ThreatQuotient

CISA Reports CDF Guide

Version 2.0.2

March 07, 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	2.0.2
Compatible with ThreatQ Versions	>= 4.52.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/us-cert-reports-cdf

Introduction

The CISA Reports CDF consumes data provided by the CISA to notify organizations about threats that exist on the Internet.

The integration provides the following endpoint:

- **CISA Reports** - ingests reports from the xml source as well as related system objects.

The integration ingests the following system object types:

- Files
- Incidents
- Indicators
- Reports
- TTPs

> ⚠ The **CISA Reports CDF** replaces the **US-CERT Reports CDF**. The US-CERT website was removed and its threat intelligence feed was migrated to the main CISA website. This resulted in a naming update as well as an update to the endpoint utilized by the 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.

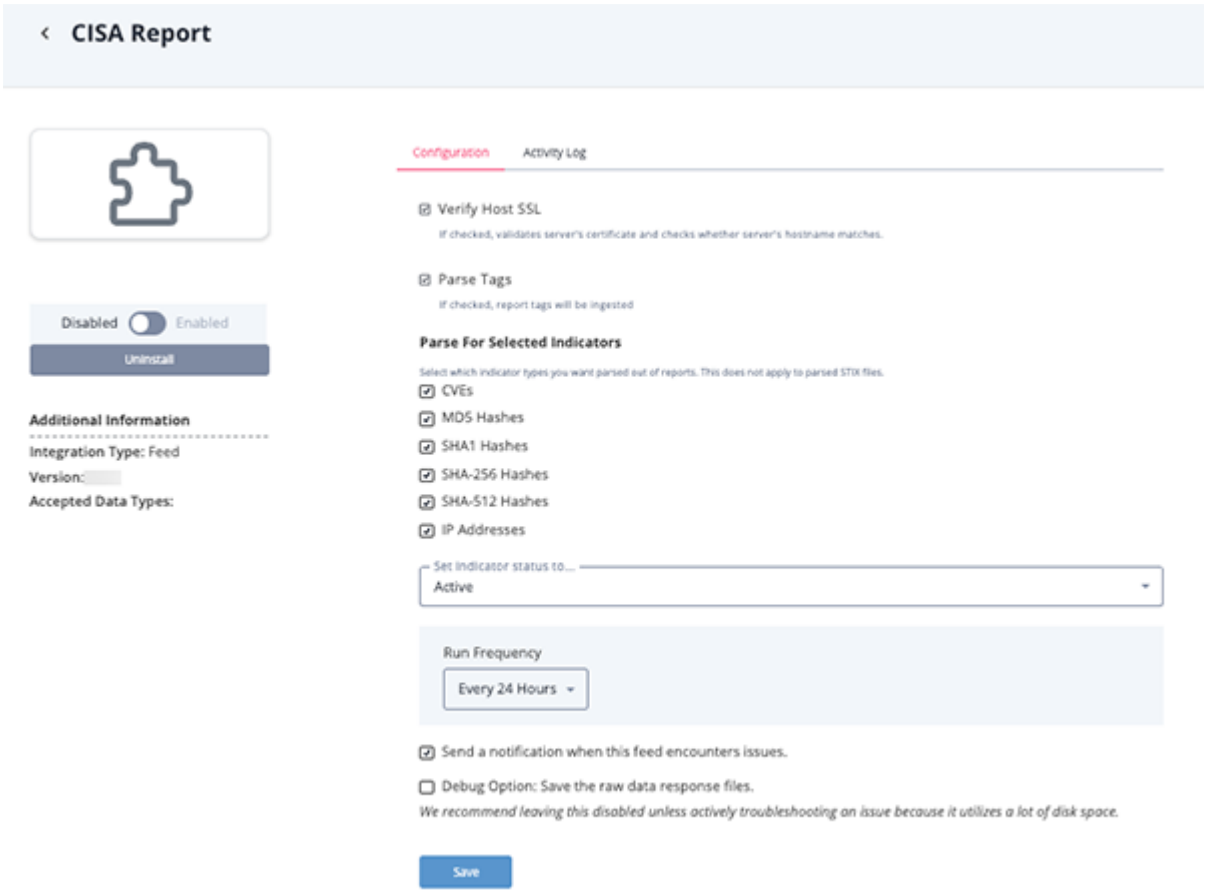
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **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. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Verify SSL	When enabled, the integration will validate the host-provided SSL certificate. This option is enabled by default.
Parse Tags	Enable this option to automatically add tags to the report object. This option is enabled by default.
Parse for Selected Indicators	Select the indicator types to be parsed for reports. Options include ◦ CVEs (default) ◦ MD5 Hashes (default) ◦ SHA-1 Hashes (default) ◦ SHA-256 Hashes (default) ◦ SHA-512 Hashes (default) ◦ IP Addresses (default) > This parameter does not apply to parsed STIX files.



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

CISA Reports

The CISA Reports endpoint ingests reports from the xml feed as well as system objects related to the report.

```
GET https://www.cisa.gov/cybersecurity-advisories/analysis-reports.xml
```

> Depending on the description length, the CDF may or may not attempt to fetch the article's HTML data via the link. The HTML data will be used in-place of the bad description. That request will be made to the following link:
>
> `GET https://www.cisa.gov/news-events/analysis-reports/<report_id>`

Sample Response:

```
<?xml version="1.0" encoding="utf-8"?>
<rss version="2.0" xml:base="https://www.cisa.gov/">
        <channel>
                <title>CISA Analysis Reports</title>
                <link>https://www.cisa.gov/</link>
                <description/>
                <language>en</language>
                <item>
                        <title><a href="/news-events/analysis-reports/ar22-272a" hreflang="en">MAR-10365227-2.v1 </
a></title>
            <link>https://www.cisa.gov/news-events/analysis-reports/ar22-272a</link>
                        <description>Original release date: October 31, 2019 ... </description>
                        <pubDate>Thu, 31 Oct 2019 14:57:45 +0000</pubDate>
                        <dc:creator>CISA</dc:creator>
                        <guid isPermaLink="false">/node/9076</guid>
                </item>
                ...
        </channel>
</rss>
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.rss.channel.item[].title	Report.title	N/A	.rss.channel.item[].pubDate	AR19-304A: MAR-10365227-2 – North Korean Trojan: HOPLIGHT	
.rss.channel.item[].description	Report.description	N/A	N/A	Original release date: October 31, 2019 ...	Base64 encoded image binaries are removed and descriptions are truncated at 65535 characters
N/A	Report.attribute	Report type	.rss.channel.item[].pubDate	CISA Report	
.rss.channel.item[].link	Report.attribute	URL	.rss.channel.item[].pubDate	https://www.cisa.gov/news-events/analysis-reports/ar22-272a	
N/A	Report.attribute	NCAS feed name	.rss.channel.item[].pubDate	Analysis Reports	
.rss.channel.item[].description	Related Indicator.value	IP Address, CVE, MD5, SHA-1, SHA-256, or SHA-512	.rss.channel.item[].pubDate	N/A	Indicators are parsed out of the description
.rss.channel.item[].description	Related File	Malware Analysis Report	.rss.channel.item[].pubDate	N/A	PDF links are parsed out of the description, downloaded, and related as an attachment
.rss.channel.item[].description	Related File	STIX	.rss.channel.item[].pubDate	N/A	STIX links are parsed out of the description, downloaded, and related as an attachment
N/A	Related Indicator/ TTP/Incident.value	N/A	.rss.channel.item[].pubDate	N/A	STIX files are parsed for their indicators, TTPs, Incidents, and Tags

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	2 minutes
Files	7
Reports	10
Report Attributes	30
Indicators	45
Incidents	16
TTPs	2

Change Log

- **Version 2.0.2**
  - Updated the integration's endpoint based on website migration updates by the provider.
  - Rebranded to integration from US-CERT Reports to CISA Reports.
- **Version 2.0.1**
  - Added the ability to parse Tags.
  - Fixed an issue where the wrong TTP objects were parsed.
- **Version 2.0.0**
  - Initial Release. This endpoint used to be included in the US-CERT integration. That integration has been deprecated and its endpoints split into four separate CDFs.