

## 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.

The screenshot shows the Microsoft Defender Content Hub interface. On the left, there's a sidebar with categories like exposure management, investigation & response, threat intelligence, assets, Microsoft Sentinel, search, threat management, content management (with content hub selected), configuration, email & collaboration, and cloud infrastructure. The main area has tabs for Solutions, Standalone contents, Installed, and Updates. A search bar at the top says "Search...". Below it, filters include Status: All, Content type: All, Support: All, Provider: All, Category: All, and Content source. A list of solutions is shown, with "Azure Activity" highlighted. It has a Microsoft Provider icon, Microsoft Support, and a 3.0.3 Version. A note says "Please refer to the following before installing the solution: Review the solution Release Notes". Below that, it says "The Azure Activity solution for Microsoft Sentinel enables you to ingest Azure Activity Administrative, Security, Service Health, Alert, Recommendation, Policy, Autoscale and Resource Health logs using Diagnostic Settings into Microsoft Sentinel. Data Connectors: 1, Workbooks: 2, Analytic Rules: 14, Hunting Queries: 15". At the bottom, it shows content types: 14 Analytics rule, 1 Data connector, 2 Workbook, and 15 Hunting query, all under the IT Operations category.

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

The screenshot shows the "Assign policy" page in Microsoft Azure. The top navigation bar includes "Microsoft Azure", "Upgrade", "Search resources, services, and docs (S+)", "Copilot", and a user profile. Below the navigation, the URL is "https://portal.azure.com/#blade/Microsoft\_Azure\_Policy/PolicyBlade/assignPolicyBlade". The main form has tabs for Basics, Parameters, Remediation, Non-compliance messages, and Review + create. Under Basics, there's a "Scope" section with "Scope" dropdown set to "Azure subscription 1/Resource\_Group" and a link "Learn more about setting the scope". There's also an "Exclusions" section with a dropdown. Under "Resource selectors (Expand)", there's a note about using resource selectors to refine applicability. The "Policy definition" field contains "Configure Azure Activity logs to stream to specified Log Analytics workspace". The "Version (preview)" field is empty. The "Overrides (Expand)" section notes using overrides to change effects or referenced versions. The "Assignment name" field is empty. The "Description" field is empty. The "Policy enforcement" section has a toggle switch set to "Enabled". At the bottom, there are "Previous", "Next", and "Review + create" buttons.

### 2.1.3 Go back to Sentinel

The screenshot shows the Microsoft Defender interface for a Default Directory. On the left, there's a navigation sidebar with sections like Exposure Management, Investigation & Response, Threat Intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management (Content hub, Repositories, Community), Configuration, Email & collaboration, and Cloud infrastructure. The main area has a "Configuration" section with a heading "This connector has been updated to use the diagnostics settings back-end pipeline, which provides increased functionality and better consistency with resource logs. Connectors using this pipeline can also be governed at scale by Azure Policy. Learn more about the new Azure Activity connector. Follow the instructions below to upgrade your connector to the diagnostics settings pipeline." Below this, there's a section titled "2. Connect your subscriptions through diagnostic settings new pipeline" with three steps: 1. In the Basics tab, click the button with the three dots under Scope to select your resources assignment scope. 2. In the Parameters tab, choose your Microsoft Sentinel workspace from the Log Analytics workspace drop-down list, and leave marked as "True" all the log and metric types you want to ingest. 3. To apply the policy on your existing resources, select the Remediation tab and mark the Create a remediation task checkbox. A blue button at the bottom right says "Launch Azure Policy Assignment wizard>".

## 2.1.4 Go to Logs To Verify Azure Activity

The screenshot shows the Microsoft Sentinel Logs interface. The left sidebar includes sections for Overview, Logs (selected), Guides, Search, Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization), Content management (Content hub, Repositories, Community), and Configuration (Workspace manager (Preview), Data connectors, Analytics). The main area displays a "New Query 1" window with a table of results. The table has columns for TimeGenerated (UTC), \_table, and ResourceGroup. The results show several entries for AzureActivity, such as:

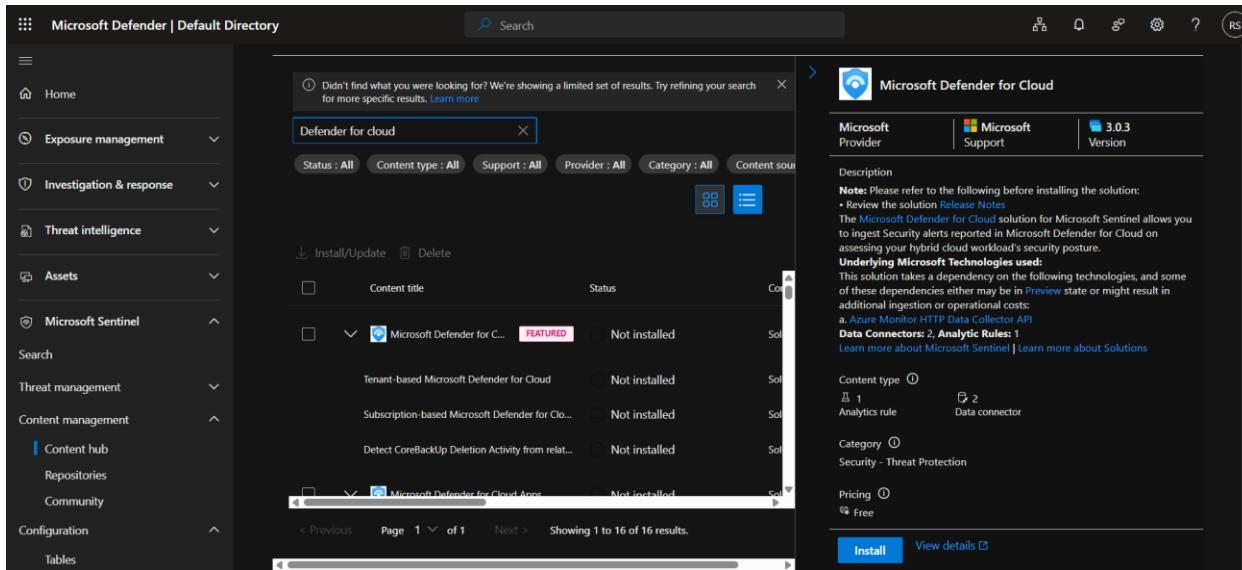
TimeGenerated (UTC)	_table	ResourceGroup
> 12/4/2025, 5:10:49.383 PM	AzureActivity	SENTINEL-MAINRG
> 12/4/2025, 5:10:49.383 PM	AzureActivity	SENTINELVANISH
> 12/4/2025, 5:10:49.383 PM	AzureActivity	BTPOC
> 12/4/2025, 5:10:49.383 PM	AzureActivity	GB801
> 12/4/2025, 5:10:49.383 PM	AzureActivity	GB801
> 12/4/2025, 5:10:49.383 PM	AzureActivity	SENTINEL-MAINRG
> 12/4/2025, 5:10:49.383 PM	AzureActivity	SENTINEL-MAINRG
> 12/4/2025, 5:10:49.383 PM	AzureActivity	SENTINELVANISH
> 12/4/2025, 5:10:49.383 PM	AzureActivity	VIM-RG01
> 12/4/2025, 5:10:49.383 PM	AzureActivity	VIM-RG01

At the bottom, it says "0s 287ms | Display time (UTC+00:00) ▾" and "Query details".

## Lab 2.2 Enable Microsoft Defender for Cloud.

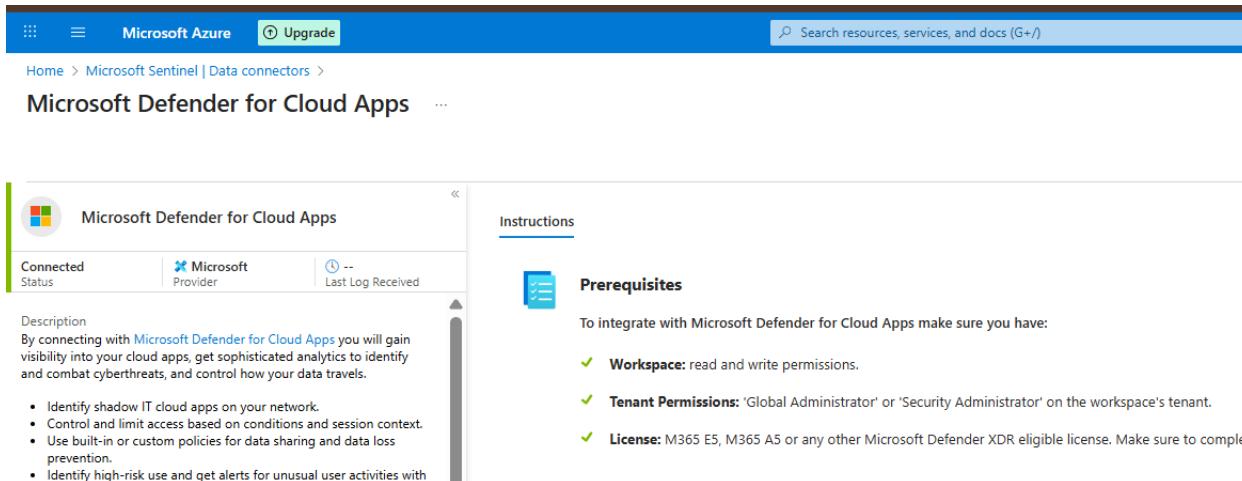
It provides **cloud workload protection** and **security posture management** across Azure, hybrid, and multicloud environments. In practice, it helps you detect threats, harden configurations, and protect resources like VMs, databases, containers, and storage.

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



The screenshot shows the Microsoft Defender Content Hub interface. On the left, there's a navigation sidebar with options like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management (Content hub is selected), Configuration, and Tables. The main area has a search bar at the top with the query "Defender for cloud". Below the search is a table with columns for Content title, Status, and Content source. One row is highlighted: "Microsoft Defender for C..." with a "FEATURED" badge, showing "Not installed" under Status and "Solution" under Content source. To the right of the table, there's a detailed view of the "Microsoft Defender for Cloud" solution. It includes sections for Microsoft Provider (Microsoft), Microsoft Support, Version (3.0.3), Note (refer to Release Notes), Underlying Microsoft Technologies used (Azure Monitor HTTP Data Collector API, Data Connectors: 2, Analytics Rules: 1), and Pricing (Free). At the bottom right of this panel are "Install" and "View details" buttons.

### 2.2.2 Checkout the Status is Connected



The screenshot shows the Microsoft Azure portal. The top navigation bar includes "Microsoft Azure", "Upgrade", and a search bar. Below the bar, the URL is "Home > Microsoft Sentinel | Data connectors > Microsoft Defender for Cloud Apps". The main content area is titled "Microsoft Defender for Cloud Apps". It shows a summary card with "Connected Status" (green), "Microsoft Provider" (blue), and "Last Log Received" (grey). The card also lists "Description" which says: "By connecting with Microsoft Defender for Cloud Apps you will gain visibility into your cloud apps, get sophisticated analytics to identify and combat cyberthreats, and control how your data travels." Below the card, there's a bulleted list of benefits: "Identify shadow IT cloud apps on your network.", "Control and limit access based on conditions and session context.", "Use built-in or custom policies for data sharing and data loss prevention.", and "Identify high-risk use and get alerts for unusual user activities with". To the right of the card, there's a "Instructions" section with a "Prerequisites" sub-section. The prerequisites list includes: "To integrate with Microsoft Defender for Cloud Apps make sure you have:", "Workspace: read and write permissions.", "Tenant Permissions: 'Global Administrator' or 'Security Administrator' on the workspace's tenant.", and "License: M365 E5, M365 A5 or any other Microsoft Defender XDR eligible license. Make sure to complete".

## 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. On the left, there's a sidebar with various navigation options like Threat management, Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization, Content management, Content hub, Repositories, Community, Configuration, Workspace manager (Preview), Data connectors, Analytics, Summary rules, Watchlist, Automation, and Settings. The main area displays a list of installed solutions under the heading '448 Solutions'. One solution, 'Threat Intelligence Taxii', is highlighted and expanded. It shows details such as 'Status: All', 'Content type: All', 'Support: All', 'Provider: All', 'Category: All', and 'Content sources: All'. The solution has 7 Installed and 0 Updates. A preview window for 'Threat Intelligence (NEW)' is open, showing a Microsoft Provider, Microsoft Support, and Version 3.0.10. The preview includes a note about the solution's purpose, supported content types (Analytics rule, Data connector, Hunting query), and its recent improvements. It also lists the number of connectors, parsers, workbooks, and analytic rules.

### 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 profile page for a user named 'rhythmsharma777'. The profile page includes a sidebar with links for Overview, Activity, Subscriptions, Your Data, Delete Account, and Sign Out. The main content area shows the user's name 'rhythmsharma' and a blurred profile picture. Below the name are sections for Actions, Update Information, and Change Password. Under the User section, it shows the role as 'LAB' and provides fields for Email, Title, and Organization, all of which are currently set to 'LAB'.

## 2.2.3 Enter Required Information From Pulsedive Server and Add

The screenshot shows the Microsoft Sentinel Threat intelligence - TAXII page. On the left, there's a sidebar with a disconnected status, provider information (Microsoft), and last log received (45 seconds ago). It also displays content source (Threat Intelligence (NEW)), version (1.0.0), author (Microsoft), and supported by (Microsoft Corporation | Email). Below this is a section for related content with 0 workbooks, 4 queries, and 47 Analytics rules templates. A chart titled 'Data received' shows a sharp increase from 0 to approximately 65 units over time. On the right, there's a configuration panel for adding a TAXII server, a list of configured servers, and a search bar.

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) \*

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 ⓘ Version

Threat Intelligence (NEW) 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) \*

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 ⓘ Version

Threat Intelligence (NEW) 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

List of configured TAXII servers

Friendly name	TAXII server	Collection ID	Last indicator r...	Polling freque...
https://pulsedive.com/taxii2/api/	981c4916-ebb2...	--	Once an hour	...