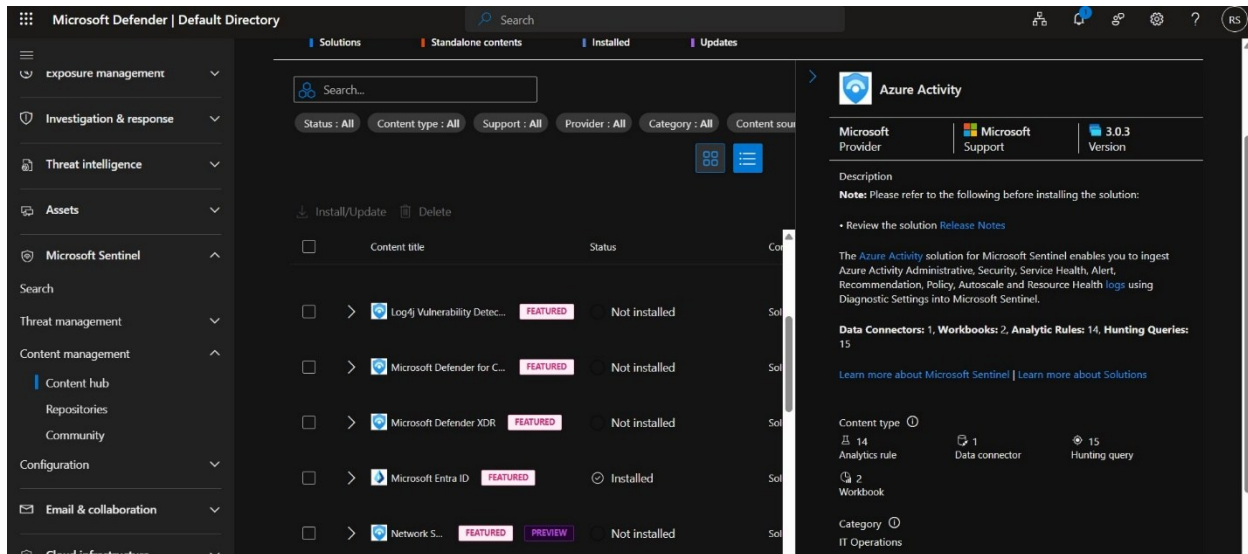


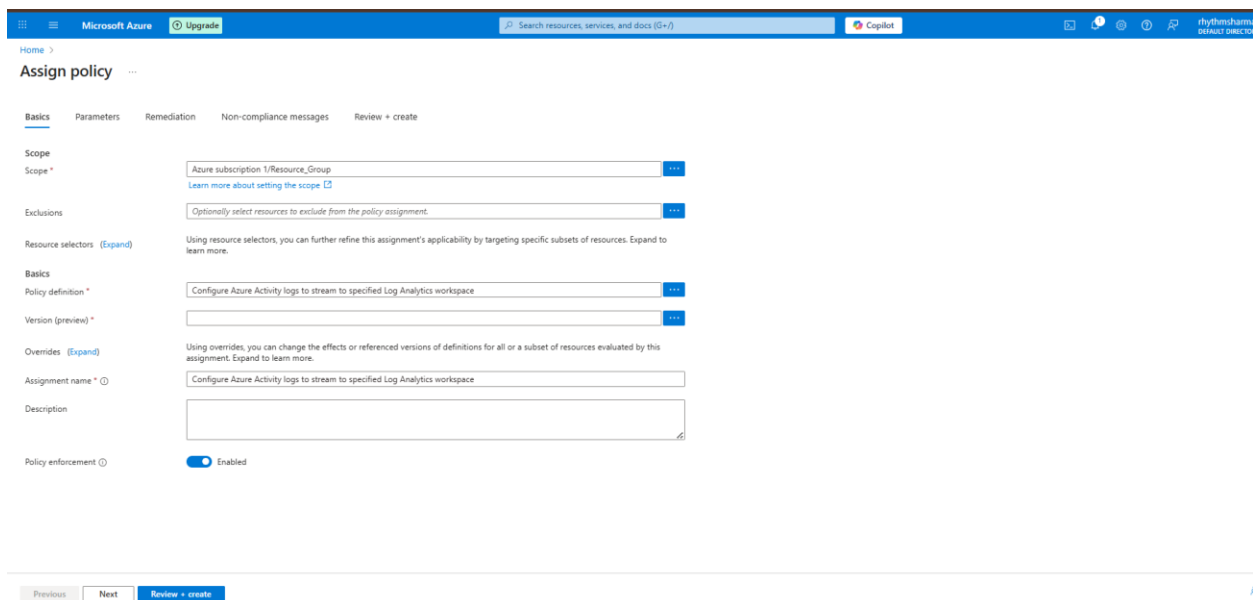
## Lab 2.1 Enable Azure Activity

The **Azure Activity data connector** in Microsoft Sentinel streams **Azure Activity Logs** (subscription-level events like resource creation, modification, deletion, and service operations) into Sentinel. This lets SOC teams monitor changes across Azure resources, detect suspicious activity, and build analytics rules for incident response

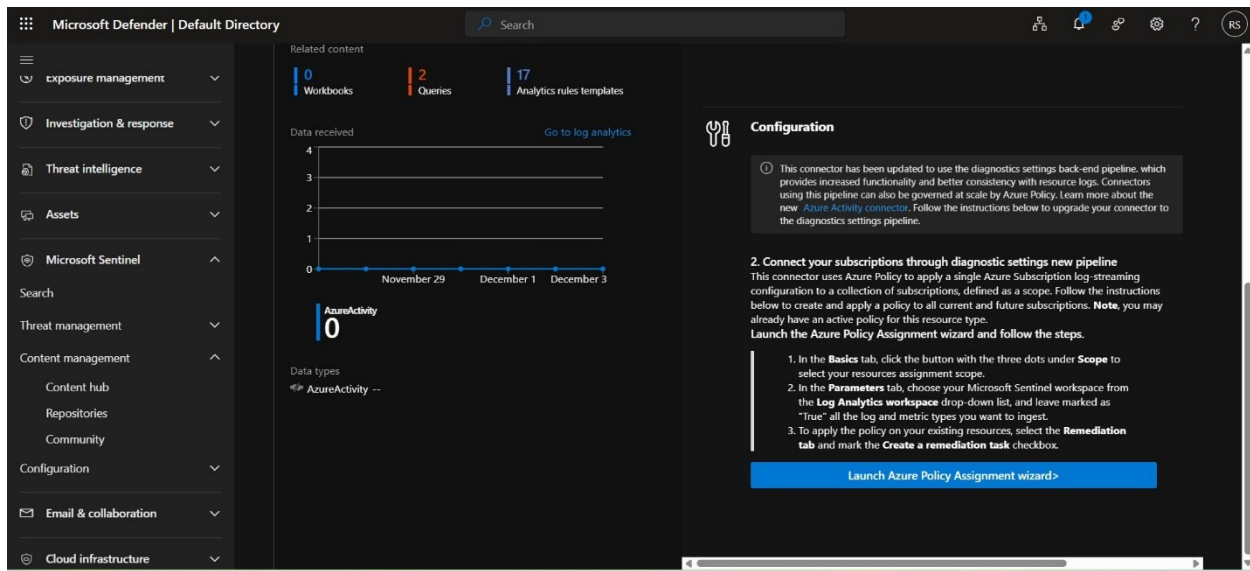
### 2.1.1: Go to Content Hub and Search for Azure Activity and Install it.



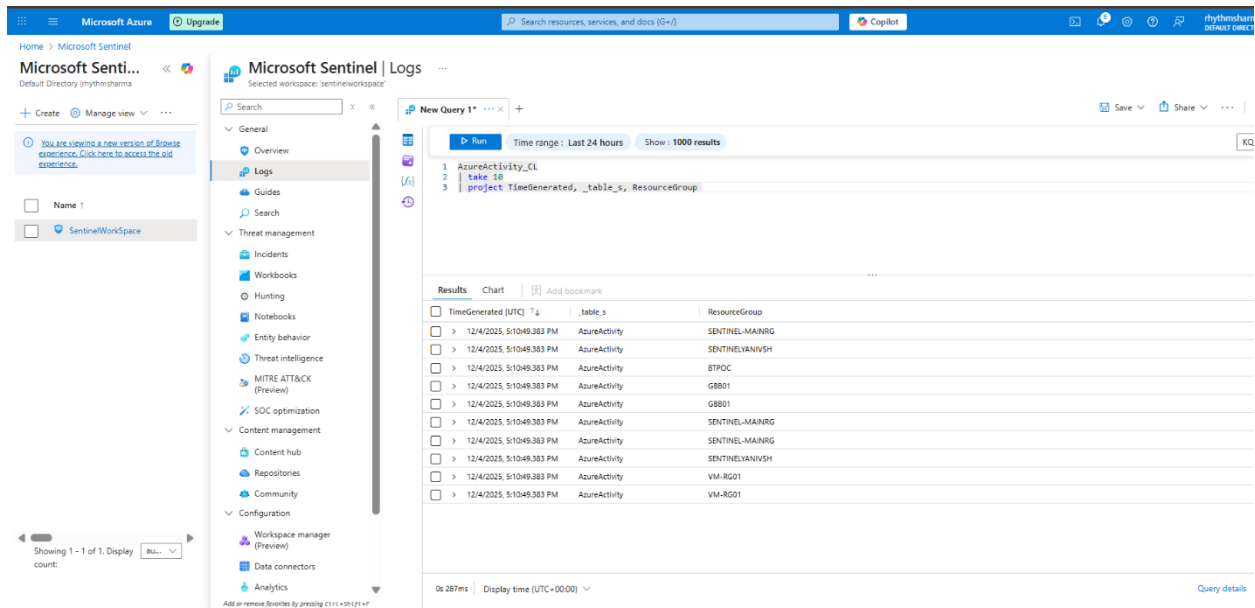
### 2.1.2 Open Connector Page and linking to Resource Group



### 2.1.3 Go back to Sentinel



## 2.1.4 Go to Logs To Verify Azure Activity



## Lab 2.2 Enable **Microsoft Defender for Cloud**.

It provides **cloud workload protection** and **security posture management** across Azure, hybrid, and multicloud environments. In practice, it helps you detect threats, harden configurations, and protect resources like VMs, databases, containers, and storage.

### 2.2.1 Open Sentinel and Go to Content Hub → Hit Install

The screenshot shows the Microsoft Defender for Cloud interface. On the left is a navigation pane with options like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management, Content hub, Repositories, Community, and Configuration. The main area displays search results for 'Defender for cloud'. A table lists several solutions, all with a status of 'Not installed'. On the right, a detailed view for 'Microsoft Defender for Cloud' is shown, including its description, underlying Microsoft technologies used, data connectors, analytics rules, category, and pricing (Free). An 'Install' button is visible at the bottom of the details pane.

### 2.2.2 Checkout the Status is Connected

The screenshot shows the Microsoft Azure portal. The top navigation bar includes the Microsoft Azure logo, an 'Upgrade' button, and a search bar. The breadcrumb trail indicates the path: Home > Microsoft Sentinel | Data connectors >. The main heading is 'Microsoft Defender for Cloud Apps'. Below this, a card for 'Microsoft Defender for Cloud Apps' shows a 'Connected' status, the 'Microsoft Provider', and the last log received. A description explains that connecting provides visibility into cloud apps for identifying and combating cyberthreats. A list of benefits includes identifying shadow IT, controlling access, using built-in or custom policies for data sharing and loss prevention, and identifying high-risk use. To the right, an 'Instructions' section lists prerequisites: Workspace (read and write permissions), Tenant Permissions (Global Administrator or Security Administrator), and License (M365 E5, M365 A5, or other eligible Microsoft Defender XDR license).

## 2.3. Connect Threat Intelligence TAXII Data Connectors

**TAXII protocol (Trusted Automated eXchange of Indicator Information)** use to pull in external cyber threat intelligence feeds (like IPs, domains, file hashes, malware signatures) into Sentinel. This lets SOC teams enrich their detections by correlating logs with known malicious indicators.

### 2.2.1 Install Threat Intelligence → Click to Threat Intelligence – TAXII and Open data connector

The screenshot shows the Microsoft Sentinel Content hub interface. The left sidebar contains navigation options like Threat management, Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization, Content management, Content hub (selected), Repositories, Community, Configuration, Workspace manager (Preview), Data connectors, Analytics, Summary rules, Watchlist, Automation, and Settings. The main area displays a search for 'Threat Intelligence Taxii' with 448 solutions, 324 standalone contents, 7 installed, and 0 updates. A table lists various solutions, including 'Threat Intelligence - TAXII', which is marked as installed. The table columns are Content title, Status, Content source, Provider, Support, Category, and Content type. The 'Threat Intelligence - TAXII' solution is a Microsoft-provided Security - Threat Intelligence data connector. A right-hand pane shows details for the 'Threat Intelligence (NEW)' solution, including a description, release notes, and a list of data connectors, parsers, workbooks, analytic rules, and hunting queries.

Content title	Status	Content source	Provider	Support	Category	Content type
TI map IP entity to OfficeActivity	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Analytics ru
Microsoft Defender Threat Intelligence	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Data connec
Premium Microsoft Defender Threat Intelli...	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Data connec
Threat Intelligence Platforms	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Data connec
Threat intelligence - TAXII	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Data connec
Threat Intelligence Upload API (Preview)	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Data connec
TI Map File Entity to Security Event	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Hunting qu
TI Map File Entity to OfficeActivity Event	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Hunting qu
TI Map File Entity to WireData Event	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Hunting qu
TI Map File Entity to VMConnection Event	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Hunting qu
TI Map File Entity to Syslog Event	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Hunting qu
Parser for ThreatIntelIndicators	Installed	Solution	Microsoft	Microsoft	Security - Threat Intelligence	Parser
NCSC-NL NDN Cyber Threat Intellig...	Not installed	Solution	NCSC-NL	Microsoft	Security - Threat Intelligence	Parser

### 2.2.2 I have used Pulsedive to practice connecting threat intelligence feeds into Microsoft Sentinel. Register your account

The screenshot shows the Pulsedive Community user profile page for 'rhythmsharma777'. The page has a dark theme with a sidebar on the left containing navigation links: Overview, Activity, Subscriptions, Your Data, Delete Account, and Sign Out. The main content area displays the user's name 'rhythmsharma' and a profile picture. Below the name, there are links for 'Actions', 'Update Information', and 'Change Password'. The user's role is listed as 'User', and their email is 'rhythmsharma...'. The organization is listed as 'LAB'.

### 2.2.3 Enter Required Information From Pulsedive Server and Add

Microsoft Azure

Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Microsoft Sentinel | Content hub >

Threat intelligence - TAXII

Threat intelligence - TAXII

Disconnected Status

Microsoft Provider

45 Seconds Ago 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

12/4/2025, 1:34:53 PM

Content source

Threat Intelligence (NEW)

Version

1.0.0

Author

Microsoft

Supported by

Microsoft Corporation | Email


Related content

0 Workbooks

4 Queries

47 Analytics rules templates

Data received



Go to log analytics

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: All available

Polling frequency: Once an hour

Add

List of configured TAXII servers

Search

Friendly name	TAXII server	Collection ID	Last indicator r...	Polling freque...
	https://pulsedive.com/taxi2/api/	981c4916-ebb2...	--	Once an hour