

Threat Intelligence Feed Configuration Guide

Legal notices

Information about the Nozomi Networks copyright and use of third-party software in the Nozomi Networks product suite.

Copyright

Copyright © 2013-2025, Nozomi Networks. All rights reserved. Nozomi Networks believes the information it furnishes to be accurate and reliable. However, Nozomi Networks assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of Nozomi Networks except as specifically described by applicable user licenses. Nozomi Networks reserves the right to change specifications at any time without notice.

Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at https://security.nozominetworks.com/licenses.

Contents

Chapter 1. Introduction5
TAXII overview7
Chapter 2. Requirements9
Server information11
Chapter 3. Configuration
taxii2client configuration15
Configure Anomali STAXX16
Configure Microsoft Sentinel
Configure ThreatQ24
Configure QRadar
Chapter 4. Troubleshooting
Error message: HTTP 401 Unauthorized37
Error message: HTTP 404 Not found
Error message: HTTP 406 Not Acceptable
Glossary



Chapter 1. Introduction



TAXII overview

TAXII standardizes the exchange of cyber threat intelligence (CTI) over the internet, enabling organizations to share security threat information more efficiently and effectively. This improves threat detection, analysis, and response.

Trusted Automated Exchange of Indicator Information (TAXII) is a protocol used for the exchange of *cyber threat intelligence (CTI)* over the internet. *TAXII* is designed to support the distribution of *CTI* using a standardized methodology, enabling organizations to share information about security threats more efficiently and effectively.

TAXII is often used in conjunction with Structured Threat Information Expression (STIX), which is a language and serialization format used to exchange CTI. STIX enables organizations to convey the full range of potential threat information, from high-level attack patterns and technical indicators to detailed threat actor profiles and the tactics, techniques, and procedures (TTPs) that they use.

Together, *TAXII* and *STIX* facilitate the automated exchange, processing, and analysis of cyber threat information among various parties, including private sector organizations, government agencies, and other entities involved in cybersecurity defense. This leverages shared knowledge about existing and emerging threats to help improve the speed and accuracy of threat detection, analysis, and response.



Chapter 2. Requirements



Server information

Server information for Trusted Automated Exchange of Indicator Information (TAXII) services, highlighting uniform resource locators (URLs) for discovery and root access, server protocol and Structured Threat Information Expression (STIX) versions, along with collection IDs for threat types such as phishing and ransomware.

Syntax	Description
TAXII Discovery uniform resource locator (URL)	https://ti-taxii.nws.nozominetworks.io/taxii/
TAXII Root URL	https://ti-taxii.nws.nozominetworks.io/root/
Server protocol	TAXII 2.0
STIX version	STIX 2.0

Table 1. Server information

Table 2. Collection IDs

Operational Technology (OT)	thw2k6rf-w130-zaiv-i606-rsm42fk4dwms
Internet of Things (IoT)	aq6odbpq-5tzs-zonm-yr2p-3djab10n5t6k
Phishing	24ml9vt0-vbi4-61td-a8l3-xhuxpwxeccha
Ransomware	sx76qzvj-bx02-vnrn-zsd7-k9fx4g8c2tqg
Hacking Frameworks	56a15872-9565-4f3a-9975-340416369a4d
General (includes indicators from all other collections)	y6bpc38c-bxvz-49ga-y96f-558drdq2x6s4



Chapter 3. Configuration



taxii2client configuration

Learn how to use the minimal Python library from OASIS to set up a **taxii2client** to interact with the TAXII server from Nozomi Networks. This includes integration for software that does not support the TAXII 2.0 protocol.

The **taxii2client** is a minimal Python *TAXII* client from OASIS, which can be used to interact with the Nozomi Networks *TAXII* server. This library is useful if you want to integrate indicators that are pulled from the Nozomi Networks *TAXII* server with software which does not support the *TAXII* 2.0 protocol. For more detailed installation instructions and library documentation, see the OASIS TC Open Repository cti-taxiicclient GitHub repository.

The code snippet below prints all indicator objects from the **Operational Technology (OT)** collection and calculates their total number:

```
from taxii2client.v20 import Collection, as_pages
COLLECTION_ID = 'thw2k6rf-w130-zaiv-i606-rsm42fk4dwms' # OT collection
TAXII_USER = 'REPLACE_WITH_PROVIDED_USERNAME_HERE'
TAXII_PASSWORD = 'REPLACE_WITH_PROVIDED_PASSWORD_HERE'
collection =
    Collection(f"https://
ti-taxii.nws.nozominetworks.io/root/collections/{COLLECTION_ID}/",
    user=TAXII_USER, password=TAXII_PASSWORD)
total_indicators = 0
for page in as_pages(collection.get_objects, per_request=99):
    for o in page['objects']:
        if 'type' in o and o['type'] == 'indicator':
            total_indicators += 1
            print(o)
print(f"total indicators: {total_indicators}")
```

Configure Anomali STAXX

Do this procedure to configure the Anomali STAXX, a free TAXII/STIX solution, for integration with the Nozomi Networks TAXII server, including setting descriptions, uniform resource locators (URLs), and authentication details.

Procedure

- 1. Download Anomali STAXX from the Anomali website.
- 2. To install the downloaded *open virtual appliance (OVA)* file, follow the Anomali instructions.
- 3. Launch Anomali STAXX.
- 4. Select Add New Site.

Result: A dialog shows.

5. In the **Description** field, enter a description.

ADD NEW SITE			8
Description *	Nozomi Networks TAXII		
	Example: Anomali Limo		
Discovery URL*	https://ti-taxii.nws.nozominetworks.io/taxii/		
	Example: https://limo.anomali.com/taxii/		
	Sasic Authentication		
Username *	secresearch@nozominetworks.com		
Password *			
	SSL Two-Way Certificate		
	* is required field		
		Cancel	Add Site

6. In the **Discovery URL** field, enter the **Discovery** URL:

https://ti-taxii.nws.nozominetworks.io/taxii/

- 7. Select the **Basic Authentication** checkbox.
- 8. In the **Username** field, enter your username.
- 9. In the **Password** field, enter your password.
- 10. Do not select the SSL Two-Way Certificate checkbox.

11. Select Add Site.

The site will be added.

12. In the section on the right, select **Discover**.

DETAILS:			۲
Name: Nozomi Networks TAXII		Task State: Pending	
Address: https://ti-taxii.nws.nozominetworks.io/taxii/			
Username: secresearch@nozominetworks.com			
Last Updated:			
TAXII Version: Unknown		Discove	er
Poll Collections Available Collections Scheduled Pushes			
25 🗸			
Feed Name / Description	✓ Last Poll ✓ Last P	oll Observables ~ Enabled ~ Actions	× ø
NO DATA AVAILABLE			

13. Select **Enable** for each item as necessary.

DETAILS:			*
Name: Nozomi Networks TAXII		Task State: Completed	
Address: https://ti-taxii.nws.nozominetworks.io/taxii/		Feed discovery is successful	
Username: secresearch@nozominetworks.com			
Last Updated:			
TAXII Version: 2.0		Discover	
Poll Collections Available Collections Scheduled Pushes			
25 🗸	1 - 5 of 5 items		
Feed Name / Description	✓ Last Poll ✓ Last	t Poll Observables × Enabled × Actions ×	¢
Operational Technology (OT)	N/A N/A	Edit	
Internet of Things (IoT)	N/A N/A	Edit	
Phishing	N/A N/A	Edit	
Ransomware	N/A N/A	Edit	
General	N/A N/A	Edit	

14. To select the time range to poll indicators from, select **Edit** for the applicable collection.

- (CONFIGURE FEED			0		
	Poll Time Range *	7		days		
DET Name Addre	Confidence *	Source Indicator Confide O Weighted Confidence Sco Confidence Score	ence ore		: Completed	
Userr Last L TAXII	Subscription ID Schedule *required field	 Default Custom 			nery is succession	Discover
Poll C	Collections Available Collections S	icheduled Pushes	Cance	Configure Feed		
25	~		1 - 5 of 5 items			
Feed	d Name / Description	~	Last Poll	Last Poll Observables	Enabled	Actions
Ope	rational Technology (OT)		N/A	N/A		Edit
Inte	rnet of Things (IoT)		N/A	N/A		Edit
Phis	hing		N/A	N/A		Edit
Ran	somware		N/A	N/A		Edit Poll Now

In order to receive historical indicators, this value should be high for the initial poll. You can then decrease it based on how often the server will be polled. For example, if polling daily, only poll for indicators that have been added within the last 24 hours.

	CONFIGURE FEED			٥		
	Poll Time Range *	1825	۵	days		
DET Name Addre Userr	Confidence * Subscription ID	Source Indicator Confide Weighted Confidence Sco Confidence Score	nce ore		: Completed wery is successful	
Last L TAXII	Schedule *required field	 Default Custom 	Cancel	Configure Feed		Discover
Poll C	ollections Available Collections S	icheduled Pushes				
25 🗸	<u> </u>		1 - 5 of 5 items			
Feed	Name / Description	~	Last Poll ~	Last Poll Observables	~ Enabled ~	Actions
Oper	rational Technology (OT)		N/A	N/A		Edit
Inter	net of Things (IoT)		N/A	N/A		Edit

15. To poll indicators, select **Poll Now**.

DETAILS:							۲
Name: Nozomi Networks TAXII Address: https://ti-taxii.nws.nozominetworks.io/taxii/			Task State: C Feed discove	ompleted ry is success	ful		
Username: secresearch@nozominetworks.com Last Updated: TAXII Version: 2.0						Discover	
Poll Collections Available Collections Scheduled Pushes							
25 🗸	1 - 5 of 5 items						
Feed Name / Description	✓ Last Poll	✓ Last Poll	Observables 🗸 🗸	Enabled	~ Actions		× ¢
Ransomware	N/A	N/A			Edit	Poll Now	
Operational Technology (OT)	N/A	N/A			Edit	true	
Internet of Things (IoT)	N/A	N/A			Edit		
Phishing	N/A	N/A			Edit		
General	N/A	N/A			Edit		

Note:

This can take some minutes depending on how large a collection is.

Once this process completes, the number of **Last Poll Observables** will show a value.

DETAILS:	۲
Name: Nozomi Networks TAXII	Task State: Completed
Address: https://ti-taxii.nws.nozominetworks.io/taxii/	
Username: secresearch@nozominetworks.com	
Last Updated:	
TAXII Version: 2.0	Discover
Poll Collections Available Collections Scheduled Pushes	
25 🗸 1 - 5 of 5 items	
API Root × Feed Name / Description × Last Poll × Last Pol	I Observables V Enabled V Actions V
root Ransomware 2023-8-18 14:26:56 1391	Edit Poll Now
root Operational Technology (OT) N/A N/A	Edit
root Internet of Things (IoT) N/A N/A	Edit
root Phishing N/A N/A	Edit
root General N/A N/A	Edit

Results

The indicators can be accessed from the **Dashboard** menu.



Configure Microsoft Sentinel

Once the Threat Intelligence - TAXII data connector is installed, you need to configure the TAXII server.

About this task

Microsoft Sentinel is a cloud-native security information and event management *(SIEM)* solution that provides intelligent security analytics. **Microsoft Sentinel** can interact with *TAXII* servers using the Threat Intelligence - TAXII data connector. For more details on Microsoft TAXII configuration, see the Microsoft documentation.

Procedure

- 1. Open Microsoft Sentinel.
- 2. Select the Threat Intelligence TAXII data connector for Microsoft Sentinel.
- 3. In the bottom right section, select **Open connector page**.



The connector settings for **Microsoft Sentinel** show.

4. Use the <code>/root/</code> endpoint to add each collection individually for $\ensuremath{\text{Microsoft}}$

Sentinel.

Configuration	
Configure TAXII convers to stream STIX 2.0 or 2.1 th	reat indicators to Microsoft Sentinel
You can connect your TAXII servers to Microsoft Sent	inel using the built-in TAXII connector. For detailed configuration instructions, see the full document
Enter the following information and select Add to co	ifigure your TAXII server.
Friendly name (for server) *	
Nozomi_Networks_TAXII	
API root URL *	
https://ti-taxii.nws.nozominetworks.io/root/	
Collection ID *	
aq6odbpq-5tzs-zonm-yr2p-3djab10n5t6k	
Username	
secresearch@nozominetworks.com	
Password	
•••••	
Import indicators:	
All available	\sim
Polling frequency	
Once an hour	V

Note:

Add

Make sure that you use the /root/ endpoint instead of the discovery endpoint /taxii/.

5. To verify that the operation was successful, make sure that you can see a message on the right.

	TAXN connector added XAXN connector "XAXNProdPhiling" has been added uscessifully for APR loca UB, "https://i- taliman.anterimetworkia.(https://i- taliman.anterimetworkia.enterimetworkia.enterimetworkia.enterimetworkia.enterimetworkia.enterimetworkia.enterimetworkia.enterimetworkia.enterimetworkia.enterimetworkia.enterimetworkia.enterimetworkia.enterimetworkia.enterimetworkia.enteri
Induction	
TAXE Server: TAXE 2.0 or TAXE 2.1 Server UR and Callection ID.	
Configuration	
Configure TAXII servers to stream STX 2.0 or 2.1 threat indicators to Microsoft Sentinel	
You can connect your TAXII servers to Microsoft Sentinel using the built-in TAXII connector. For detailed configuration instructions, see the full documentation.	
Enter the following information and select Add to configure your TAXB server.	
Friendly name (for saver) *	
API root URL *	
Collection ID *	
Usenane	
Passood	
Import indicators:	
R most one day old v	
Poling frequency	
Once an hour V	
Add	
List of configured TAXII servers	
0 Seach	

You can now access the indicators from the **Threat Intelligence** page.

Но	me > Microsoft Sentinel > Microsoft Sentin	el								
»	Microsoft Sentinel Selected workspace: "taxii"	Threat intellige	ence							×
	🔎 Search	🖒 Refresh 🕂 Add r	new Import 🗸 🔞 /	Add tags 📋 Delete	e 📑 Columns	Threat intelligence workbo	ook 🛛 🔗 Guides & Fe	edback		
	r Logs	~ ~								
	News & guides	U O								
	Search	Tuero	T Indicators	in sources						
	Threat management	Search by name, value	ues, description or tags	Type : All	Source : All	Threat Type : All	V More (2)	Malicious U	RL - http://1	15.60.225.73:41972/i
	Incidents	D Norma Av	Velues		T	6 A	Confidence Av		0	al url
	Workbooks	Name ⊤↓	Values		Types	Source TU	Confidence TJ	Confidence	Alerts ①	Types
	Hunting	Malicious URL - htt	p://115.6 http://115.60.22	25.73:41972/i	🔗 url	TAXIIProdIOT				
	Notebooks	Malicious URL - htt	p://61.52 http://61.52.138	8.124:60518/i	🔗 url	TAXIIProdIOT		Values url :		
	Entity behavior	Malicious URL - htt	p://121.2 http://121.206.3	7.228:37828/Mozi.m	🔗 url	TAXIIProdIOT		http://115.60.22	5.73:41972/i	
	Threat intelligence	Malicious URL - htt	p://115.5 http://115.56.14	7.95:48467/bin.sh	🔗 url	TAXIIProdIOT		Tags		Threat types
	MITTE ATTR/CK (Dreavieux)	Malicious URL - htt	p://112.2 http://112.248.1	90.229:50632/bin.sh	🔗 url	TAXIIProdIOT		+		malicious-activity
	- Minte Arrace (Terren)	Malicious URL - htt	p://58.25 http://58.252.18	3.94:56247/Mozi.m	🖉 url	TAXIIProdIOT				
	Content management	Malicious URL - htt	p://108.7 http://108.70.55	.129:39206/Mozi.a	🤗 url	TAXIIProdIOT		Description		Name
	Content hub	Malicious URL - htt	p://182.1 http://182.120.5	7.226:34651/i	🔗 url	TAXIIProdIOT		Malicious URL inv Trojan	volved with	Malicious URL - http://115.60.225.73:41972/i
	 Repositories (Preview) 	Malicious URL - htt	p://61.3.9 http://61.3.97.2	1:59893/Mozi.m	🔗 url	TAXIIProdIOT				
	Community	Malicious LIRL + htt	n://119.1 http://119.186.2	205 42:38168/bin sh	a url	TAXIIProdiOT		Revoked		Confidence
	Configuration	Malicious URL htt	p;//117.2 http://117.201.1	09 E1/E2642/Mari m	and and	TAXIIPredIOT				
	A Workspace manager (Preview)	Mancious URL - htt	p.//11/.2 http://11/.201.1	190.31.33042/MOZI.M		TAXIPTODIOT		Source		Pattern
	Dete connector	Malicious URL - htt	p://101.1 nttp://101.108.1	101.108:50621/Moz	or un	TAXIIProdIOT		TOIborNIXAL		[urr:value = 'http://115.60.225.73:41972/i']
		Malicious URL - htt	p://123.1 http://123.14.11	2.31:45671/Mozi.m	♂ url	TAXIIProdIOT				

Results

Microsoft Sentinel has now been configured.

Configure ThreatQ

Follow these steps to add and enable a new TAXII feed integration in ThreatQ, verify indicator ingestion, and monitor the integration's status through the Activity Log.

Procedure

- 1. Open ThreatQ.
- 2. Go to Integrations > My Integrations.

THREATQ 🍞	네 Dashboards	🛍 Threat Library	▲ Investigations	ਡੰਡ Data Exchange	습 Integrations	+ Create	Q I		0 4	z 🖂
Overview Overview	of Intelligend	ce by Score			Marketplace My Integrations Actions My Integrations Intelligence Feeds & Connectors Operations Matchlist Activity		Ë Sine	Ce Yes		
VERY HIGH				0% (0)						
HIGH	•			0% (0)	You currently don't have any ite	ns on your watchlist.				
MEDIUM	•			0% (0)						
LOW	•			0% (0)	⊘ Tasks	Му Ор	en Tasks (0)	All O	pen Task	s (0)
VERY LOW	P			0% (0)						
NOT SCORED				0% (0)	ID • NAME ÷ ASSIGNED TO ÷	DUE DATE 🗢		STATUS		
🐼 Incoming I	Intelligence									
Before you can view Inco	oming Intelligence, you n	nust configure one or more a	tive feeds.							
https://3.79.17.127/integrations										

3. In the top right section, select Add New Integration.

THREATQ 🎅	네 Dashboards	🚻 Threat Library	▲ Investigations	🖧 Data Exchange			+ Create	۹	¢ (?	•	Ad
	My Integratio	ıs				Go To Marketplace	O Add New Int	egration			
	Q Start typing All (4) Enabled (4)	Disabled (0)				Type All	▼ Clear	Search Filter	rs		
	GreyNoise Communit	y 🌣	IPinfo Action	۵	Shodan Action	VirusTotal		٥			
	Version: 1.0.1	Enabled	Version: 1.0.1	Enabled	Version: 1.0.1	Enabled Version: 1.0.1	(Enabled			

Result: A dialog shows.

4. Select Add New TAXII Feed.

- What woul Nozomi T	d you like Feed	to name this feed? ———————————————————————————————————
- How often Every Day	would you	u like to pull new data from this feed? ———————————————————————————————————
Discovery	 JRL	
Discovery	JRL	nozominetworks.io/taxii/
Path to the	TAXII Server	r's Discovery Service
Poll URL (Optional	l)
		g a specific endpoint on the TAXII Server to poll for data. If not supplied, the
Optional UF TAXII Client	will attempt	t to determine the appropriate path via the Collections Service.
Optional UF TAXII Client - Collection	will attempt	t to determine the appropriate path via the Collections Service.

5. Enter the details in each field.



Do not use Collection *identifier (ID)*s, use Collection names.

6. Select Add TAXII Feed.

7. In the **My Integrations** page, select the integration that you just created.

THREATQ 🍞	네 Dashboards	🛍 Threat Library	▲ Investigations	ਡੋਡ Data Exchange	∑ Integrations		+ Create Q	۰	o 🌣	•
1	My Integratior	IS				Go To Marketplace	Add New Integration			
[Q Start typing					Type All	▼ Category All	•		
-	All (5) Enabled (4)	Disabled (1)					T Clear Search Filte	rs		
	GreyNoise Community	\$	IPinfo Action	\$	Nozomi TI Feed	Shodan	¢			
	Version: 1.0.1	Enabled	Version: 1.0.1	Enabled	Category: STD/TAXII Version: 2.0	Version: 1.0.1	Enabled			
	VirusTotal Action	۵								
	Version: 1.0.1	Enabled								

8. In the top left section, select the toggle to **Enabled**.

_	Configuration Activity Log
53	
7 7	TAXII Server Version
	2.0
	The version of the TAXII Server to poll for data.
	Discovery Path URL
Disabled C Enabled	https://ti-taxii.nws.nozominetworks.io/taxii/
Run Integration	Path to the TAXII Server's Discovery Service
	Poll URI (Ontional)
Uninstall	Optional URL specific endpoint on the TAXII Server to poil for data. If not supplied, the TAXII Client will attempt to determine the
Additional Information	appropriate path via the Collections Service.
Integration Type: Feed	Collection Name
Version: 2.0	
Accepted Data Types:	Name of the collection to poll data from
	Disable Proxies If true, specifies that this feed should not honor any provies setup in ThreatQuotient.
	Cusername
	nozominetworks
	Basic Authentication Username
	Password
	Basic Authentication Password
	Client Certificate
	Client Certificate for authentication with the TAYII Server
	Chent Rey
	Private Key for authentication with the TAXII Server.
	✓ Verify SSL
	Specifies whether the TAXII client should verify a provider's SSL certificate
	Host CA Certificate Bundie
	Used to specify a provider's CA Certificate Bundle to verify SSL against. This denotes that Verify SSL is True.
	- Set indicator status to
	Active
	Run Frequency
	Every 30 Days Next scheduled run: 2023-10-20 11:12am (+02:00)
	I Send a notification when this feed encounters issues.
	Debug Option: save the raw data response files. We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.
	Save

- 9. Select Save.
- 10. Select Activity Log.

11. In the **Activity Log Details** section, make sure that the first manual, or scheduled, run shows as **Completed**.

THREATQ 🌛 🔟 Dashboards 🛍 Thi	reat Library 🗛 Investigations	중 Data Exchange	S Integrations	+ Create	۹	<u></u>	0	\$
< Nozomi Tl Feed								
ப	Configuration Activity Lo	Activity Log			Ø			
	Manual Run 09/14/2023 10:55am			Completed	•			
Disabled Disabled Run Integration	Manual Run 09/14/2023 09:38am			✓ Completed	•			
Uninstall	Scheduled Run 09/14/2023 09:38am			✓ Completed	•			

12. Make sure that the indicators have been ingested correctly.

THREAT (?) 🕑 🗠 Dashboards 🗰 Threat Library	🗛 Investigations 🔗 Data Exchange 🏠 Integrations	🕂 Create 🔍 🌲 🛞 🛤
< Nozomi Tl Feed		
ப	Configuration Activity Log Activity Log Details	c k
Disabled C Enabled Ruin Integration Uninstall	Scheduled Run 69/02/223 09/12am Data Requested Run Started 09/02/023 09/12am © Response Received 09/02/023 09/34am	Completed
Additional Information Integration Type: Feed Version: 2.0 Accepted Data Types:	Query Range 08/21/2023 09:12am to 09/20/2023 09:12am Deveload of files Password: threato Deveload Pres	Ingestion Summary 1 Identity 2 Identity Attributes 2 Identity Attributes 78784 Indicator Attributes 10 Malware 2 334 Malware Attributes 2 25465 Signatures 78205 Signature Attributes

Results

ThreatQ has been configured.

Configure QRadar

Do this procedure to integrate a new TAXII feed into QRadar to enhance threat intelligence capabilities. This procedure covers adding the feed, ensuring full indicator ingestion, and monitoring the integration via the Activity Log for optimal security posture.

About this task

Note:

The Threat Intelligence application version 2.4.2, and earlier, has a bug that can lead to only partial ingestion of the TAXII data. IBM is aware of the bug.

Procedure

- 1. Download QRadar from the IBM website.
- 2. Go to Admin > Extensions Management.



3. Select All items.

4. Make sure that you have the latest version of the Threat Intelligence app installed.

insions management	Search by extension name	Q		IBM Security App Exchang
LITEMS INSTALLED NOT INSTALLED				Add
1e		Status	Author	Added On 👻
Threat Intelligence – QRadar v7.3.3 F	× P9+/7.4.1 FP2+ my threat intelligence feed using the	Installed	IBM QRadar	August 23, 2023
open standard STIX and TAXII formats, and to deploy to correlation, searching, and reporting. For example, you collections of dangerous IP addresses from IBM X-For- raise the magnitude of any offense that includes IP add Uninstall Contents: Contents: Contents: Reference Data Collections (51)	he data to create custom rules for can use the App to import public te Exchange and create a rule to resses from that watch list.			

5. Select Threat Intelligence.

	BM QRadar	l p. Y														(Ċ	<u> </u>
Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vuherabilities	Admin	Pulse	Use Case Manager	Nozomi Networks Vantage	Threat Intelligence				Syste	em Time: 8	57 AM
												License: Free Tier	Expiration Date: N/A		Feeds Do	wnloader	0	
														4				
	Re	ecent (Collectic	ons	View Mo	re												

- 6. Select Feeds Downloader.
- 7. Select Add Threat Feed > Add TAXII Feed.

	IBM QRadar	Ų.															(III.	Ċ	<u> </u>
Dashboar	Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Nozomi Networks Vantage	Threat Intelligence					Sys	tem Time:	8:58 AM
												License: Free Tier	Expiration Date: N/A	=	1	17	¢		l
	Threat	Feed	s Down	load	er														
		reat Feed	- 🛃 Create	e Rule Ac	tion -														
		XII Figed uration	hreat Inte	lligenc	e Fee	ds (4)													

8. In the **Connection** page, in the **Version** dropdown, select **TAXII 2.0**.

	IBM QRadar	ļ.															(II)	Ċ º
Dashboar	d Offenses	Log Activity	Network	Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Nozomi Netv	vorks Vantage	Threat Intelligence			Syn	stern Time: 9.01 AM
				Add 1		eed												0
	Threat	Feed	s D													^		
				Conr	nection													
				ТАХ	II Endpo	int	https://	ti-taxii.nws.no.	ominetwo	rks.io/roo	t/collections			Version	TAXII 2.0 🗸			-
	Client Certifica Client Key No Collection y6I	https://te None opc38c-bxvz-4	ti-taxi 19ga-y9	Auth Meti	ienticati hod	on		Basic							~	2023, 12:52:38 P) mins		
			iPs	Use	rname	nozomir	ietworks				Pas	sword				F		-
				If you	i need to a	add a Cli	ent Certifica	ite, please upl	oad the PE	M file be	low.	Kev				2023, 12:14:28 P) mins		
					Choose fil	8					Ch	oose file				F		
																2023, 12:21:31 P		1
		pc38c-bxvz- pe AddressO Anonymizer	19ga-y9 bjectTyr IPs											Discover Q	Cancel ⊗	- F		
		ne 🚍 🧿													Poll Inter		4∎ 12 ,	1:02 PM

- 9. Enter the details as necessary in the other fields. Make sure the endpoint string has /root/collections at the end.
- 10. Select **Discover**.
- 11. Select Parameter.
- 12. From the **Collections** dropdown, select the applicable option.

:=,,	IBM QRadar	2															(Ļ	<u> </u>
Dashboa	rd Offenses	Log Activity	Network	Activity As	isets Repo	rts Risks	Vulnerabilities	Admin	Pulse	Use Case	e Manager	Nozomi Netwo	nks Vantage	Threat Intelligence				ystem Time:	9:13 AM
	Threat	Feed	s D	Add TA	XII Feed	Paramet	er	Summar								· •			
				Colle	ections	Hacking	- rameworks				Obse Type	rvable	IPv4 Add	Iress					
				Polli Inter	ng vals	Daily					Poll I	nitial Date	3 months	ago					
	. () N			Refe	rence Set	Anonymi	ter IPs						agement 📑		Add +				
				Endpoi Collect Observ Poll Ini Polling Refere	int https://ti- tion 56a158 rable Type tial Date V Interval 1 nce Set An	taxii.nws.nozo 72-9565-4f3a AddressObjec /ed, 14 Jun 20 440minutes onymizer IPs	minetworks.io/ 9975-3404163 tType:ipv4-adc 23 13:14:25 G	root/collectio 69a4d Ir MT	ons							✓ of 1 p			
	() N																		
				Items	per page:	3 ~ 1-1	of 1 items								of 1 page 🕢 🕨	✓of 1 p			
													Previou	is ← Next	→ Cancel ⊗	¥	k		

- 13. From the **Observable Type** dropdown, select the applicable indicator type.
- 14. To the right of **Reference Set Management**, select **Add**.
- 15. In the bottom right section, select Next.

16. In the **Summary** page, select **Save**.

Deabloard Otherwise Log Adulty Needer Market Register Register Name Register Name Register Name Register Name Register Name Register Register </th <th>م</th> <th>stem Time:</th> <th>9:14 AM</th>	م	stem Time:	9:14 AM
Add TAXII Feed Add Threat Feeds D			
Politing Interval 1400minutes References Set Anommere IPs Items per page: 5 v 1-1 of 1 tems 1 v of 1 page 4 >			
Weite per page: 5 v 0-0 v of 1			

17. You can now select **Poll Now** to force the indicator collection.

IE	M QRadar															(III)	Ļ	<u>o</u>
board	Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Nozomi Networks Var	ntage Threat Intelligence					System Ti	me: 9:14 AM
												License: Free Tier	Expiration Date: N/A	= 8	Ū	76	9 ()	
Т	hreat	Feed	s Down	load	er													
		eat Feed	-	e Rule A	ction 👻													
	 Confi 	gured T	hreat Inte	lligend	e Fee	ds (1)												
		https://t	ti-taxii.nws.	nozom	inetwo	rks.io/ro	oot/colled	ctions							4	1 🖉 i	Ū	
	lient Certificati lient Key Nor ollection 56a	None ne 15872-9565-	413a-9975-34041	16369a4d							27	1 27	Last Poll 9/ Poll Interval	14/2023, 1:15 1440 mins	:14 PM			
	bservable Typ	AddressOl	bjectType:ipv4-ac	dr						Signatures re	ceived last poll	Total signatures receiv	ed					
	eterence Set	Anonymizer	IPS															
	ltems per pa	ge: 5 🗸	1-1 of 1 item	is										1 ∨ of	1 page	•	•	

Results

QRadar has been configured.



Chapter 4. Troubleshooting



Error message: HTTP 401 Unauthorized

Possible cause

This error will show if the incorrect credentials were used.

Procedure

Make sure that the user is using the correct credentials that were provided to them.

If none of the previous solutions work, please contact our Customer Support team.

Error message: HTTP 404 Not found

Possible cause

The incorrect discovery, or root, URL has been used.

Procedure

Make sure that the discovery URL used in the configuration is correct.

Procedure

Make sure that the root URL used in the configuration is correct.

If none of the previous solutions work, please contact our Customer Support team.

Error message: HTTP 406 Not Acceptable

Possible cause

This error will show if the client sent a *hypertext transfer protocol (HTTP)* header, which the server cannot accept. The expected header can be found in the official TAXII 2.0 specification. This might happen if the client is not correctly configured to use TAXII 2.0 as its protocol, and instead uses TAXII 1.x or TAXII 2.1.

Procedure

- 1. Make sure that you specify that the server is TAXII 2.0.
- 2. If this does not solve the problem, contact our Customer Support team with this information:
 - $^{\circ}$ The name of the client
 - The version of the client
 - All logs that you can export
 - A timestamp of when the error occurred

Note:

This information will be extremely valuable for further debugging.

Glossary



Cyber threat intelligence

CTI collects and analyzes information on cyber threats and vulnerabilities, providing insights for organizations to proactively understand, prevent, and mitigate cyberattacks. To do this, it learns about the tactics, techniques, and procedures of attackers.

Hypertext Transfer Protocol

HTTP is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

Identifier

A label that identifies the related item.

Internet of Things

The IoT describes devices that connect and exchange information through the internet or other communication devices.

Open Virtual Appliance

An OVA file is an open virtualization format (OVF) directory that is saved as an archive using the .tar archiving format. It contains files for distribution of software that runs on a virtual machine. An OVA package contains a .ovf descriptor file, certificate files, an optional .mf file along with other related files.

Operational Technology

OT is the software and hardware that controls and/ or monitors industrial assets, devices and processes.

Security Information and Event Management

SIEM is a field within the computer security industry, where software products and services combine security event management (SEM) and security information management (SIM). SIEMs provide real-time analysis of security alerts.

Structured Threat Information Expression

STIX[™] is a language and serialization format for the exchange of cyber threat intelligence (CTI). STIX is free and open source.

Tactics, techniques, and procedures

TTPs are the patterns of behavior that describe how cyber adversaries operate, encompassing their strategies (tactics), tools and methods (techniques), and specific procedures for executing attacks. Understanding TTPs aids in predicting and defending against future cyber threats.

Trusted Automated Exchange of Indicator Information

TAXII is a protocol for the exchange of cyber threat intelligence (CTI) online. It is often used with Structured Threat Information Expression (STIX) to share detailed threat information.

Uniform Resource Locator

An URL is a reference to a resource on the web that gives its location on a computer network and a mechanism to retrieving it.

