ThreatQuotient

PhishTank CDF Guide

Version 2.1.0

November 07, 2022

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.

Copyright © 2022 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	2.1.0
Compatible with ThreatQ Versions	>= 4.56.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/phishtank

Introduction

PhishTank returns to ThreatQ a collection of Indicators which we normalize and relate to their associated structures. Within this document details how the data is normalized and constructed in the platform. Mainly, URLs form relationships to IPs, and IPs relate to the reported CIDR Blocks. Attributes are only attributed to the URLs in which they are assigned.

The integration provides the following feed:

- **PhishTank** - ingests URLs and related IP Addresses, CIDR Blocks.

The integration ingests the following Indicator types:

- CIDR Block
- IP Address
- URL - this may be normalized to FQDN.

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).

   > 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
Application Key	Optional - your PhishTank Application Key.
Feed URL	Display Only - update the name that will display in the ThreatQ UI.
Verify SSL	If enabled, the integration will verify SSL connections with the provider.
Context Filter	Multi-select yielding control of attribute selection to the user.

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

PhishTank

The PhishTank feed returns a compressed file `online-valid.json.gz`. The sample response below shows the file in a uncompressed format.

```
GET https://data.phishtank.com/data/{{user_fields.app_key}}/online-valid.json.gz
```

Sample Response:

```
[
    {
        "details": [
            {
                "announcing_network": "44476",
                "cidr_block": "185.176.43.0/24",
                "country": "BG",
                "detail_time": "2022-10-03T15:13:50+00:00",
                "ip_address": "185.176.43.98",
                "rir": "ripencc"
            }
        ],
        "online": "yes",
        "phish_detail_url": "http://www.phishtank.com/phish_detail.php?phish_id=7809274",
        "phish_id": "7809274",
        "submission_time": "2022-10-03T15:02:29+00:00",
        "target": "Other",
        "url": "http://movilappitau3hgm.c1.biz/",
        "verification_time": "2022-10-03T15:13:36+00:00",
        "verified": "yes"
    },
    {
        "details": [
            {
                "announcing_network": "44476",
                "cidr_block": "185.176.43.0/24",
                "country": "BG",
                "detail_time": "2022-10-03T15:13:50+00:00",
                "ip_address": "185.176.43.98",
                "rir": "ripencc"
            }
        ],
        "online": "yes",
        "phish_detail_url": "http://www.phishtank.com/phish_detail.php?phish_id=7809269",
        "phish_id": "7809269",
        "submission_time": "2022-10-03T15:02:25+00:00",
        "target": "HSBC Group",
        "url": "http://itau--000000.royalwebhosting.net/",
        "verification_time": "2022-10-03T15:13:36+00:00",
        "verified": "yes"
    }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
url	URL	Indicator	N/A	http://itau--000000.royalwebhosting.net	Main URL reported by PhishTank, draws a relationships to the IP and CIDR Block.
details.ip_address	IP Address	Related Indicator	N/A	1.2.3.4	IP which the URL is related to
details.cidr_block	CIDR Block	Related Indicator	N/A	198.23.171.0/20	CIDR Block of related IP
phish_id	PhishTank ID	Indicator.Attribute	N/A	7809269	If 'Phishtank ID' Context Filter is selected
phish_detail_url	PhishTank URL	Indicator.Attribute	N/A	http://www.phishtank.com/phish_detail.php?phish_id=7809269	If 'Phishtank Details URL' Context Filter is selected
target	Target	Indicator.Attribute	N/A	HSBC Group	If 'Target' Context Filter is selected
details.announcing_network	Announcing Network	Indicator.Attribute	N/A	44476	If 'Announcing Network' Context Filter is selected
details.country	Country	Indicator.Attribute	N/A	BG	If 'Country' Context Filter is selected
details.rir	RIR	Indicator.Attribute	N/A	ripencc	If 'RIR' Context Filter is selected

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	80 Minutes
Indicators	72,761
Indicator Attributes	440,297

Change Log

- **Version 2.1.0**
  - Updated the Report Structure to provide better organization of relational data and attributes.
- **Version 2.0.0**
  - Initial release