COURSE: CLOUD AND NEWTORK SECURITY
NAME: DENISE SOPHY ONDISO MUTAYI
STUDENT NO: CS-CN09-25047

AZURE MONITOR, MICROSOFT DEFENDER FOR CLOUD, ENABLE JUST-IN TIME ACCESS IN VMS, MICROSOFT SENTINEL

Table of Contents.

Introduction

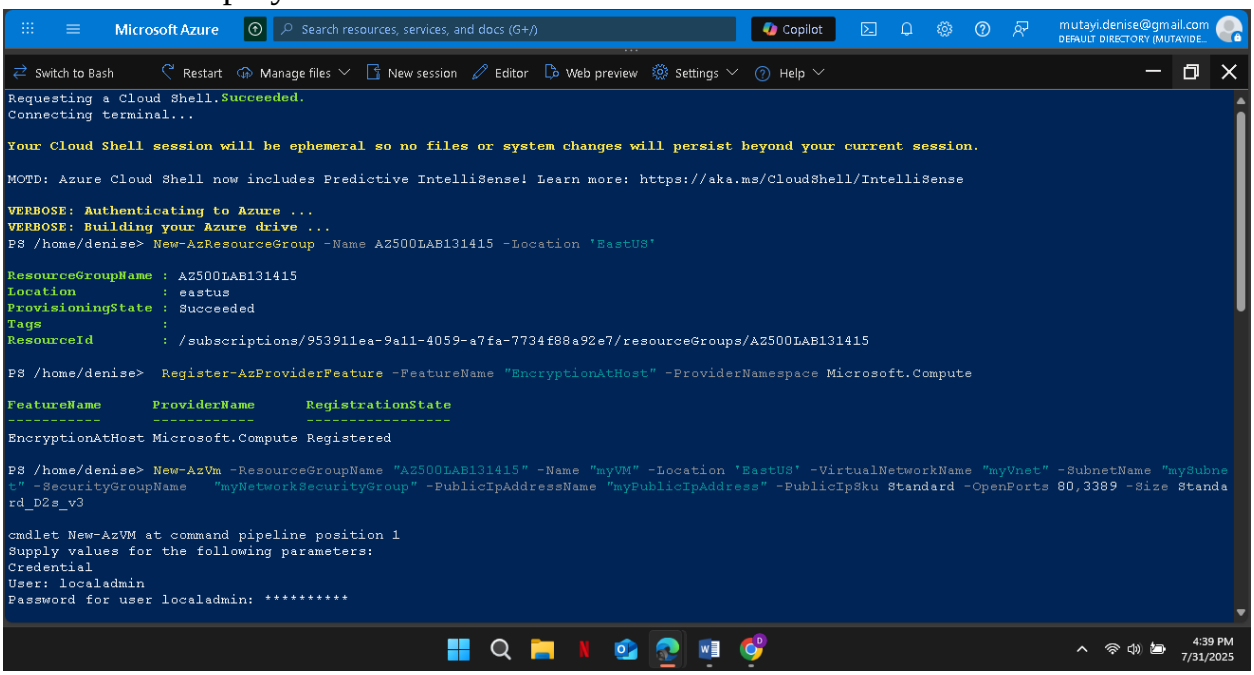
In this lab series, I configured and implemented several security features using Microsoft Defender for Cloud and Microsoft Sentinel on Azure. I began by deploying an Azure virtual machine in the East US region, followed by the creation of a Log Analytics workspace, an Azure storage account, and a data collection rule (DCR) to collect performance counters and event logs. These components were essential in establishing a central point for monitoring and telemetry collection.

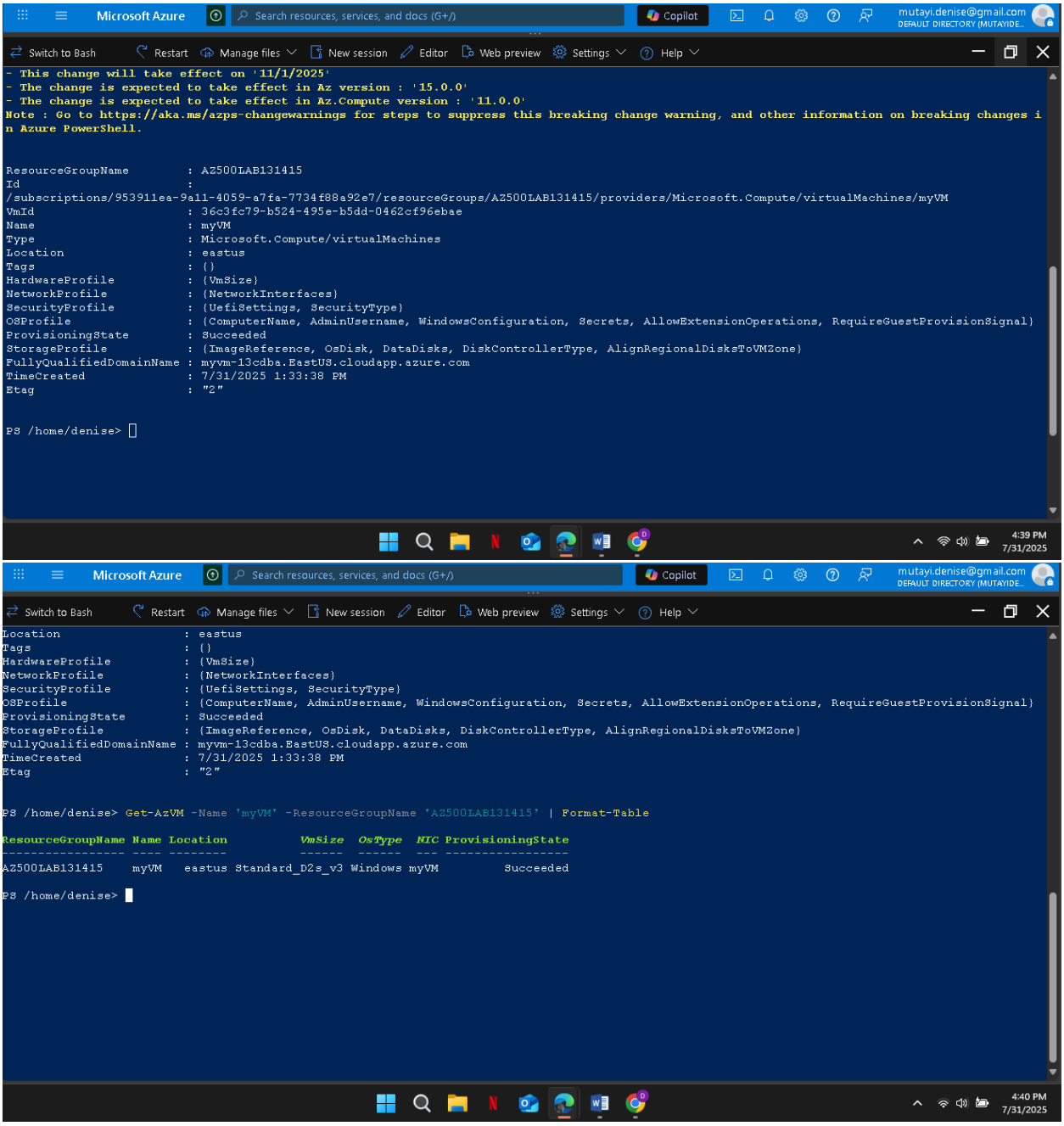
Next, I enabled Microsoft Defender for Servers Plan 2 under Cloud Workload Protection (CWP), which provided enhanced security features, including vulnerability assessment, endpoint detection and response (EDR), and just-in-time (JIT) access for virtual machines. I then configured JIT VM access on the deployed virtual machine to minimize exposure to threats by restricting open ports and access duration.

Finally, I onboarded Microsoft Sentinel by connecting it to the previously created Log Analytics workspace. I configured data connectors to collect logs from Azure Activity and Defender for Cloud, created built-in and custom analytics rules to detect suspicious activity, and built a playbook using a Logic App to automate incident response. I also simulated an incident by deleting a JIT access policy to verify that Microsoft Sentinel correctly triggered the alert and executed the playbook.

Lab 08: Create a Log Analytics Workspace, Azure Storage Account, and Data Collection Rule (DCR)

Exercise 1: Deploy an Azure virtual machine

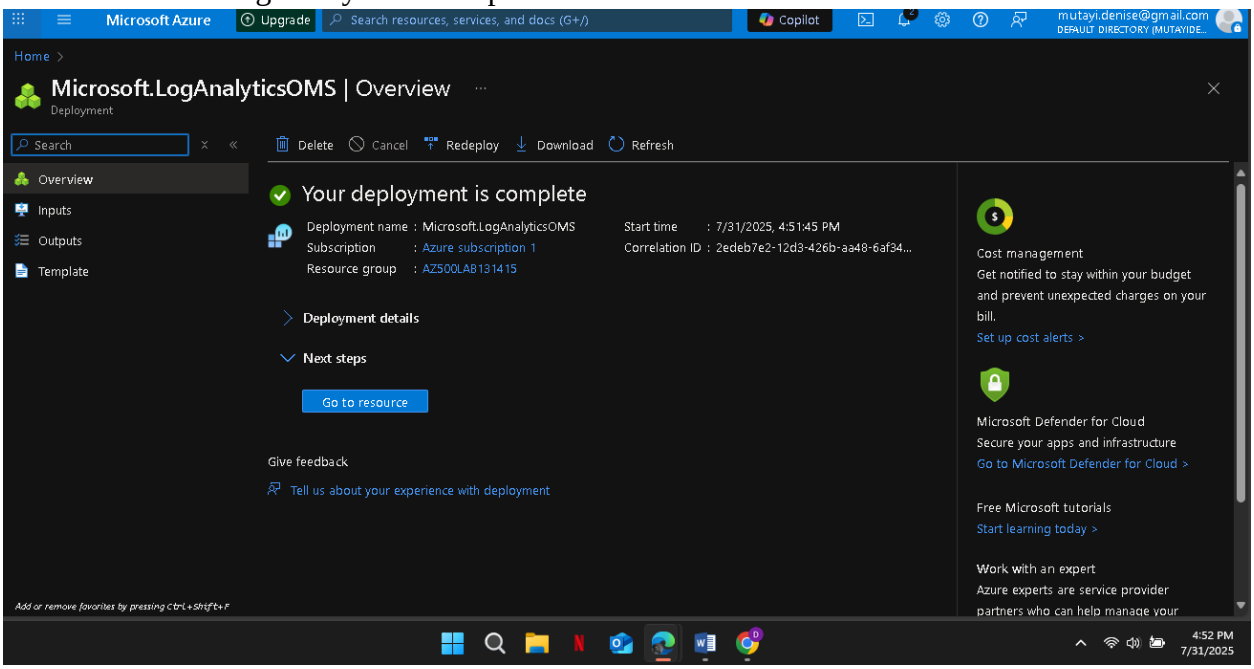


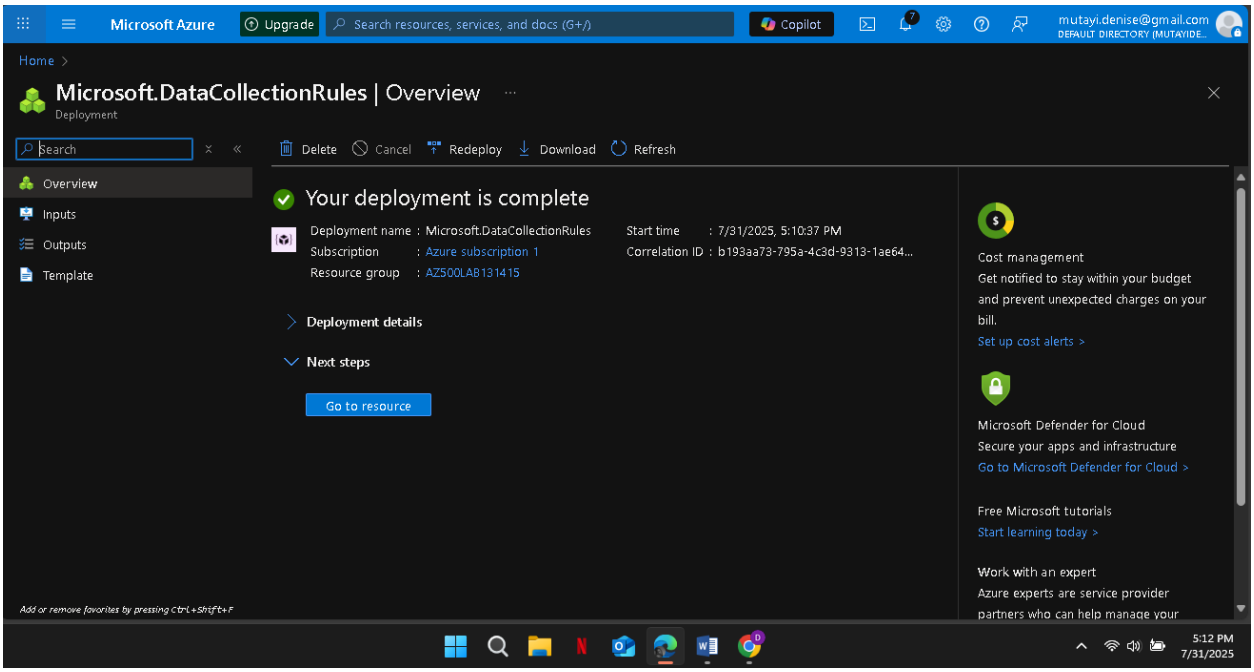


Created a new resource group and deploy a Windows-based virtual machine using PowerShell in Azure Cloud Shell.

Exercise 2: Create an Log Analytics workspace

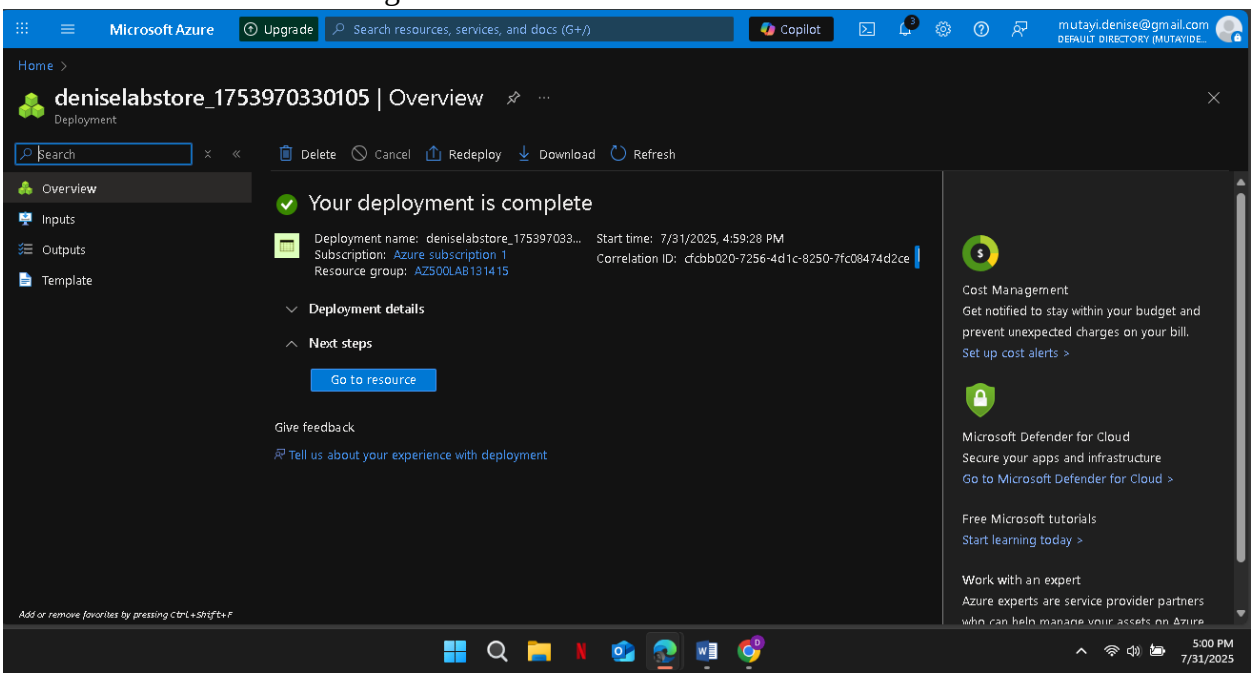
Task 1: Create a Log Analytics workspace





Exercise 3: Create an Azure storage account

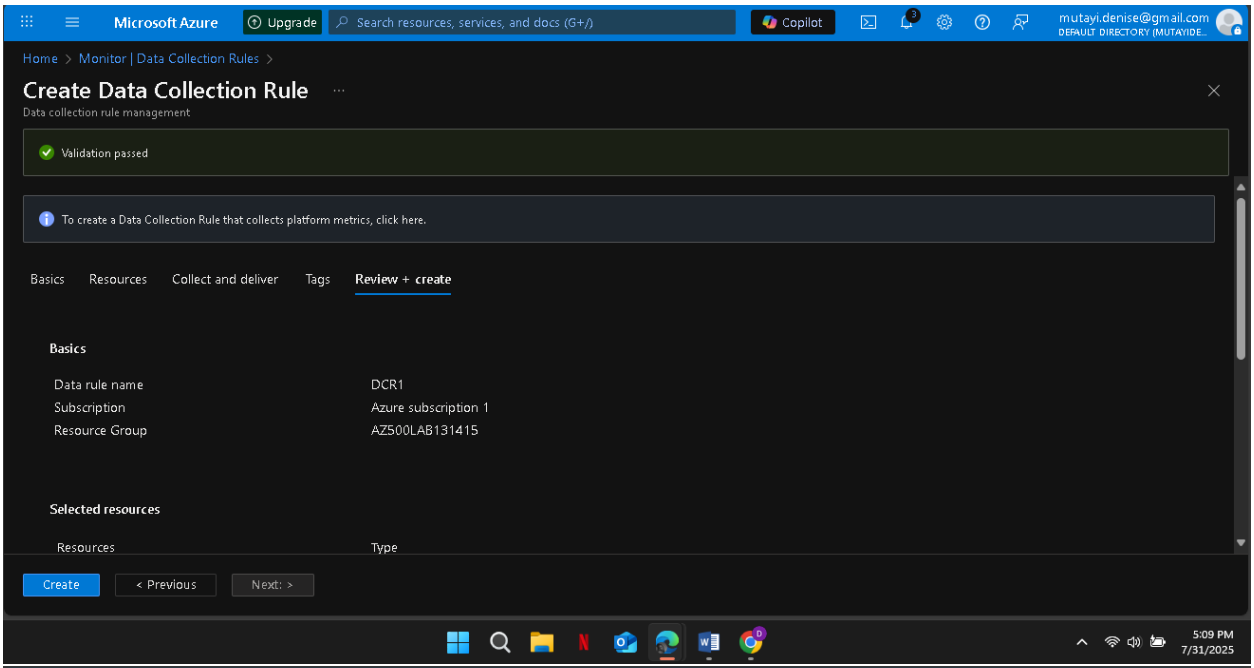
Task 1: Create an Azure storage account

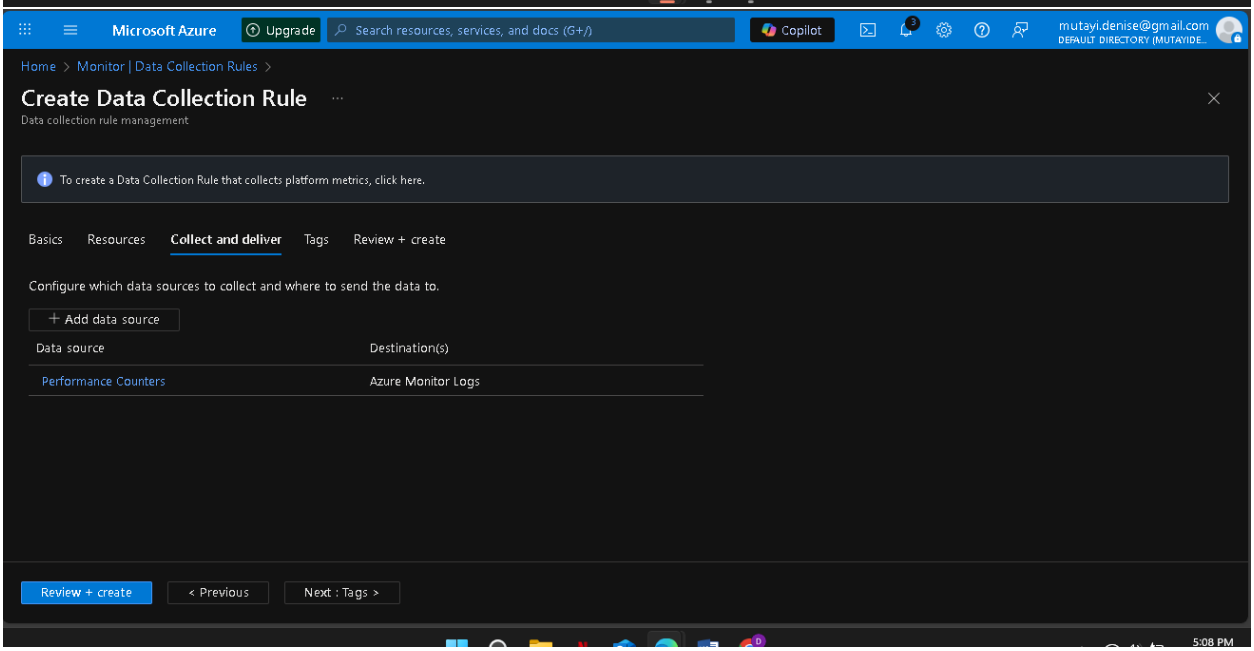


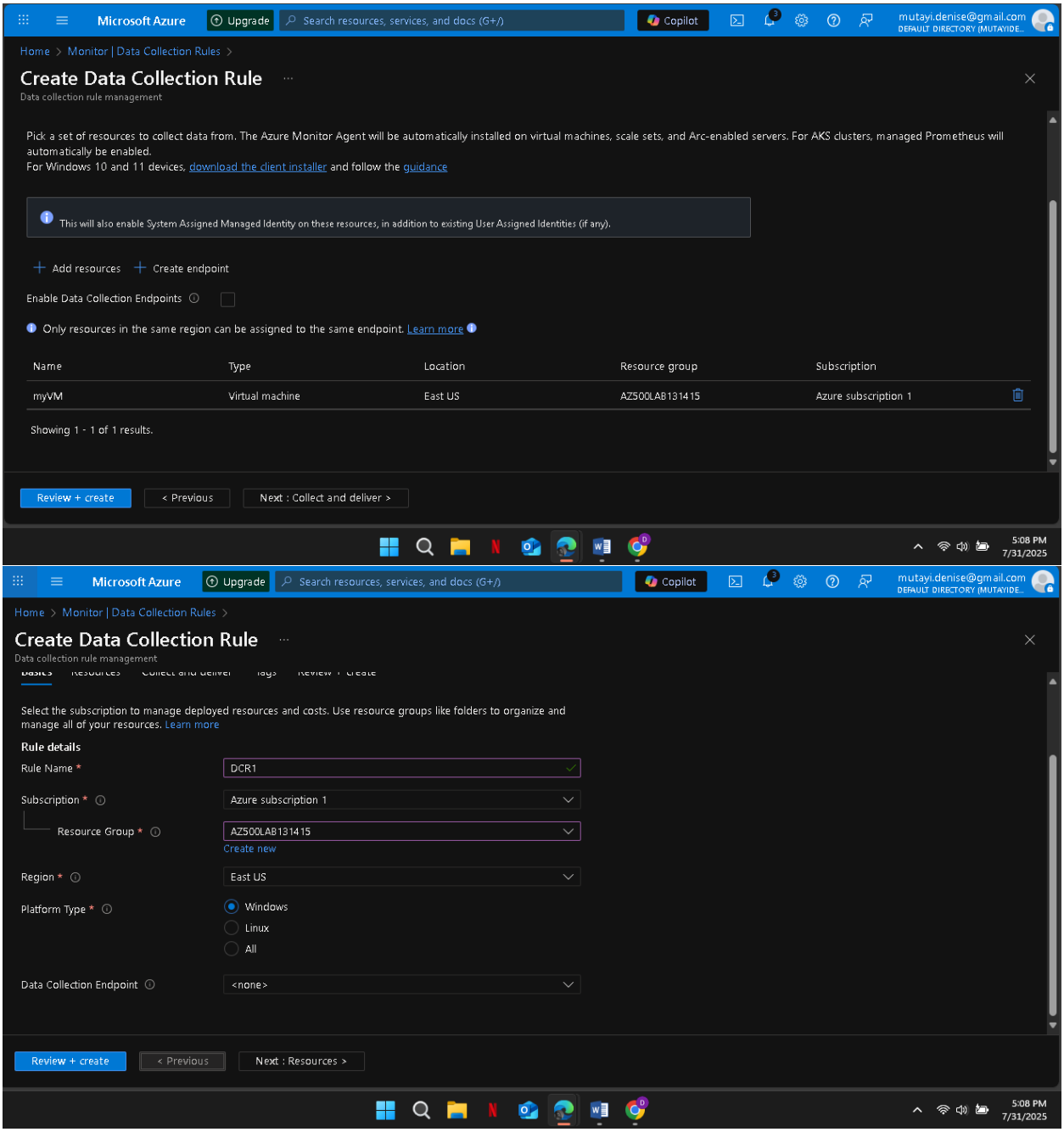
Created an Azure storage account

Exercise 4: Create a Data Collection Rule

Task 1: Create a Data Collection Rule.



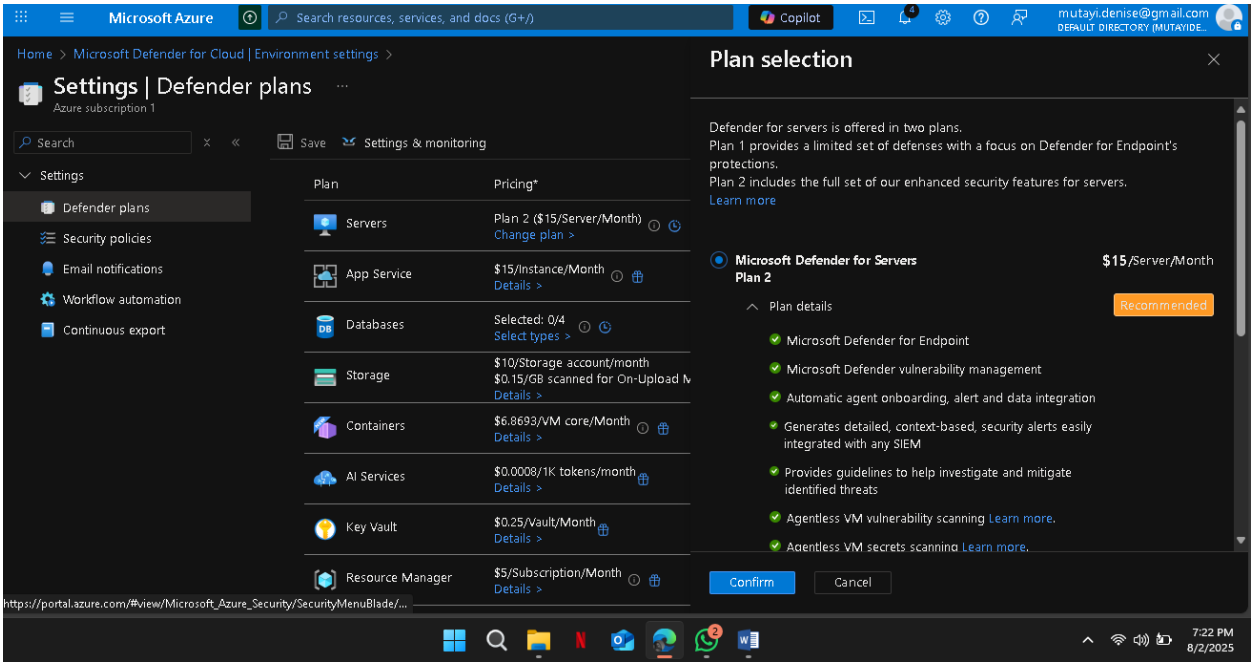




Created a data collection rule

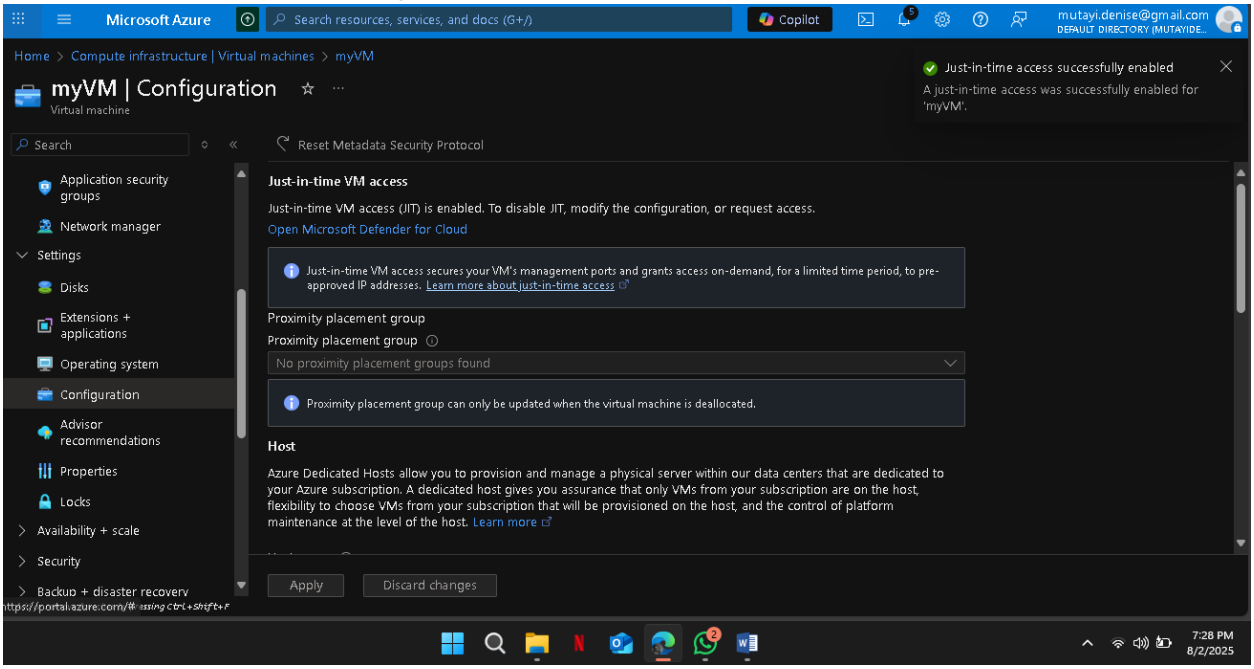
Lab 09: Configuring Microsoft Defender for Cloud Enhanced Security Features for Servers

Configure Microsoft Defender for Cloud Enhanced Security Features for Serve

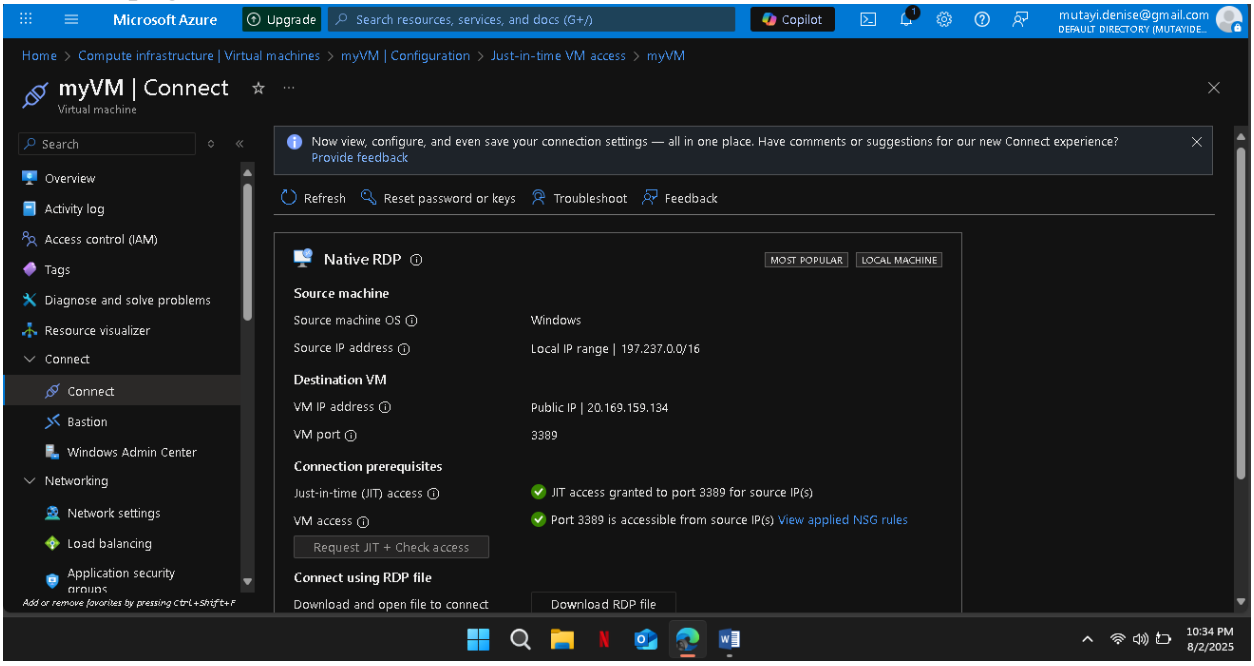


Lab 10: Enable just-in-time access on VMs

Exercise 1: Enable JIT on your VMs from Azure virtual machines



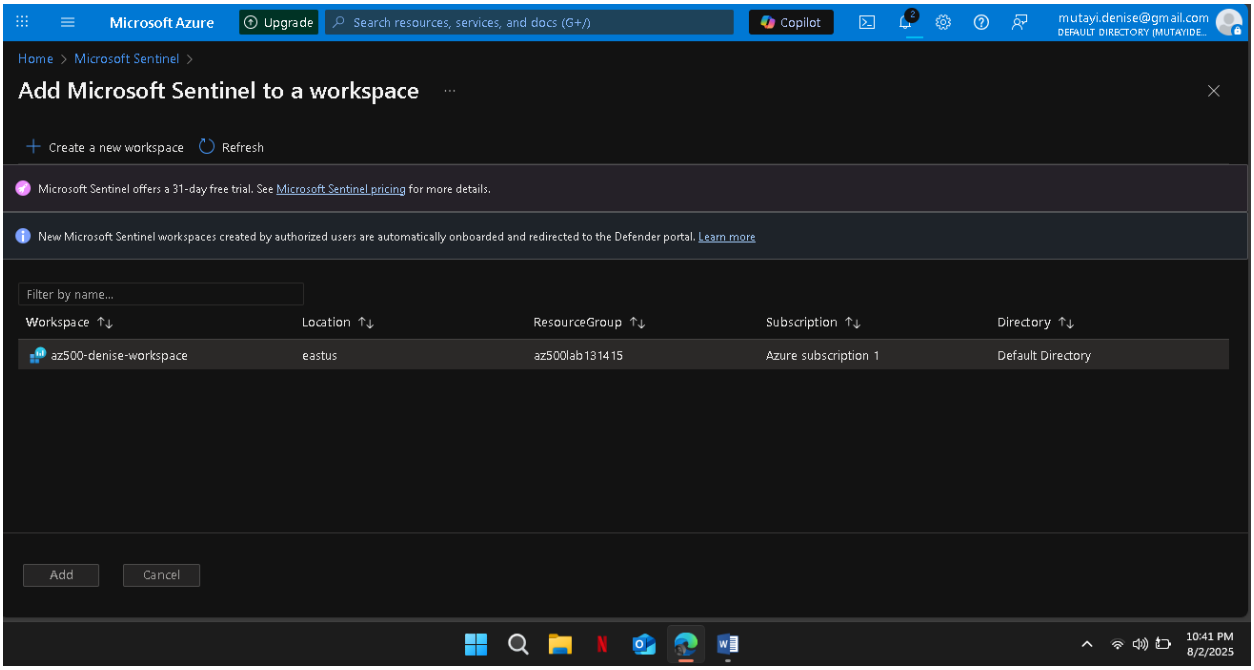
Exercise 2: Request access to a JIT-enabled VM from the Azure virtual machine's connect page.

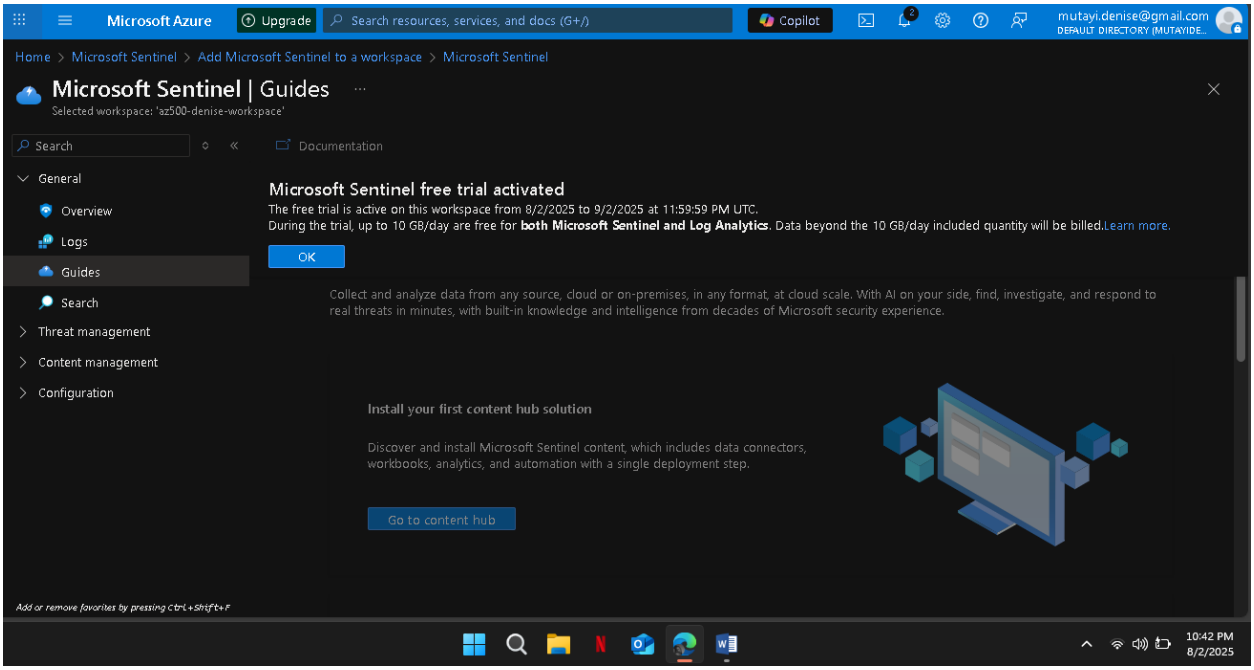


Lab 11: Microsoft Sentinel

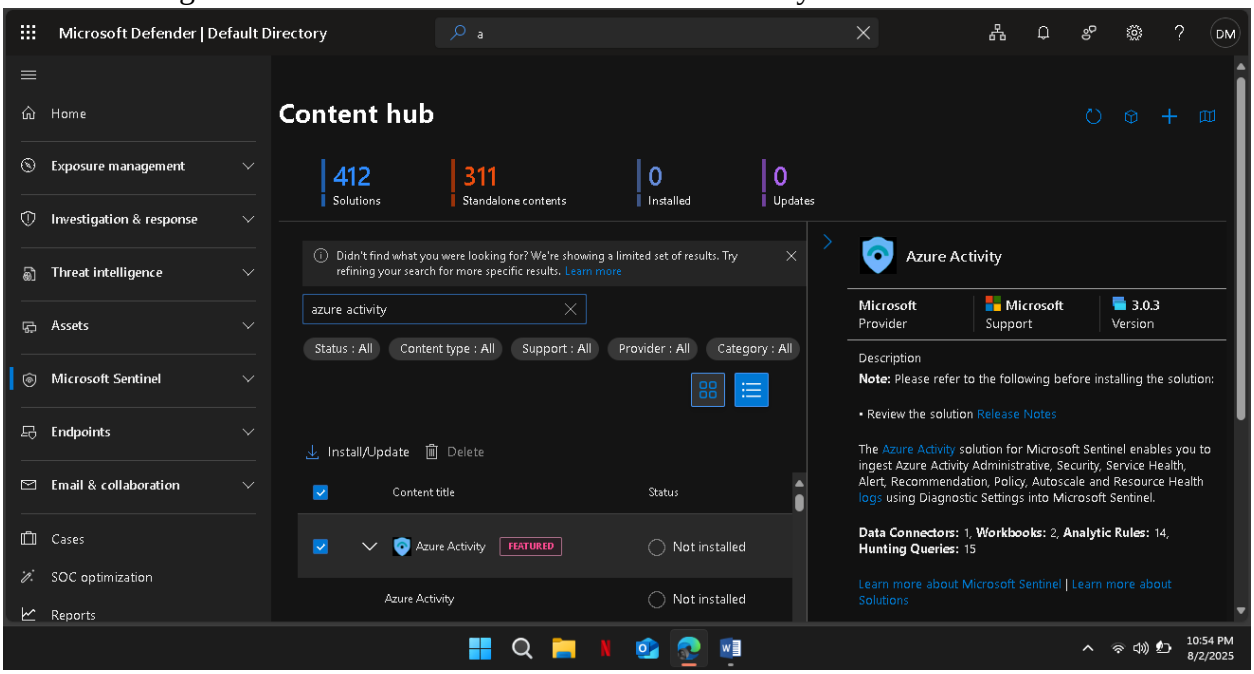
Exercise 1: Implement Microsoft Sentinel

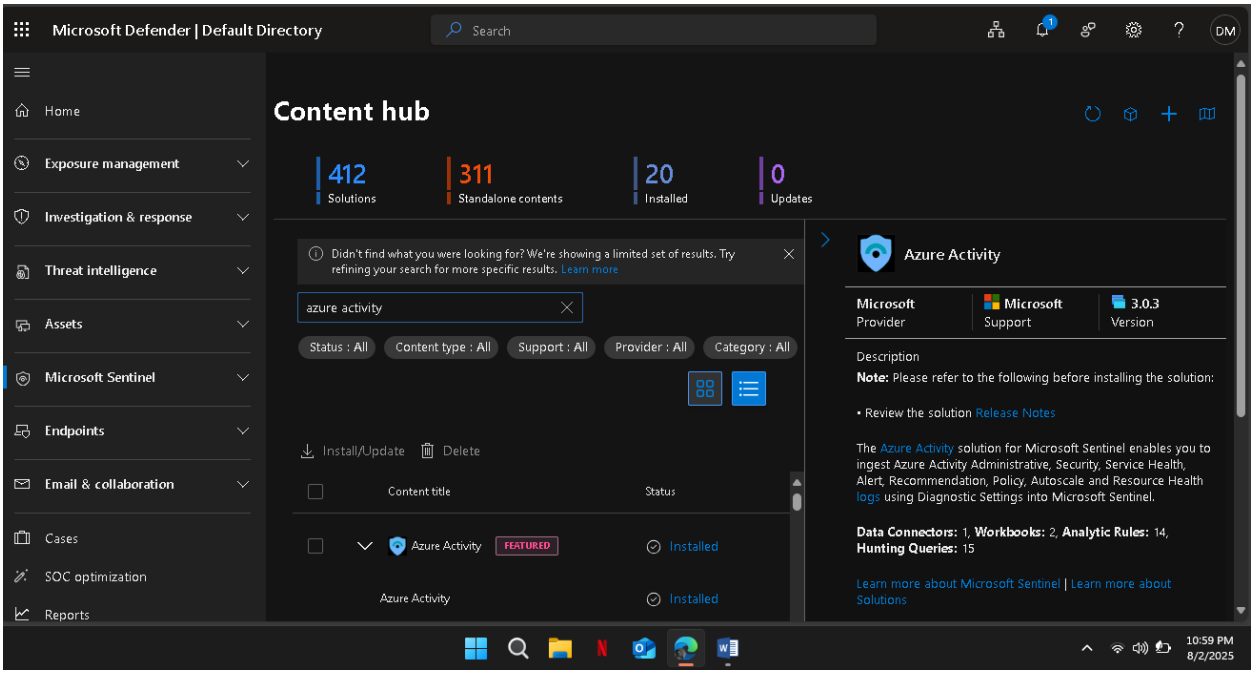
Task 1: On-board Microsoft Sentinel

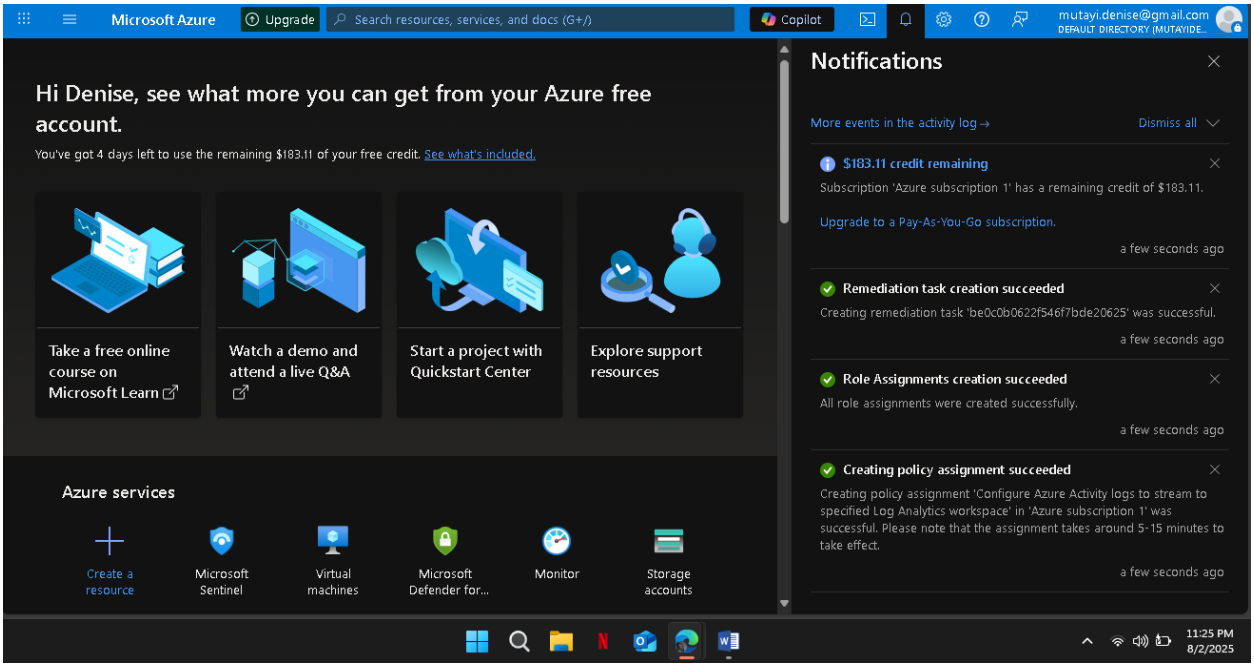




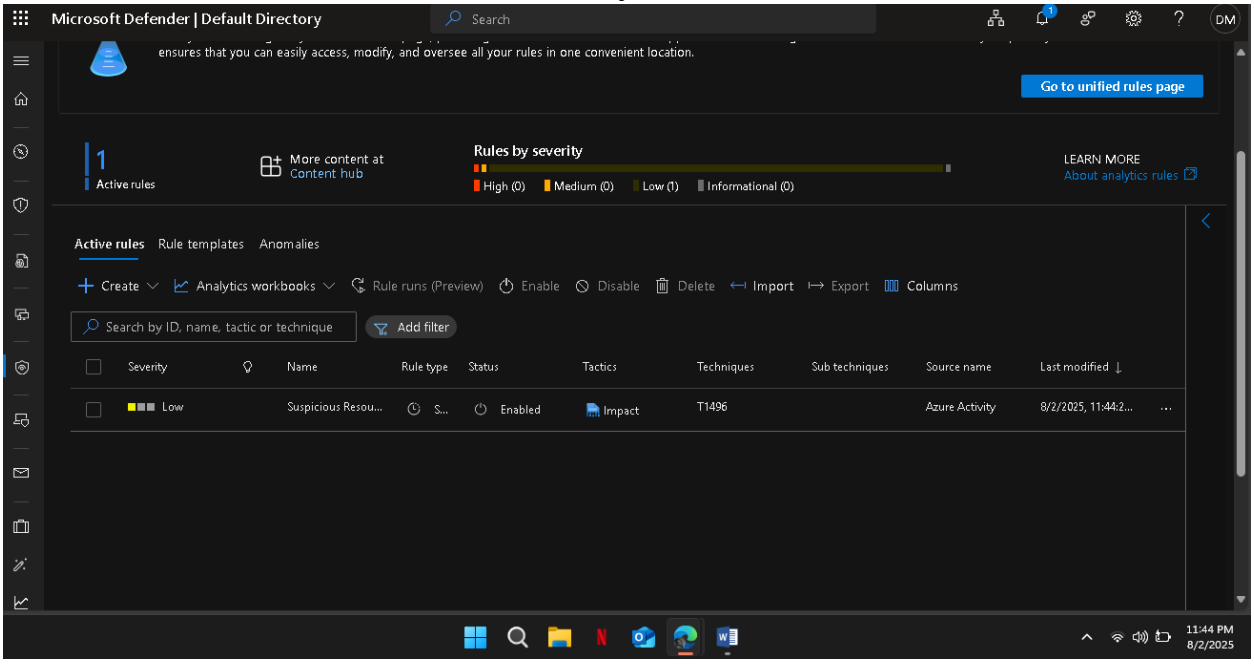
Task 2: Configure Microsoft Sentinel to use the Azure Activity data connector.




Microsoft Defender | Default Directory
Search
DM
Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Endpoints
Email & collaboration
Cases
SOC optimization
Reports
Content hub
412
Solutions
311
Standalone contents
20
Installed
0
Updates
Didn't find what you were looking for? We're showing a limited set of results. Try refining your search for more specific results. Learn more
azure activity
Status : All
Content type : All
Support : All
Provider : All
Category : All
Install/Update
Delete
Content title
Status
Azure Activity
FEATURED
Installed
Azure Activity
Installed
Azure Activity
Microsoft
Provider
Microsoft
Support
3.0.3
Version
Description
Note: Please refer to the following before installing the solution:
• Review the solution Release Notes
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
Learn more about Microsoft Sentinel | Learn more about Solutions
10:59 PM
8/2/2025

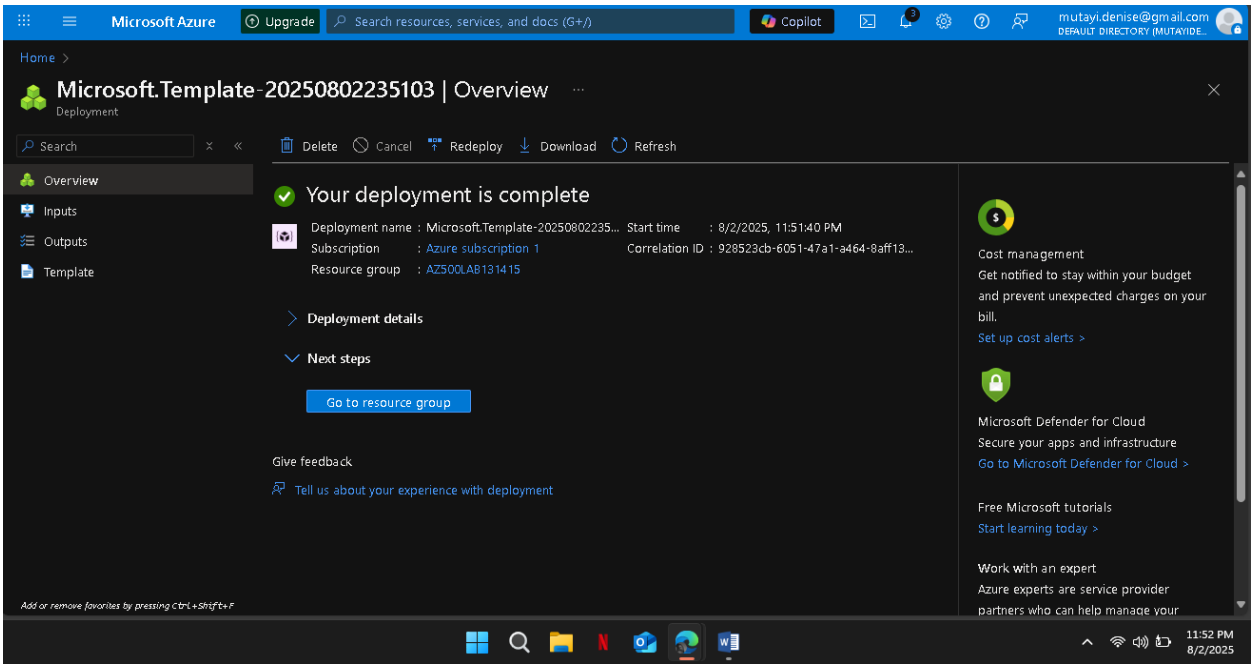

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
mutayi.denise@gmail.com
DEFAULT DIRECTORY (MUTAVIDE...
Hi Denise, see what more you can get from your Azure free account.
You've got 4 days left to use the remaining $183.11 of your free credit. See what's included.
Take a free online course on Microsoft Learn
Watch a demo and attend a live Q&A
Start a project with Quickstart Center
Explore support resources
Azure services
Create a resource
Microsoft Sentinel
Virtual machines
Microsoft Defender for...
Monitor
Storage accounts
Notifications
More events in the activity log →
Dismiss all
$183.11 credit remaining
Subscription 'Azure subscription 1' has a remaining credit of $183.11.
Upgrade to a Pay-As-You-Go subscription.
a few seconds ago
Remediation task creation succeeded
Creating remediation task 'be0c0b0622f546f7bde20625' was successful.
a few seconds ago
Role Assignments creation succeeded
All role assignments were created successfully.
a few seconds ago
Creating policy assignment succeeded
Creating policy assignment 'Configure Azure Activity logs to stream to specified Log Analytics workspace' in 'Azure subscription 1' was successful. Please note that the assignment takes around 5-15 minutes to take effect.
a few seconds ago
11:25 PM
8/2/2025

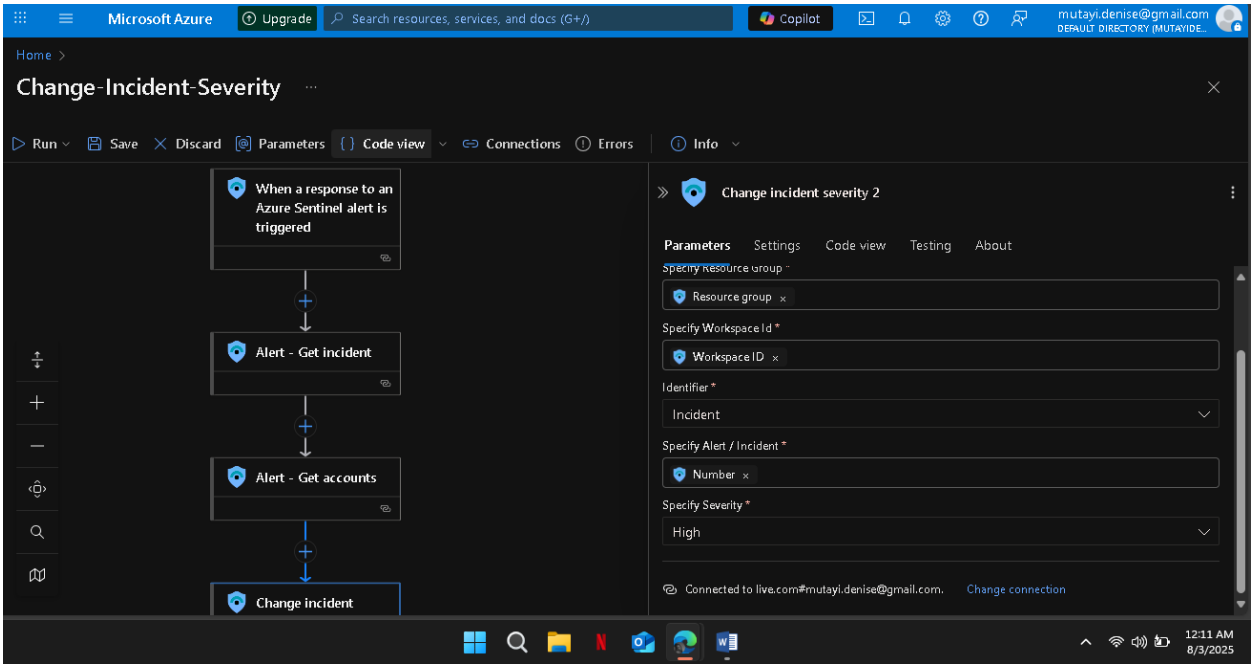
Task 3: Create a rule that uses the Azure Activity data connector.

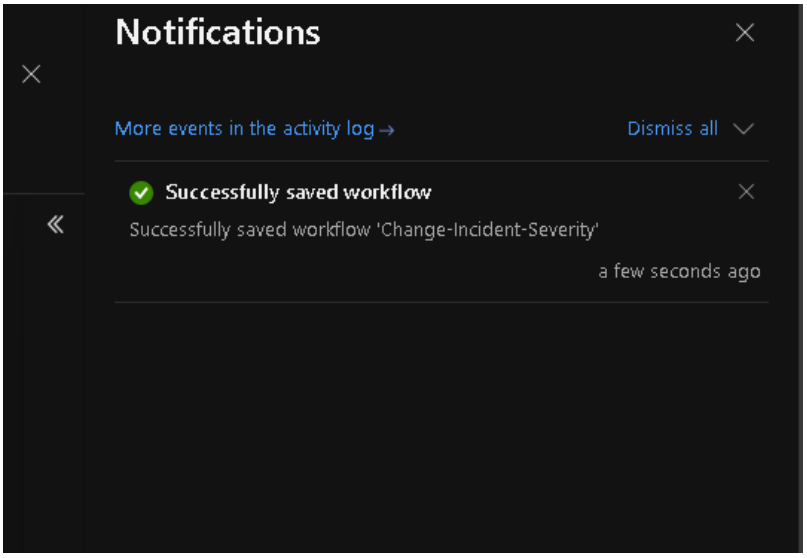


Task 4: Create a playbook

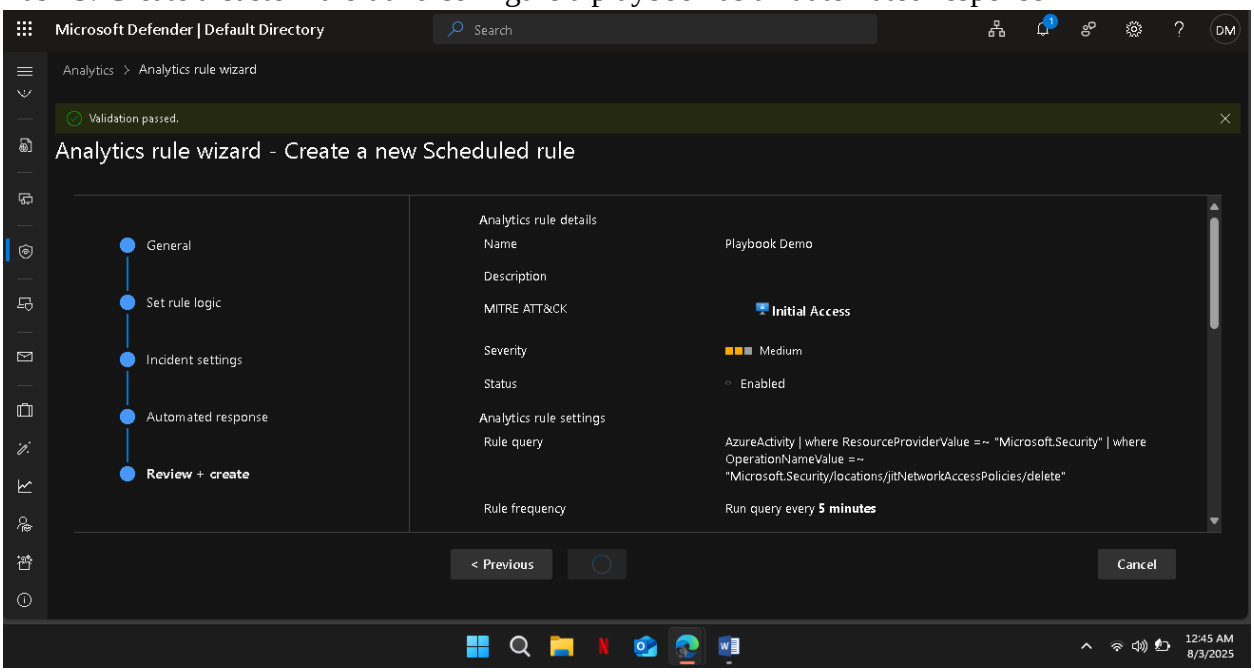
A security playbook is a collection of tasks that can be invoked by Microsoft Sentinel in response to an alert.

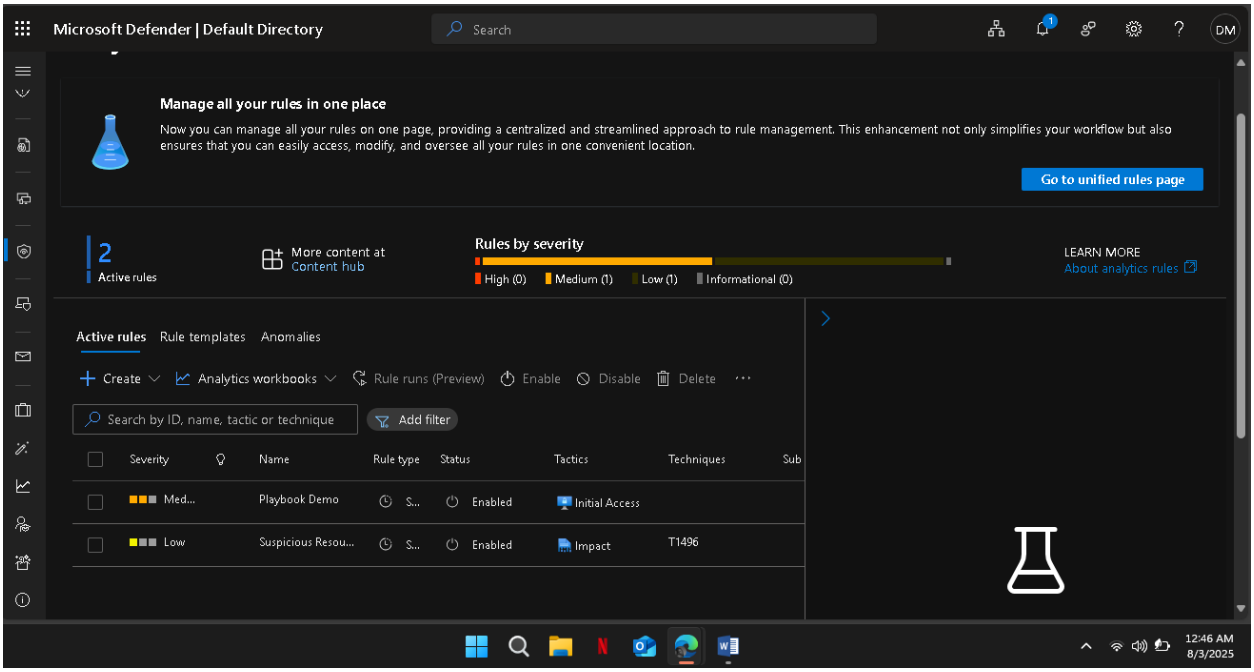



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
mutayi.denise@gmail.com
DEFAULT DIRECTORY (MUTAYIDE...
Home
Change-Incident-Severity
Run
Save
Discard
Parameters
Code view
Connections
Errors
Info
When a response to an Azure Sentinel alert is triggered
Alert - Get incident
Alert - Get accounts
Change incident
Change incident severity 2
Parameters
Settings
Code view
Testing
About
Specify Resource Group *
Resource group
Specify Workspace Id *
Workspace ID
Identifier *
Incident
Specify Alert / Incident *
Number
Specify Severity *
High
Connected to live.com#mutayi.denise@gmail.com.
Change connection
12:11 AM
8/3/2025

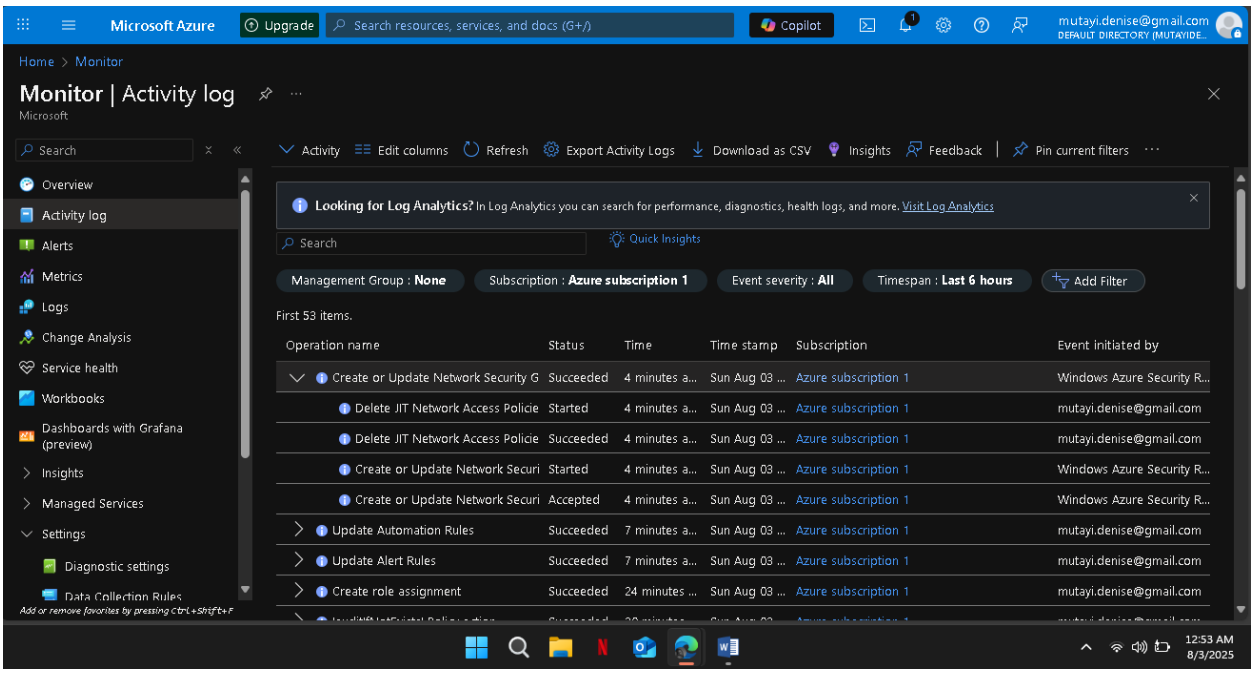

Notifications
More events in the activity log →
Dismiss all
Successfully saved workflow
Successfully saved workflow 'Change-Incident-Severity'
a few seconds ago

Task 5: Create a custom alert and configure a playbook as an automated response

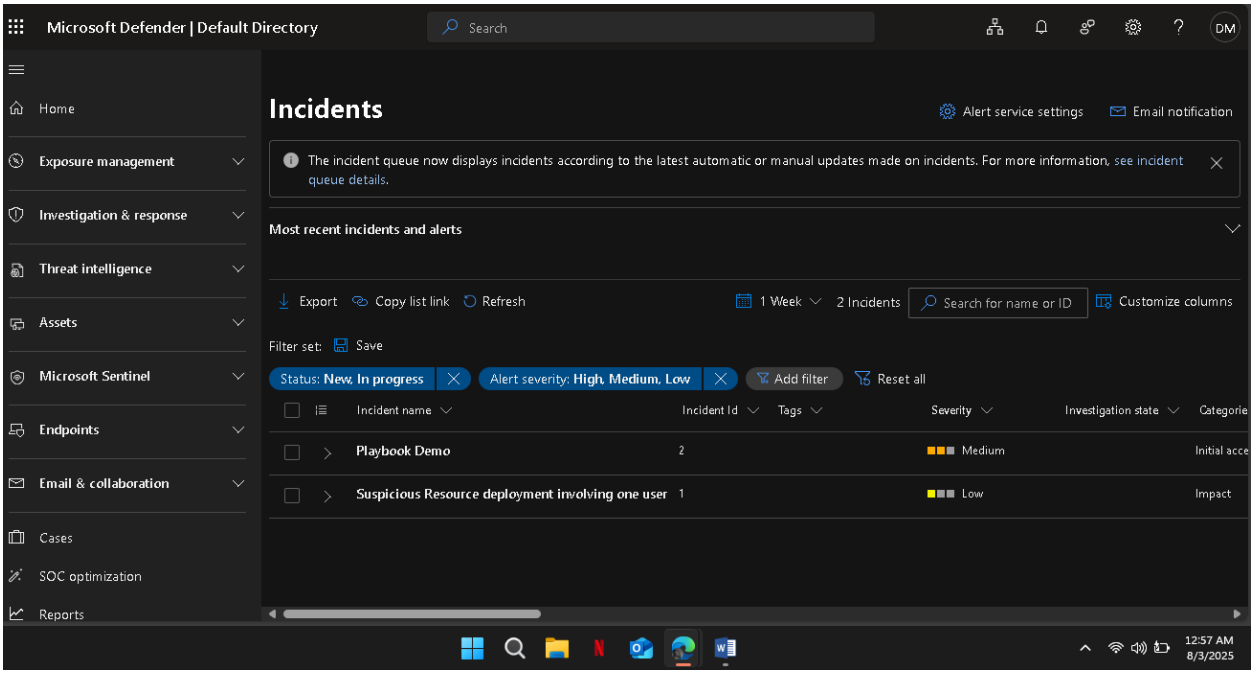




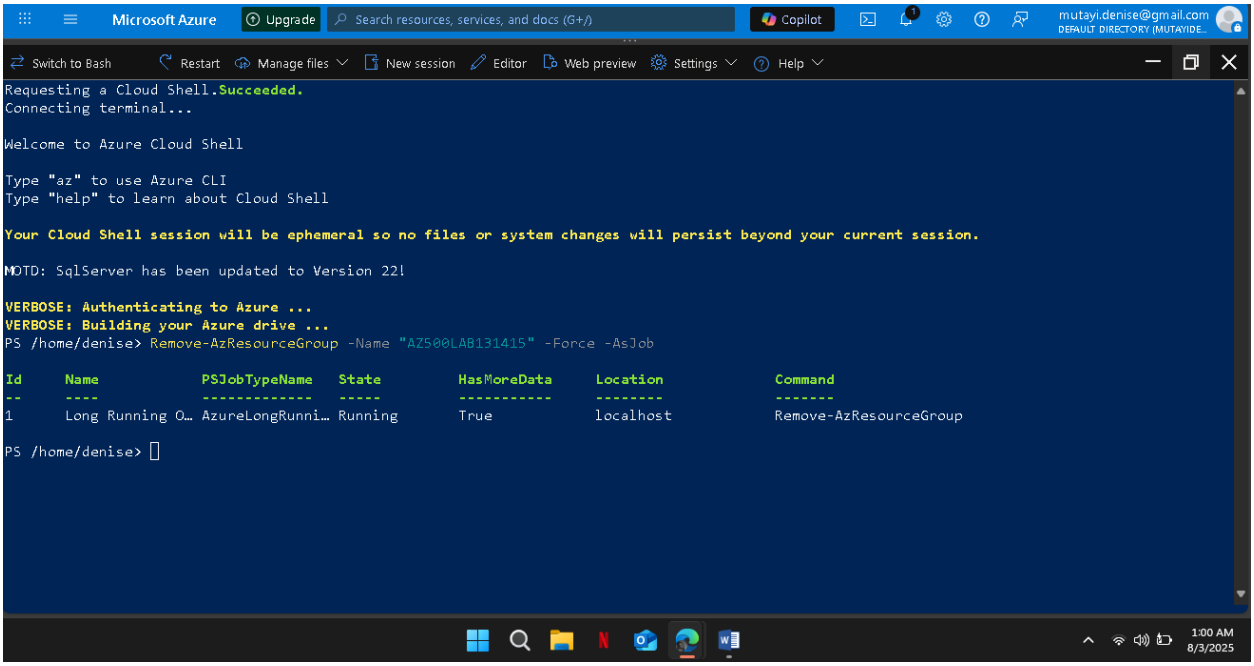
Task 6: Invoke an incident and review the associated actions.



Deleted JIT Network Access Policies entry.



An incident of medium seniority.



Cleaning up resources

Conclusion

By completing these labs, I implemented a full-stack security monitoring and automation solution on Azure. I successfully deployed the infrastructure, enabled Microsoft Defender for Servers, configured just-in-time VM access, and integrated Azure Activity logs into Microsoft Sentinel. I created analytics rules and a custom playbook that responded to specific security events, such as the removal of a JIT access policy.

This process allowed me to observe how Microsoft Sentinel and Defender for Cloud work together to detect threats, trigger alerts, and respond through automation. The hands-on experience gave me practical skills in setting up cloud-based threat protection, monitoring, and incident response mechanisms using Microsoft's native security tools.