



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 © 2013-2024, 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. Introduction.....	5
TAXII overview.....	7
Chapter 2. Requirements.....	9
Server information.....	11
Chapter 3. Configuration.....	13
taxii2client configuration.....	15
Configure Anomali STAXX.....	16
Configure Microsoft Sentinel.....	21
Configure ThreatQ.....	24
Configure QRadar.....	30
Chapter 4. Troubleshooting.....	35
Error message: HTTP 401 Unauthorized.....	37
Error message: HTTP 404 Not found.....	37
Error message: HTTP 406 Not Acceptable.....	38
Glossary.....	39



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.

Table 1. Server information

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

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-a813-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-taxii-client 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

Description * Nozomi Networks TAXII
Example: Anomali Limo

Discovery URL * https://ti-taxii.nws.nozominetworks.io/taxii/
Example: https://limo.anomali.com/taxii/

☒ Basic 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:

Name: Nozomi Networks TAXII
Address: https://ti-taxii.nws.nozominetworks.io/taxii/
Username: secresearch@nozominetworks.com
Last Updated:
TAXII Version: Unknown

Task State: Pending

Discover

Poll Collections

Available Collections

Scheduled Pushes

25

Feed Name / DescriptionLast PollLast Poll ObservablesEnabledActions

NO DATA AVAILABLE

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

DETAILS:

Name: Nozomi Networks TAXII
Address: https://ti-taxii.nws.nozominetworks.io/taxii/
Username: secresearch@nozominetworks.com
Last Updated:
TAXII Version: 2.0

Task State: Completed
Feed discovery is successful

Discover

Poll Collections

Available Collections

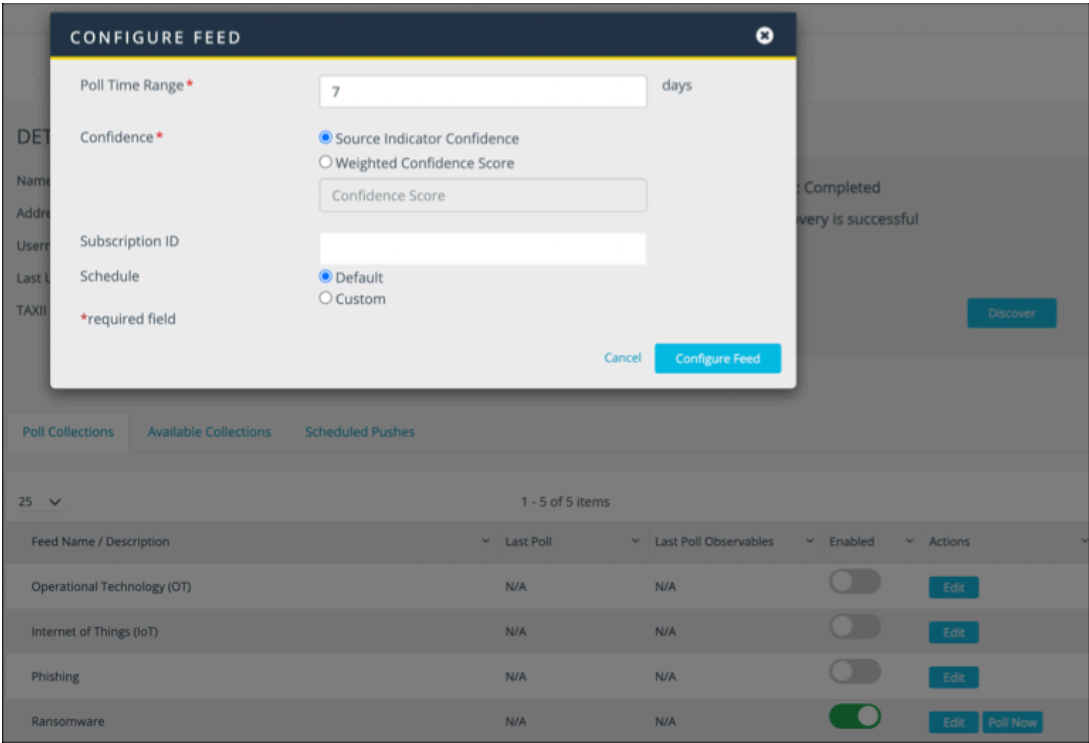
Scheduled Pushes

25

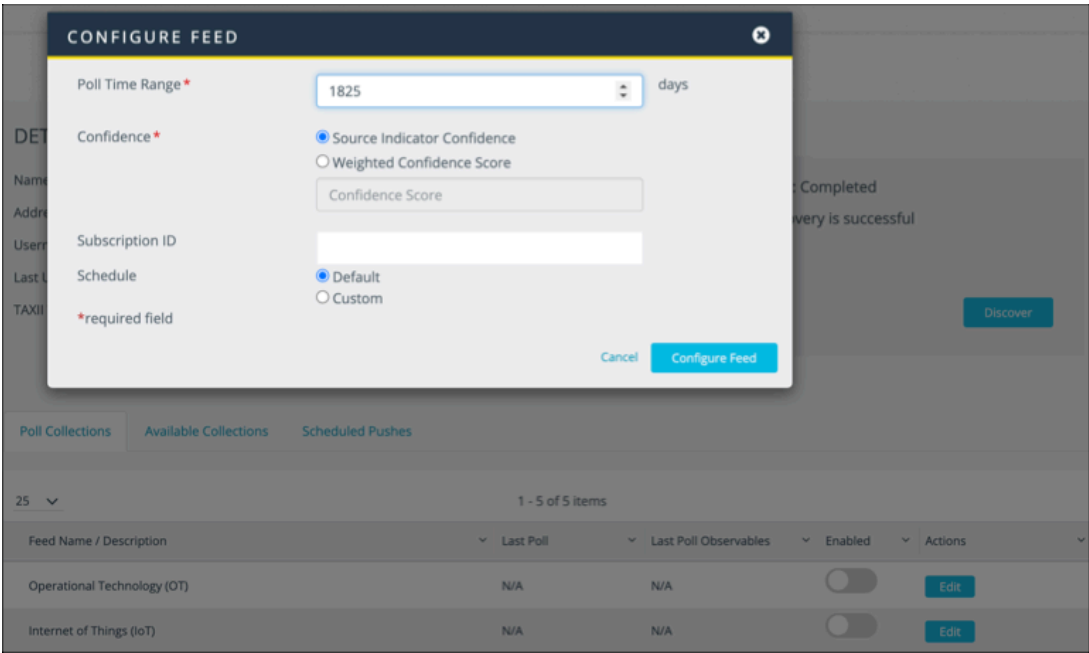
1 - 5 of 5 items

Feed Name / Description	Last Poll	Last Poll Observables	Enabled	Actions
Operational Technology (OT)	N/A	N/A	<input type="checkbox"/>	Edit
Internet of Things (IoT)	N/A	N/A	<input type="checkbox"/>	Edit
Phishing	N/A	N/A	<input type="checkbox"/>	Edit
Ransomware	N/A	N/A	<input type="checkbox"/>	Edit
General	N/A	N/A	<input type="checkbox"/>	Edit

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



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.



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

DETAILS:

Name: Nozomi Networks TAXII
Address: https://ti-taxii.nws.nozominetworks.io/taxii/
Username: secresearch@nozominetworks.com
Last Updated:
TAXII Version: 2.0

Task State: Completed
Feed discovery is successful

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	<input checked="" type="checkbox"/>	<div>Edit</div> <div>Poll Now</div>
Operational Technology (OT)	N/A	N/A	<input type="checkbox"/>	<div>Edit</div> <div>true</div>
Internet of Things (IoT)	N/A	N/A	<input type="checkbox"/>	<div>Edit</div>
Phishing	N/A	N/A	<input type="checkbox"/>	<div>Edit</div>
General	N/A	N/A	<input type="checkbox"/>	<div>Edit</div>

**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:

Name: Nozomi Networks TAXII
Address: https://ti-taxii.nws.nozominetworks.io/taxii/
Username: secresearch@nozominetworks.com
Last Updated:
TAXII Version: 2.0

Task State: Completed

Discover

Poll Collections

Available Collections

Scheduled Pushes

25

1 - 5 of 5 items

API Root	Feed Name / Description	Last Poll	Last Poll Observables	Enabled	Actions
root	Ransomware	2023-8-18 14:26:56	1391	<input checked="" type="checkbox"/>	<div>Edit</div> <div>Poll Now</div>
root	Operational Technology (OT)	N/A	N/A	<input type="checkbox"/>	<div>Edit</div>
root	Internet of Things (IoT)	N/A	N/A	<input type="checkbox"/>	<div>Edit</div>
root	Phishing	N/A	N/A	<input type="checkbox"/>	<div>Edit</div>
root	General	N/A	N/A	<input type="checkbox"/>	<div>Edit</div>

Results

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



Configure Microsoft Sentinel

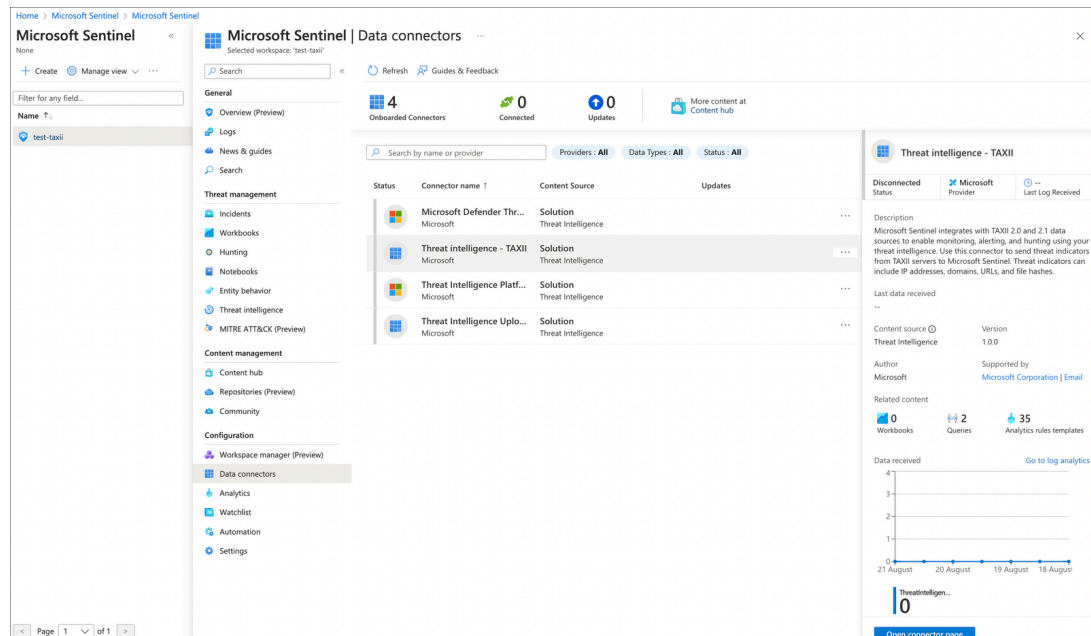
Once the Threat Intelligence - TAXII data connector is installed, you need to configure the TAXII server.

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 `/root/` endpoint to add each collection individually for **Microsoft Sentinel**.

**Configuration**

Configure TAXII servers to stream STIX 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 TAXII server.

Friendly name (for server) *

API root URL *

Collection ID *

Username

Password

Import indicators:

Polling frequency

Add

**Note:**

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

TAXII connector added
TAXII connector "TAXIIProdIoT" has been added successfully for API Root URL: <https://115.60.225.73:41972/i> and Collection ID: 24e3b3d5-4b41-4761-a833-0b9a9a9a9a9a

Instructions
TAXII Server: TAXII 2.0 or TAXII 2.1 Server URL and Collection ID.

Configuration
Configure TAXII servers to stream STIX 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 TAXII server:

Friendly name (for server) *

API root URL *

Collection ID *

Username

Password

Import indicators:
As most one day old

Polling frequency:
Once an hour

Add

List of configured TAXII servers

Search

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

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Threat intelligence

Selected workspace: 'taxii'

Search

Refresh + Add new Import Add tags Delete Columns Threat intelligence workbook Guides & Feedback

0 TI alerts 95.3K TI indicators 3 TI sources

Search by name, values, description or tags Type: All Source: All Threat Type: All More (2)

Name	Values	Types	Source	Confidence
Malicious URL - http://115.6...	http://115.60.225.73:41972/i	url	TAXIIProdIoT	--
Malicious URL - http://61.52...	http://61.52.138.124:60518/i	url	TAXIIProdIoT	--
Malicious URL - http://121.2...	http://121.206.37.228:37828/Mozi.m	url	TAXIIProdIoT	--
Malicious URL - http://115.5...	http://115.56.147.95:48467/bin.sh	url	TAXIIProdIoT	--
Malicious URL - http://112.2...	http://112.248.190.229:50632/bin.sh	url	TAXIIProdIoT	--
Malicious URL - http://58.25...	http://58.252.183.94:56247/Mozi.m	url	TAXIIProdIoT	--
Malicious URL - http://108.7...	http://108.70.55.129:39206/Mozi.a	url	TAXIIProdIoT	--
Malicious URL - http://182.1...	http://182.120.57.226:34651/i	url	TAXIIProdIoT	--
Malicious URL - http://61.3.9...	http://61.3.97.21:59893/Mozi.m	url	TAXIIProdIoT	--
Malicious URL - http://119.1...	http://119.186.205.42:38168/bin.sh	url	TAXIIProdIoT	--
Malicious URL - http://117.2...	http://117.201.198.51:53642/Mozi.m	url	TAXIIProdIoT	--
Malicious URL - http://101.1...	http://101.108.101.168:56621/Moz...	url	TAXIIProdIoT	--
Malicious URL - http://123.1...	http://123.14.112.31:45671/Mozi.m	url	TAXIIProdIoT	--

Malicious URL - http://115.60.225.73:41972/i

Confidence Alerts url Types

Values
url :
http://115.60.225.73:41972/i

Tags Threat types
malicious-activity

Description
Malicious URL involved with Trojan

Revoked Confidence
--

Source
TAXIIProdIoT

Pattern
[url:value =
"http://115.60.225.73:41972/i"]

Results

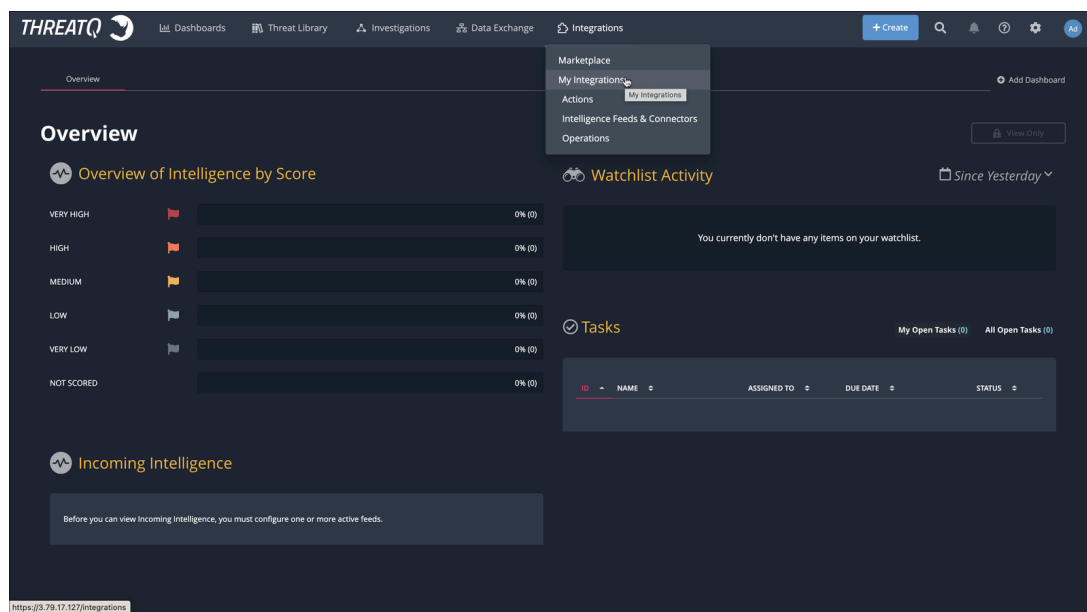
Microsoft Sentinel has now been configured.

Configure ThreatQ

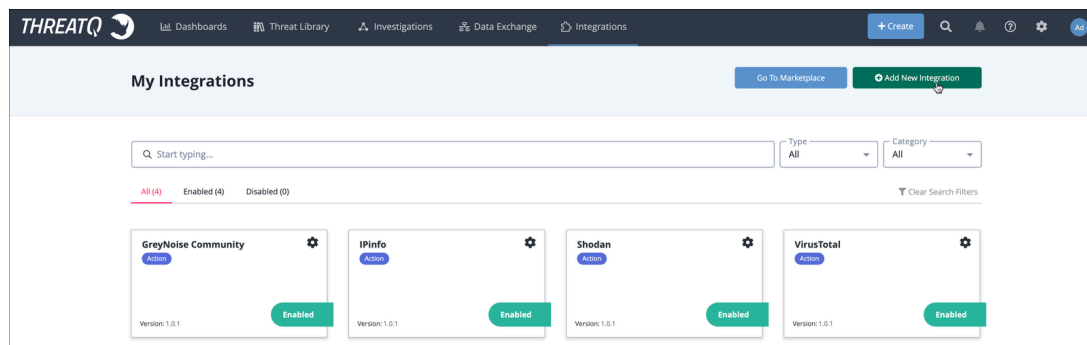
Follow these steps to add and enable a new TAXII feed integration in ThreatQ, verify indicator ingestion, and monitor the integration's status through the Activity Log.

Procedure

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



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



Result: A dialog shows.

4. Select **Add New TAXII Feed**.

Add New Integration ✕

Add New Integration **Add New TAXII Feed**

What would you like to name this feed?

How often would you like to pull new data from this feed?

TAXII Connection Settings

TAXII Server Version

Discovery URL

Path to the TAXII Server's Discovery Service

Poll URL (Optional)

Optional URL specifying a specific endpoint on the TAXII Server to poll for data. If not supplied, the TAXII Client will attempt to determine the appropriate path via the Collections Service.

Collection Name

Name of the collection to poll data from

☐ **Disable Proxies**

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

5. Enter the details in each field.

Login Credentials (if applicable)

Username

nozominetworks

Basic Authentication Username

Password

.....

Basic Authentication Password

Certificates/Keys (if applicable)

Certificate

Client Certificate for authentication with the TAXII Server.

Private Key

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 Bundle

Used to specify a provider's CA Certificate Bundle to verify SSL against. This denotes that Verify SSL is True.

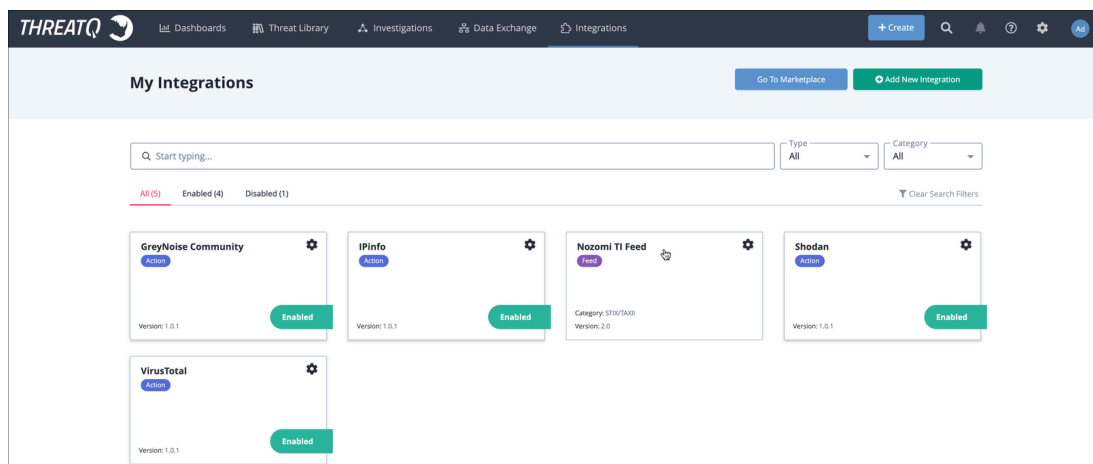
Add TAXII Feed

Cancel


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.



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



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version: 2.0

Accepted Data Types:

Configuration Activity Log

TAXII Server Version
2.0
The version of the TAXII Server to poll for data.

Discovery Path URL
https://ti-taxii.nws.nozominetworks.io/taxii/
Path to the TAXII Server's Discovery Service

Poll URL (Optional)
Optional URL specifying a specific endpoint on the TAXII Server to poll for data. If not supplied, the TAXII Client will attempt to determine the appropriate path via the Collections Service.

Collection Name
Hacking Frameworks
Name of the collection to poll data from

☐ Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Username
nozominetworks
Basic Authentication Username

Password
.....
Basic Authentication Password

Client Certificate
Client Certificate for authentication with the TAXII Server.

Client Key
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 Bundle
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)

☒ Send a notification when this feed encounters issues.

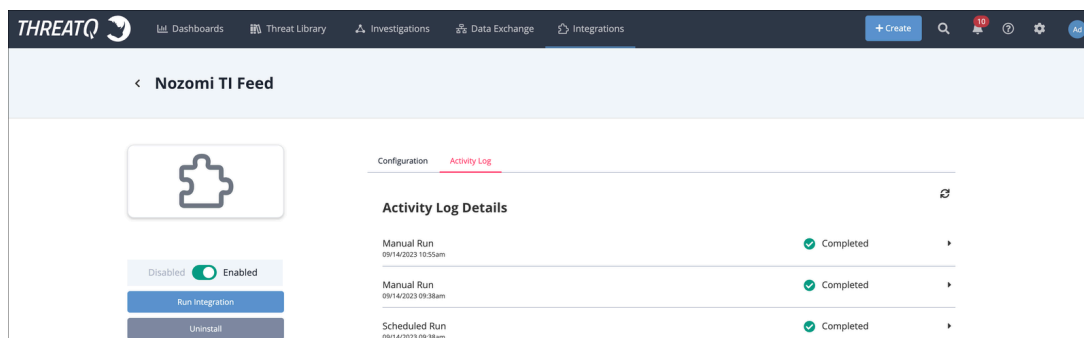
☐ Debug Option: Save the raw data response files.
We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

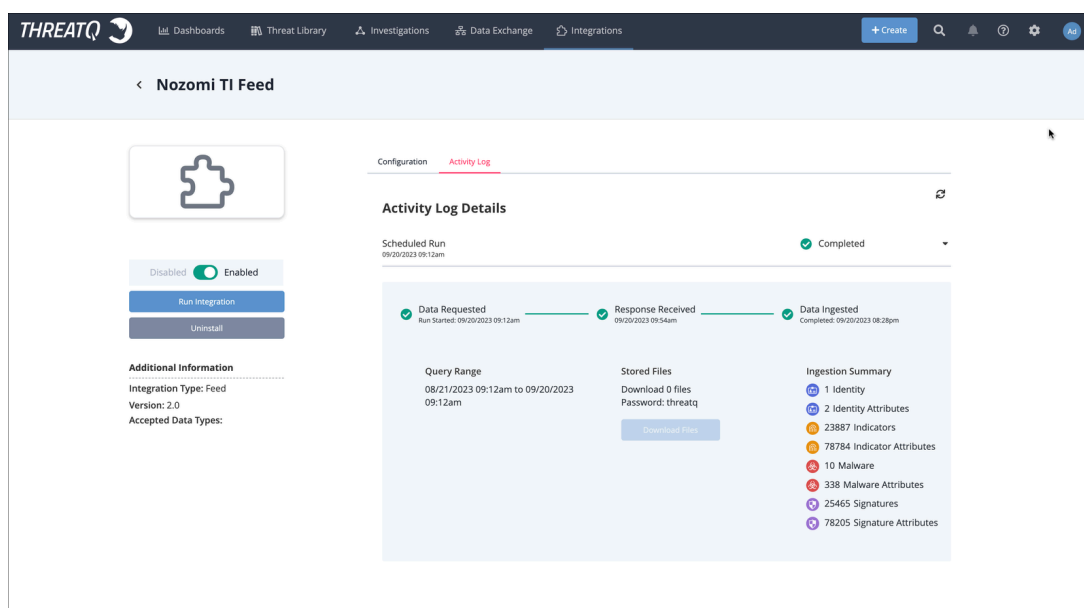
9. Select **Save**.

10. Select **Activity Log**.

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



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



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.

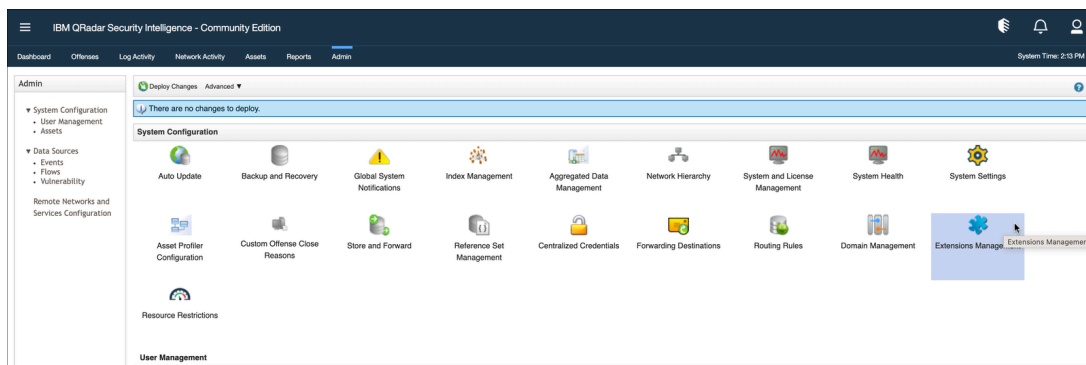
About this task

**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.

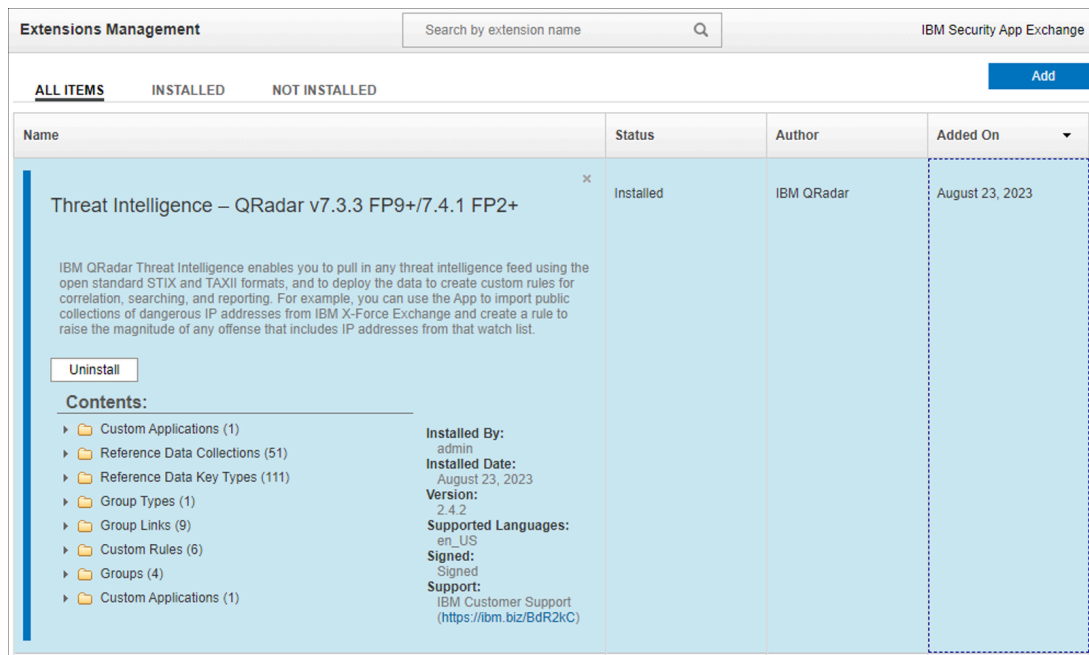
Procedure

1. Download QRadar from the [IBM website](#).
2. Go to **Admin > Extensions Management**.

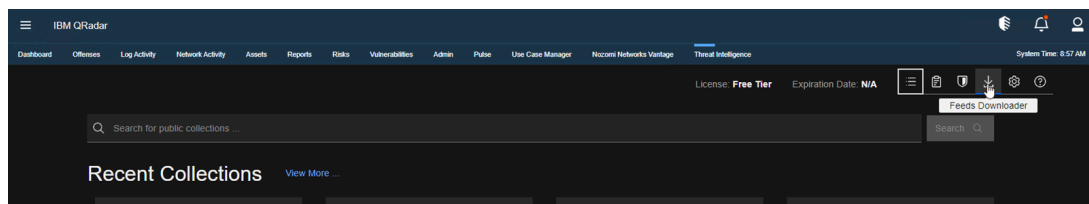


3. Select **All items**.

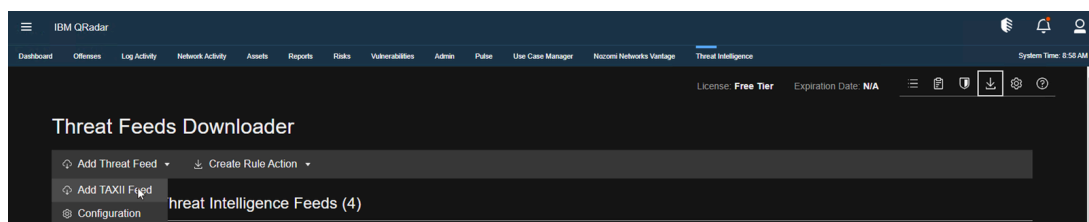
- Make sure that you have the latest version of the Threat Intelligence app installed.



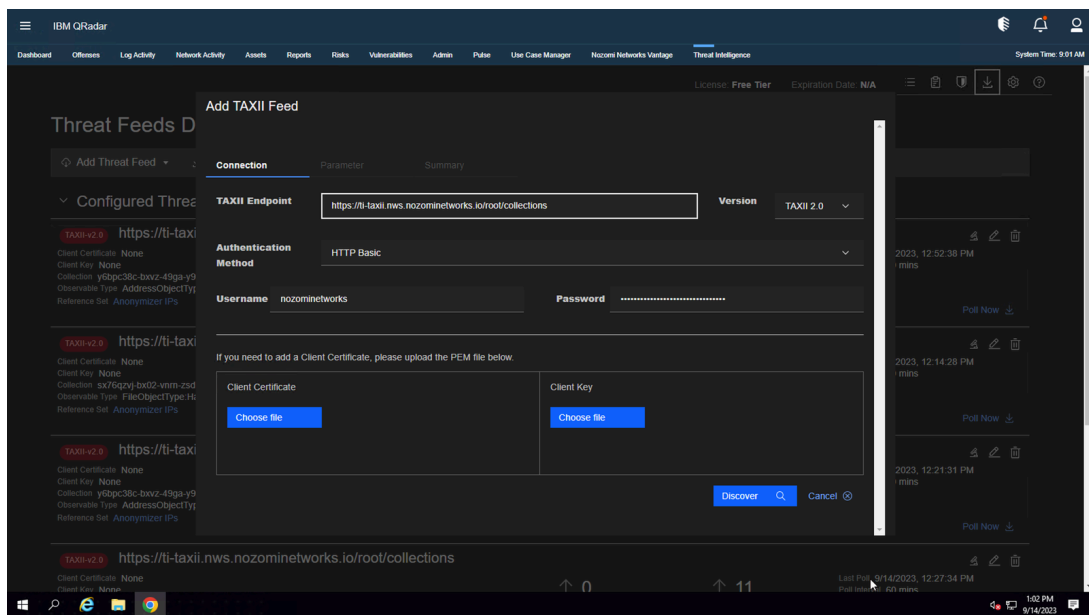
- Select **Threat Intelligence**.



- Select **Feeds Downloader**.
- Select **Add Threat Feed > Add TAXII Feed**.



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

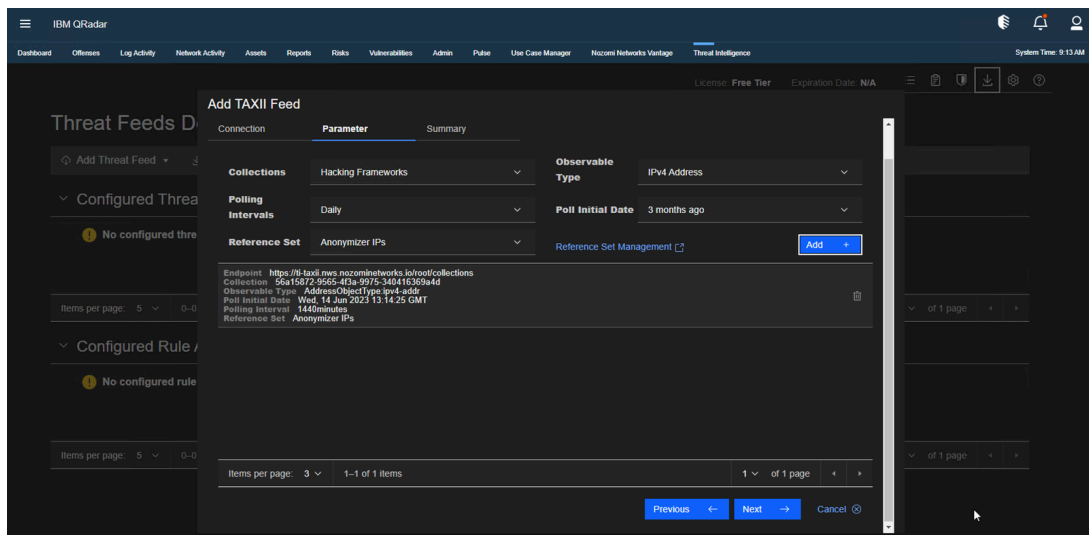


9. Enter the details as necessary in the other fields. Make sure the endpoint string has **/root/collections** at the end.

10. Select **Discover**.

11. Select **Parameter**.

12. From the **Collections** dropdown, select the applicable option.

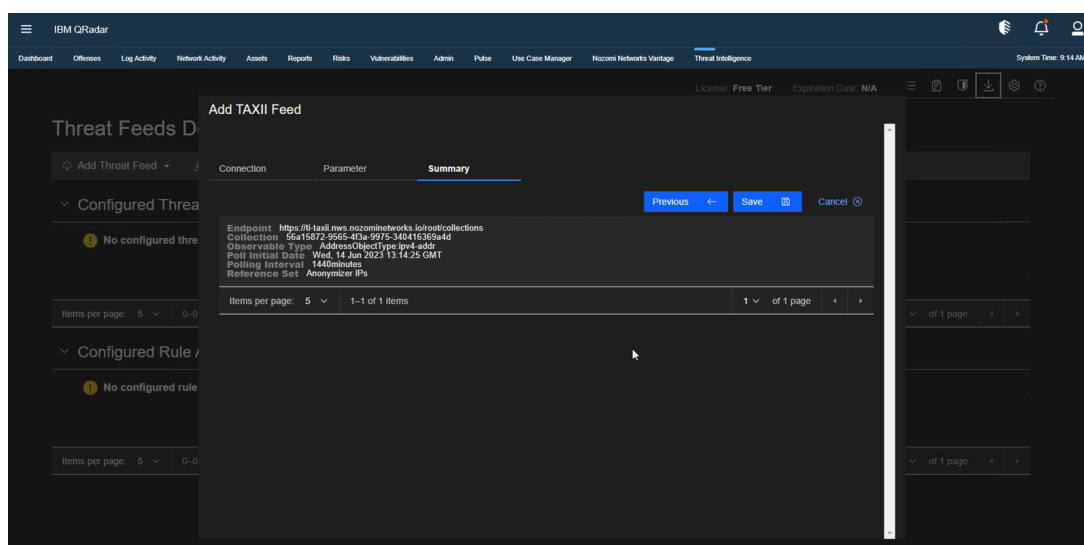


13. From the **Observable Type** dropdown, select the applicable indicator type.

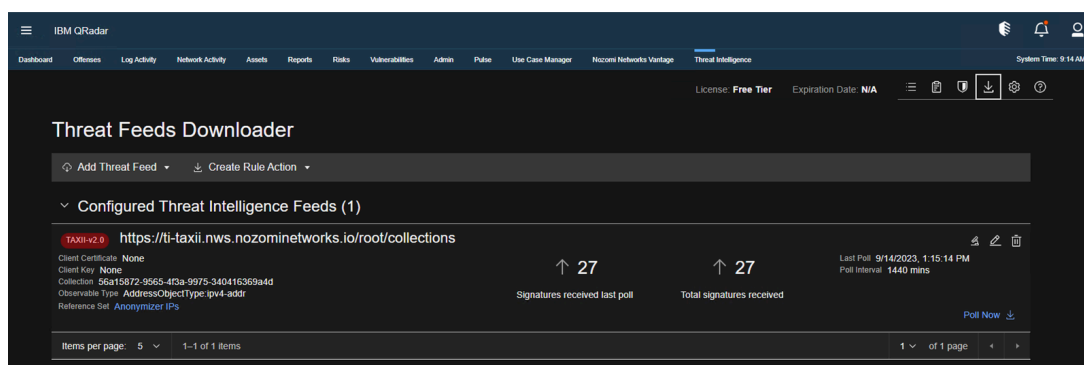
14. To the right of **Reference Set Management**, select **Add**.

15. In the bottom right section, select **Next**.

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



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



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:
 - 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.

