ThreatQuotient

CCN CERT Reyes CDF

Version 1.0.1

May 03, 2024

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	1.0.1
Compatible with ThreatQ Versions	>= 5.22.0
Support Tier	ThreatQ Supported

Introduction

The CCN CERT Reyes integration downloads indicator object types from the blocklists provided by CCN CERT Reyes. Users can select the blocklists, time range, and indicator types to ingest.

The integration provides the following feed:

- **CCN CERT Reyes** - downloads indicators from the CCN CERT blocklists.

The integration ingests the following indicator types:

- FQDN
- IP Address
- MD5
- SHA-1
- SHA-256
- URL

Prerequisites

The following is required to utilize the the integration:

- CCN CERT Reyes Hostname
- CCN CERT Reyes API Key
- CCN CERT Reyes Client Certification (PEM)
- CCN CERT Reyes Client Private Key (PEM)

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the yaml file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the 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.

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:

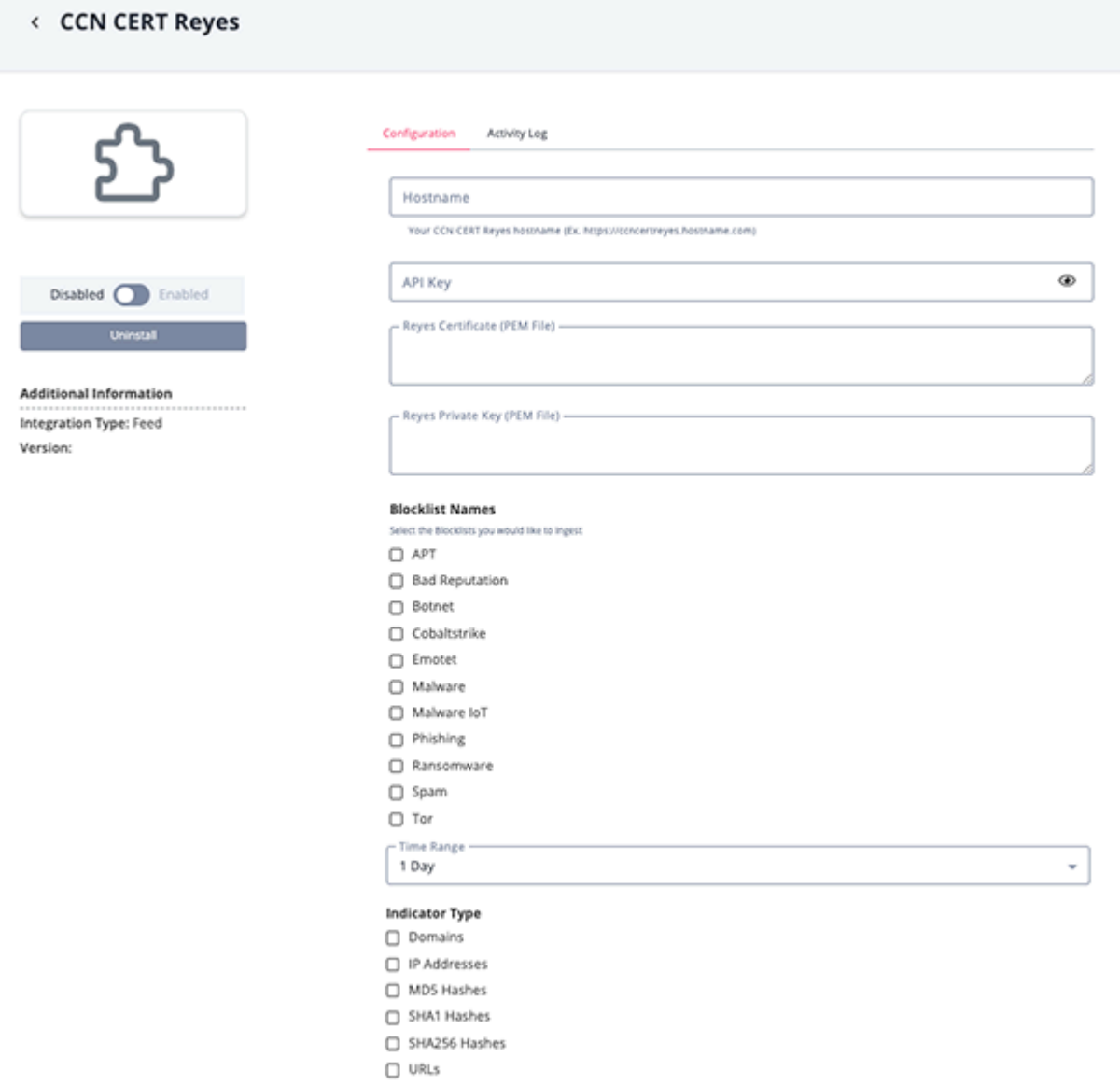
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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
Hostname	Your CCN-CERT Reyes hostname.
API Key	Your CCN-CERT Reyes API key.
Client Certificate	Paste your CCN-CERT Reyes Client Certificate PEM file contents.
Client Private Key	Paste your CCN-CERT Reyes Client Private Key PEM file contents.
Blocklists	Select one or more blocklists for the feed it ingest. Options include: ◦ APT ◦ Bad Reputation ◦ Botnet ◦ Cobaltstrike ◦ Emotet ◦ Malware ◦ Malware IoT ◦ Phishing ◦ Ransomware ◦ Spam ◦ Tor
Time Range	Select a time range, in days, for the feed to ingest. Options include: ◦ 1 Day (default) ◦ 7 Days ◦ 30 Days

PARAMETER	DESCRIPTION
Indicator Type	Select which indicator types to download. Options include: ◦ Domains ◦ IP Addresses ◦ MD5 ◦ Hashes ◦ SHA1 Hashes ◦ SHA256 Hashes ◦ URLs



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

CCN CERT Reyes

The CCN CERT Reyes feed downloads indicators from CCN-CERT blocklists specified by the user.

`GET {reyes_host}/apireyes/api/v4/blocklists/{blocklist_name}/{ioc_type}/{time_range}`

IP Addresses

`GET {reyes_host}/apireyes/api/v4/blocklists/{blocklist_name}/{IP ADDRESSES}/{time_range}`

Sample Response:

```
"#2024-01-24 21:00:06"
1.1.1.1
2.2.2.2
3.3.3.3
...
```

FQDNs

`GET {reyes_host}/apireyes/api/v4/blocklists/{blocklist_name}/{FQDNs}/{time_range}`

Sample Response:

```
"#2024-01-24 21:00:06"
domain1.example.com
domain2.example.com
domain3.example.com
...
```

MD5 Hashes

`GET {reyes_host}/apireyes/api/v4/blocklists/{blocklist_name}/{MD5 HASHES}/{time_range}`

Sample Response:

```
"#2024-01-24 21:00:06"
912ec803b2ce49e4a541068d495ab570
6a204bd89f3c8348afd5c77c717a097a
a95c530a7af5f492a74499e70578d150
...
```

SHA-1 Hashes

`GET {reyes_host}/apireyes/api/v4/blocklists/{blocklist_name}/{SHA-1 HASHES}/{time_range}`

Sample Response:

```
"#2024-01-24 21:00:06"
cf8653876c1e6ad5406df4363e65b439e65de521
92429d82a41e930486c6de5ebda9602d55c39986
79437f5edda13f9c0669b978dd7a9066dd2059f1
...
```

SHA-256 Hashes

`GET {reyes_host}/apireyes/api/v4/blocklists/{blocklist_name}/{SHA-256 HASHES}/{time_range}`

Sample Response:

```
"#2024-01-24 21:00:06"
f0e4c2f76c58916ec258f246851bea091d14d4247a2fc3e18694461b1816e13b
2413fb3709b05939f04cf2e92f7d0897fc2596f9ad0b8a9ea855c7bfebaae892
421c76d77563afa1914846b010bd164f395bd34c2102e5e99e0cb9cf173c1d87
...
```

URLs

`GET {reyes_host}/apireyes/api/v4/blocklists/{blocklist_name}/{URLs}/{time_range}`

Sample Response:

```
"#2024-01-24 21:00:06"
https://url1.com/example1
https://url2.com/example2
https://url3.com/example3
...
```

CCN-CERT to ThreatQ Indicator Mapping

The table below outlines the CCN-CERT Reyes to ThreatQ indicator type mapping.

CCN-CERT REYES INDICATOR TYPE	THREATQ INDICATOR TYPE
ip	IP Address
domain	FQDN
md5	MD5
sha1	SHA-1
sha256	SHA-256
url	URL

Change Log

- **Version 1.0.1**
  - Resolved a casing issue with one of the Blocklist options that would cause errors.
- **Version 1.0.0**
  - Initial release