



# **Data Connectors in Microsoft Sentinel**

Adrian Cortez

## Overview

A data connector in Microsoft Sentinel is a tool that connects external data sources like firewalls, servers, or cloud services to Sentinel, allowing it to collect and ingest security logs and events. By using data connectors, Sentinel can gather the information it needs to analyze threats, detect attacks, and generate alerts across your entire environment.

## Integrate Threat Intelligence into Sentinel

Content Management > Content Hub > Search for Threat Intelligence and Install

The screenshot shows the Microsoft Sentinel Content Hub interface. The left sidebar contains navigation options: General, Threat management, Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization, Content management, Content hub (selected), Repositories, Community, and Configuration. The main area displays search results for 'threat intelligence'. At the top, there are statistics: 414 Solutions, 318 Standalone contents, 0 Installed, and 0 Updates. A search bar contains 'threat intelligence'. Below the search bar, a table lists search results. The first result, 'Threat Intelligence', is highlighted with a red box. The table has columns: Content title, Status, Content source, Provider, Support, and Category. The 'Threat Intelligence' row shows it is 'Not installed', a 'Solution' from 'Microsoft', with 'Microsoft' support, and categorized under 'Security - Threat Intelligence'. To the right of the table, there is a detailed view for the 'Threat Intelligence' solution, including a description, release notes, and a list of data connectors, workbooks, analytic rules, and hunting queries.

Content title	Status	Content source	Provider	Support	Category
Threat Intelligence	Not installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence
Microsoft Defender Threat Intelligence	Not installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence
Threat intelligence - TAXII	Not installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence
Premium Microsoft Defender Threat Intelli...	Not installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence
Threat Intelligence Platforms	Not installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence
Threat Intelligence Upload API (Preview)	Not installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence
Ti map IP entity to AzureFirewall	Not installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence
Ti Map URL Entity to PaloAlto Data	Not installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence
Ti map Email entity to EmailEvents	Not installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence
Ti Map URL Entity to UrlClickEvents	Not installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence
Ti Map IP Entity to AzureActivity	Not installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence

Create an Account on Pulsedive or any threat intelligence platform



Get API Root URL from STIX via TAXII

## Supported Versions

STIX/TAXII 1.x	✗ Not supported
STIX/TAXII 2.0	✗ Not supported
STIX/TAXII 2.1	✓ Supported




## Server Information

Your TAXII client may ask for only one of these values.

Discovery URL	<a href="https://pulsedive.com/taxii2/">https://pulsedive.com/taxii2/</a> 
API Root URL	<a href="https://pulsedive.com/taxii2/api/">https://pulsedive.com/taxii2/api/</a> 

## Get Collection ID from STIX via TAXII

### Collection IDs

Test collection <small>FOR TESTING ONLY</small>	981c4916-ebb2-4567-aece-54ae970c4230 
Indicator collection	a5cffbfe-c0ff-4842-a235-cb3a7a040a37 
Threat collection	dc9ecfa5-7769-4cf3-b699-38a9776b431d 

## Get API Key

Your API key:

[Redacted API key]

You're on the free API plan. Affordable plans with higher limits and commercial licenses are available.

[View plans](#)

## Configure the data source

Go to Threat Intelligence > Select Threat Intelligence – TAXII > Open Connector Page

Configure with the information collected in the previous steps

1. IMPORTANT: For the password field, input the API key

## 2. IMPORTANT: Username will be taxii2

Home > Threat Intelligence

Refresh Delete Reinstall

64 Installed content items 58 Configuration needed

Threat Intelligence

Microsoft Provider Microsoft Support 3.1.2 Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)

The Threat Intelligence solution contains data connectors for import of threat indicators into Microsoft Sentinel, analytic rules for matching TI data with event data, workbook, and hunting queries. Threat indicators can be malicious IPs, URLs, file hashes, domains, email addresses etc.

Data Connectors: 5, Workbooks: 1, Analytic Rules: 52, Hunting Queries: 5

Learn more about Microsoft Sentinel | Learn more about Solutions

Content type

- 53 Analytics rule
- 5 Data connector
- 5 Hunting query

1 Workbook

Category

Security - Threat Intelligence

Pricing

Free

Manage Actions View details

Search...

Content name	Created content	Conte...	Version	Status
<input type="checkbox"/> Microsoft Defender Threat Intelligence	1 items	Data co...	1.0.0	Install
<input type="checkbox"/> Premium Microsoft Defender Threat Intelligence	1 items	Data co...	1.0.0	Install
<input checked="" type="checkbox"/> Threat intelligence - TAXII	1 items	Data co...	1.0.0	Install
<input type="checkbox"/> Threat Intelligence Platforms	1 items	Data co...	1.0.0	Install
<input type="checkbox"/> Threat Intelligence Upload API (Preview)	1 items	Data co...	1.0.0	Install
<input type="checkbox"/> Preview - TI map Domain entity to Cloud App Events	--	Analyti...	1.0.3	Install
<input type="checkbox"/> Preview - TI map Email entity to Cloud App Events	--	Analyti...	1.0.3	Install
<input type="checkbox"/> Preview - TI map File Hash entity to Cloud App Events	--	Analyti...	1.0.3	Install
<input type="checkbox"/> Preview - TI map IP entity to Cloud App Events	--	Analyti...	1.0.3	Install
<input type="checkbox"/> Preview - TI map URL entity to Cloud App Events	--	Analyti...	1.0.3	Install
<input type="checkbox"/> TI Map Domain Entity to DeviceNetworkEvents	--	Analyti...	1.0.1	Install
<input type="checkbox"/> TI map Domain entity to Dns Events (ASIM DNS Schema)	--	Analyti...	1.1.8	Install
<input type="checkbox"/> TI map Domain entity to DnsEvents	--	Analyti...	1.4.3	Install
<input type="checkbox"/> TI map Domain entity to EmailEvents	--	Analyti...	1.0.2	Install
<input type="checkbox"/> TI map Domain entity to EmailUrlInfo	--	Analyti...	1.0.3	Install
<input type="checkbox"/> TI map Domain entity to PaloAlto	--	Analyti...	1.4.2	Install

Previous Page 1 of 3 Next Showing 1 to 30 of 64 results.

Threat intelligence - TAXII

Disconnected Status Microsoft Provider Last Log Received

Description

Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send the supported STIX object types from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes. For more information, see the [Microsoft Sentinel documentation](#).

Last data received

Content source Threat intelligence Version 1.0.0

Author Microsoft Supported by Microsoft Corporation | Email

Data received 4 3 2 1 0

Go to query

Open connector page

Related content

- 0 Workbooks
- 2 Queries
- 48 Analytics rules templates

Data received

Go to log analytics

ThreatIntelligen...

0

Data types

ThreatIntelligenceIndicator --

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) \*

threat-intel

API root URL \*

https://pulsedive.com/taxii2/api/

Collection ID \*

981c4916-ebb2-4567-aece-54ae970c4230

Username

adrianco

Password

Import indicators:

All available

Polling frequency


Once an hour



Add

### List of configured TAXII servers

Friendly name	TAXII server	Collection ID	Last indicator received
threat-intel	https://pulsedive...	981c4916-ebb2-...	--

## The data connector is now connected

 Threat intelligence - TAXII ✕

Connected Status	 Microsoft Provider	 53 Minutes ... Last Log Receiv...
------------------	--	--

Description

Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send the supported STIX object types from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes. For more information, see the [Microsoft Sentinel documentation](#) >.

Last data received

8/12/2025, 12:27:56 PM

Content source ⓘ	Version
Threat Intelligence	1.0.0
Author	Supported by
Microsoft	<a href="#">Microsoft Corporation</a>   <a href="#">Email</a>

Related content

## Integrating Windows Security Event Logs Into Sentinel

Create a VM and ensure the VM has an inbound rule that allows RDP

Install Windows Security Events in Content Hub

Create data collection rule and select the VM.



# CreateVm-MicrosoftWindowsDesktop.Windows-10-rs5-e-20250812160123 | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

## Overview

### Inputs

### Outputs

### Template

## ✓ Your deployment is complete



Deployment name: CreateVm-MicrosoftWindowsDesktop.Windows...

Start time: 8/12/2025, 4:04:43 PM

Subscription: [Azure for Students](#)

Resource group: [Sentinel-Project](#)

Correlation ID: 5d2f3cc0-2437-4d30-902e-27bbe3caab22



### Deployment details

### Next steps

[Setup auto-shutdown](#) Recommended

[Monitor VM health, performance and network dependencies](#) Recommended

[Run a script inside the virtual machine](#) Recommended

[Go to resource](#)

[Create another VM](#)

### Give feedback

[Tell us about your experience with deployment](#)

Install/Update Delete

<input type="checkbox"/>	Content title	Status	Content source	Provider	Support	Category
<input checked="" type="checkbox"/>	Windows Security Events	Not installed	Solution	Microsoft	Microsoft	Security
	Windows Security Events via AMA	Not installed	Solution	Microsoft	Microsoft	Security
	Security Events via Legacy Agent	Not installed	Solution	Microsoft	Microsoft	Security
	NRT Security Event log cleared	Not installed	Solution	Microsoft	Microsoft	Security
	Windows System Time changed on hosts	Not installed	Solution	Microsoft	Microsoft	Security
	Excessive Windows Logon Failures	Not installed	Solution	Microsoft	Microsoft	Security
	Windows System Shutdown/Reboot(Sysmon)	Not installed	Solution	Microsoft	Microsoft	Security
	NRT Base64 Encoded Windows Process Comm...	Not installed	Solution	Microsoft	Microsoft	Security
	New EXE deployed via Default Domain or Defa...	Not installed	Solution	Microsoft	Microsoft	Security
	Gain Code Execution on ADFS Server via SMB ...	Not installed	Solution	Microsoft	Microsoft	Security
	Starting or Stopping HealthService to Avoid De...	Not installed	Solution	Microsoft	Microsoft	Security
	Process Execution Frequency Anomaly	Not installed	Solution	Microsoft	Microsoft	Security
	AD FS Remote Auth Sync Connection	Not installed	Solution	Microsoft	Microsoft	Security

< Previous Page 1 of 2 Next > Showing 1 to 20 of 25 results.

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

1. **Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent [here](#). **Microsoft recommends using this Data Connector.**

2. **Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

**NOTE:** Microsoft recommends installation of Windows Security Events via AMA Connector. Legacy connector uses the Log Analytics agent which is about to be deprecated by **Aug 31, 2024**, and thus should only be installed where AMA is not supported.

**Data Connectors:** 2, **Workbooks:** 2, **Analytic Rules:** 20, **Hunting Queries:** 50

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Content type

Analytics rule

2

Workbook

2

Category

Security - Threat Protection


Pricing

Free

Install



View details

# Connector details



Windows Security Events via AMA

<

Connected Status	 Microsoft Provider	 -- Last Log Received
------------------	--	--

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received

--

Content source ⓘ

Version

Windows Security Events

1.0.0

Author

Supported by

Microsoft

[Microsoft Corporation ⓘ](#) | [Email](#)

Related content

0

Workbooks

1

Queries

22

Analytics rules templates

Data received

[Go to log analytics](#)



Date	Data Received
August 5	0
August 6	0
August 7	0
August 8	0
August 9	0
August 10	0
August 11	0