ThreatQuotient

Spamhaus ZEN Operation User Guide

Version 1.0.0

November 03, 2023

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	1.0.0
Compatible with ThreatQ Versions	>= 4.9.0
Support Tier	ThreatQ Supported

Introduction

The Spamhaus ZEN Operation queries IP addresses and domains against the ZEN blocklist.

The operation provides the following action:

- **DNS Lookup** - queries one of two Spamhaus DNS servers, based on the object's Indicator type, and maps DNS responses to attributes.

The operation is compatible with IP Address and FQDN type Indicators.

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 operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your Spamhaus API Key.

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.

Actions

The operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
DNS Lookup	Queries one of two Spamhaus DNS servers, based on the object's Indicator type, and maps DNS responses to attributes.	Indicator	IP Address, FQDN

IP Address

The operation uses the following server to query for IP Addresses.

```
{ DOMAIN }}.{{ KEY }}.dbl.dq.spamhaus.net
```

ThreatQuotient provides the following response map to the following attributes:

RETURN CODE (ADDRESS)	ATTRIBUTE KEY	ATTRIBUTE VALUE
127.0.0.2	Spamhaus List	SBL
127.0.0.3	Spamhaus List	SBL (CSS)
127.0.0.4	Spamhaus List	XBL
127.0.0.9	Spamhaus List	SBL (DROP/EDROP)
127.0.0.10	Spamhaus List	PBL (ISP Maintained)
127.0.0.11	Spamhaus List	PBL (Spamhaus Maintained)

FQDN

The operation uses the following server to query for FQDNs.

```
{{ REVERSE IP }}.{{ KEY }}.zen.dq.spamhaus.net
```

ThreatQuotient provides the following response map to the following attributes:

RETURN CODE (ADDRESS)	ATTRIBUTE KEY	ATTRIBUTE VALUE
127.0.1.2	Spamhaus List	Spam Domain
127.0.1.4	Spamhaus List	Phish Domain
127.0.1.5	Spamhaus List	Malware Domain
127.0.1.6	Spamhaus List	Botnet C&C Domain
127.0.1.102	Spamhaus List	Abuse Legit Spam
127.0.1.103	Spamhaus List	Abuse Spammed Redirector Domain
127.0.1.104	Spamhaus List	Abused Legit Phish
127.0.1.105	Spamhaus List	Abused Legit Malware
127.0.1.106	Spamhaus List	Abuse Legit Botnet C&C

Change Log

- **Version 1.0.0**
  - Initial release