

ANY.RUN's TI Feeds:

STIX/TAXII Connector for Microsoft Sentinel

Configuration guide

Threat Intelligence Feeds (TI Feeds)

TI Feeds help MSSPs and SOC teams fortify their security with filtered, high-fidelity indicators of compromise (IPs, domains, URLs) enriched with threat context from ANY.RUN's Interactive Sandbox.

Sourced from real-time sandbox investigations of active attacks across 15,000+ organizations, TI Feeds integrate seamlessly with SIEMs/XDRs/firewalls and other security solutions to monitor and identify malware and phishing threats.

ANY.RUN's feeds are updated every two hours, allowing you to track threats as they emerge, develop, and spread to take critical security actions early.

- **Unique data:** Fresh indicators from live detonations of attacks with links to sandbox sessions with full threat context, including TTPs.
- **No false alerts:** TI Feeds provide reliable IOCs with a near-zero false positive rate thanks to pre-processing.
- **Prioritization of incidents:** SOC teams use TI Feeds as part of alert triage, incident response, and proactive hunting to effectively handle urgent threats.

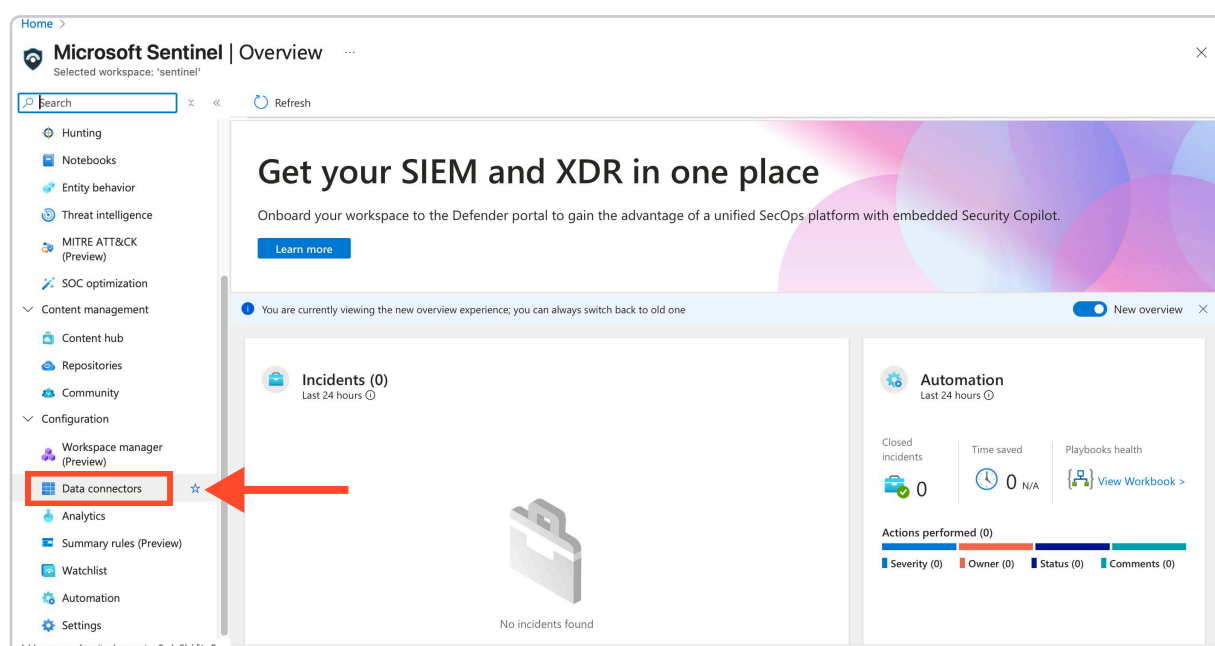
TI Feeds are available for integration using API or SDK and support TAXII protocol.

➡ For more details, feel free to [contact us](#).

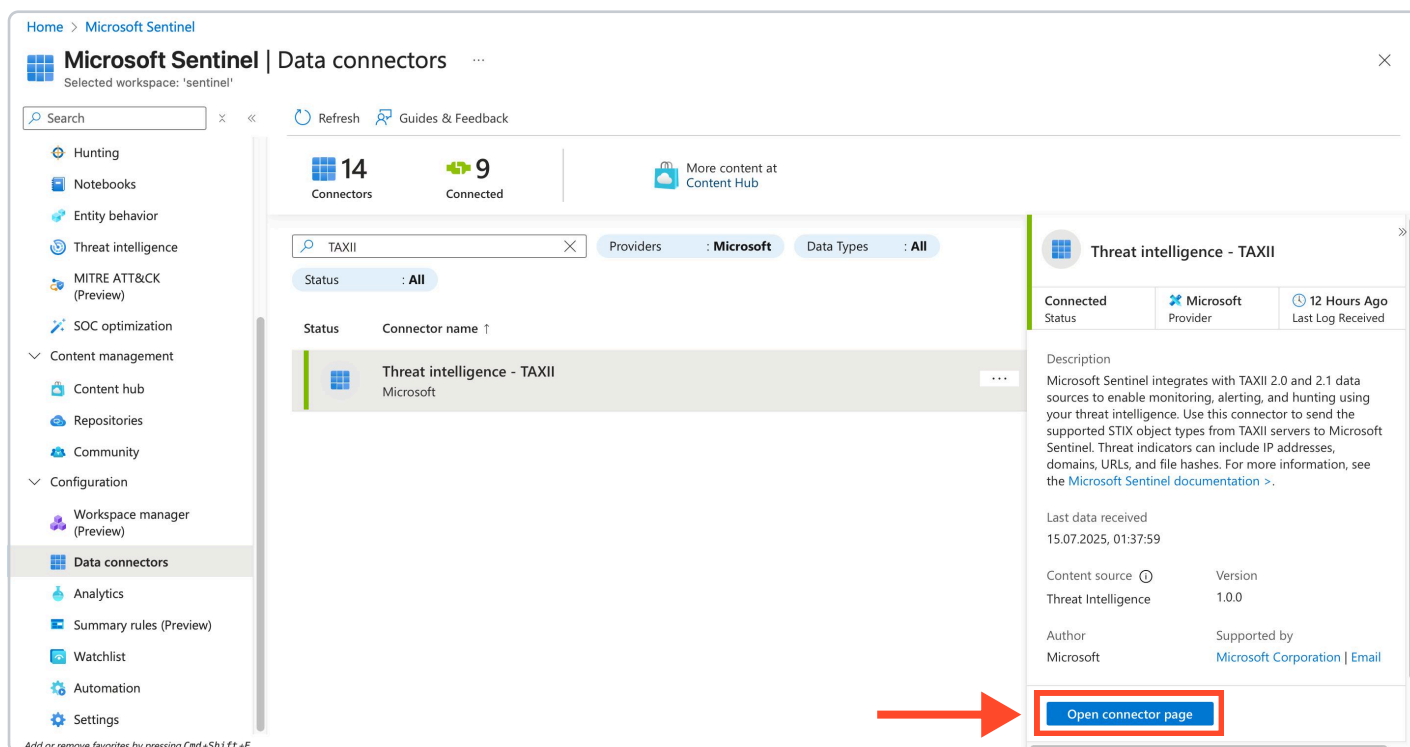
How to Connect TI Feeds to MS Sentinel

Connecting to TAXII server

1. Open MS Sentinel and go to the **Data connectors** tab in the **Configuration** section.



2. Search for the **Threat Intelligence TAXII** connector and click **Open connector page**.



3. You will see the list of prerequisites for the connector. If you lack any of them, see this documentation:

<https://learn.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence-taxii>

Prerequisites

To integrate with Threat intelligence - TAXII make sure you have:

- Workspace:** read and write permissions.
- TAXII Server:** TAXII 2.0 or TAXII 2.1 Server URI and Collection ID.

4. Fill out the **Configuration** form:

- Name the server via the **Friendly name** field.
- Insert **API root URL**: <https://api.any.run/v1/feeds/taxii2/api1/>
- Choose a **Collection ID**:

Name	Description	ID
All indicators	Contains IOCs of all formats (IPs, Domains, URLs)	3dce855a-c044-5d49-9334-533c24678c5a
IPs collection	Contains only IPs	55cda200-e261-5908-b910-f0e18909ef3d
Domains collection	Contains only Domains	2e0aa90a-5526-5a43-84ad-3db6f4549a09
URLs collection	Contains only URLs	05bfa343-e79f-57ec-8677-3122ca33d352

- Enter your **Username** and **Password**.

If you don't have these credentials, contact your account manager at ANY.RUN or fill out [this form](#).

You can also choose to import all available indicators or those that are one day, week, or month old via the field **Import indicators**.

Another optional setting is **Polling frequency** that determines how often you'd like to connect to the TAXII server to retrieve new feeds: once a minute, once an hour, or once a day.

If you need more information, see TAXII documentation by ANY.RUN: <https://intelligence.any.run/guide>



Configuration

Configure TAXII servers to stream STIX 2.0 or 2.1 STIX objects 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

Finally, click **Add** and you're all set up.

Browsing indicators

To access the indicators you've retrieved, go to the **Threat intelligence** tab.

You'll find a table with fields describing each indicator:

- **Values** – indicator itself
- **Names** – name of an indicator
- **Types** – type of an indicator (IP, URL, or Domain)
- **Sources** – source of an indicator
- **Confidence** – this rate determines our level of certainty on whether an indicator is malicious (50 – suspicious, 75 – likely malicious, 100 – malicious).
- **Alerts** – number of alerts related to an indicator
- **Tags** – descriptors of an indicator
- **Valid from** and **Valid until** – time period during which an indicator is considered valid

Home > Microsoft Sentinel

Microsoft Sentinel | Threat intelligence

Selected workspace: 'sentinel'

Refresh

New

Add tags

Delete

Columns

Import

Ingestion rules

Threat intelligence workbook

Guides & Feedback

Filters

Indicators (62,494)

Attack patterns (0)

Identities (0)

Threat actors (0)

Relationships (0)

<input type="checkbox"/>	Values	Name	Types	Source	Confidence	Alerts	Tags	Valid from	Valid until
<input checked="" type="checkbox"/>	http://185.163.45.87/fak...	--	URL	ANYRUN-taxii	100	0	malware +2	7/14/2025, 11:57:2...	--
<input type="checkbox"/>	http://45.142.193.119/fa...	--	URL	ANYRUN-taxii	100	0	malware +2	7/14/2025, 2:21:01 ...	--
<input type="checkbox"/>	http://139.129.32.152:80...	--	URL	ANYRUN-taxii	100	0	malware	7/14/2025, 11:54:3...	--
<input type="checkbox"/>	http://193.143.1.216/fak...	--	URL	ANYRUN-taxii	100	0	malware +2	7/14/2025, 10:51:1...	--
<input type="checkbox"/>	http://176.46.157.32/file...	--	URL	ANYRUN-taxii	75	0	banker	7/14/2025, 9:28:08 ...	--
<input type="checkbox"/>	http://176.46.157.32/file...	--	URL	ANYRUN-taxii	75	0	banker	7/14/2025, 9:27:57 ...	--
<input type="checkbox"/>	http://176.46.157.32/lu...	--	URL	ANYRUN-taxii	75	0	banker	7/14/2025, 9:27:51 ...	--
<input type="checkbox"/>	http://176.46.157.32/file...	--	URL	ANYRUN-taxii	75	0	banker	7/14/2025, 9:27:45 ...	--
<input type="checkbox"/>	http://176.46.157.32/tes...	--	URL	ANYRUN-taxii	75	0	banker	7/14/2025, 9:27:41 ...	--
<input type="checkbox"/>	http://176.46.157.32/file...	--	URL	ANYRUN-taxii	75	0	banker	7/14/2025, 9:27:35 ...	--
<input type="checkbox"/>	http://176.46.157.32/file...	--	URL	ANYRUN-taxii	75	0	banker	7/14/2025, 9:27:31 ...	--
<input type="checkbox"/>	http://176.46.157.32/file...	--	URL	ANYRUN-taxii	75	0	banker	7/14/2025, 9:27:26 ...	--

< Previous

1 - 100

Next >

If you have any questions,
contact us via [this form](#) or write to support@any.run