ThreatQuotient

Kaspersky APT Reports CDF User Guide

Version 1.0.2

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	>= 4.37.0
Support Tier	ThreatQ Supported

Introduction

The Kaspersky APT DEMO CDF ingest threat intelligence data used in malicious APT campaigns from Kaspersky Threat Intelligence.

The CDF includes the following feeds:

- **Kaspersky APT IPs DEMO** - ingests `IP Address` indicators and attributes.
- **Kaspersky APT URLs DEMO** - ingests indicators and attributes.
- **Kaspersky APT Hashes DEMO** - ingests hash indicators and attributes.

The integration ingests the following system object types:

- Indicators
    - Indicator Attributes

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.

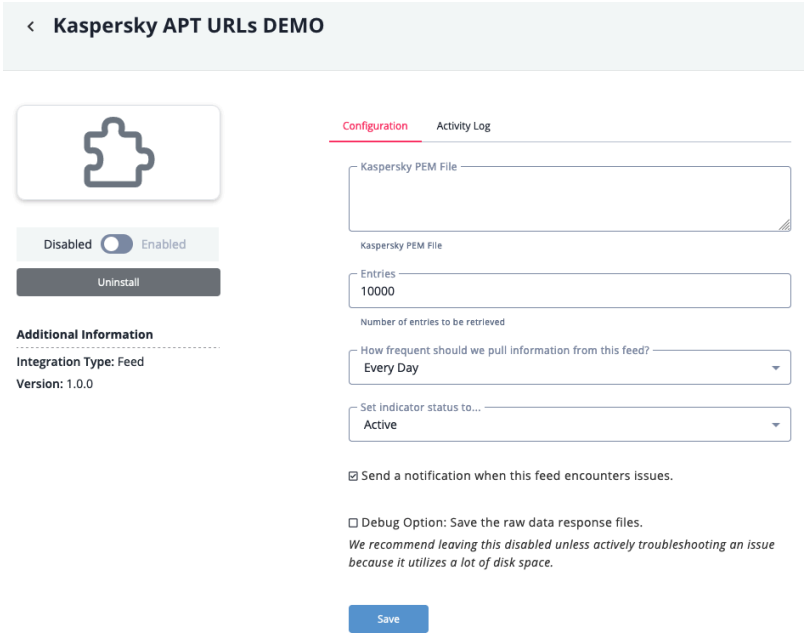
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **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
Kaspersky PEM	You Kaspersky Client Certificate for authentication.
Entries	The number of entries to be retrieved. The default setting is 10,000.



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

Kaspersky APT IPs DEMO

The Kaspersky APT IPs DEMO feed ingests `IP Address` indicators and attributes.

`GET https://wlinfo.kaspersky.com/api/v1.0/feeds/142/updates`

Sample Response:

```
[
    {
        "detection_date": "20.04.2017 00:00",
        "id": 16453205,
        "ip": "69.64.59.133",
        "publication_name": "ShadowBrokers Lost in translation leak - SWIFT
attacks analysis"
    },
    ...
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].ip	Indicator.Value	IP Address	[].detection_date	69.64.59.133	N/A
[].publication_name	Indicator.Attribute	Publication	[].detection_date	ShadowBrokers Lost in translation leak - SWIFT attacks analysis	N/A

Kaspersky APT URLs DEMO

The Kaspersky APT URLs DEMO feed ingests indicators and attributes.

`GET https://wlinfo.kaspersky.com/api/v1.0/feeds/143/updates`

Sample Response:

```
[
    {
        "detection_date": "09.03.2017 00:00",
        "id": 16451625,
        "mask": "ec2-52-74-203-151.ap-southeast-1.compute.amazonaws.com",
        "publication_name": "APT10 Spearphishes Japanese Policy Experts late
2016 to early 2017",
        "type": 2
    },
    ...
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].mask	Indicator.Value	See Kaspersky Type Mapping table	[].detection_date	ec2-52-74-203-151.ap-southeast-1.compute.amazonaws.com	N/A
[].publication_name	Indicator.Attribute	Publication	[].detection_date	ShadowBrokers Lost in translation leak - SWIFT attacks analysis	N/A

Kaspersky APT Hashes DEMO

The Kaspersky APT Hashes DEMO feed ingests hash indicators and attributes.

```
GET https://wlinfo.kaspersky.com/api/v1.0/feeds/144/updates
```

Sample Response:

```
[
    {
        "detection_date": "23.06.2017 00:00",
        "id": 16456071,
        "MD5": "F805882CC276B583D9CA7E16AD957E7B",
        "publication_name": "Ismdoor - possible Shamoon attack vector found in
Saudi Arabia",
        "SHA1": "2E4DB721DBD2ACEFD851BEDF95492BF789F588FD",
        "SHA256":
"D76024256AC35424EB02B6A47565F8859B12050F5DE49EF16DEC449A61DA1EFC"
    },
    ...
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
].MD5	Indicator.Value	MD5	[].detection_date	F805882CC276B583D9CA7E16AD957E7B	Inter-related with other hash Indicators
[].SHA1	Indicator.Value	SHA-1	[].detection_date	2E4DB721DBD2ACEFD851BEDF95492BF789F588FD	Inter-related with other hash Indicators
[].SHA256	Indicator.Value	SHA256	[].detection_date	D76024256AC35424EB02B6A47565F8859B12050F5DE49EF16DEC449A61DA1EFC	Inter-related with other hash Indicators
[].publication_name	Indicator.Attribute	Publication	[].detection_date	ShadowBrokers Lost in translation leak - SWIFT attacks analysis	N/A

Kaspersky Type Mapping

[].TYPE VALUE	INDICATOR TYPE VALUE	NOTES
1, 2	FQDN	N/A
3, 4	URL	N/A
19	FQDN	Value is formatted with `lstrip('*.')`
20	URL	Value is formatted with `rstrip('/*')`
21	URL	Value is formatted with `rstrip('*')`

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.

Kaspersky APT URLs

METRIC	RESULT
Run Time	< 1 minute
Indicators	42
Indicator Attributes	42

Kaspersky APT IPs

METRIC	RESULT
Run Time	< 1 minute
Indicators	35
Indicator Attributes	35

Kaspersky APT Hashes

METRIC	RESULT
Run Time	< 1 minute
Indicators	431
Indicator Attributes	431

Change Log

- **Version 1.0.0**
  - Initial release