ThreatQuotient

Nozomi Networks TI TAXII Feed User Guide

Version 1.0.0

November 21, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Developer Supported

Support

Email: N/A
Web: https://www.nozominetworks.com/support
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: N/A
Support Web: https://www.nozominetworks.com/support
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	2.0.0
Compatible with ThreatQ Versions	>= 5.6.0
Support Tier	Developer Supported
Developer Contact	https://www.nozominetworks.com/support

Introduction

The Nozomi Networks Threat Feed is a data feed of the latest emerging threat data from across the industry that can be used outside or independent of our Guardian and Vantage platforms.

This data feed is comprised of Nozomi Networks' operational technology (OT) Indicators of Compromise (IOCs). The content is hosted on Nozomi Networks Trusted Automated eXchange of Intelligence Information (TAXII) server in the cloud and can be accessed globally.

IOC classes in the feed include malicious URLs, malicious MD5, malicious domains, malicious SHA-1, malicious IP addresses, and malicious SHA-256.

This feed is a TAXII feed and does not require installation files from the ThreatQ Marketplace.

Prerequisites

You will need your Nozomi Networks username and password to set up this TAXII feed in ThreatQ.

Setting up the TAXII Feed

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

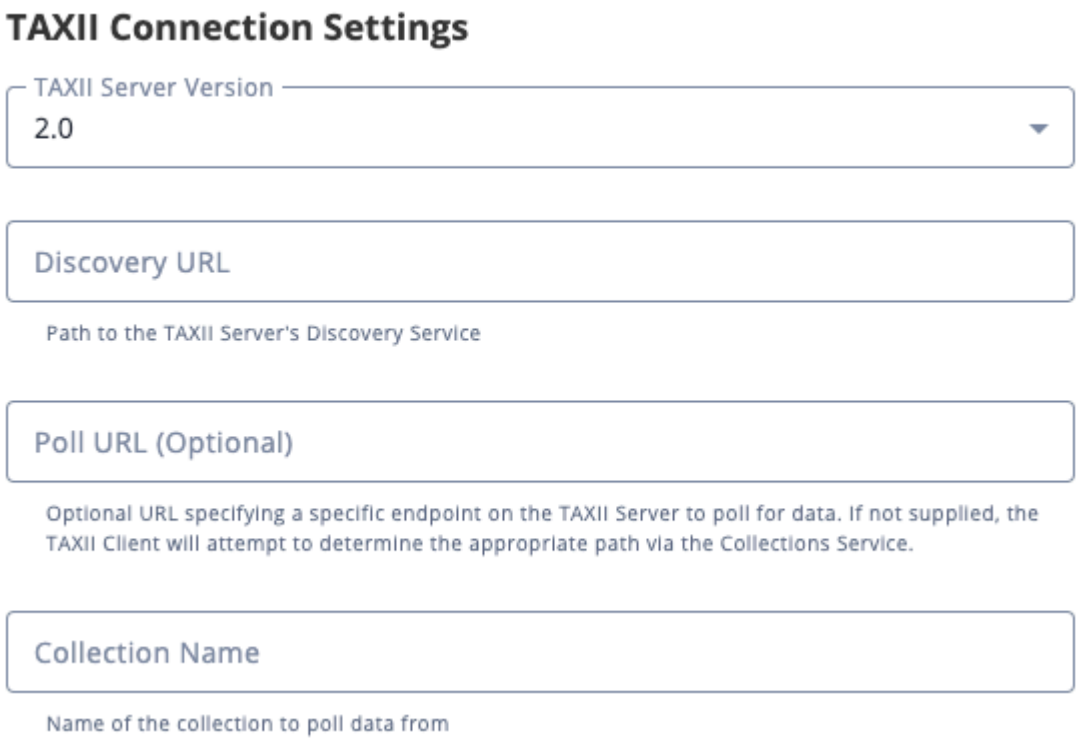
To set up and configure the TAXII feed:

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:

PARAMETER	DESCRIPTION
What would you like to name this feed	Enter the name of the feed. This is the name that the ThreatQ UI will display.
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

4. Enter the **TAXII Connection Settings**:

PARAMETER	DESCRIPTION
TAXII Server Version	Select the **2.0** option from the dropdown menu.
Discovery URL	Enter the Nozomi URL: **https://ti-taxii.nws.nozominetworks.io/taxii/**
Poll URL	Optional - enter a URL for specific entpoint on the TAXII server to poll for data. If this field is left blank, the TAXII client will determine the appropriate path via the Collections Service.
Collection Name	Enter the Nozomi collection name to pull.



5. Leave the **Disable Proxies** setting unchecked.

6. Enter your **Nozomi Login Credentials**:

PARAMETER	DESCRIPTION
Username	Enter your Nozomi username.
Password	Enter your Nozomi password.

7. Leave the **Certificate/Key**s fields blank.
8. Leave the Verify SSL field selected and paste a Host Bundle (if applicable).
9. Click on **Add TAXII Feed**.

   The TAXII feed will now appear as an integration tile card on your My Integrations page using the display name you supplied in step 3. You can also click on the **Category** dropdown and select **STIX/TAXII** to filter your view.
10. Click on the TAXII feed's tile card to open up its details page.
11. Click on the **Enable** toggle switch, located above the *Additional Information* section, to enable the TAXII feed.

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.

Every Day (24 hours)

METRIC	RESULT
Run Time	1 minute
Indicator	1
Indicator Attributes	3
Malware	1
Malware Attributes	2
Signature	1
Signature Attributes	3

Change Log

- **Version 1.0.0**
  - Initial release