ThreatQuotient

Kaspersky COVID-19 CDF Guide

Version 1.0.0

July 28, 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.

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	>= 4.34.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/kaspersky-covid

Introduction

Kaspersky provides businesses with a free feed to effectively mitigate COVID-related phishing threats.

The Kaspersky COVID-19 CDF provides the following feed:

- **Kaspersky COVID-19** - `https://opentip.kaspersky.com/feed/covid19`

The integration ingests indicators and indicator attributes into the ThreatQ platform.

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

ThreatQ Mapping

Kaspersky COVID-19

`GET https://opentip.kaspersky.com/feed/covid19`

Sample Response:


```
[
  {
    "id": 44578981,
    "type": 1,
    "mask": "corona-propusk.ru",
    "domains": [
      {
        "domain": "corona-propusk.ru"
      }
    ],
    "industry": "Web Service",
    "first_seen": "27.04.2020 08:33",
    "last_seen": "21.05.2020 16:26",
    "popularity": 5,
    "geo": "ru, ua, de",
    "IP": "212.129.18.73, 95.216.94.72, 23.235.227.108, 176.222.58.82, 84.17.58.49, 87.255.9.22, 185.5.136.107",
    "whois": {
      "domain": "corona-propusk.ru",
      "created": "15.04.2020",
      "expires": "15.04.2021",
      "name": "Private Person",
      "registrar_name": "R01-RU",
      "NS": "ns1.coopertino.org, ns2.coopertino.org",
      "NS_ips": "51.15.172.173, 95.217.212.111",
      "MX": "corona-propusk.ru",
      "MX_ips": "212.129.18.73"
    }
  },
  {
    "id": 44065054,
    "type": 1,
    "mask": "stopkoronovirus.ru",
    "hosts": [
      {
        "host": "uslugi.stopkoronovirus.ru"
      }
    ],
    "domains": [
      {
        "domain": "stopkoronovirus.ru"
      }
    ],
    "industry": "Web Service",
    "first_seen": "10.04.2020 07:57",
    "last_seen": "15.05.2020 06:35",
    "popularity": 2,
```

```
    "geo": "ru",
    "IP": "144.76.182.49",
    "whois": {
      "domain": "stopkoronovirus.ru",
      "created": "16.03.2020",
      "expires": "16.03.2021",
      "name": "Private Person",
      "registrar_name": "REGTIME-RU",
      "NS": "ns37.hostia.name, ns38.hostia.name",
      "NS_ips": "144.76.182.49, 144.76.182.61",
      "MX": "mail.stopkoronovirus.ru",
      "MX_ips": "144.76.182.49"
    }
  },
  {
    "id": 43836635,
    "type": 4,
    "mask": "covid19statistika.lt/dashboard/snapshot/covid19statistikalt?orgid=1&kiosk",
    "urls": [
      {
        "url": "covid19statistika.lt/dashboard/snapshot/covid19statistikalt?orgid=1&kiosk"
      }
    ],
    "first_seen": "31.03.2020 10:16",
    "last_seen": "13.05.2020 11:53",
    "popularity": 2,
    "geo": "lt, ca",
    "whois": {
      "domain": "covid19statistika.lt",
      "created": "15.03.2020",
      "expires": "16.03.2021",
      "registrar_name": "UAB \"Interneto vizija\"",
      "registrar_email": "hostmaster@iv.lt",
      "NS": "jade.ns.cloudflare.com, thomas.ns.cloudflare.com",
      "NS_ips": "173.245.58.167, 173.245.59.238"
    }
  },
  ...
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.[].urls[].url	Indicator.Value	URL	.[].first_seen	covid19statistika.lt/dashboard/snapshot/covid19statistikalt?orgid=1&kiosk	
.[].hosts[].host	Indicator.Value	FQDN	.[].first_seen	stopkoronavirus.ru	
.[].domains[].domain	Indicator.Value	FQDN	.[].first_seen	corona-propusk.ru	
.[].IP	Indicator.Value	IP Address	.[].first_seen	144.76.183.49	
.[].mask	Indicator.Value	URL/FQDN	.[].first_seen	covid19statistika.lt/dashboard/snapshot/covid19statistikalt?orgid=1&kiosk	May be URL or FQDN depending on .[].type (see below)
.[].id	Indicator.Attribute	Kaspersky ID	.[].first_seen	43836635	
.[].popularity	Indicator.Attribute	Popularity	.[].first_seen	2	
.[].industry	Indicator.Attribute	Industry	.[].first_seen	Web Service	
.[].threat	Indicator.Attribute	Threat	.[].first_seen		
.[].geo	Indicator.Attribute	Country Code	.[].first_seen	ca	
.[].port	Indicator.Attribute	Port	.[].first_seen	8080	
.[].protocol	Indicator.Attribute	Protocol	.[].first_seen	http	
.[].last_seen	Indicator.Attribute	Last Seen	.[].first_seen	13.05.2020 11:53	
.[].first_seen	Indicator.Attribute	First Seen	.[].first_seen	13.05.2020 11:53	
.[].whois.registrar_email	Indicator.Value	Email Address	.[].whois.created	hostmaster@iv.lt	
.[].whois.NS	Indicator.Value	FQDN	.[].whois.created	jade.ns.cloudflare.com	Values in response may be comma-separated

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.[].whois .MX	Indicator.Value	FQDN	.[].whois.created	mail.stop koronavirus.ru	Values in response may be comma-separated
.[].whois .domain	Indicator.Value	FQDN	.[].whois.created	covid19statistika.lt	
.[].whois .NS_ips	Indicator.Value	IP Address	.[].whois.created	173.245.58.167	Values in response may be comma-separated
.[].whois .MX_ips	Indicator.Value	IP Address	.[].whois.created	144.76.182.49	Values in response may be comma-separated
.[].whois .created	Indicator.Attribute	Whois Created	.[].whois.created	15.02.2020	
.[].whois .updated	Indicator.Attribute	Whois Updated	.[].whois.created	15.03.2020	
.[].whois .expires	Indicator.Attribute	Whois Expires	.[].whois.created	14.02.2021	
.[].whois .name	Indicator.Attribute	Whois Name	.[].whois.created	Private Person	
.[].whois .registrar_name	Indicator.Attribute	Whois Registrar Name	.[].whois.created	UAB "Interneto vizija"	
.[].whois .org	Indicator.Attribute	Whois Organization	.[].whois.created	Private Person	
.[].whois .country	Indicator.Attribute	Whois Country Code	.[].whois.created	ca	
.[].whois .city	Indicator.Attribute	Whois City	.[].whois.created	Montreal	

Kaspersky to ThreatQ Indicator Mapping

KASPERSKY TYPE	THREATQ INDICATOR TYPE	STRING FORMATTING	EXAMPLE
19	FQDN	Removes `*.` from the beginning of the string	`*.google.com` -> `google.com`
20	URL	Removes `/*` from the end of the string	`google.com/*` -> `google.com`
21	URL	Removes `*` from the end of the string	`google.com/test/*` -> `google.com/test/`
1, 2	FQDN	None	`example.google.com`
3, 4	URL	None	`example.google.com/badguys`

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	35 minutes
Indicators	8,000
Indicator Attributes	76,000

Change Log

- **Version 1.0.0**
  - Initial release