ThreatQuotient

CISA ICS Medical Advisories 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 ICS Medical Advisories CDF consumes data provided by the CISA about current security issues, vulnerabilities, and exploits surrounding ICS (Industrial Control Systems).

The integration provides the following feed:

- **CISA ICS Medical Advisories** - creates a ThreatQ Report for each CISA advisory.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Reports
  - Report Attributes

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.

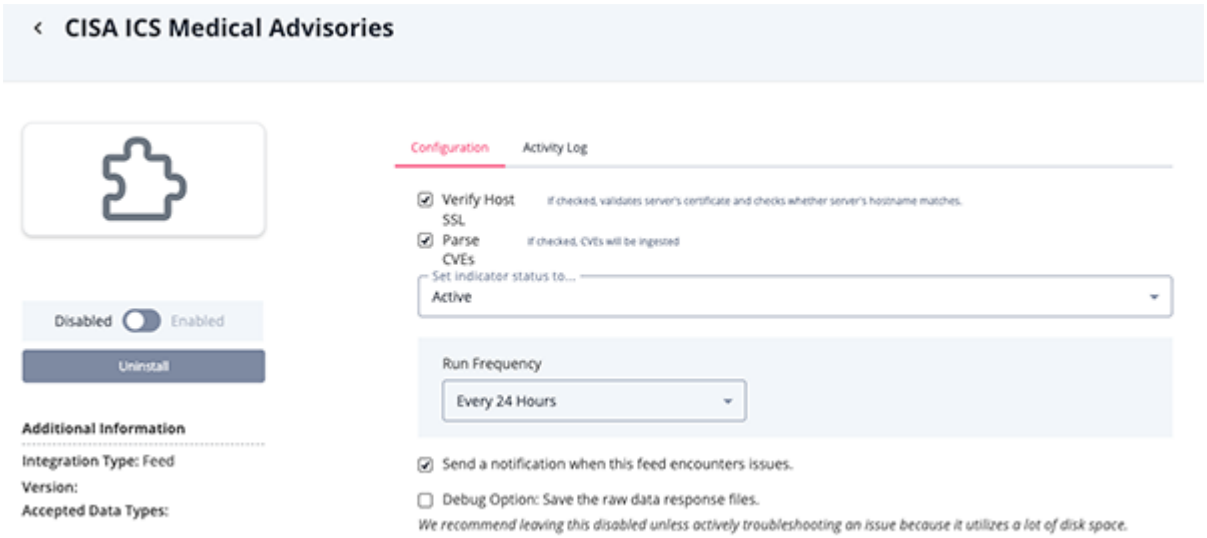
To configure the integration:

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 enabled, the integration will validate the host-provided SSL certificate. This parameter is enabled by default.
Parse CVEs	When enabled, all the CVEs found in the description will be ingested. This parameter is enabled by default.



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 ICS Medical Advisories

The CISA ICS Medical Advisories feed ingests threat intelligence data in the form of ThreatQ Reports.

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

Sample Response (truncated XML):

```
<?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>ICS Medical Advisories</title>
    <link>https://www.cisa.gov/</link>
    <description/>
    <language>en</language>

    <item>
            <title>Medtronic Micro Clinician and InterStim Apps</title>
            <link>https://www.cisa.gov/news-events/ics-medical-advisories/icsma-23-061-01</link>
            <description>&lt;h2&gt;1. EXECUTIVE SUMMARY&lt;/h2&gt;
                &lt;ul&gt;&lt;li&gt;&lt;strong&gt;CVSS v3 6.4&lt;/strong&gt;&lt;/li&gt;
                &lt;li&gt;&lt;strong&gt;ATTENTION:&lt;/strong&gt; Low attack complexity &lt;/li&gt;
                &lt;li&gt;&lt;strong&gt;Vendor:&lt;/strong&gt; Medtronic &lt;/li&gt;
                &lt;li&gt;&lt;strong&gt;Equipment:&lt;/strong&gt; Micros Clinician (A51200) app and InterStim X
Clinician (A51300) app &lt;/li&gt;
                &lt;li&gt;&lt;strong&gt;Vulnerabilities:&lt;/strong&gt; Unverified Password Change &lt;/li&gt;
                &lt;/ul&gt;&lt;h2&gt;2. RISK EVALUATION&lt;/h2&gt;
                &lt;p&gt;Successful exploitation of this vulnerability could cause the clinician application’s custom
                password to be reset to default, resulting in unauthorized control of the clinician therapy
application.
                &lt;/p&gt;
                &lt;h2&gt;3. TECHNICAL DETAILS&lt;/h2&gt;
                &lt;h3&gt;3.1 AFFECTED PRODUCTS&lt;/h3&gt;
                &lt;p&gt;The following versions of Medtronic Clinician App are affected: &lt;/p&gt;
                &lt;ul&gt;&lt;li&gt;Micro Clinician (A51200) &lt;/li&gt;
                &lt;li&gt;InterStim X Clinician (A51300) &lt;/li&gt;
                &lt;/ul&gt;&lt;h3&gt;3.2 VULNERABILITY OVERVIEW&lt;/h3&gt;
                &lt;p&gt;&lt;strong&gt;3.2.1 &lt;a href="https://cwe.mitre.org/data/definitions/
620.html"&gt;UNVERIFIED
                PASSWORD CHANGE CWE-620&lt;/a&gt; &lt;/strong&gt;&lt;/p&gt;
                &lt;p&gt;Medtronic Clinician (A51200) and InterStim X Clinicain App (A51300) contain a vulnerability
                that exists under certain reset conditions, which could cause the clinician application’s custom
                password to be reset to a default password. This could result in unauthorized control of the
clinician
                therapy application, which has greater control over therapy parameters than the patient app. Changes
                still cannot be made outside of the established therapy parameters of the programmer. To gain
                unauthorized access, an individual would need physical access to the Smart Programmer. &lt;/p&gt;
                &lt;p&gt;&lt;a href="http://web.nvd.nist.gov/view/vuln/detail?
vulnId=CVE-2023-25931"&gt;CVE-2023-25931&lt;/a&gt;
                has been assigned to this vulnerability. A CVSS v3 base score of 6.4 has been calculated; the CVSS
```

```
                vector string is (&lt;a
                href="https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:H/
A:H"&gt;AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H&lt;/a&gt;).
                &lt;/p&gt;
                &lt;h3&gt;3.3 BACKGROUND&lt;/h3&gt;
                &lt;ul&gt;&lt;li&gt;&lt;strong&gt;CRITICAL INFRASTRUCTURE SECTORS:&lt;/strong&gt; Healthcare and
Public
                Health &lt;/li&gt;
                &lt;li&gt;&lt;strong&gt;COUNTRIES/AREAS DEPLOYED:&lt;/strong&gt; Worldwide &lt;/li&gt;
                &lt;li&gt;&lt;strong&gt;COMPANY HEADQUARTERS LOCATION:&lt;/strong&gt; Ireland &lt;/li&gt;
                &lt;/ul&gt;&lt;h3&gt;3.4 RESEARCHER&lt;/h3&gt;
                &lt;p&gt;Medtronic reported this vulnerability to CISA. &lt;/p&gt;
                &lt;h2&gt;4. MITIGATIONS&lt;/h2&gt;
                &lt;p&gt;The following mitigations have been provided by Medtronic: &lt;/p&gt;
                &lt;ul&gt;&lt;li&gt;An app update is available as of February 23, 2023 that will fix the
vulnerability.
                &lt;/li&gt;
                &lt;li&gt;Users should refer to the Medtronic &lt;a
                href="https://global.medtronic.com/xg-en/product-security/security-bulletins/pelvic-health-interstim-
micro.html"&gt;Security
                Bulletin&lt;/a&gt; for the correct Medtronic Support contact for help updating the app. &lt;/li&gt;
                &lt;/ul&gt;&lt;p&gt;CISA reminds organizations to perform proper impact analysis and risk assessment
                prior to deploying defensive measures.&lt;/p&gt;
                &lt;p&gt;CISA also provides a section for &lt;a
                href="https://us-cert.cisa.gov/ics/Recommended-Practices"&gt;control systems security recommended
                practices&lt;/a&gt; on the ICS webpage at &lt;a href="https://cisa.gov/ics"&gt;cisa.gov/ics&lt;/
a&gt;.
                Several CISA products detailing cyber defense best practices are available for reading and download,
                including &lt;a
                href="https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-
CERT_Defense_in_Depth_2016_S508C.pdf"&gt;Improving
                Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies&lt;/a&gt;.&lt;/p&gt;
                &lt;p&gt;Additional mitigation guidance and recommended practices are publicly available on the ICS
                webpage at &lt;a href="https://cisa.gov/ics"&gt;cisa.gov/ics&lt;/a&gt; in the technical information
                paper, &lt;a href="https://www.cisa.gov/uscert/ics/tips/ICS-TIP-12-146-01B"&gt;ICS-TIP-12-146-01B--
Targeted
                Cyber Intrusion Detection and Mitigation Strategies&lt;/a&gt;.&lt;/p&gt;
            </description>
            <pubDate>Thu, 02 Mar 2023 00:09:28 EST</pubDate>
            <dc:creator>CISA</dc:creator>
            <guid isPermaLink="false">/node/17499</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	Medtronic Micro Clinician and InterStim Apps: Thu, 02 Mar 2023 00:09:28 EST	PubDate appended to title
.rss.channel.item[].description	Report.Description	N/A	N/A	1. EXECUTIVE SUMMARY...	N/A
.rss.channel.item[].description	Indicator.Value	CVE	.rss.channel.item[].pubDate	CVE-2023-25931	CVEs are parsed out of the description and ingested based on selection
.rss.channel.item[].description	Report.Attribute	Vendor	.rss.channel.item[].pubDate	Medtronic	Attribute parsed from the description
.rss.channel.item[].description	Report.Attribute	Equipment	.rss.channel.item[].pubDate	Micros Clinician (A51200) app and InterStim X Clinician (A51300) app	Attribute parsed from the description
.rss.channel.item[].description	Report.Attribute	CVSS_Score	.rss.channel.item[].pubDate	6.4	Attribute parsed from the description
.rss.channel.item[].link	Report.Attribute	URL	.rss.channel.item[].pubDate	https://www.cisa.gov/news-events/ics-medical-advisories/icsma-23-061-01	N/A
N/A	Report.Attribute	CISA Feed Name	.rss.channel.item[].pubDate	ICS Medical Advisory	N/A
N/A	Indicator.Attribute	CISA Activity	.rss.channel.item[].pubDate	True	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	<1 minute
Reports	10
Report Attributes	50
Indicators	29
Indicator Attributes	29

Change Log

- **Version 1.0.0**
  - Initial release