

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.

AZURE MONITOR, MICROSOFT DEFENDER FOR CLOUD, ENABLE JUST-IN TIME ACCESS IN VMS, MICROSOFT SENTINEL	1
Introduction	3
Lab 08: Create a Log Analytics Workspace, Azure Storage Account, and Data Collection Rule (DCR)	4
Exercise 1: Deploy an Azure virtual machine	4
Exercise 2: Create an Log Analytics workspace	6
Task 1: Create a Log Analytics workspace.....	6
Exercise 3: Create an Azure storage account.....	7
Task 1: Create an Azure storage account.....	7
Exercise 4: Create a Data Collection Rule	8
Task 1: Create a Data Collection Rule.	8
Lab 09: Configuring Microsoft Defender for Cloud Enhanced Security Features for Servers	10
Configure Microsoft Defender for Cloud Enhanced Security Features for Serve	10
Lab 10: Enable just-in-time access on VMs.....	10
Exercise 1: Enable JIT on your VMs from Azure virtual machines	10
Exercise 2: Request access to a JIT-enabled VM from the Azure virtual machine's connect page.	11
Lab 11: Microsoft Sentinel	11
Exercise 1: Implement Microsoft Sentinel	11
Task 1: On-board Microsoft Sentinel	11
Task 2: Configure Microsoft Sentinel to use the Azure Activity data connector.....	12
Task 3: Create a rule that uses the Azure Activity data connector.....	14
Task 4: Create a playbook	14
Task 5: Create a custom alert and configure a playbook as an automated response	16
Task 6: Invoke an incident and review the associated actions.	17

Introduction

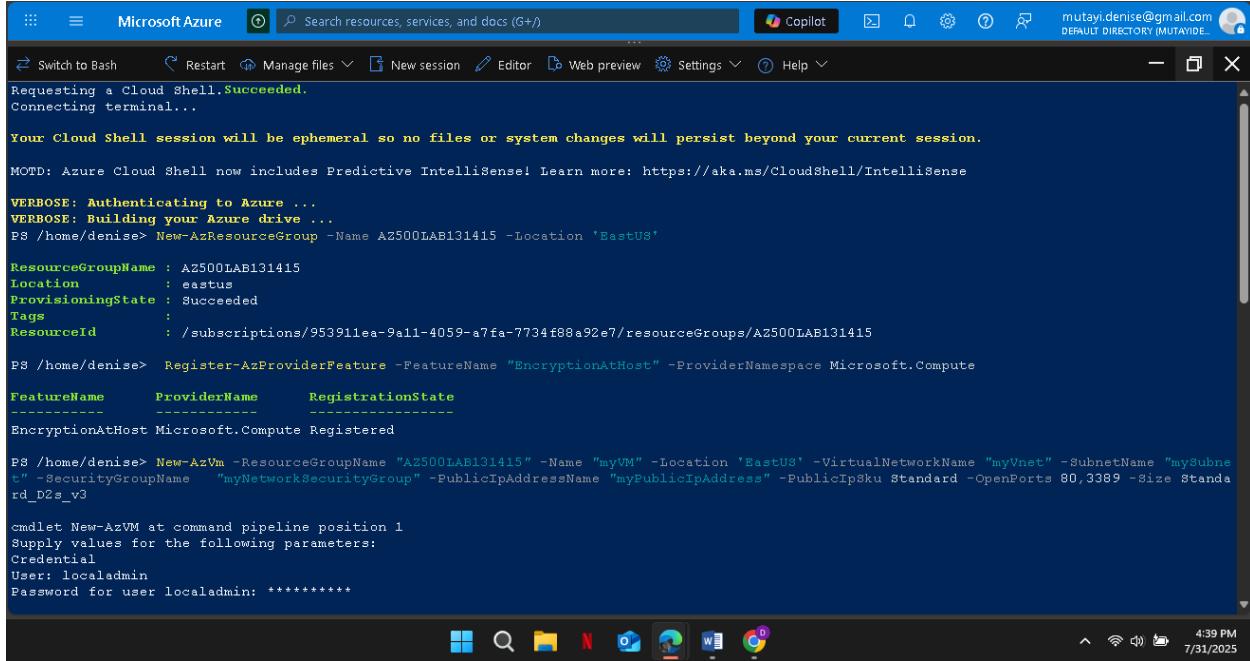
In this lab series, I configured and implemented several security features using Microsoft Defender for Cloud and Microsoft Sentinel on Azure. I began by deploying an Azure virtual machine in the East US region, followed by the creation of a Log Analytics workspace, an Azure storage account, and a data 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



The screenshot shows a Microsoft Azure Cloud Shell window with a dark theme. The terminal output is as follows:

```
Microsoft Azure Search resources, services, and docs (G+) Copilot
Switch to Bash Restart Manage files New session Editor Web preview Settings Help
mutayi.denise@gmail.com DEFAULT DIRECTORY (MUTAYI...)
Requesting a Cloud Shell. Succeeded.
Connecting terminal...
Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
MOTD: Azure Cloud Shell now includes Predictive IntelliSense! Learn more: https://aka.ms/CloudShell/IntelliSense

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/denise> New-AzResourceGroup -Name AZ500LAB131415 -Location "EastUS"

ResourceGroupName : AZ500LAB131415
Location         : eastus
ProvisioningState : Succeeded
Tags             :
ResourceId       : /subscriptions/953911ea-9a11-4059-a7fa-7734f88a92e7/resourceGroups/AZ500LAB131415

PS /home/denise> Register-AzProviderFeature -FeatureName "EncryptionAtHost" -ProviderNamespace Microsoft.Compute

FeatureName      ProviderName      RegistrationState
-----          -----          -----
EncryptionAtHost Microsoft.Compute Registered

PS /home/denise> New-AzVm -ResourceGroupName "AZ500LAB131415" -Name "myVM" -Location "EastUS" -VirtualNetworkName "myVnet" -SubnetName "mySubnet" -SecurityGroupName "myNetworkSecurityGroup" -PublicIpAddressName "myPublicIpAddress" -PublicIpSku Standard -OpenPorts 80,3389 -Size Standard_D2s_v3

cmdlet New-AzVm at command pipeline position 1
Supply values for the following parameters:
Credential
User: localadmin
Password for user localadmin: *****
```

The taskbar at the bottom shows various icons for Windows 10, including File Explorer, Task View, and Edge browser.

The screenshot shows two sessions of the Microsoft Azure Cloud Shell interface. Both sessions are connected to the user 'mutayi.denise@gmail.com' with the default directory '(MUTAYIDE..)'.

Session 1 (Top):

```
- This change will take effect on '11/1/2025'
- The change is expected to take effect in Az version : '15.0.0'
- The change is expected to take effect in Az.Compute version : '11.0.0'
Note : Go to https://aka.ms/azps-changewarnings for steps to suppress this breaking change warning, and other information on breaking changes in Azure PowerShell.

ResourceGroupName      : AZ500LAB131415
Id                   :
/subscriptions/953911ea-9a11-4059-a7fa-7734f88a92e7/resourceGroups/AZ500LAB131415/providers/Microsoft.Compute/virtualMachines/myVM
VmId                : 36c3fc79-b524-495e-b5dd-0462cf96ebae
Name                 : myVM
Type                 : Microsoft.Compute/virtualMachines
Location             : eastus
Tags                : {}
HardwareProfile     : {VmSize}
NetworkProfile       : {NetworkInterfaces}
SecurityProfile     : {UefiSettings, SecurityType}
OSProfile            : {ComputerName, AdminUsername, WindowsConfiguration, Secrets, AllowExtensionOperations, RequireGuestProvisionSignal}
ProvisioningState    : Succeeded
StorageProfile       : {ImageReference, OsDisk, DataDisks, DiskControllerType, AlignRegionalDisksToVMZone}
FullyQualifiedDomainName : myvm-13cdba.EastUS.cloudapp.azure.com
TimeCreated          : 7/31/2025 1:33:38 PM
Etag                : "2"

PS /home/denise> 
```

Session 2 (Bottom):

```
Location           : eastus
Tags              : {}
HardwareProfile   : {VmSize}
NetworkProfile     : {NetworkInterfaces}
SecurityProfile   : {UefiSettings, SecurityType}
OSProfile          : {ComputerName, AdminUsername, WindowsConfiguration, Secrets, AllowExtensionOperations, RequireGuestProvisionSignal}
ProvisioningState  : Succeeded
StorageProfile     : {ImageReference, OsDisk, DataDisks, DiskControllerType, AlignRegionalDisksToVMZone}
FullyQualifiedDomainName : myvm-13cdba.EastUS.cloudapp.azure.com
TimeCreated        : 7/31/2025 1:33:38 PM
Etag              : "2"

PS /home/denise> Get-AzVM -Name 'myVM' -ResourceGroupName 'AZ500LAB131415' | Format-Table
ResourceGroupName Name Location      VmSize OsType  NIC ProvisioningState
-----          -----  -----      -----  -----  -----  -----
AZ500LAB131415  myVM  eastus  Standard_D2s_v3  Windows  myVM      Succeeded

PS /home/denise> 
```

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

The screenshot shows the Microsoft Azure Log Analytics OMS Overview page. The main content area displays a green checkmark icon and the message "Your deployment is complete". Below this, it shows deployment details: Deployment name: Microsoft.LogAnalyticsOMS, Subscription: Azure subscription 1, Resource group: AZ500LAB131415. To the right, there are sections for Cost management, Microsoft Defender for Cloud, Free Microsoft tutorials, and Work with an expert. At the bottom, there are links for "Give feedback" and "Tell us about your experience with deployment". The top navigation bar includes Microsoft Azure, Upgrade, Search resources, services, and docs, Copilot, and user information.

The screenshot shows the Microsoft Azure Data Collection Rules Overview page. The main content area displays a green checkmark icon and the message "Your deployment is complete". Below this, it shows deployment details: Deployment name: Microsoft.DataCollectionRules, Subscription: Azure subscription 1, Resource group: AZ500LAB131415. To the right, there are sections for Cost management, Microsoft Defender for Cloud, Free Microsoft tutorials, and Work with an expert. At the bottom, there are links for "Give feedback" and "Tell us about your experience with deployment". The top navigation bar includes Microsoft Azure, Upgrade, Search resources, services, and docs, Copilot, and user information.

Exercise 3: Create an Azure storage account

Task 1: Create an Azure storage account

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure', 'Upgrade' (with a blue circular icon), a search bar ('Search resources, services, and docs (G+)'), and user information ('mutayi.denise@gmail.com' and 'DEFAULT DIRECTORY (MUTAYIDE...)'). Below the navigation bar is a deployment overview card for 'deniselabstore_1753970330105'. The card displays a green checkmark indicating 'Your deployment is complete'. It shows deployment details: Deployment name: deniselabstore_175397033..., Start time: 7/31/2025, 4:59:28 PM, Subscription: Azure subscription 1, Resource group: AZ500LAB131415. There are sections for 'Deployment details' and 'Next steps' with a 'Go to resource' button. On the right side of the main content area, there are promotional cards for 'Cost Management', 'Microsoft Defender for Cloud', 'Free Microsoft tutorials', and 'Work with an expert'. The bottom of the screen shows a taskbar with various icons (File Explorer, Task View, File History, Netflix, Mail, Edge, Word, Google Chrome) and system status indicators (Wi-Fi, battery, date/time).

Created an Azure storage account

Exercise 4: Create a Data Collection Rule

Task 1: Create a Data Collection Rule.

The screenshot displays two consecutive steps of the 'Create Data Collection Rule' wizard in the Microsoft Azure portal.

Step 1: Basics

Validation passed

To create a Data Collection Rule that collects platform metrics, click here.

Basics Resources Collect and deliver Tags Review + create

Data rule name: DCR1
Subscription: Azure subscription 1
Resource Group: AZ500LAB131415

Step 2: Collect and deliver

To create a Data Collection Rule that collects platform metrics, click here.

Selected resources

Resources	Type

Create < Previous Next: >

Basics Resources Collect and deliver Tags Review + create

Configure which data sources to collect and where to send the data to.

+ Add data source

Data source	Destination(s)
Performance Counters	Azure Monitor Logs

Review + create < Previous Next : Tags >

Pick a set of resources to collect data from. The Azure Monitor Agent will be automatically installed on virtual machines, scale sets, and Arc-enabled servers. For AKS clusters, managed Prometheus will automatically be enabled.

For Windows 10 and 11 devices, [download the client installer](#) and follow the [guidance](#)

This will also enable System Assigned Managed Identity on these resources, in addition to existing User Assigned Identities (if any).

+ Add resources + Create endpoint

Enable Data Collection Endpoints ○ □

Only resources in the same region can be assigned to the same endpoint. [Learn more](#)

Name	Type	Location	Resource group	Subscription
myVM	Virtual machine	East US	AZ500LAB131415	Azure subscription 1

Showing 1 - 1 of 1 results.

Review + create < Previous Next : Collect and deliver >

5:08 PM 7/31/2025

Microsoft Azure Upgrade Search resources, services, and docs (G+) Copilot Home > Monitor | Data Collection Rules > Create Data Collection Rule ... Data collection rule management

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. [Learn more](#)

Rule details

Rule Name * DCR1

Subscription * Azure subscription 1

Resource Group * AZ500LAB131415 [Create new](#)

Region * East US

Platform Type * Windows

Data Collection Endpoint <none>

Review + create < Previous Next : Resources >

5:08 PM 7/31/2025

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 Servers

The screenshot shows the Microsoft Azure portal interface. The user is navigating through the 'Microsoft Defender for Cloud | Environment settings' section under 'Settings | Defender plans'. A modal window titled 'Plan selection' is displayed, detailing the two available plans:

- Plan 1:** \$15/Server/Month. Description: Provides a limited set of defenses with a focus on Defender for Endpoint's protections.
- Plan 2:** \$15/Server/Month. Description: Includes the full set of enhanced security features for servers.

The 'Plan 2' option is selected. The modal also lists several security features:

- Microsoft Defender for Endpoint
- Microsoft Defender vulnerability management
- Automatic agent onboarding, alert and data integration
- Generates detailed, context-based, security alerts easily integrated with any SIEM
- Provides guidelines to help investigate and mitigate identified threats
- Agentless VM vulnerability scanning [Learn more](#).
- Agentless VM secrets scanning [Learn more](#).

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

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

The screenshot shows the Microsoft Azure portal interface. The user is navigating through the 'Compute infrastructure | Virtual machines' section for a VM named 'myVM'. The 'Configuration' tab is selected. A success message is displayed: 'Just-in-time access successfully enabled'.

The 'Just-in-time VM access' section contains the following information:

- Just-in-time VM access (JIT) is enabled. To disable JIT, modify the configuration, or request access.
- Open Microsoft Defender for Cloud
- Just-in-time VM access secures your VM's management ports and grants access on-demand, for a limited time period, to pre-approved IP addresses. [Learn more about just-in-time access](#)
- Proximity placement group: No proximity placement groups found.
- Host: Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

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

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', 'Upgrade', 'Search resources, services, and docs (G+)', 'Copilot', and user information 'mutayi.denise@gmail.com DEFAULT DIRECTORY (MUTAYIDE...)'. The main title is 'myVM | Connect'. The left sidebar has sections like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Resource visualizer', 'Connect' (which is expanded to show 'Native RDP', 'Bastion', 'Windows Admin Center'), 'Networking' (with 'Network settings', 'Load balancing', and 'Application security groups'), and a note about favorite items. The 'Native RDP' section shows the 'Source machine' (Windows) and 'Destination VM' (Public IP 20.169.159.134, VM port 3389). Under 'Connection prerequisites', it indicates 'JIT access granted to port 3389 for source IP(s)' and 'Port 3389 is accessible from source IP(s)'. A 'Request JIT + Check access' button is present. At the bottom, there are download options for 'Download and open file to connect' or 'Download RDP file'.

Lab 11: Microsoft Sentinel

Exercise 1: Implement Microsoft Sentinel

Task 1: On-board Microsoft Sentinel

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', 'Upgrade', 'Search resources, services, and docs (G+)', 'Copilot', and user information 'mutayi.denise@gmail.com DEFAULT DIRECTORY (MUTAYIDE...)'. The main title is 'Add Microsoft Sentinel to a workspace'. Below it, a message says 'Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.' Another message states 'New Microsoft Sentinel workspaces created by authorized users are automatically onboarded and redirected to the Defender portal. [Learn more](#)'. A 'Filter by name...' input field is available. A table lists existing workspaces: 'az500-denise-workspace' (Location: eastus, ResourceGroup: az500lab131415, Subscription: Azure subscription 1, Directory: Default Directory). At the bottom, there are 'Add' and 'Cancel' buttons.

The screenshot shows the Microsoft Sentinel | Guides page. At the top, it says "Microsoft Sentinel free trial activated". Below that, it states: "The free trial is active on this workspace from 8/2/2025 to 9/2/2025 at 11:59:59 PM UTC. During the trial, up to 10 GB/day are free for both Microsoft Sentinel and Log Analytics. Data beyond the 10 GB/day included quantity will be billed." There is an "OK" button. To the right, there is a section titled "Install your first content hub solution" with a "Go to content hub" button and an illustration of a computer monitor displaying data. On the left, there is a navigation sidebar with options like General, Overview, Logs, Guides (which is selected), Search, Threat management, Content management, and Configuration.

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

The screenshot shows the Microsoft Defender | Default Directory page. On the left, there is a navigation sidebar with categories like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel (which is selected), Endpoints, Email & collaboration, Cases, SOC optimization, and Reports. The main area is titled "Content hub" and displays statistics: 412 Solutions, 311 Standalone contents, 0 Installed, and 0 Updates. A search bar shows "azure activity". Below the search bar, there are filters for Status: All, Content type: All, Support: All, Provider: All, and Category: All. A "Install/Update" button is present. To the right, there is a detailed view of the "Azure Activity" solution, including its provider (Microsoft), support (Microsoft), version (3.0.3), and a note: "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." It also lists Data Connectors: 1, Workbooks: 2, Analytic Rules: 14, and Hunting Queries: 15. There are links to "Learn more about Microsoft Sentinel" and "Learn more about Solutions".

Microsoft Defender | Default Directory

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](#)

Search: azure activity

Status: All Content type: All Support: All Provider: All Category: All

Install/Update Delete

Content title	Status
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

Home | Exposure management | Investigation & response | Threat intelligence | Assets | Microsoft Sentinel | Endpoints | Email & collaboration | Cases | SOC optimization | Reports

Microsoft Azure

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

Notifications

\$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

Create a resource | Microsoft Sentinel | Virtual machines | Microsoft Defender for... | Monitor | Storage accounts

11:25 PM 8/2/2025

More events in the activity log → Dismiss all

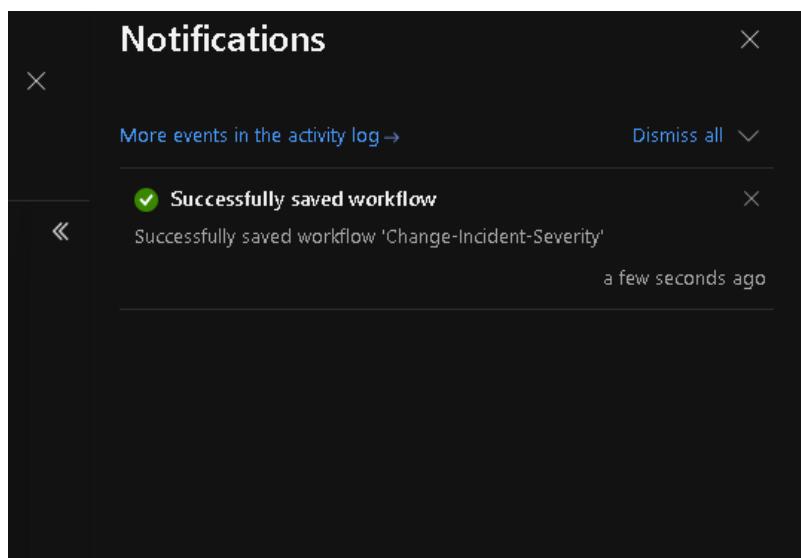
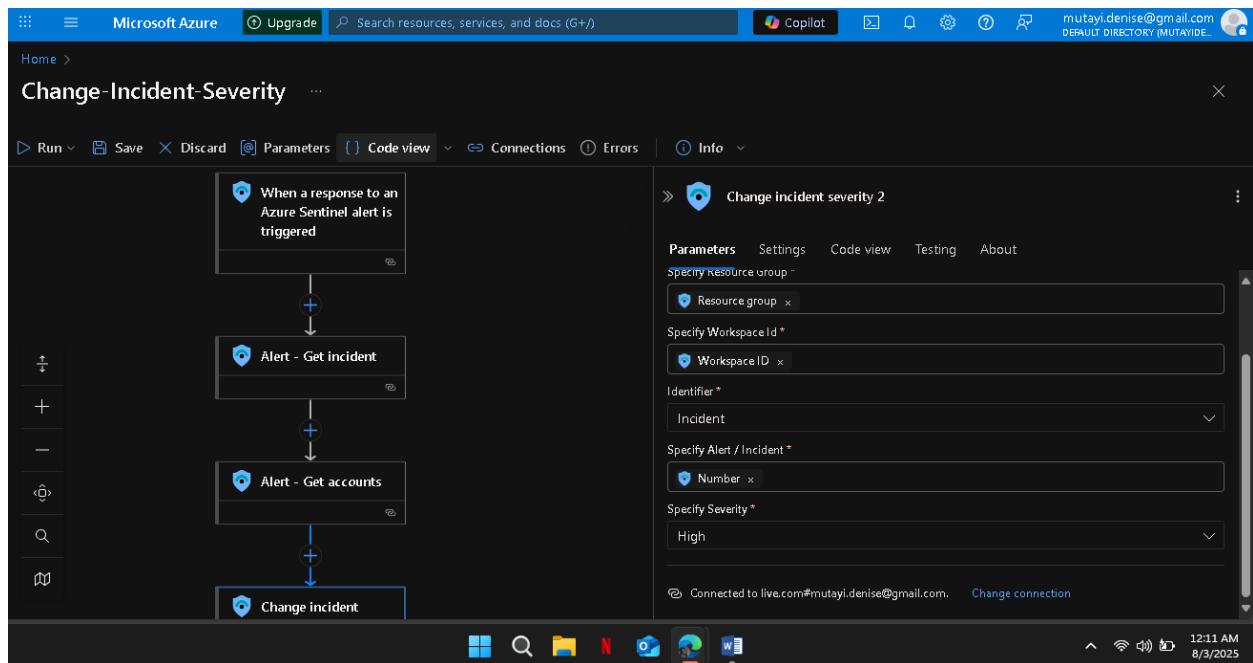
Task 3: Create a rule that uses the Azure Activity data connector.

The screenshot shows the Microsoft Defender interface for a 'Default Directory'. At the top, it says 'Microsoft Defender | Default Directory' and 'Search'. Below that, there's a banner stating 'ensures that you can easily access, modify, and oversee all your rules in one convenient location.' A blue button at the top right says 'Go to unified rules page'. In the center, it displays '1 Active rules' and 'Rules by severity' with a color-coded bar for High (red), Medium (orange), Low (green), and Informational (light blue). A link 'More content at Content hub' is also present. On the left, there's a sidebar with various icons. The main area shows a table with columns: Severity, Name, Rule type, Status, Tactics, Techniques, Sub techniques, Source name, and Last modified. One row is visible: 'Suspicious Resou...' (Severity: Low, Status: Enabled, Tactics: Impact, Techniques: T1496, Source name: Azure Activity, Last modified: 8/2/2025, 11:44:2...). At the bottom, there are buttons for 'Create', 'Analytics workbooks', 'Rule runs (Preview)', 'Enable', 'Disable', 'Delete', 'Import', 'Export', and 'Columns'. A search bar and a 'Add filter' button are also at the bottom.

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.

The screenshot shows the Microsoft Azure portal with the URL 'Microsoft.Template-20250802235103 | Overview'. It indicates that the deployment is complete with a green checkmark icon. Deployment details are listed: Deployment name: Microsoft.Template-20250802235..., Start time: 8/2/2025, 11:51:40 PM, Subscription: Azure subscription 1, Correlation ID: 928523cb-6051-47a1-a464-8aff13..., Resource group: AZ500LAB131415. Below this, there are sections for 'Deployment details' and 'Next steps'. A 'Go to resource group' button is available. At the bottom, there are links for 'Give feedback' and 'Tell us about your experience with deployment'. On the right side, there are promotional cards: 'Cost management' (Get notified to stay within your budget and prevent unexpected charges on your bill, Set up cost alerts >), 'Microsoft Defender for Cloud' (Secure your apps and infrastructure, Go to Microsoft Defender for Cloud >), 'Free Microsoft tutorials' (Start learning today >), and 'Work with an expert' (Azure experts are service provider partners who can help manage your).



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

The screenshot shows the 'Analytics rule wizard' interface for creating a new scheduled rule. The left sidebar lists steps: General, Set rule logic, Incident settings, Automated response, and Review + create. The right panel displays 'Analytics rule details' for a rule named 'Playbook Demo'. The rule is set to 'Initial Access' (Medium severity, Enabled) and uses the query 'AzureActivity | where ResourceProviderValue =~ "Microsoft.Security" | where OperationNameValue =~ "Microsoft.Security/locations/jitNetworkAccessPolicies/delete"' to run every 5 minutes.

The screenshot shows the 'Manage all your rules in one place' page. It features a summary section with 2 active rules, a 'Rules by severity' chart, and a table of active rules. The table includes columns for Severity, Name, Rule type, Status, Tactics, Techniques, and Sub. Two rules are listed: 'Playbook Demo' (Medium, Enabled, Initial Access) and 'Suspicious Resou...' (Low, Enabled, Impact, T1496).

Severity	Name	Rule type	Status	Tactics	Techniques	Sub
Medium	Playbook Demo	Scheduled	Enabled	Initial Access		
Low	Suspicious Resou...	Scheduled	Enabled	Impact	T1496	

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

The screenshot shows the Microsoft Azure Monitor Activity log interface. The left sidebar includes links for Overview, Activity log (selected), Alerts, Metrics, Logs, Change Analysis, Service health, Workbooks, Dashboards with Grafana (preview), Insights, Managed Services, Settings (Diagnostic settings, Data Collection Rules), and a note to add or remove favorites. The main area displays a table of recent events with columns for Operation name, Status, Time, Time stamp, Subscription, and Event initiated by. The table lists various successful operations such as creating or updating Network Security Groups, deleting JIT Network Access Policies, and updating automation rules, all initiated by 'Windows Azure Security R...' or 'mutayi.denise@gmail.com' on August 3, 2025.

Deleted JIT Network Access Policies entry.

The screenshot shows the Microsoft Defender Incidents page. The left sidebar includes links for Exposure management, Investigation & response (selected), Threat intelligence, Assets, Microsoft Sentinel (selected), Endpoints, Email & collaboration, Cases, SOC optimization, and Reports. The main area displays a table of incidents with columns for Status, Alert severity, Incident name, Incident ID, Tags, Severity, Investigation state, and Categories. Two incidents are listed: 'Playbook Demo' (Medium severity) and 'Suspicious Resource deployment involving one user' (Low severity). A message at the top states: 'The incident queue now displays incidents according to the latest automatic or manual updates made on incidents. For more information, see incident queue details.'

An incident of medium seniority.

The screenshot shows the Microsoft Azure Cloud Shell interface. At the top, there's a navigation bar with links like 'Switch to Bash', 'Restart', 'Manage files', 'New session', 'Editor', 'Web preview', 'Settings', and 'Help'. The main area displays a terminal session:

```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...
Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.

MOTD: SqlServer has been updated to Version 221

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/denise> Remove-AzResourceGroup -Name "AZ500LAB131415" -Force -AsJob
```

Id	Name	PSJobTypeName	State	HasMoreData	Location	Command
1	Long Running O...	AzureLongRunni...	Running	True	localhost	Remove-AzResourceGroup

```
PS /home/denise> 
```

The taskbar at the bottom includes icons for File Explorer, Task View, Task Manager, and Edge browser. The system tray shows the date and time as 1:00 AM, 8/3/2025.

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.