ThreatQuotient

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

The integration provides the following feeds:

- **CISA ICS Advisories** - ingests threat intelligence from CISA and creates ThreatQ reports and related indicators.

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.

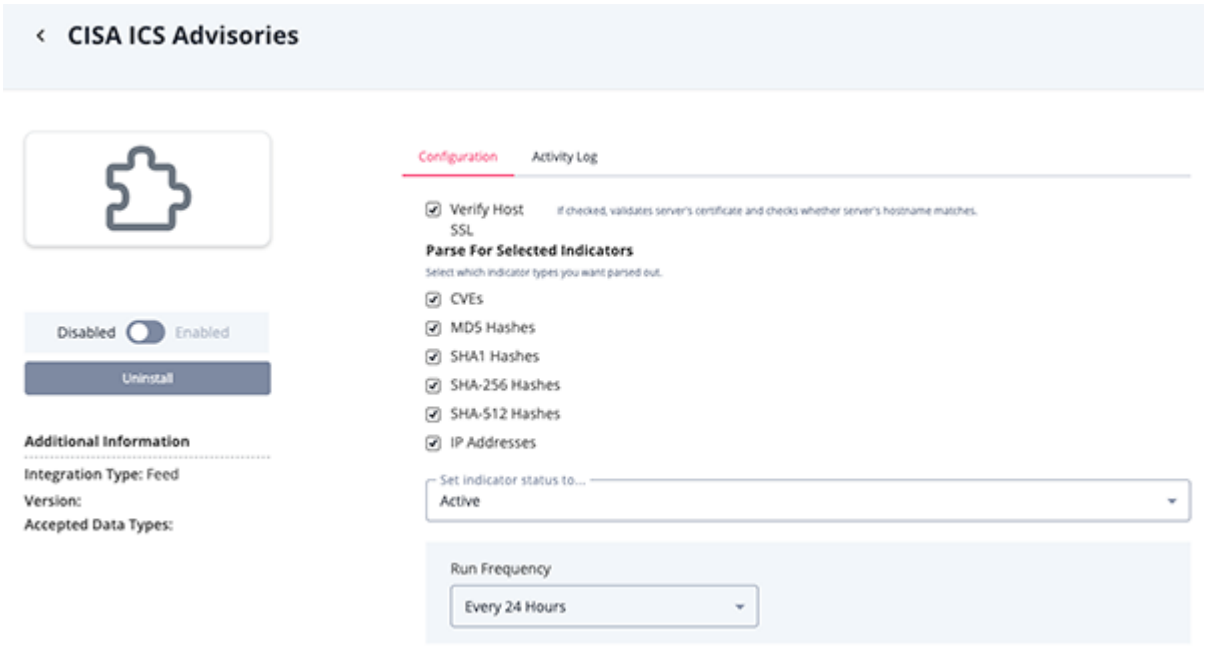
To configure the integration:

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 for Selected Indicators	Select the type of indicators to parse. 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

CISA ICS Advisories

The CISA ICS Advisories feed consumes data provided by the CISA to create reports and related indicators.

```
GET https://www.cisa.gov/cybersecurity-advisories/ics-advisories.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>ICS Advisories</title>
    <link>https://www.cisa.gov/</link>
    <description/>
    <language>en</language>

    <item>
  <title>Carlo Gavazzi Powersoft</title>
  <link>https://www.cisa.gov/news-events/ics-advisories/icsa-23-138-01</link>
  <description>&lt;h2&gt;1. EXECUTIVE SUMMARY&lt;/h2&gt;
&lt;ul&gt;&lt;li&gt;&lt;strong&gt;CVSS v3 7.5&lt;/strong&gt;&lt;/li&gt;
&lt;li&gt;&lt;strong&gt;ATTENTION:&lt;/strong&gt; Exploitable remotely/low attack complexity/public exploits are
available&lt;/li&gt;
&lt;li&gt;&lt;strong&gt;Vendor:&lt;/strong&gt; Carlo Gavazzi&lt;/li&gt;
&lt;li&gt;&lt;strong&gt;Equipment:&lt;/strong&gt; Powersoft&lt;/li&gt;
&lt;li&gt;&lt;strong&gt;Vulnerabilities:&lt;/strong&gt; Path Traversal&lt;/li&gt;
&lt;/ul&gt;&lt;h2&gt;2. RISK EVALUATION&lt;/h2&gt;
&lt;p&gt;Successful exploitation of this vulnerability could allow an attacker to access and retrieve any file from
the server. &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 Carlo Gavazzi Powersoft, an energy management software, are affected:&lt;/p&gt;
&lt;ul&gt;&lt;li&gt;Powersoft: Versions 2.1.1.1 and prior&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/22.html" rel="noreferrer noopener"
target="_blank"&gt;IMPROPER LIMITATION OF A PATHNAME TO A RESTRICTED DIRECTORY ('PATH TRAVERSAL') CWE-22&lt;/
a&gt;&lt;/strong&gt;&lt;/p&gt;
&lt;p&gt;Carlo Gavazzi Powersoft versions 2.1.1.1 and prior have a directory traversal vulnerability that can allow
an attacker to access and retrieve any file through specially crafted GET requests to the server.&lt;/p&gt;
&lt;p&gt;&lt;a href="http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-20184" rel="noreferrer noopener"
target="_blank"&gt;CVE-2017-20184&lt;/a&gt; has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has
been calculated; the CVSS vector string is (&lt;a href="https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/
PR:N/UI:N/S:U/C:H/I:N/A:N" rel="noreferrer noopener" target="_blank"&gt;AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N&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;Critical Manufacturing&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;Switzerland&lt;/li&gt;
&lt;/ul&gt;&lt;h3&gt;3.4 RESEARCHER&lt;/h3&gt;
&lt;p&gt;CISA discovered a public proof-of-concept as authored by James Fitts.&lt;/p&gt;
```

```
&lt;h2&gt;4. MITIGATIONS&lt;/h2&gt;
&lt;p&gt;Carlo Gavazzi will not issue a fix as this product is end-of-life.&lt;/p&gt;
&lt;p&gt;Users should contact &lt;a href="https://www.gavazziautomation.com/nsc/HQ/EN/our_sales_network"
rel="noreferrer noopener" target="_blank"&gt;Carlo Gavazzi&lt;/a&gt; for more information.&lt;/p&gt;
&lt;p&gt;CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability.
Specifically, users should:&lt;/p&gt;
&lt;ul&gt;&lt;li&gt;Minimize network exposure for all control system devices and/or systems, and ensure they are
&lt;a href="https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-10-301-01" rel="noreferrer noopener"
target="_blank"&gt;not accessible from the Internet&lt;/a&gt;.&lt;/li&gt;
&lt;li&gt;Locate control system networks and remote devices behind firewalls and isolate them from business
networks.&lt;/li&gt;
&lt;li&gt;When remote access is required, use secure methods, such as virtual private networks (VPNs), recognizing
VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only
as secure as its connected devices.&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"
rel="noreferrer noopener" target="_blank"&gt;control systems security recommended practices&lt;/a&gt; on the ICS
webpage at &lt;a href="https://cisa.gov/ics" rel="noreferrer noopener" target="_blank"&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" rel="noreferrer noopener" target="_blank"&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" rel="noreferrer noopener" target="_blank"&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" rel="noreferrer noopener"
target="_blank"&gt;ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies&lt;/a&gt;.&lt;/
p&gt;
&lt;p&gt;Organizations observing suspected malicious activity should follow established internal procedures and
report findings to CISA for tracking and correlation against other incidents.&lt;/p&gt;
</description>
  <pubDate>Thu, 18 May 23 12:00:00 +0000
</pubDate>
    <dc:creator>CISA</dc:creator>
    <guid isPermaLink="false">/node/18185</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	Carlo Gavazzi Powersoft: Thu, 18 May 23 12:00:00 +0000	PubDate is appended to the title
.rss.channel.item[].description	Report Description	N/A	N/A	As of January 10, 2023, CISA will no longer be updating ICS security advisories for Siemens ...	Description is formatted and truncated
.rss.channel.item[].link	Report Attribute	URL	.rss.channel.item[].pubDate	https://www.cisa.gov/news-events/ics-advisories/icsa-23-138-01	N/A
N/A	Report Attribute	CISA Feed Name	.rss.channel.item[].pubDate	ICS Advisories	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.rss.channel.item[].description	Report Attribute	Vendor	.rss.channel.item[].pubDate	Carlo Gavazzi	Attribute parsed from description
.rss.channel.item[].description	Report Attribute	Equipment	.rss.channel.item[].pubDate	Powersoft	Attribute parsed from description
.rss.channel.item[].description	Report Attribute	CVSS Score	.rss.channel.item[].pubDate	7.5	Attribute parsed from description
.rss.channel.item[].description	Indicator Value	IP Address, CVE, MD5, SHA-1, SHA-256, or SHA-512	.rss.channel.item[].pubDate	CVE-2017-20184	Indicators are parsed out of the description and ingested based on Parse For Selected Indicators selection
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 min
Reports	10
Report Attributes	50
Indicators	40
Indicator Attributes	40

Change Log

- **Version 1.0.0**
  - Initial release