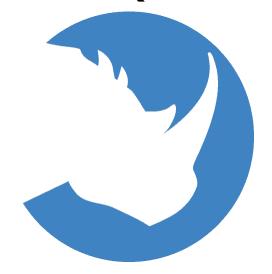
# **ThreatQuotient**



### RSS Feed Reader CDF User Guide Version 1.0.2

July 31, 2023

### **ThreatQuotient**

20130 Lakeview Center Plaza Suite 400 Ashburn, VA 20147



### Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893



### **Contents**

Warning and Disclaimer	. З
Support	. 4
Integration Details	
Introduction	. 6
Installation	
Configuration	. 8
ThreatQ Mapping	11
RSS Feed Reader	11
Average Feed Run	15
Known Issues / Limitations	16
Change Log	17



## 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@threatg.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** 1.0.2

**Compatible with ThreatQ** >= 5.6.0

Versions

Support Tier ThreatQ Supported



### Introduction

The RSS Feed Reader CDF enables analysts to automatically ingest RSS feeds from multiple sources, directly into ThreatQ.

The integration provides the following feed:

• RSS Feed Reader - ingests reports as a main object and indicators as related objects.

The integration ingests the following system objects:

- Reports
  - Report Attributes
- Indicators



### 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

#### Preset RSS Feeds

Select one or more RSS feeds to ingest posts from. This parameter can be used in conjunction with the **Custom RSS Feeds** parameter below. Options include:

- Avast Threat Labs
- BAE Systems Threat Research Blog
- BankInfo Security
- BleepingComputer
- CERT Australia
- CERT Austria
- · CERT Polska
- CERT Romania
- CIS Security Advisories
- Cisco Talos Blog
- Check Point Research
- Check Point Threat Center
- Contagio
- Crowdstrike Blog
- CSO Online
- Cybereason
- Dark Reading
- ESET WeLiveSecurity

- Juniper Threat Research
- Krebs on Security
- Kryptos Logic Blog
- Latest Hacking News
- Malwarebytes Malware Analysis: The Final Frontier
- Malware Traffic Analysis
- Microsoft Security
- NCC Group Research
- Netskope Threat Research
- News ENISA
- Palo Alto Blog Palo
- Alto Unit 42
- Qualys Security Blog
- Quick Heal
- SANS Internet Storm Center



#### **PARAMETER**

#### **DESCRIPTION**

- Flashpoint
- Fortinet Threat

Research

- Fox-IT Blog
- GovCERT Switzerland
- Infosecurity Magazine
- InfoSec Malware
  - **Analysis**

- Secureworks Threat
- **Analysis**
- Securlist
- Security Affairs
- X-Force Feed
- Sophos: Naked Security
- Threatpost
- TrendMicro
- Veloxity Blog
- Yoroi Blog

#### **Custom RSS Feeds**

Enter a line-separated list of RSS feeds (URLs) to ingest posts from. This parameter can be used in conjunction with the **Preset RSS** 

Feeds parameter above.

#### Ingest **Categories As**

Select one or more entities to ingest the Category field as. Options include:

- Attributes
- Tags (default)

#### Parsed IOC **Types**

Select the IOC types to automatically parse from the content. Options include:

- CVE (default)
- MD5
- IP Address
- ° SHA-1
- IPv6 Address CIDR Block
- ∘ SHA-256 SHA-512

- FQDN
- Email Address

URL

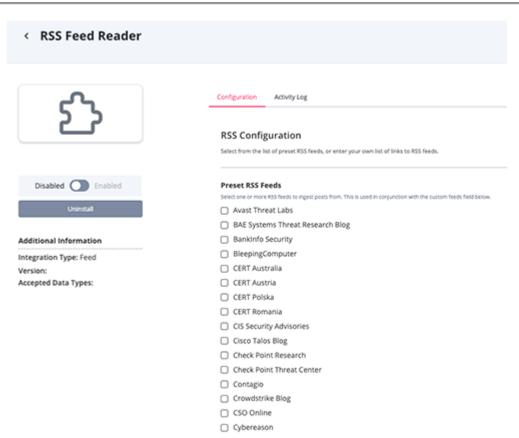
Registry Key

#### **Parsing Options**

Select the parsing options to use when parsing IOCs from the content. Options include:

- Normalize IOCs
- Derive FQDNs from URLs





- 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

### **RSS Feed Reader**

The RSS Feed Reader feed periodically pulls entries from one or more RSS feeds. Entries will be parsed and uploaded to ThreatQ as Reports.

#### Sample Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<rss version="2.0" xmlns:content="http://purl.org/rss/1.0/modules/content/"</pre>
xmlns:wfw="http://wellformedweb.org/CommentAPI/" xmlns:dc="http://purl.org/dc/
elements/1.1/" xmlns:atom="http://www.w3.org/2005/Atom" xmlns:sy="http://
purl.org/rss/1.0/modules/syndication/" xmlns:slash="http://purl.org/rss/1.0/
modules/slash/">
        <channel>
                <title>
                         Graham Cluley
                </title>
                <link href="https://grahamcluley.com/feed/" rel="self"</pre>
type="application/rss+xml" />
                k>
                         https://grahamcluley.com
                </link>
                <description>
                         Computer security news, advice, and opinion
                </description>
                <lastBuildDate>
                        Wed, 15 Feb 2023 13:51:41 +0000
                </lastBuildDate>
                <language>
                         en-GB
                </language>
                <updatePeriod>
                         hourly
                </updatePeriod>
                <updateFrequency>
                </updateFrequency>
                <generator>
                         https://wordpress.org/?v=6.1.1
                </generator>
                <image>
                         <url>
                                 https://grahamcluley.com/wp-content/uploads/
2022/12/cropped-android-chrome-512x512-2-32x32.png
                         </url>
                         <title>
```



```
Graham Cluley
                        </title>
                        k>
                                https://grahamcluley.com
                        </link>
                        <width>
                                32
                        </width>
                        <height>
                                32
                        </height>
                </image>
                <item>
                        <title>
                                Ransomware attackers steal over 3 million
patients' medical records
                        </title>
                        k>
                                https://www.bitdefender.com/blog/
hotforsecurity/ransomware-attackers-steal-over-3-million-patients-medical-
records/
                        </link>
                        <comments>
                                https://www.bitdefender.com/blog/
hotforsecurity/ransomware-attackers-steal-over-3-million-patients-medical-
records/#respond
                        </comments>
                        <creator>
                                <![CDATA[Graham Cluley]]>
                        </creator>
                        <pubDate>
                                Tue, 14 Feb 2023 10:59:57 +0000
                        </pubDate>
                        <category>
                                <![CDATA[Data loss]]>
                        </category>
                        <category>
                                <![CDATA[Guest blog]]>
                        </category>
                        <category>
                                <![CDATA[Ransomware]]>
                        </category>
                        <category>
                                <![CDATA[data breach]]>
                        </category>
                        <category>
                                <![CDATA[medical]]>
                        </category>
                        <category>
                                <![CDATA[ransomware]]>
```



```
</category>
                        <guid isPermaLink="false">
                                https://grahamcluley.com/?p=12336776
                        </guid>
                        <description>
                                 <! [CDATA [
                                A ransomware attack has again put the personal
information of innocent parties at risk after it was revealed that a data
breach has potentially exposed the medical records of more than three million
people.
                                Read more in my article on the Hot for Security
blog.
                                 ]]>
                        </description>
                        <commentRss>
                                https://www.bitdefender.com/blog/
hotforsecurity/ransomware-attackers-steal-over-3-million-patients-medical-
records/feed/
                        </commentRss>
                        <comments>
                        </comments>
                </item>
        </channel>
</rss>
```

ThreatQuotient provides the following default mapping for this feed:



RSS Feeds typically follow a standard format, but the content will be different from feed to feed. Each mapping below is based on the available fields for each item in the feed.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.title	Report.Value	N/A	.pubDate	Ransomware attackers steal over 3 million patients' medical records	N/A
.link	Report.Attribute	Web Link	N/A	N/A	N/A
.categor y	Report.Attribute, Report.Tag	Category	N/A	N/A	Field may be a list or single value
.content Type	Report.Attribute	Туре	N/A	N/A	Non-standard field
.severit y	Report.Attribute	Severity	N/A	Critical	Non-standard field
.dc:type	Report.Attribute	Туре	N/A	News	Non-standard field
.pubDate	Report.Attribute	Published At	N/A	Tue, 14 Feb 2023 10:59:57 +0000	N/A



FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.author	Report.Attribute	Author	N/A	N/A	N/A
.dc:crea	Report.Attribute, Report.Source	Author	N/A	Graham Cluley	N/A
.country	Report.Attribute	Country Code, Country	N/A	US	Non-standard field
.feed_ur l	Report.Attribute	RSS Feed	N/A	https://decoded.avast.io/feed/	N/A
<pre>.descrip tion, .content :encoded</pre>	Report.Description	N/A	N/A	N/A	N/A
<pre>.descrip tion, .content :encoded, .title</pre>	Related Indicator.Value	CVE	N/A	N/A	Parsed from content, when enabled



## 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 minutes
Reports	521
Report Attributes	981
Indicators	437



### **Known Issues / Limitations**

• The CDF utilizes since and until dates to ensure that entries are not re-ingested if they haven't been updated. Use the **Run Integration** button to ingest historical entries from feeds.



## **Change Log**

- Version 1.0.2
  - Resolved an issue where some RSS feeds contained encoded content with additional tags, which caused run errors.
- Version 1.0.1
  - Resolved an issue regarding parsing dates for several custom RSS feeds.
  - $^{\circ}\,$  Resolved an issue regarding RSS feeds consisting of a single post.
- Version 1.0.0
  - Initial release