ThreatQuotient

RST Threat Feed TAXII Feeds User Guide

Version 1.0.0

September 17, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Developer Supported

Support

Email:	support@rstcloud.net
Web:	N/A
Phone:	N/A

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 **Developer Supported**.

Support Email: support@rstcloud.net
Support Web: N/A
Support Phone: N/A

Integrations designated as **Developer Supported** are supported and maintained by the developer who submitted the integration to the ThreatQ Marketplace. The developer's contact information can be found on the integration's download page within the Marketplace as well as in this guide.

You are responsible for engaging directly with the developer of Developer Supported integrations/apps/add-ons to ensure proper functionality and version compatibility with the applicable ThreatQuotient Software.

If functional or compatibility issues that may arise are not resolved, you may be required to uninstall the app or add-on from their ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply for any issues caused by Developer Supported integrations/apps/add-ons.

ThreatQuotient reserves the right to remove the Developer-Supported designation of third-party apps and add-ons if the developer is not, in ThreatQuotient's determination, fulfilling reasonable obligations for support and maintenance.

> Failure by the developer to update compatibility of an app or add-on within 90 days of the release of a new version of applicable ThreatQuotient Software will result in reclassification to Not Actively Supported.

Integration Details

ThreatQuotient provides the following details for this integration:

Guide Version	1.0.0
TAXII Server Version	2.1.0
Compatible with ThreatQ Versions	>= 5.29.0
Support Tier	Developer Supported
Developer Contact	support@rstcloud.net

Introduction

The RST Threat Feed is comprehensive threat intel feed of indicators (IP, Domain, URL, Hash) with their relationships to malware, TTPs, tools, threat groups, sectors, CVE, and other objects. Compiled from over 260 sources, including Twitter, Telegram, online sandboxes (Any.Run, Hybrid Analysis, VMRay, etc.), threat reports, CERTs, malware research sites, GitHub, pastebin, closed sources and our global RST Honeypot network.

This guide will provide you with the steps to install the following RST TAXII feeds:

- RST Threat Feed: High Risk Indicators
- RST Threat Feed: Medium Risk Indicators
- RST Threat Feed: Low Risk Indicators

> These feeds are TAXII feeds and do not require installation files from the ThreatQ Marketplace.

Prerequisites

You will need to the following to install and utilize the RST Threat TAXII Feeds:

- RST Cloud Account
- Access to the RST default data collections

Default Collections

The following three collections are available to you by default. These collection IDs can be entered in the Poll URL configuration field for the feed.

COLLECTION NAME	COLLECTION ID
RST Threat Feed: High Risk Indicators	689709ee-8496-4da2-997d-e9face24eee9
RST Threat Feed: Medium Risk Indicators	98ab279c-a6cc-4efc-9442-87bd8a9b4577
RST Threat Feed: Low Risk Indicators	b2e8fa09-1389-4fab-be65-ba337b190f92

> You can contact RST Cloud Support to receive a custom collection of indicators.

Setting up the TAXII Feeds

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To set up and configure the TAXII feeds:

1. Navigate to your integrations management page in ThreatQ.
2. Click on the **Add New Integration** button and select the **Add New TAXII Feed** option.
3. Enter the following feed settings:

RST Threat Feed: High Risk Indicators

PARAMETER	DESCRIPTION
What would you like to name this feed	Enter **RST Threat Feed: High Risk Indicator**s as the feed name.
How ofter would you like to pull new data from this feed	Select the frequency in which the feed it pulled. Options include: ◦ Every Hour ◦ Every6 Hours ◦ Every Day ◦ Every 2 Days ◦ Every 14 Days ◦ Every 30 Days
TAXII Server Version	Select the **2.1** option from the dropdown menu.
Discovery URL	Enter the Discovery URL: **https://taxii.rstcloud.net/taxii2/**
Poll URL	Enter the Poll URL https://taxii.rstcloud.net/taxii2/root/collections/689709ee-8496-4da2-997d-e9face24eee9

PARAMETER	DESCRIPTION
Collection Name/Title	Enter **RST Threat Feed: High Risk Indicator**s as the collection name.
Disable Proxies	Leave this option unselected.
Username	Enter your RST Cloud username.
Password	Enter your RST Cloud password.
Verify SSL	Enable this parameter for the feed to verify the provider's certificate. The certificate can be found at https://taxii.rstcloud.net/.
Host CA Certificate Bundle	If you enabled the **Verify SSL** configuration field, copy the certificate you obtained from https://taxii.rstcloud.net/ into this field.

RST Threat Feed: Medium Risk Indicators

PARAMETER	DESCRIPTION
What would you like to name this feed	Enter **RST: Threat Feed: Medium Risk Indicators** as the name of the feed.
How ofter would you like to pull new data from this feed	Select the frequency in which the feed it pulled. Options include: ◦ Every Hour ◦ Every6 Hours ◦ Every Day ◦ Every 2 Days ◦ Every 14 Days ◦ Every 30 Days
TAXII Server Version	Select the **2.1** option from the dropdown menu.

PARAMETER	DESCRIPTION
Discovery URL	Enter the Discovery URL: **https://taxii.rstcloud.net/taxii2/**
Poll URL	Enter the URL for medium collection endpoint on the TAXII server to poll for data: https://taxii.rstcloud.net/taxii2/root/collections/98ab279c-a6cc-4efc-9442-87bd8a9b4577
Collection Name/Title	Enter **RST Threat Feed: Medium Risk Indicator**s as the collection name.
Disable Proxies	Leave this option unselected.
Username	Enter your RST Cloud username.
Password	Enter your RST Cloud password.
Verify SSL	Enable this parameter for the feed to verify the provider's certificate. The certificate can be found at https://taxii.rstcloud.net/.
Host CA Certificate Bundle	If you enabled the **Verify SSL** configuration field, copy the certificate you obtained from https://taxii.rstcloud.net/ into this field.

RST Threat Feed: Low Risk Indicators

PARAMETER	DESCRIPTION
What would you like to name this feed	Enter **RST: Threat Feed: Low Risk Indicators** as the name of the feed.
How ofter would you like to pull new data from this feed	Select the frequency in which the feed it pulled. Options include:

PARAMETER	DESCRIPTION
	◦ Every Hour ◦ Every6 Hours ◦ Every Day ◦ Every 2 Days ◦ Every 14 Days ◦ Every 30 Days
TAXII Server Version	Select the **2.1** option from the dropdown menu.
Discovery URL	Enter the Discovery URL: **https://taxii.rstcloud.net/taxii2/**
Poll URL	Enter the URL for medium collection endpoint on the TAXII server to poll for data: https://taxii.rstcloud.net/taxii2/root/collections/b2e8fa09-1389-4fab-be65-ba337b190f92
Collection Name/Title	Enter **RST Threat Feed: Medium Risk Indicator**s as the collection name.
Disable Proxies	Leave this option unselected.
Username	Enter your RST Cloud username.
Password	Enter your RST Cloud password.
Verify SSL	Enable this parameter for the feed to verify the provider's certificate. The certificate can be found at https://taxii.rstcloud.net/.
Host CA Certificate Bundle	If you enabled the **Verify SSL** configuration field, copy the certificate you obtained from https://taxii.rstcloud.net/ into this field.

4. Click on **Add TAXII Feed**.
5. The TAXII feed will now appear as an integration tile card on your My Integrations page using the display name you supplied. You can also click on the **Category** dropdown and select **STIX/ TAXII** to filter your view.
6. Click on the TAXII feed's tile card to open up its details page.
7. Click on the **Enable** toggle switch, located above the *Additional Information* section, to enable the TAXII feed.

Change Log

- **Version 1.0.0**
    - Initial release