

ThreatQuotient



CISA Bulletins CDF User Guide

Version 1.0.1

September 18, 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 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

ThreatQ Mapping..... 10

 CISA Bulletins..... 10

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

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

The integration provides the following feeds:

- **CISA Bulletins** - creates a ThreatQ Alert Event and ingests related objects.

The integration ingests the following system objects:

- Events
 - Event Attributes
- Indicators
 - Indicator Attributes
- TTPs
 - TTP 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	<p>Select the type of indicators to parse. Options include:</p> <ul style="list-style-type: none"> ◦ CVEs ◦ MD5 ◦ Hashes ◦ SHA-1 Hashes ◦ SHA-256 Hashes ◦ SHA-512 Hashes ◦ IP Addresses



This parameter does not apply to parsed STIX files.

ThreatQ Mapping

CISA Bulletins

The CISA Bulletins feed creates a ThreatQ Alert Event and ingests related objects.

GET <https://www.cisa.gov/cybersecurity-advisories/bulletins.xml>



CISA Bulletins, Get Report HTML (Supplemental) and Get Attachment (Supplemental) feeds bring in information about current security issues, vulnerabilities and exploits into ThreatQ.

Sample Response (XML):

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

    <item>
      <title>Vulnerability Summary for the Week of May 8, 2023</title>
      <link>https://www.cisa.gov/news-events/bulletins/sb23-135</link>
      <description>&lt;h3&gt;Summary&lt;/h3&gt;
&lt;p&gt;&lt;em&gt;Note: This joint Cybersecurity Advisory (CSA) is part of an
ongoing #StopRansomware effort to publish advisories for network defenders that
detail various ransomware variants and ransomware threat actors. These
#StopRansomware advisories include recently and historically observed tactics,
techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help
organizations protect against ransomware. Visit &lt;/em&gt;&lt;a href="https://
www.cisa.gov/stopransomware"&gt;&lt;em&gt;stopransomware.gov&lt;/em&gt;&lt;/
a&gt;&lt;em&gt; to see all #StopRansomware advisories and learn more about
other ransomware threats and no-cost resources.&lt;/em&gt;&lt;/p&gt;
&lt;p&gt;The Federal Bureau of Investigation (FBI), Cybersecurity and
Infrastructure Security Agency (CISA), and Australian Cyber Security Centre
(ACSC) are releasing this joint Cybersecurity Advisory to disseminate known
BianLian ransomware and data extortion group IOCs and TTPs identified through
FBI and ACSC investigations as of March 2023.&lt;/p&gt;
&lt;table&gt;&lt;tbody&gt;&lt;tr&gt;&lt;td&gt;
&lt;/div&gt;
&lt;p&gt;&lt;strong&gt;Actions to take today to mitigate cyber threats from
BianLian ransomware and data extortion: &lt;/strong&gt;&lt;br /&gt;
      • Strictly limit the use of RDP and other remote
desktop services.&lt;br /&gt;
```

```

        • Disable command-line and scripting activities and
permissions.<br />
        • Restrict usage of PowerShell and update Windows
PowerShell or PowerShell Core to the latest version.</p>
</div>
</td>
</tr>
</tbody>
</table>
<p>BianLian is a ransomware
developer, deployer, and data extortion cybercriminal group that has targeted
organizations in multiple U.S. critical infrastructure sectors since June 2022.
They have also targeted Australian critical infrastructure sectors in addition
to professional services and property development. The group gains access to
victim systems through valid Remote Desktop Protocol (RDP) credentials, uses
open-source tools and command-line scripting for discovery and credential
harvesting, and exfiltrates victim data via File Transfer Protocol (FTP),
Rclone, or Mega. BianLian group actors then extort money by threatening to
release data if payment is not made. BianLian group originally employed a
double-extortion model in which they encrypted victims' systems after
exfiltrating the data; however, around January 2023, they shifted to primarily
exfiltration-based extortion.</p>
<p>FBI, CISA, and ACSC encourage critical infrastructure organizations
and small- and medium-sized organizations to implement the recommendations in
the Mitigations section of this advisory to reduce the likelihood and impact of
BianLian and other ransomware incidents.</p>
<p>Download the PDF version of this report (710kb):</p>
</description>
<pubDate>Mon, 15 May 2023 08:09:48 EDT</pubDate>
<dc:creator>CISA</dc:creator>
<guid isPermaLink="false">/node/18173</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	Event.Title	N/A	.rss.channel.item[]. pubDate	Vulnerability Summary for the Week of May 8, 2023	N/A
N/A	Event.Type	Alert	N/A	Alert	N/A
.rss.channel.item[].description	Event.Description	N/A	N/A	Note: This joint Cybersecurity Advisory (CSA) is part	Depending on the description length, the value can be replaced by the actual article's HTML. That HTML is get by Get Report HTML (Supplemental) feed

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.rss.channel.item[].pubDate	Event.Happened_at	N/A	N/A	Mon, 15 May 2023 08:09:48 EDT	N/A
N/A	Event.Attribute/ Indicator.Attribute	CISA Bulletins	.rss.channel.item[]. pubDate	True	N/A
N/A	Event.Attribute	Alert type	.rss.channel.item[]. pubDate	CISA Bulletins	N/A
.rss.channel.item[].link	Event.Attribute	URL	.rss.channel.item[]. pubDate	https:// www.cisa.gov/ news-events/ bulletins/ sb23-135	N/A
.rss.channel.item[].description	Event.Attribute	PDF Link	.rss.channel.item[]. pubDate	N/A	The link is extracted from the article's description
.rss.channel.item[].description	Event.Attribute	Stix Link	.rss.channel.item[]. pubDate	N/A	The link is extracted from the article's description
.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
STIX File	(Indicator,TTP,Incident).value	Indicator, TTP, Incident	.rss.channel.item[]. pubDate	N/A	STIX file is get by the Get Attachment (Supplemental) feed and then it's parsed for the indicators, TTPs, and incidents

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	5 hours
Events	10
Event Attributes	30
Indicators	6,859
Indicator Attributes	6,859
TTPs	37
TTP Attributes	37

Change Log

- **Version 1.0.1**
 - Removed the inter-related relationships flag which caused a large amount of relationships to be created. Indicators will now only be related to their respective events.
- **Version 1.0.0**
 - Initial release