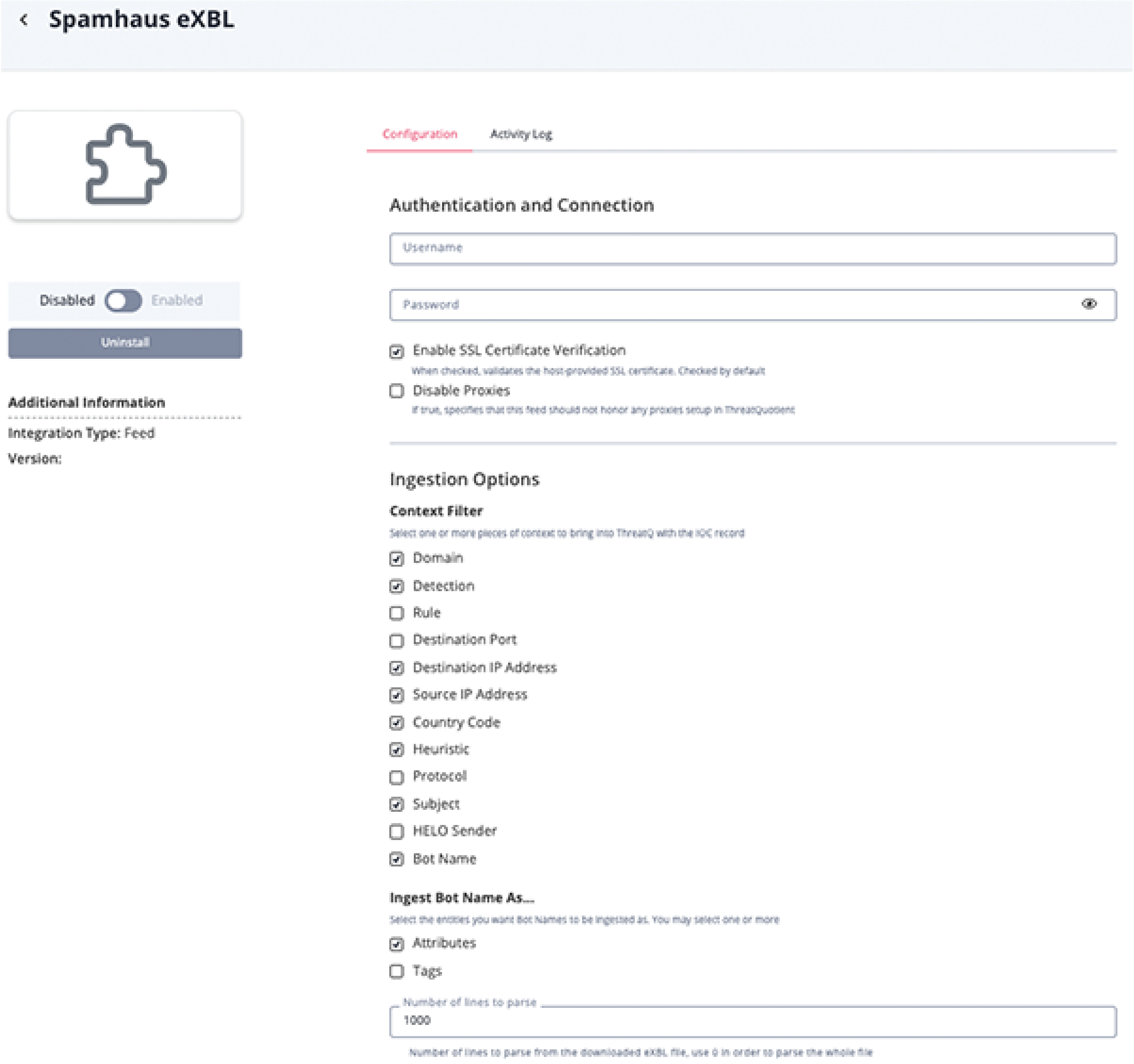
> The Spamhaus DROP List and EDROP List will be located under the OSINT category and does not require you to set additional parameters. You must still enable these feeds. The Spamhaus eXBL entry will be located under the Commercial category and with additional parameters.

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:

Spamhaus eXBL Parameters

PARAMETER	DESCRIPTION
Username	Your Spamhaus Username.
Password	Your Spamhaus Password.
Enable SSL Certificate Verification	Enable or disable verification of the server's SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.
Attributes to Ingest	Select one or more attributes to bring into ThreatQ with the IOC record. Options include: ◦ Domain (Attribute) (Default) ◦ Detection (Default) ◦ Rule

PARAMETER	DESCRIPTION
	◦ Destination Port ◦ Destination IP Address (Default) ◦ Source IP Address (Default) ◦ Country Code (Default) ◦ Heuristic (Default) ◦ Protocol ◦ Subject (Default) ◦ HELO Sender ◦ Bot Name (Default)
Ingest Bot Name As	Select the entities you want Bot Names to be ingested as into the ThreatQ platform. Options include ◦ Attributes (default) ◦ Tags
Number of Lines to Parse	Enter the number of lines to parse from the downloaded eXBL file. The default setting is **1000**. You can use **0** in order to parse the entire file.



Spamhaus eXBL

Additional Information

Integration Type: Feed

Version:

Authentication and Connection

Username

Password

☑ 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

Ingestion Options

Context Filter

Select one or more pieces of context to bring into ThreatQ with the IOC record

☑ Domain
☑ Detection
□ Rule
□ Destination Port
☑ Destination IP Address
☑ Source IP Address
☑ Country Code
☑ Heuristic
□ Protocol
☑ Subject
□ HELO Sender
☑ Bot Name

Ingest Bot Name As...

Select the entities you want Bot Names to be ingested as. You may select one or more

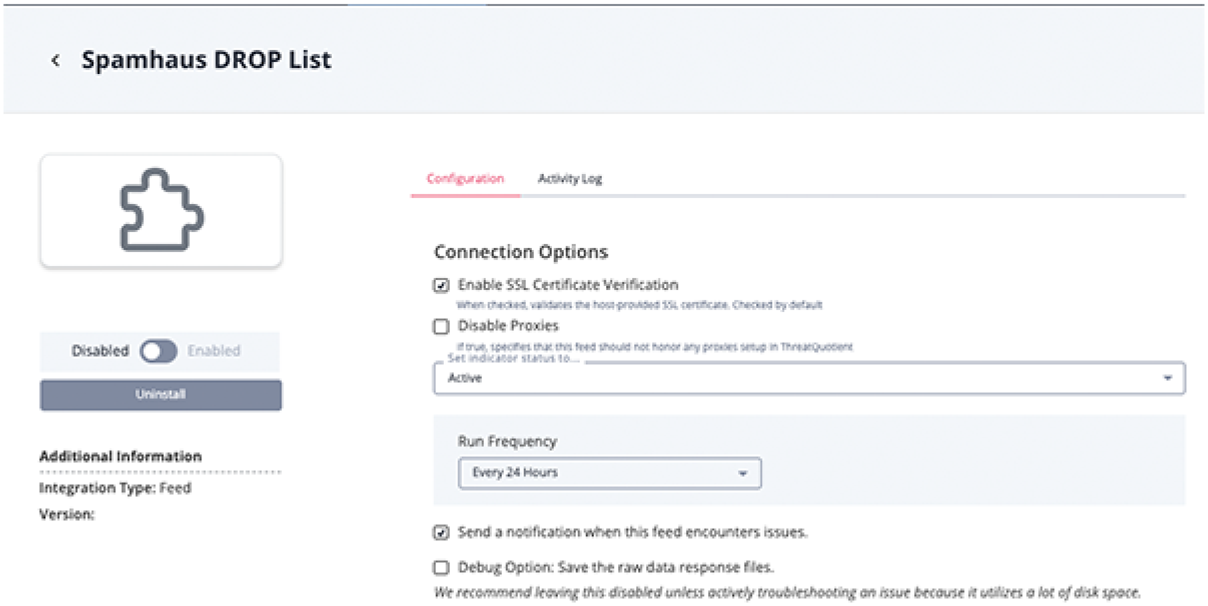
☑ Attributes
□ Tags

Number of lines to parse: 1000

Number of lines to parse from the downloaded eXBL file, use 0 in order to parse the whole file

Spamhaus Drop List Parameters

PARAMETER	DESCRIPTION
Enable SSL Certificate Verification	Enable or disable verification of the server's SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



Spamhaus DROP List

Additional Information

Integration Type: Feed

Version:

Connection 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...: Active

Run Frequency: Every 24 Hours

☑ 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

Spamhaus DROP List

The Spamhaus Don't Route Or Peer List (DROP) feed allows a user to ingest CIDR Block indicators from netblocks allocated directly by an established Regional Internet Registry (RIR) or National Internet Registry (NIR) that are "hijacked" or leased by professional spam or cyber-crime operations (used for dissemination of malware, trojan downloaders, botnet controllers).

```
GET http://www.spamhaus.org/drop/drop.txt
```

Sample Response:

```
; Spamhaus DROP List 2020/07/30 - (c) 2020 The Spamhaus Project
; https://www.spamhaus.org/drop/drop.txt
; Last-Modified: Sat, 25 Jul 2020 08:39:55 GMT
; Expires: Thu, 30 Jul 2020 16:52:29 GMT
1.10.16.0/20 ; SBL256894
1.19.0.0/16 ; SBL434604
1.32.128.0/18 ; SBL286275
2.56.255.0/24 ; SBL444288
2.59.200.0/22 ; SBL463003
5.134.128.0/19 ; SBL270738
5.183.60.0/22 ; SBL463004
5.188.10.0/23 ; SBL402741
23.92.80.0/20 ; SBL372561
23.239.64.0/19 ; SBL372562
24.233.0.0/19 ; SBL210084
27.126.160.0/20 ; SBL257064
27.146.0.0/16 ; SBL326434
36.0.8.0/21 ; SBL225949
36.37.48.0/20 ; SBL258006
36.116.0.0/16 ; SBL303895
36.119.0.0/16 ; SBL303894
37.252.220.0/22 ; SBL461634
41.77.240.0/21 ; SBL478585
41.93.128.0/17 ; SBL464277
```

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.Value	CIDR Block	N/A	223.254.0.0/16	
1 (second token)	Indicator.Attribute	SBL ID	N/A	SBL212803	
1 (second token)	Indicator.Attribute	SBL Link	N/A	https://www.spamhaus.org/sbl/query/SBL212803	The base url `https://www.spamhaus.org/sbl/query/` is always prepended to the second token value

Spamhaus eXBL

The Spamhaus eXBL will automatically ingest a Spamhaus eXBL JSON file into ThreatQ.

`POST https://api.spamhaus.org/api/intel/v1/download/ext/xbl`

Sample Response:

```
{"type": "metadata", "timestamp": 1639409701, "rsync": [50,60,10,1,512,65536], "message": ""}
{"ipaddress":"99.99.6.12","botname":"unknown","seen":1639052434,"firstseen":1639012462,"listed":1639052542,"valid_until":1639657234,"detection":"SMTP protocol violation","rule":"05d0018d","dstport":25,"helo":"127.0.0.1","heuristic":"INVALID","asn":"7018","lat":26.718,"lon":-80.0989,"cc":"US","srcip":"99.99.6.12"}
{"ipaddress":"99.99.233.76","botname":"zloader","seen":1639347086,"firstseen":1633108277,"listed":1639347131,"valid_until":1639951886,"rule":"0ba70226","dstip":"87.106.18.125","dstport":443,"heuristic":"SINKHOLE","asn":"7018","lat":30.0516,"lon":-95.4707,"cc":"US","protocol":"tcp","srcip":"99.99.233.76","srcport":54172,"domain":"yuidskadjna.com"}
{"ipaddress":"99.99.233.188","botname":"gozi","seen":1639403174,"firstseen":1636738290,"listed":1639403294,"valid_until":1640007974,"rule":"0b990220","dstip":"87.106.18.141","dstport":80,"heuristic":"SINKHOLE","asn":"7018","lat":30.0516,"lon":-95.4707,"cc":"US","protocol":"tcp","srcip":"99.99.233.188","srcport":56135,"domain":"vv.malorun.at"}
{"ipaddress":"99.99.229.29","botname":"zloader","seen":1639230958,"firstseen":1632223600,"listed":1639230967,"valid_until":1639835758,"rule":"0ba70226","dstip":"87.106.18.125","dstport":443,"heuristic":"SINKHOLE","asn":"7018","lat":29.7912,"lon":-95.4182,"cc":"US","protocol":"tcp","srcip":"99.99.229.29","srcport":51493,"domain":"yuidskadjna.com"}
{"ipaddress":"99.99.229.187","botname":"zloader","seen":1639339532,"firstseen":1639162100,"listed":1639339570,"valid_until":1639944332,"rule":"0ba70226","dstip":"87.106.18.125","dstport":443,"heuristic":"SINKHOLE","asn":"7018","lat":29.7912,"lon":-95.4182,"cc":"US","protocol":"tcp","srcip":"99.99.229.187","srcport":49428,"domain":"yuidskadjna.com"}
```

ThreatQ provides the following default mapping for the feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
.ipaddress	Indicator Value	IP Address	N/A	.firstseen	N/A	N/A
.botname	Indicator Tag	N/A	N/A	.firstseen	zloader	N/A
.detection	Attributes	Detection	N/A	.firstseen	multiple personalities observed in SMTP traffic data	N/A
.rule	Attributes	Rule	N/A	.firstseen	1a5803d0	N/A
.dstport	Attributes	Destination Port	N/A	.firstseen	N/A	N/A
.dstip	Attributes	Destination IP Address	N/A	.firstseen	N/A	N/A
.srcip	Attributes	Source IP Address	N/A	.firstseen	N/A	N/A
.cc	Attributes	Country Code	N/A	.firstseen	CN	N/A
.heuristic	Attributes	Heuristic	N/A	.firstseen	N/A	INVALID is ignored
.protocol	Attributes	Protocol	N/A	.firstseen	tcp	N/A
.subject	Attributes	Subject	N/A	.firstseen	Patricia found the meaning of life in a bowl of Cheerios. HAYM6LYMONF6	N/A
.helo[]	Attributes	HELO Sender	N/A	.firstseen	newsblaze.com	N/A
.botname	Attributes	Bot Name	N/A	.firstseen	zloader	N/A
.domain	Attributes	Associated Domain	N/A	.firstseen	differentia[.]ru	N/A

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.

Spamhaus DROP List

METRIC	RESULT
Run Time	1 minute
Indicators	777
Indicator Attributes	1,554

Spamhaus eXBL

METRIC	RESULT
Run Time	7 minutes
Indicators	4,216
Indicator Attributes	31,922

> This test was done against a subset of the eXBL dataset. The eXBL dataset is extremely large, and full ingestion times can vary.

Known Issues / Limitations

- The eXBL dataset is incredibly large and can get up to millions and millions of indicators. As a result, this feed may take a very long time to run. It's advised you utilize the attribute filters to make sure you are only ingesting the context you need.

Change Log

- **Version 2.0.1**
  - All URLs now use SSL to avoid HTTP redirects.
  - The **Spamhaus EDROP List** feed has been removed from the integration as the provider has merge the list into the S**pamhaus Drop Lis**t feed.
  - Added the following configuration parameters:
    - **Enable SSL Certificate Verification** - enable or disable verification of the server's SSL certificate.
    - **Disable Proxies** - determines if the feed should honor proxy settings set in the ThreatQ UI.
- **Version 2.0.0**
  - The Spamhaus eXBL feed now uses the REST API when fetching the eXML file. Previously, the feed required access to the eXBL dataset via rsync.
  - Updated the ThreatQ UI configuration parameters for the Spamhaus eXBL feed.
- **Version 1.1.1**
  - Removed `Source Port`, `Longitude`, & `Latitude` attributes.
  - Switched `data.domain` to an attribute opposed to related FQDN.
- **Version 1.1.0**
  - Added new eXBL feed.
- **Version 1.0.1**
  - Updated the `namespace`, `category`, and `default_indicator_status` fields.
- **Version 1.0.0**
  - Initial release