ThreatQuotient

Seclytics CDF Guide

Version 1.0.0

January 31, 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

Integration Details 5
Introduction 6
Prerequisites 7
Installation 8
Configuration 9
ThreatQ Mapping 11
Seclytics Predictions 11
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.

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/seclytics-cdf

Introduction

The Seclytics CDF retrieves a compressed csv file, with all seen predicted IPs since 2015, along with detection info.

The integration provides the following feed:

- **Seclytics Predictions** - retrieves and ingests all seen predicted IPs based on user filters.

The integration ingests IP Address type indicators.

Prerequisites

A Seclytics Access Token Key is required to use this integration.

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.

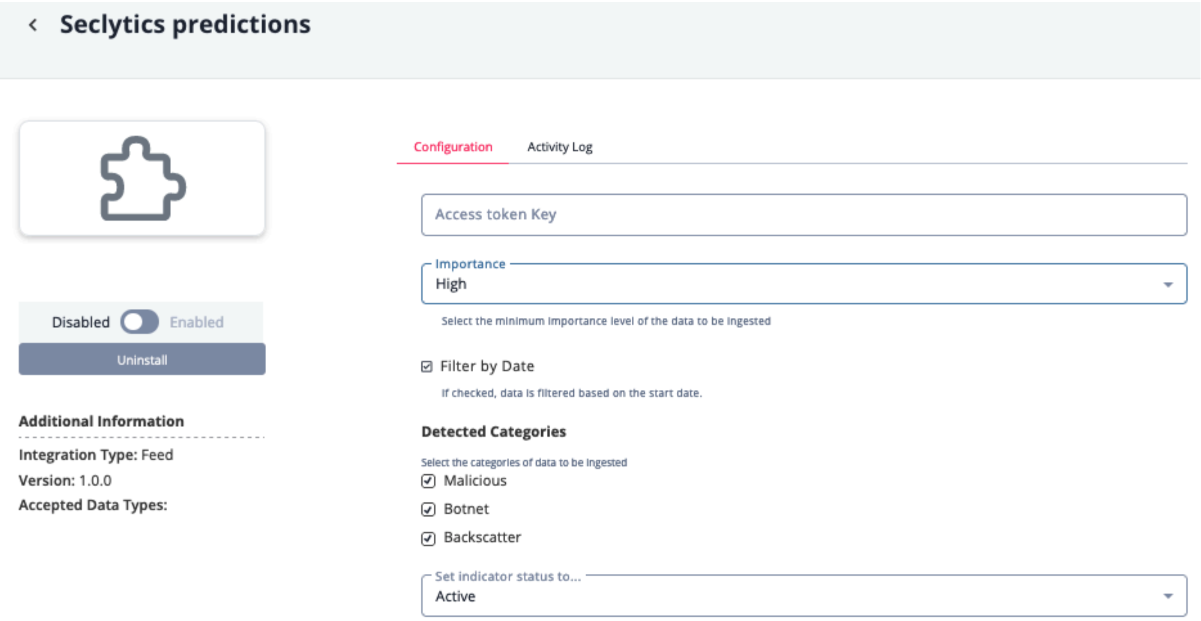
To configure the integration:

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
Access Token Key	Your Seclytics Access Token Key.
Importance	Filter the data by importance. Options include: ◦ High (61-100) (default) ◦ Medium (31-60) ◦ Low (10-30)
Filter by Date	Select this option to filter data based on the Start Date.
Detected Categories	Filter the data by selected categories. Options include: ◦ Malicious (default) ◦ Botnet (default) ◦ Backscatter (default)



Seclytics predictions

Disabled ○ Enabled

Additional Information

Integration Type: Feed

Version: 1.0.0

Accepted Data Types:

Access token Key

Importance: High

Select the minimum importance level of the data to be ingested

☑ Filter by Date

If checked, data is filtered based on the start date.

Detected Categories

Select the categories of data to be ingested

☑ Malicious

☑ Botnet

☑ Backscatter

Set indicator status to...: Active

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

Seclytics Predictions

The Seclytics Predictions feed retrieves and ingests all seen predicted IPs based on user filters.

```
GET https://api.seclytics.com/bulk/seen-predictions-dump-a.json.gz?
access_token=<access_token>
```

Sample CSV Response:

```
ip,predicted_at,predicted_netblock,predicted_category,cluster,detected_by,detected_ident
ifiers,detected_categories,detected_at,last_seen_at,importance
102.140.192.0,2018-06-21T02:03:48,102.140.192.0/24,
spam,3caa3b5744f91251e7ec2b45ef2d6d892786935b,uceprotect_level2,,spam,2021-02-09T00:00:00,
2022-11-27T00:00:00,10102.140.192.1,2018-06-21T02:03:48,102.140.192.0/24,
spam,3caa3b5744f91251e7ec2b45ef2d6d892786935b,uceprotect_level2,,spam,2021-02-09T00:00:00,
2022-11-27T00:00:00,10
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value	IP Address	N/A	102.140.192.0	N/A
1 (second token)	Indicator.Attribute	Predicted At	N/A	2018-06-21T02:03:48	N/A
2 (third token)	Indicator.Attribute	Predicted Netblock	N/A	102.140.192.0/24	N/A
3 (fourth token)	Indicator.Attribute	Predicted Category	N/A	spam	N/A
4 (fifth token)	Indicator.Attribute	Cluster	N/A	3caa3b5744f91251e7ec2b45ef2d6d892786935b	N/A
5 (sixth token)	Indicator.Attribute	Detected By	N/A	uceprotect_level2	N/A
6 (seventh token)	Indicator.Attribute	Detected Identifiers	N/A	N/A	N/A
7 (eighth token)	Indicator.Attribute	Detected Categories	N/A	spam	N/A
8 (ninth token)	Indicator.Attribute	Detected At	N/A	2021-02-09T00:00:00	N/A
9 (tenth token)	Indicator.Attribute	Last Seen At	N/A	2022-11-27T00:00:00	N/A
10 (eleventh token)	Indicator.Attribute	Importance	N/A	10	N/A

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	3 hours
Indicators	6,543
Indicator Attributes	129,600

Change Log

- **Version 1.0.0**
    - Initial release