

ThreatQuotient



Kaspersky C&C Tracking CDF Guide

Version 1.0.2

March 08, 2022

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

 ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Support	4
Versioning.....	5
Introduction	6
Installation.....	7
Configuration	8
ThreatQ Mapping	10
Kaspersky C&C Tracking Feed	10
Average Feed Run.....	12
Change Log.....	13

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 © 2022 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.

Versioning

- Current integration version: 1.0.2
- Compatible with ThreatQ versions \geq 4.37.0

Introduction

The Kaspersky C&C Tracking CDF ingests IP Addresses and related ASN data from the Kaspersky C&C Tracking API.

The Kaspersky C&C Tracking CDF integration for ThreatQ provides the following feeds:

- **Kaspersky C&C Tracking Feed** - ingests IP Addresses of infrastructure connected to advanced threats and ASN data.

The integration ingests the following system objects:

- 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).
3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Account Username	Your Kaspersky account username.
Account Password	The password associated with the username above.
Kaspersky PEM File	Your Kaspersky PEM file.



Disabled ☒ Enabled

Uninstall

Additional Information

Integration Type: Feed

Version: 1.0.2

Configuration Activity Log

Account Username

Account Username

Account Password

Account Password

PEM File

PEM File

How frequent should we pull information from this feed?

Every Day

Set indicator status to...

Active

☒ 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

5. Review the **Settings** configuration, 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 C&C Tracking Feed

GET https://tip.kaspersky.com/api/apt_cnc/all

Response Sample:

```
[
  {
    "ip": "54.215.129.6" ,
    "first_seen": "2021-04-18" ,
    "last_seen": "2021-04-18" ,
    "country_code": "us" ,
    "tags": [
      {
        "name": "CobaltStrike" ,
        "source": null ,
        "type": "Organic" ,
        "description": "Cobalt Strike is a commercially available attack platform developed by Raphael Mudge and used by multiple threat actors."
      }
    ] ,
    "asn": 16509 ,
    "asn_name": "AMAZON-02" ,
    "ip_whois": {
      "net_range": "54.215.0.0 - 54.215.255.255" ,
      "net_name": "AMAZO-ZSF02" ,
      "descr": null ,
      "created": "2013-03-19" ,
      "updated": "2013-03-19" ,
      "country": null ,
      "city": null ,
      "contact_owner_name": "Amazon.com, Inc." ,
      "contact_owner_code": "AMAZO-48" ,
      "contact_owner_country": "US" ,
      "contact_owner_city": "Seattle" ,
      "contact_owner_email": "amzn-noc-contact@amazon.com" ,
      "contact_abuse_name": "Amazon EC2 Abuse" ,
      "contact_abuse_country": null ,
      "contact_abuse_city": null ,
      "contact_abuse_email": "abuse@amazonaws.com" ,
      "net_asn": "16509"
    }
  } ,
  {
    "ip": "72.45.135.213" ,
    "first_seen": "2021-04-18" ,
    "last_seen": "2021-04-18" ,
    "country_code": "us" ,
    "tags": [
      {
        "name": "CobaltStrike" ,
        "source": null ,
```

```
    "type": "Organic" ,
    "description": "Cobalt Strike is a commercially available attack platform developed by Raphael Mudge and used
by multiple threat actors."
  }
] ,
"asn": 11351 ,
"asn_name": "TWC-11351-NORTHEAST" ,
"ip_whois": {
  "net_range": "72.45.128.0 - 72.45.255.255" ,
  "net_name": "RCACI" ,
  "descr": null ,
  "created": "2006-08-10" ,
  "updated": "2007-07-18" ,
  "country": null ,
  "city": null ,
  "contact_owner_name": "Time Warner Cable Internet LLC" ,
  "contact_owner_code": "RCNY" ,
  "contact_owner_country": "US" ,
  "contact_owner_city": "Herndon" ,
  "contact_owner_email": "abuse@rr.com" ,
  "contact_abuse_name": "Abuse" ,
  "contact_abuse_country": null ,
  "contact_abuse_city": null ,
  "contact_abuse_email": "abuse@rr.com" ,
  "net_asn": null
}
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.return_data[].ip	Indicator.Value	IP Address	.return_data[].first_seen	140.82.41.202	Indicator will be created with 'Indirect' status.
return_data[].country_code	Indicator.Attribute	Country code	.return_data[].first_seen	us	N/A
return_data[].tags[].name	Indicator.Attribute	Tag Name	.return_data[].first_seen	Empire C2	N/A
return_data[].asn	Related Indicator.Value	ASN	.return_data[].first_seen	20473	Indicator will be created with 'Indirect' status.
return_data[].asn_name	Indicator.Attribute	ASN Name	.return_data[].first_seen	AS-CHOOPA	N/A

Average Feed Run

METRIC	RESULT
Run Time	12 min
Indicators	9,552
Indicator Attributes	21,942



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 1.0.2**
 - Fixed the response property that contains the data that is ingested.
- **Version 1.0.1**
 - Added support between IP Address Indicators and their ASN data.
 - Updated integration support tier from Not Supported to ThreatQ Supported.
- **Version 1.0.0**
 - Initial Release