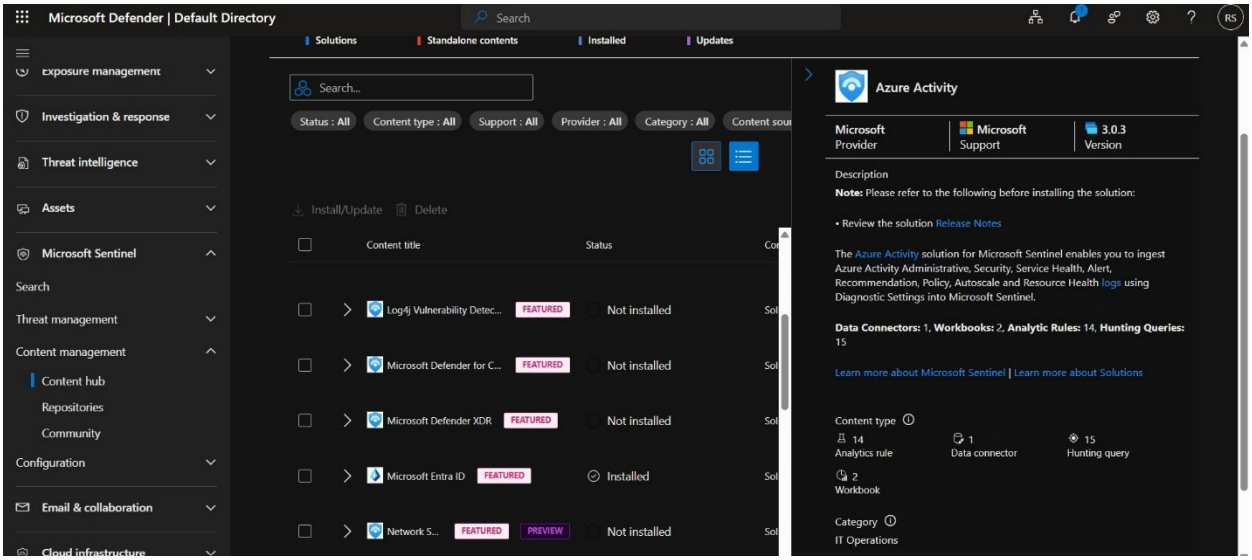
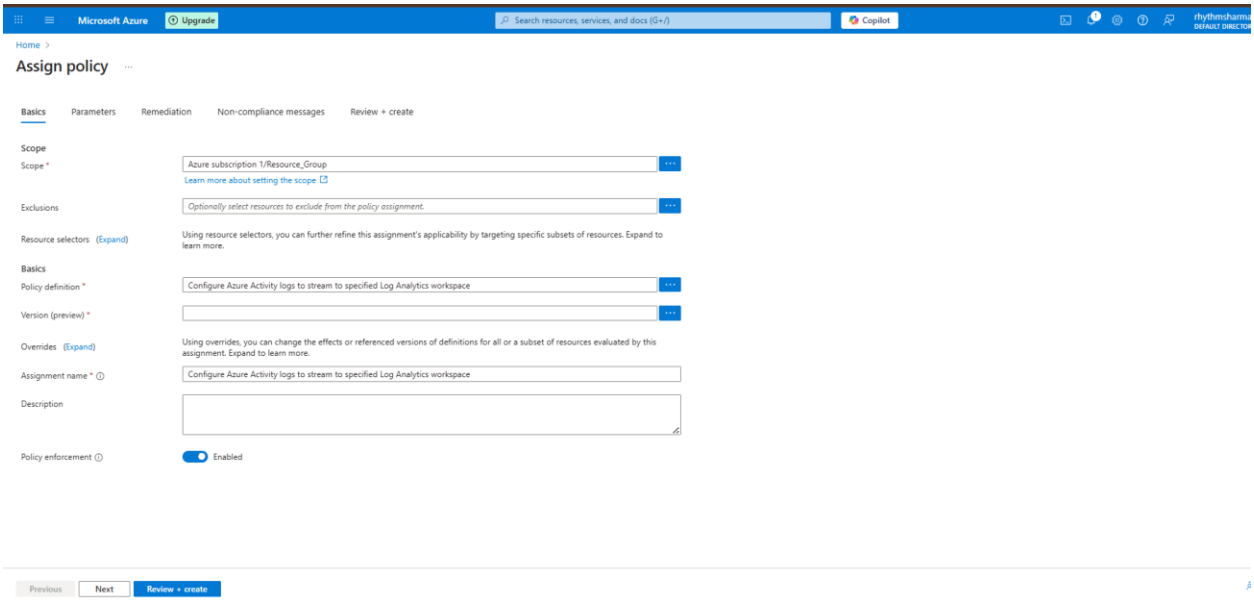
Lab 2.1 Enable Azure Activity

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

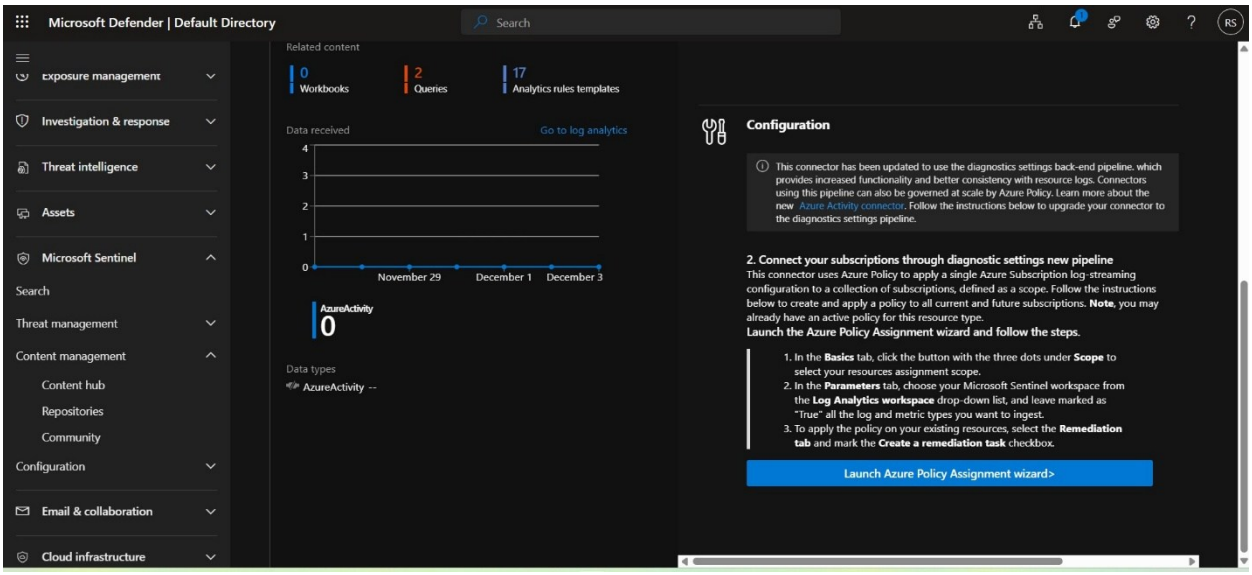
2.1.1: Go to Content Hub and Search for Azure Activity and Install it.



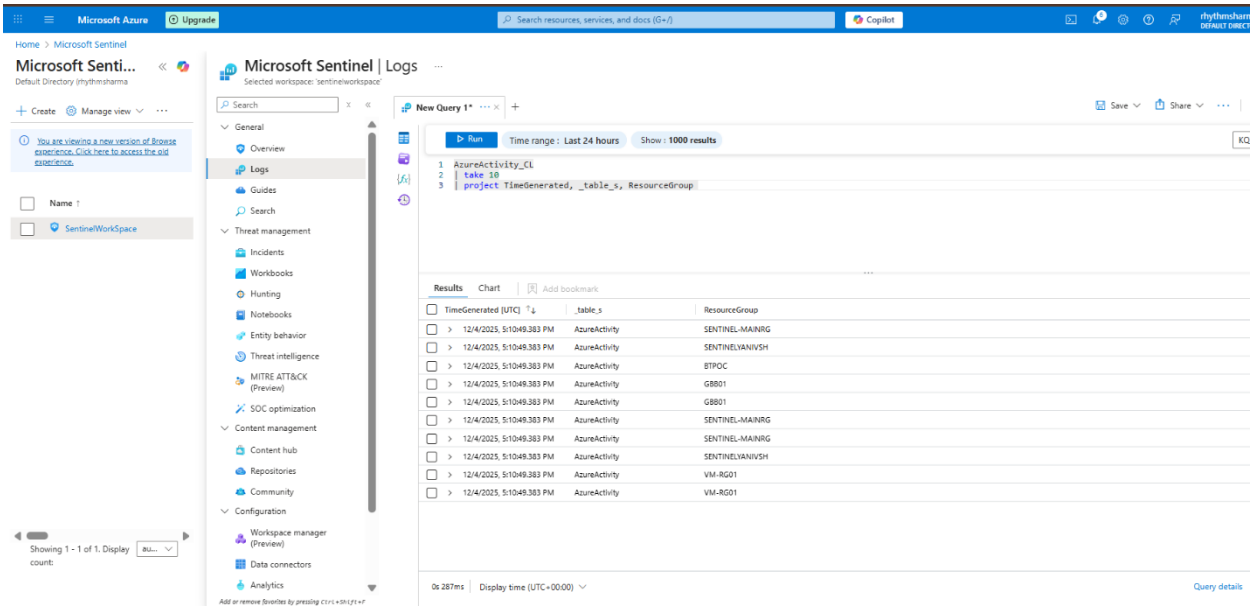
2.1.2 Open Connector Page and linking to Resource Group



2.1.3 Go back to Sentinel



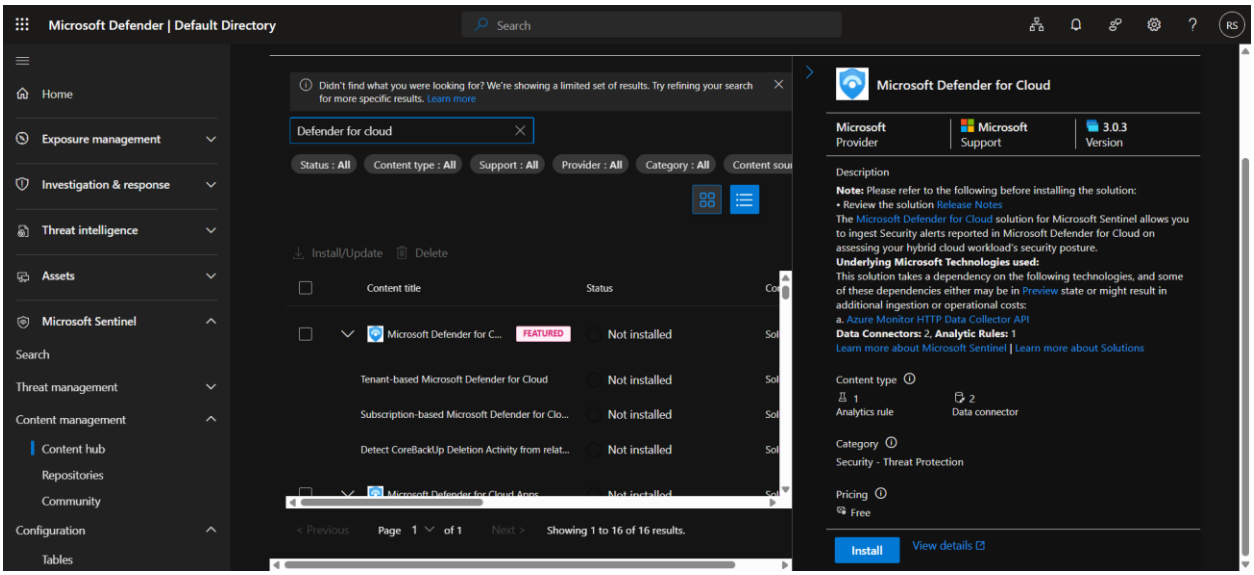
2.1.4 Go to Logs To Verify Azure Activity



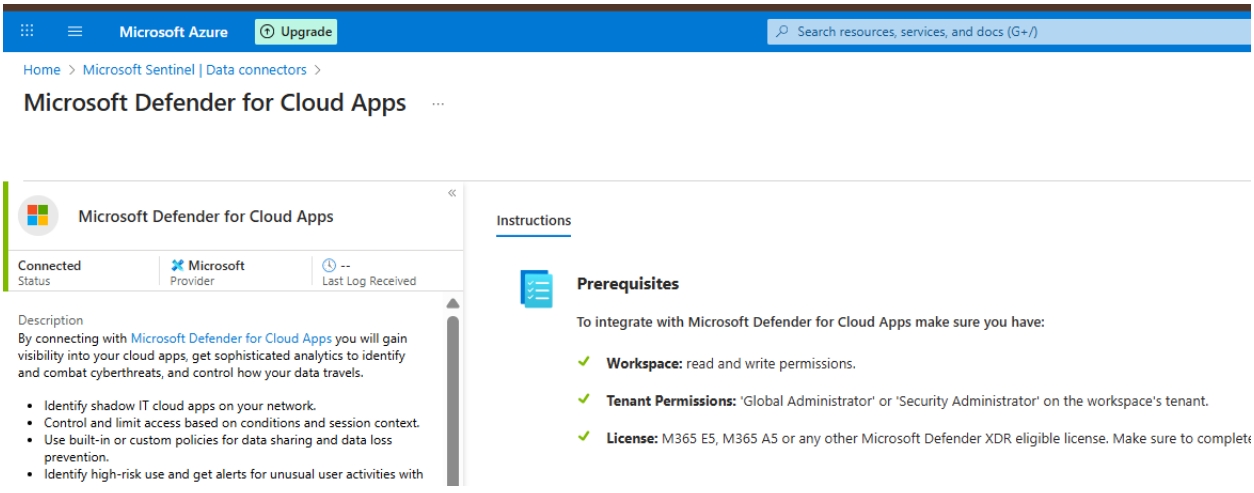
Lab 2.2 Enable **Microsoft Defender for Cloud**.

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



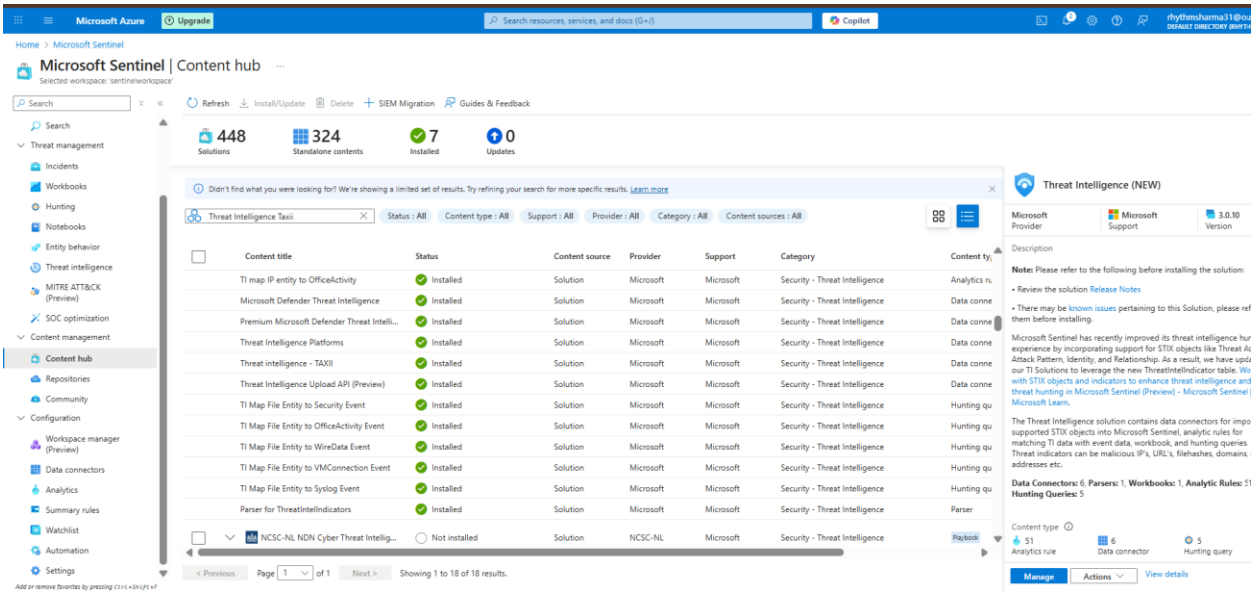
2.2.2 Checkout the Status is Connected



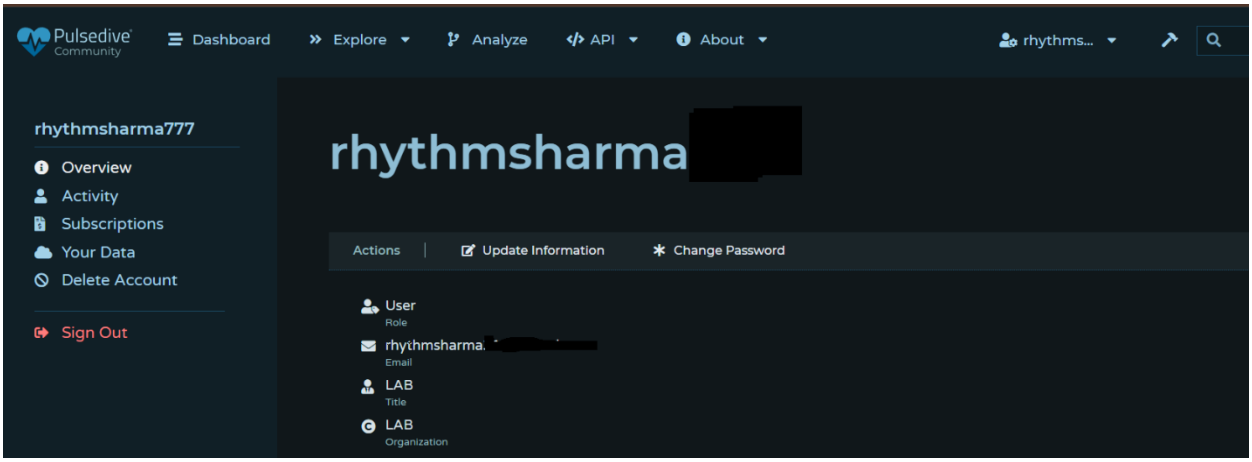
2.3. Connect Threat Intelligence TAXII Data Connectors

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



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



2.2.3 Enter Required Information From Pulsedive Server and Add