# ThreatQuotient

# Phishlabs Global CDF User Guide

## Version 1.0.0

October 18, 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** | >= 4.24.0 |
| **Support Tier** | ThreatQ Supported |

# Introduction

The Phishlabs Global CDF ingests indicators of compromise from directly-observed phishing attacks around the world.

The integration provides the following feed:

- **Phishlabs Global** - `https://ioc.phishlabs.com/api/v1/globalfeed`

The integration ingests the following indicator types:

- URL
- FQDN
- MD5
- Email Address
- Filename
- File Type

# 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.

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 **Commercial** 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 |
|---|---|
| **API ID** | Your Phishlabs account API ID. |
| **API Key** | Your Phishlabs account 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.

# ThreatQ Mapping

## Phishlabs Global

```
GET https://ioc.phishlabs.com/api/v1/globalfeed
```

**Sample Response:**

```
{
    "data": [
        {
            "id": "45cfc6ec-c525-4372-b25f-53365dc39a8f",
            "createdAt": "2020-03-20T17:58:00Z",
            "value": "ca8322bf26ff997c39c1d568d931d7d8",
            "type": "Attachment",
            "attributes": [
                {
                    "id": "2b2f0e9e-1d18-4cbb-aa29-e01ade0e1c34",
                    "createdAt": "2020-03-20T17:58:00Z",
                    "value": "ca8322bf26ff997c39c1d568d931d7d8",
                    "name": "md5"
                },
                {
                    "id": "a390c924-8b66-425d-89b5-58fcc0ac665a",
                    "createdAt": "2020-03-20T17:58:00Z",
                    "value": "application/zip",
                    "name": "filetype"
                },
                {
                    "id": "d678a22f-0f07-4397-995a-6d330e4f5a5e",
                    "createdAt": "2020-03-20T17:58:00Z",
                    "value": "covid37_form.zip",
                    "name": "name"
                }
            ],
            "falsePositive": false
        },
        {
            "id": "508b322f-5cb9-41f7-bc52-f1806a83d84f",
            "createdAt": "2020-03-20T17:55:17Z",
            "value": "https://firebasestorage.googleapis.com/?obfuscated",
            "type": "URL",
            "falsePositive": false
        }
    ],
    "meta": {
        "count": 2,
        "statusCode": 0,
        "statusMessage": ""
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| .data[].type | Indicator.Type | N/A | N/A | Attachment | |
| .data[].value | Indicator.Value | See `Phishlabs Indicator Type to ThreatQ Indicator Type mapping` | .data[].createdAt | ca8322bf26ff997c39c1d568d931d7d8 | |
| .data[].falsePositive | Indicator.Attribute | False Positive | .data[].createdAt | False | Attributed to all indicators created from a given object |
| .data[].attributes[].value | Indicator.Value | Filename | .data[].createdAt | covid37_form.zip | Created if `.data[].type` is `Attachment` and `.data[].attributes[].name` is name; related to the top-level indicator |
| .data[].attributes[].value | Indicator.Attribute | File Type | .data[].createdAt | application/zip | Created if `.data[].type` is `Attachment` and `.data[].attributes[].name` is `filetype`; attributed to all indicators created from a given object |

## Indicator Type Mapping

ThreatQuotient provides the following indicator type mapping:

| PHISHLABS INDICATOR TYPE | THREATQ INDICATOR TYPE |
|---|---|
| URL | URL |
| Domain | FQDN |
| Sender | Email Address |
| ReturnPath | Email Address |
| ReplyTo | Email Address |
| HeaderReplyTo | Email Address |
| Attachment | MD5 |

# 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** | 90 |
| **Indicator Attributes** | 86 |

# Change Log

- **Version 1.0.0**
    - Initial release