ThreatQuotient

MISP COVID-19 Warning List Feed Guide

Version 1.0.0

Friday, May 15, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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.

Last Updated: Friday, May 15, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.32.0`

Introduction

MISP provides a series of warning lists for the detection of known valid domains. This is selection of COVID-19 related whitelist feeds.

Installation

Perform the following steps to install the feed:

The same steps can be used to upgrade the feed to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **MISP COVID-19 Warning List** integration file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed 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.

The feeds will be added to the **OSINT** tab for Incoming Feeds. 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 feed-related credentials.

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **OSINT** tab.
3. Click on the **Feed Settings** link for the feed.
4. Review the configuration under the **Settings** tab and make any updates as needed.
5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed name to enable the feed.

ThreatQ Mapping

MISP Warning List - COVID-19 CTC Whitelist

A MISP Warning list of valid COVID-19 related domains provided by the Cyber Threat Coalition.

```
GET https://raw.githubusercontent.com/MISP/misp-warning-lists/master/lists/covid-19-cyber-threat-coalition-whitel-ist/list.json
```

```
    {
        "description": "The Cyber Threat Coalition's whitelist of COVID-19 related websites.",
        "list": [
           "2019novelcoronavirusoracle.com",
           ...
        ]
    }
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.list[]	Indicator	FQDN	N/A	2019novelcoronavirusoracle.com	Status: Whitelisted
N/A	Indicator.Attribute	Warning List	N/A	Covid-19 CTC Whitelist	Hard-coded

Average Feed Run - MISP Warning List - COVID-19 CTC Whitelist:

Metric	Result
Run Time	1 minute
Indicators	697
Indicator Attributes	697

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.

MISP Warning List - COVID-19 Domains

A MISP Warning list "maintained using different lists (such as Jaime Blasco's and Krassimir's lists)"

```
GET https://raw.githubusercontent.com/MISP/misp-warning-lists/master/lists/covid/list.json
```

```
    {
        "description": "Maintained using different lists (such as Jaime Blasco's and Krassimir's lists).",
        "list": [
            "3d.nicovideo.jp",
            ...
        ]
    }
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.list[]	Indicator	FQDN	N/A	3d.nicovideo.jp	Status: Whitelisted
N/A	Indicator.Attribute	Warning List	N/A	Valid COVID-19 Related Domains	Hard-coded

Average Feed Run - MISP Warning List -COVID-19 Domains

Metric	Result
Runtime	< 1 minute
Indicators	318
Indicator Attributes	318

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.

Change Log

- **Version 1.0.0**
  - Initial Release