

# ThreatQuotient



## CISA ICS Medical Advisories CDF User Guide

**Version 1.0.1**

October 13, 2023

### **ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147



**ThreatQ Supported**

### **Support**

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

Warning and Disclaimer ..... 3

Support ..... 4

Integration Details..... 5

Introduction ..... 6

Installation..... 7

Configuration ..... 8

ThreatQ Mapping..... 9

    CISA ICS Medical Advisories..... 9

Average Feed Run..... 13

Change Log ..... 14

# 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.

Copyright © 2023 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

# Support

This integration is designated as **ThreatQ Supported**.

**Support Email:** [support@threatq.com](mailto: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	>= 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

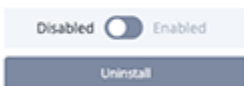
**Verify Host  
SSL**

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.

### < CISA ICS Medical Advisories



#### Additional Information

Integration Type: Feed

Version:

Accepted Data Types:

Configuration

Activity Log

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

☒ **Parse  
CVEs** If checked, CVEs will be ingested

Set indicator status to... 

Active

Run Frequency  

Every 24 Hours

☒ 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 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><h2>1. EXECUTIVE SUMMARY</h2>
        <ul><li><strong>CVSS v3 6.4</strong>
</li>
<li><strong>ATTENTION:</strong> Low attack
complexity </li>
<li><strong>Vendor:</strong> Medtronic </li>
<li><strong>Equipment:</strong> Micros
Clinician (A51200) app and InterStim X Clinician (A51300) app </li>
<li><strong>Vulnerabilities:</strong>
Unverified Password Change </li>
</ul><h2>2. RISK EVALUATION</h2>
<p>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.
</p>
<h2>3. TECHNICAL DETAILS</h2>
<h3>3.1 AFFECTED PRODUCTS</h3>
<p>The following versions of Medtronic Clinician App are
affected: </p>
<ul><li>Micro Clinician (A51200) </li>
<li>InterStim X Clinician (A51300) </li>
</ul>
<h3>3.2 VULNERABILITY OVERVIEW</h3>
<p><strong>3.2.1 <a href="https://cwe.mitre.org/
data/definitions/620.html">UNVERIFIED
```

PASSWORD CHANGE CWE-620</a> </strong></p>  
 <p>Medtronic Clinician (A51200) and InterStim X Clinician  
 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. </p>  
 <p><a href="http://web.nvd.nist.gov/view/vuln/detail?<br>vulnId=CVE-2023-25931">http://web.nvd.nist.gov/view/vuln/detail?<br>vulnId=CVE-2023-25931">  
 has been assigned to this vulnerability. A CVSS v3 base score  
 of 6.4 has been calculated; the CVSS  
 vector string is (<a  
 href="https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:P/<br>AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H">https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:P/<br>AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H">  
 a>);</p>  
 </p>  
 <h3>3.3 BACKGROUND</h3>  
 <ul><li><strong>CRITICAL INFRASTRUCTURE<br>SECTORS:</strong> Healthcare and Public<br>Health </li>  
 <li><strong>COUNTRIES/AREAS DEPLOYED:</strong><br>Worldwide </li>  
 <li><strong>COMPANY HEADQUARTERS LOCATION:</strong><br>Ireland </li></ul>  
 <h3>3.4 RESEARCHER</h3>  
 <p>Medtronic reported this vulnerability to CISA. </p>  
 <h2>4. MITIGATIONS</h2>  
 <p>The following mitigations have been provided by<br>Medtronic: </p>  
 <ul><li>An app update is available as of February<br>23, 2023 that will fix the vulnerability.</li>  
 <li>Users should refer to the Medtronic <a<br>href="https://global.medtronic.com/xg-en/product-security/<br>security-bulletins/pelvic-health-interstim-micro.html">Security<br>Bulletin</a> for the correct Medtronic Support contact<br>for help updating the app. </li></ul>  
 <p>CISA reminds organizations to perform<br>proper impact analysis and risk assessment<br>prior to deploying defensive measures.</p>  
 <p>CISA also provides a section for <a<br>href="https://us-cert.cisa.gov/ics/Recommended-<br>Practices">control systems security recommended

```

practices</a> on the ICS webpage at <a href="https://
cisa.gov/ics">cisa.gov/ics</a>.
Several CISA products detailing cyber defense best practices
are available for reading and download,
including <a
href="https://us-cert.cisa.gov/sites/default/files/
recommended_practices/NCCIC_ICS-
CERT_Defense_in_Depth_2016_S508C.pdf">Improving
Industrial Control Systems Cybersecurity with Defense-in-Depth
Strategies</a>.</p>
<p>Additional mitigation guidance and recommended
practices are publicly available on the ICS
webpage at <a href="https://cisa.gov/ics">cisa.gov/
ics</a> in the technical information
paper, <a href="https://www.cisa.gov/uscert/ics/tips/ICS-
TIP-12-146-01B">ICS-TIP-12-146-01B--Targeted
Cyber Intrusion Detection and Mitigation Strategies</a>
a</p>
</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	<a href="https://www.cisa.gov/news-events/ics-medical-advisories/icsma-23-061-01">https://www.cisa.gov/news-events/ics-medical-advisories/icsma-23-061-01</a>	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 1.0.1**
  - Resolved a date parsing issue.
- **Version 1.0.0**
  - Initial release