ThreatQuotient

US-CERT Reports CDF Guide

Version 2.0.0

August 30, 2021

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

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.

Versioning

- Current integration version: `2.0.0`
- Supported on ThreatQ versions >= `4.52.0`

Introduction

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

> ⚠ The endpoint for this CDF was formerly included in ThreatQuotient's **US-CERT CDF**. That CDF was deprecated and its endpoints split into four separate CDFs: **US-CERT Activity**, **US-CERT Alerts**, **US-CERT Reports**, and **US-CERT Tips**.

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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Verify SSL Host	When checked, ThreatQ will validate the host-provided SSL certificate. This option is checked by default.
Parse for Selected Indicators	Select which indicator types you want parsed out of alerts. This does not apply to parsed STIX files. Options include: • CVEs • MD5 Hashes • SHA-1 Hashes • SHA-256 Hashes • SHA-512 Hashes • IP Addresses

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

US-CERT Reports

`GET https://us-cert.cisa.gov/ncas/analysis-reports.xml`

Sample response data in XML formatting:

```
<?xml version="1.0" encoding="utf-8"?>
<rss version="2.0" xml:base="https://www.us-cert.gov/">
        <channel>
                <title>CISA Analysis Reports</title>
                <link>https://www.us-cert.gov/</link>
                <description/>
                <language>en</language>
                <item>
                        <title><a href="/ncas/analysis-reports/ar21-055a" hreflang="en">MAR-10325064-1.v1 -
Accellion FTA</a></title>
                        <link>https://www.us-cert.gov/ncas/analysis-reports/ar19-304a</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">13131 at https://www.us-cert.gov</guid>
                </item>
                <item>
                        <title>AR19-252A: MAR-10135536-10 – North Korean Trojan: BADCALL </title>
                        <link>https://www.us-cert.gov/ncas/analysis-reports/ar19-252a</link>
                        <description>Original release date: September 9, 2019  ... </description>
                        <pubDate>Mon, 09 Sep 2019 14:30:49 +0000</pubDate>
                        <dc:creator>CISA</dc:creator>
                        <guid isPermaLink="false">12830 at https://www.us-cert.gov</guid>
                </item>
                <item>
                        <title>AR19-252B: MAR-10135536-21 – North Korean Proxy Malware: ELECTRICFISH</title>
                        <link>https://www.us-cert.gov/ncas/analysis-reports/ar19-252b</link>
                        <description>Original release date: September 9, 2019 ... </description>
                        <pubDate>Mon, 09 Sep 2019 14:23:08 +0000</pubDate>
                        <dc:creator>CISA</dc:creator>
                        <guid isPermaLink="false">12828 at https://www.us-cert.gov</guid>
                </item>
                ...
        </channel>
</rss>
```

> ⚠ 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.us-cert.gov/ncas/analysis-reports/<report_id>`

ThreatQ 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-10135536-8 – 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	CERT Report	
.rss.channel.item[].link	report.attribute	URL	.rss.channel.item[].pubDate	https://www.us-cert.gov/ncas/analysis-reports/ar19-304a	
N/A	report.attribute	NCAS feed name	.rss.channel.item[].pubDate	Analysis Reports	
.rss.channel.item[].description	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	file.content	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	file.content	STIX	.rss.channel.item[].pubDate	N/A	STIX links are parsed out of the description, downloaded, and related as an attachment
N/A	{indicator,ttp,incident}.value	N/A	.rss.channel.item[].pubDate	N/A	STIX files are parsed for their indicators, TTPs, and incidents

Average Feed Run

METRIC	RESULT
Run Time	2 minutes
Files	7
Reports	10
Report Attributes	30

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.

Known Issues / Limitations

- 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.us-cert.gov/ncas/analysis-reports/<report_id>
  ```

Change Log

- **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.