

ThreatQuotient



ThreatQ CDF for Microsoft Interflow Bing Malicious URL

Version 1.1.1

April 15, 2024

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 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

ThreatQ Mapping..... 10

 Interflow to ThreatQ Object Type Mapping 10

Average Feed Run..... 11

Change Log 12

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 © 2024 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	1.1.1
Compatible with ThreatQ Versions	>= 4.57.3
Support Tier	ThreatQ Supported

Introduction

The ThreatQ CDF for Microsoft Interflow Bing Malicious URL integration downloads URLs identified as malicious by Microsoft Interflow. The URLs and their corresponding Destination IP addresses are then imported into your ThreatQ instance and related to one another.

The integration provides the following feed:

- **Microsoft Interflow Bing Malicious URL** - returns files specified within `{fileName}` as well as a JSON list of files within Microsoft Interflow Bing Malicious URLs.

The integration ingests URL and IP Address Indicator types.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml 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. 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 **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 parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Interflow Subscription Key	Your Interflow API Key used to access Microsoft Interflow.
Ingest URLs as FQDNs	Enable this option to only ingest FQDNs from their URLs.
Ingest IPs Addresses	Enable this option to ingest IP Addresses.



Disabled

☐

Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

Subscription Key

Your Microsoft Interflow Subscription Key

☐ Verify Host SSL
 ☐ Ingest URLs as FQDNs?

Select this box if you only want FQDNs to be ingested and not the full URLs.

☒ Ingest IP Addresses?

Select this box if you want to ingest IP Addresses

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.

Save

- Review any additional settings, make any changes if needed, and click on **Save**.
- Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

The integration utilizes the following endpoints:

`https://interflow.azure-api.net/file/api/file/download?fileName={fileName}`

This endpoint returns the files specified within {fileName}.

`https://interflow.azure-api.net/file/api/file/listsharedfiles`

This endpoint returns a JSON list of all files within Microsoft Interflow Bing Malicious URLs.

Interflow to ThreatQ Object Type Mapping

ThreatQuotient provides the following type mapping:

INTERFLOW TYPE	THREATQ OBJECT TYPE
URL	URL
URL	FQDN
DestinationIPv4 Address	IP Address

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	16 Hours
URL	199,000
IP Address	1,000

Change Log

- **Version 1.1.1**
 - Resolved an issue where parsing a date would result in a filter mapping error.
- **Version 1.1.0**
 - Added two new configuration options:
 - **Ingest URLs as FQDNs** - select whether to only ingest FQDNs or the entire URL.
 - **Ingest IP Addresses** - enable the ingestion of IP Addresses.
- **Version 1.0.0**
 - Initial release