

Data Connectors in Microsoft Sentinel

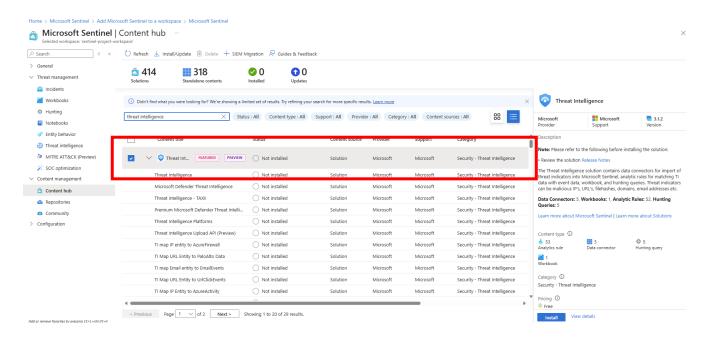
Adrian Cortez

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

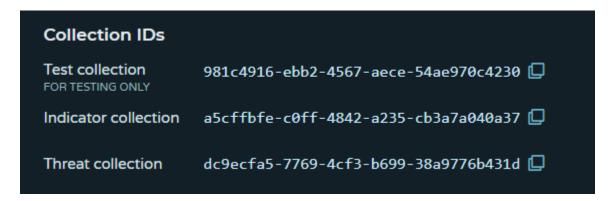


Create an Account on Pulsedive or any threat intelligence platform

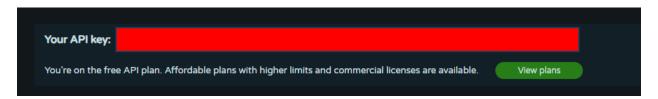
Get API Root URL from STIX via TAXII



Get Collection ID from STIX via TAXII



Get API Key



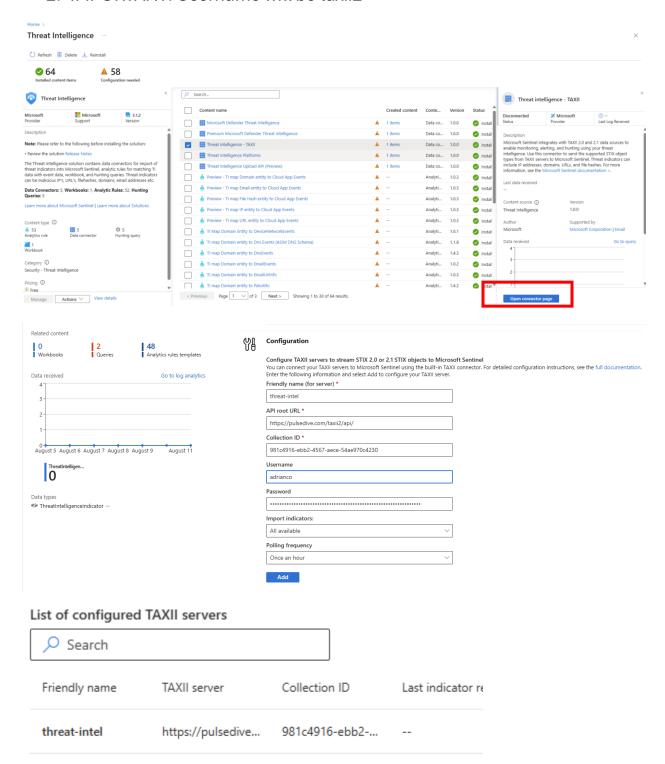
Configure the data source

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



The data connector is now connected



Last Log Receiv...

Provider

Description

Status

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 Corporation | Email

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 \varkappa 🥌 Delete ○ Cancel Redeploy Download Refresh × « Search Overview Your deployment is complete Inputs

Subscription: Azure for Students Resource group: Sentinel-Project Deployment details

Deployment name: CreateVm-MicrosoftWindowsDesktop.Windows... Start time: 8/12/2025, 4:04:43 PM Correlation ID: 5d2f3cc0-2437-4d30-902e-27bbe3caab22

∧ Next steps

Template

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

	II/Update 📋 Delete					
	Content title	Status	Content source	Provider	Support	Catego
	✓	O Not installed	Solution	Microsoft	Microsoft	Securi
	Windows Security Events via AMA	O Not installed	Solution	Microsoft	Microsoft	Securi
	Security Events via Legacy Agent	O Not installed	Solution	Microsoft	Microsoft	Securi
	NRT Security Event log cleared	Not installed	Solution	Microsoft	Microsoft	Securi
	Windows System Time changed on hosts	Not installed	Solution	Microsoft	Microsoft	Securi
	Excessive Windows Logon Failures	Not installed	Solution	Microsoft	Microsoft	Securi
	Windows System Shutdown/Reboot(Sysmon)	Not installed	Solution	Microsoft	Microsoft	Securi
	NRT Base64 Encoded Windows Process Comm	Not installed	Solution	Microsoft	Microsoft	Securi
	New EXE deployed via Default Domain or Defa	Not installed	Solution	Microsoft	Microsoft	Securi
	Gain Code Execution on ADFS Server via SMB	Not installed	Solution	Microsoft	Microsoft	Securi
	Starting or Stopping HealthService to Avoid De	O Not installed	Solution	Microsoft	Microsoft	Securi
	Process Execution Frequency Anomaly	Not installed	Solution	Microsoft	Microsoft	Securi
	AD FS Remote Auth Sync Connection	Not installed	Solution	Microsoft	Microsoft	Securi
4						•

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.

- 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 the first part of the Azure Monitor Agent here. Microsoft recommends using this Data Connector.
- 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 depreciated 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:

Learn more about Microsoft Sentinel I Learn more about Solutions

Content type ① △ 20 Analytics rule ©a 2 Workbook Category ① Security - Threat Protection

Pricing ① □ Free

Install View details ☑

Connector details

