ThreatQuotient

CISA Alerts CDF Guide

Version 1.0.0

May 30, 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	1.0.0
Compatible with ThreatQ Versions	>= 4.52.0
Support Tier	ThreatQ Supported

Introduction

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

The integration provides the following feeds:

- **CISA Alerts** - creates a ThreatQ Alert Event and any related objects

The integration ingests the following system objects:

- Reports
    - Report Attributes

The CISA Advisories and CISA Alerts CDFs replace the deprecated US-CERT Alerts CDF.

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.

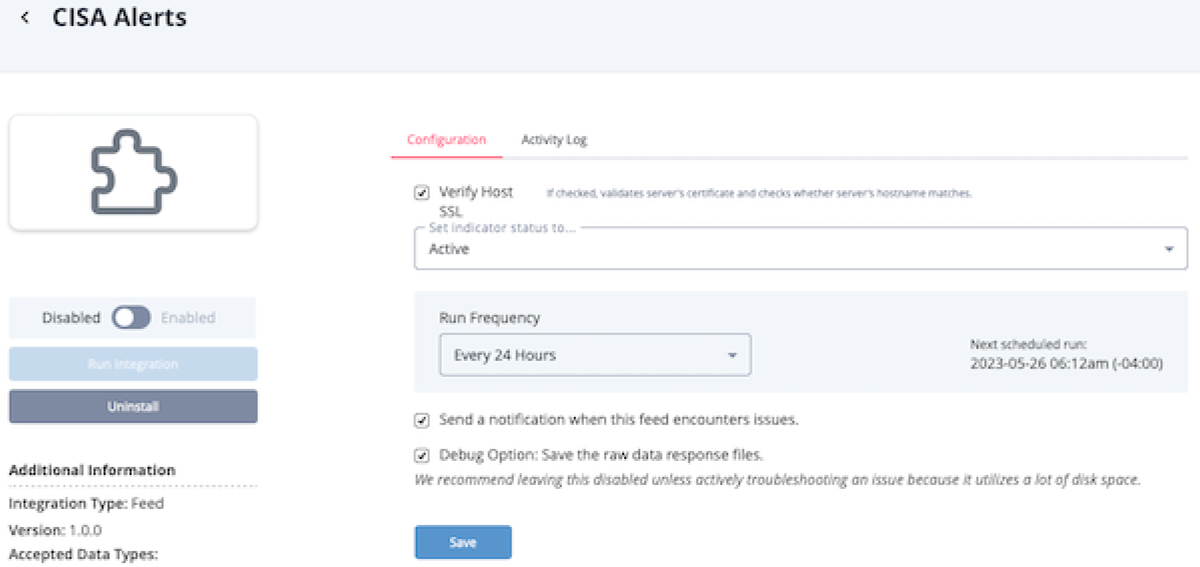
To configure the integration:

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 Host SSL	When checked, validates the host-provided SSL certificate. This option is checked by default.



CISA Alerts

Additional Information

Integration Type: Feed

Version: 1.0.0

Accepted Data Types:

☑ Verify Host SSL — If checked, validates server's certificate and checks whether server's hostname matches.

Set indicator status to... Active

Run Frequency: Every 24 Hours

Next scheduled run: 2023-05-26 06:12am (-04:00)

☑ 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.

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 Alerts

This feed creates a ThreatQ Alert Event and any related objects.

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

Sample Response:

```
<?xml version="1.0" encoding="utf-8"?>
<rss xmlns:dc="http://purl.org/dc/elements/1.1/" version="2.0" xml:base="https://www.cisa.gov/">
  <channel>
    <title>Alerts</title>
    <link>https://www.cisa.gov/</link>
    <description/>
    <language>en</language>

    <item>
  <title>CISA Releases Five Industrial Control Systems Advisories</title>
  <link>https://www.cisa.gov/news-events/alerts/2023/05/18/cisa-releases-five-industrial-control-systems-advisories</
link>
  <description>&lt;p&gt;CISA released five Industrial Control Systems (ICS) advisories on May 16, 2023. These
advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.
&lt;/p&gt;
&lt;ul&gt;&lt;li&gt;ICSA-23-138-01 &lt;a href="https://cisa.gov/news-events/ics-advisories/icsa-23-138-01"&gt;Carlo
Gavazzi Powersoft&lt;/a&gt;&lt;/li&gt;
&lt;li&gt;ICSA-23-138-02 &lt;a href="https://cisa.gov/news-events/ics-advisories/icsa-23-138-02"&gt;Mitsubishi
Electric MELSEC WS&lt;/a&gt;&lt;/li&gt;
&lt;li&gt;ICSA-23-138-03 &lt;a href="https://cisa.gov/news-events/ics-advisories/icsa-23-138-03"&gt;Hitachi Energy
MicroSCADA Pro/X SYS600&lt;/a&gt;&lt;/li&gt;
&lt;li&gt;ICSA-23-138-04 &lt;a href="https://cisa.gov/news-events/ics-advisories/icsa-23-138-04"&gt;Johnson Controls
OpenBlue Enterprise Manager Data Collector&lt;/a&gt;&lt;/li&gt;
&lt;li&gt;ICSA-20-051-02 &lt;a href="https://cisa.gov/news-events/ics-advisories/icsa-20-051-02"&gt;Rockwell
Automation FactoryTalk Diagnostics Update B&lt;/a&gt;&lt;/li&gt;
&lt;/ul&gt;&lt;p&gt; &lt;/p&gt;
&lt;p&gt;CISA encourages users and administrators to review the newly released ICS advisories for technical details
and mitigations.&lt;/p&gt;
</description>
  <pubDate>Thu, 18 May 23 12:00:00 +0000
</pubDate>
    <dc:creator>CISA</dc:creator>
    <guid isPermaLink="false">/node/18192</guid>
    </item>
  </channel>
</rss>
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREAT Q OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.rss.channel.item[].title	Report.Title	N/A	.rss.channel.item[].pubDate	CISA Releases Five Industrial Control Systems Advisories: Thu, 18 May 23 12:00:00 +0000	PubDate appended to title
.rss.channel.item[].description	Report.Description	N/A	N/A	CISA released five Industrial Control Systems (ICS) ...	N/A
.rss.channel.item[].link	Report.Attribute	URL	.rss.channel.item[].pubDate	https://www.cisa.gov/news-events/alerts/2023/05/18/cisa-releases-five-industrial-control-systems-advisories	N/A
N/A	Report.Attribute	NCAS Feed Name	.rss.channel.item[].pubDate	Current Activity	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.

CISA Alerts CDF

METRIC	RESULT
Run Time	<1 minute
Reports	10
Report Attributes	20

Change Log

- **Version 1.0.0**
    - Initial release