Cyber Shujaa

NAME: STEPHEN KYALO -ADC-DP01-25005

PROGRAM: DATA PROTECTION SPECIALIST

CLOUD SLICE TOPIC: CAPABILITIES OF MICROSOFT SECURITY SOLUTION

EXECUTIVE SUMMARY

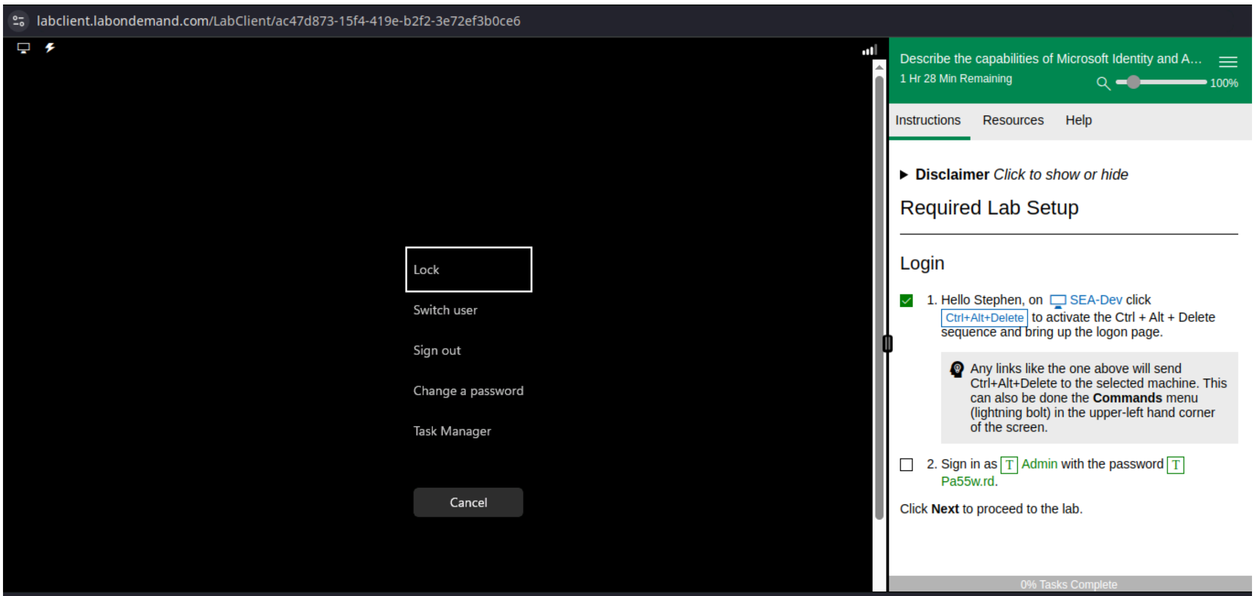
Microsoft Security offers a comprehensive suite of services designed to enhance the security of an organisation's IT infrastructure. The services and applications included in the Microsoft Security solutions are: Azure Firewalls, Network Security Groups, Microsoft Defender for Cloud and Cloud Apps, Microsoft Sentinel, the Microsoft Defender portal, and Microsoft XDR. This report details the capabilities of Microsoft Security solutions explored in the provided labs.

GLOSSARY

XDR- Extended Detection and Response
SIEM -Security Incident and Event Management
SOAR - Security Orchestration, Automation, and Response

1. LAB SETUP

Upon launching the cloud slice, the user is required to log out of the default account and log in with the provided **ADMIN** account and **PASSWORD,** as shown on the attached screenshots.



labclient.labondemand.com/LabClient/ac47d873-15f4-419e-b2f2-3e72ef3b0ce6
Lock
Switch user
Sign out
Change a password
Task Manager
Cancel
Describe the capabilities of Microsoft Identity and A...
1 Hr 28 Min Remaining
100%
Instructions
Resources
Help
0% Tasks Complete

▸ **Disclaimer** *Click to show or hide*

Required Lab Setup

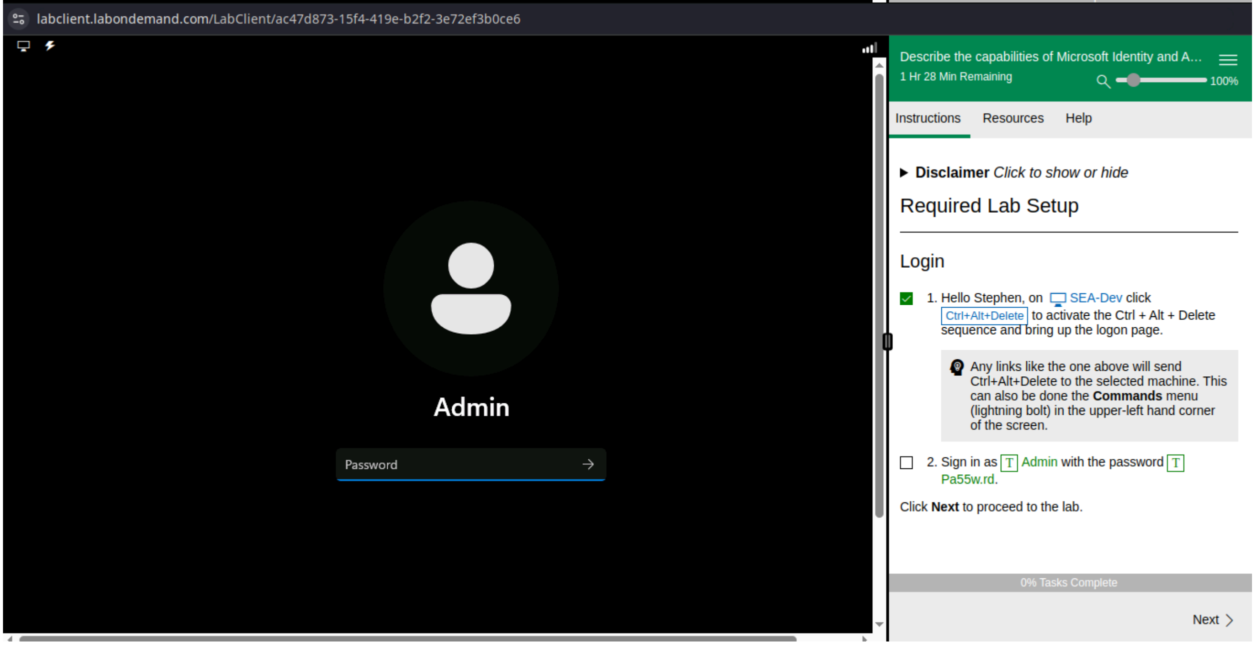
Login

☑ 1. Hello Stephen, on SEA-Dev click Ctrl+Alt+Delete to activate the Ctrl + Alt + Delete sequence and bring up the logon page.

Any links like the one above will send Ctrl+Alt+Delete to the selected machine. This can also be done the **Commands** menu (lightning bolt) in the upper-left hand corner of the screen.

☐ 2. Sign in as T Admin with the password T Pa55w.rd.

Click **Next** to proceed to the lab.



labclient.labondemand.com/LabClient/ac47d873-15f4-419e-b2f2-3e72ef3b0ce6
Admin
Password
Describe the capabilities of Microsoft Identity and A...
1 Hr 28 Min Remaining
100%
Instructions
Resources
Help
0% Tasks Complete
Next

▸ **Disclaimer** *Click to show or hide*

Required Lab Setup

Login

☑ 1. Hello Stephen, on SEA-Dev click Ctrl+Alt+Delete to activate the Ctrl + Alt + Delete sequence and bring up the logon page.

Any links like the one above will send Ctrl+Alt+Delete to the selected machine. This can also be done the **Commands** menu (lightning bolt) in the upper-left hand corner of the screen.

☐ 2. Sign in as T Admin with the password T Pa55w.rd.

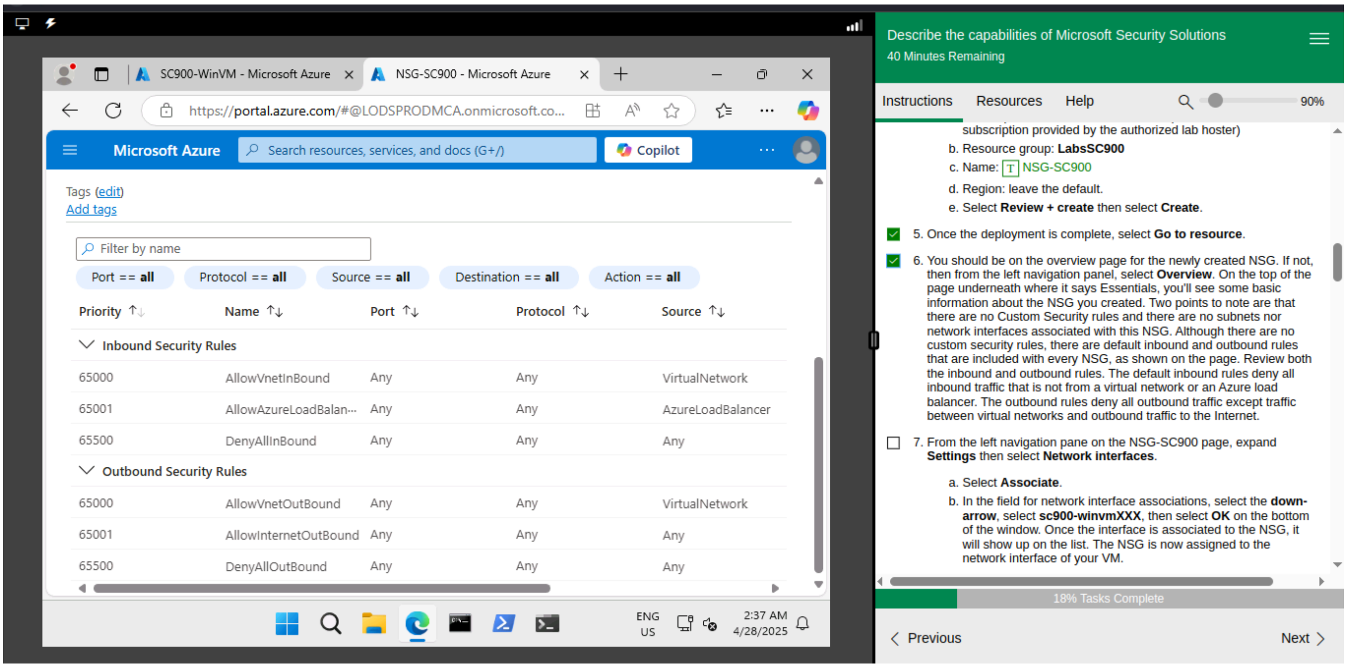
Click **Next** to proceed to the lab.

2. AZURE NETWORK SECURITY GROUPS

Azure NSG acts like a virtual firewall, controlling inbound and outbound traffic to Azure resources within a virtual network.

NSGS contain a list of security rules that allow or deny network traffic to NICs, VMs, subnets, or other resources. By default, Azure NSGs have 6 predefined security rules: 3 for inbound traffic and 3 for outbound traffic. Each rule has a priority level indicated by numbers; the lower the value, the higher the priority of the rule.

Administrators can override the default security rules, but cann't delete them, by creating rules with a lower value, hence higher priority.



Priority	Name	Port	Protocol	Source
Inbound Security Rules				
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer
65500	DenyAllInBound	Any	Any	Any
Outbound Security Rules				
65000	AllowVnetOutBound	Any	Any	VirtualNetwork
65001	AllowInternetOutBound	Any	Any	Any
65500	DenyAllOutBound	Any	Any	Any

subscription provided by the authorized lab hoster)

b. Resource group: **LabsSC900**

c. Name: NSG-SC900

d. Region: leave the default.

e. Select **Review + create** then select **Create**.

☑ 5. Once the deployment is complete, select **Go to resource**.

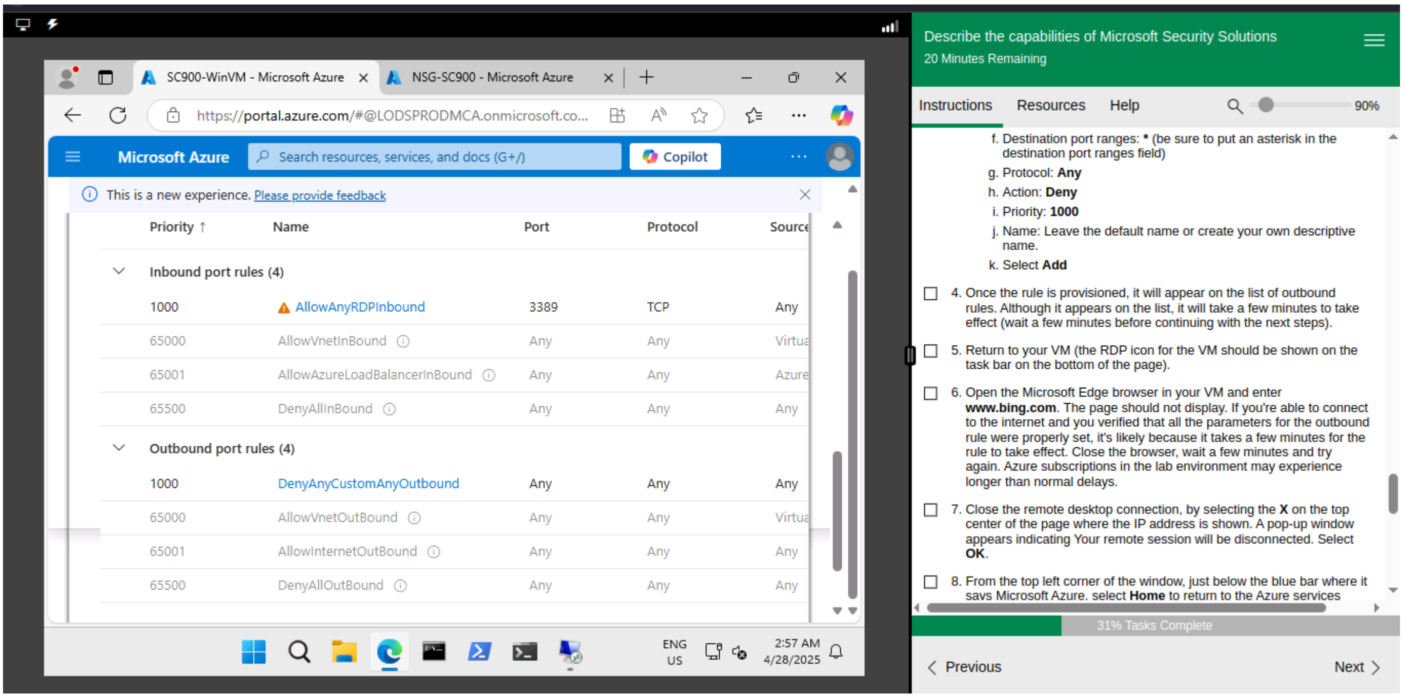
☑ 6. You should be on the overview page for the newly created NSG. If not, then from the left navigation panel, select **Overview**. On the top of the page underneath where it says Essentials, you'll see some basic information about the NSG you created. Two points to note are that there are no Custom Security rules and there are no subnets nor network interfaces associated with this NSG. Although there are no custom security rules, there are default inbound and outbound rules that are included with every NSG, as shown on the page. Review both the inbound and outbound rules. The default inbound rules deny all inbound traffic that is not from a virtual network or an Azure load balancer. The outbound rules deny all outbound traffic except traffic between virtual networks and outbound traffic to the Internet.

□ 7. From the left navigation pane on the NSG-SC900 page, expand **Settings** then select **Network interfaces**.

a. Select **Associate**.

b. In the field for network interface associations, select the **down-arrow**, select **sc900-winvmXXX**, then select **OK** on the bottom of the window. Once the interface is associated to the NSG, it will show up on the list. The NSG is now assigned to the network interface of your VM.

Default Azure Network Security Groups Default Security Rules.



SC900-WinVM - Microsoft Azure
NSG-SC900 - Microsoft Azure
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.co...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
This is a new experience. Please provide feedback
ENG US
2:57 AM 4/28/2025

Priority ↑	Name	Port	Protocol	Source
Inbound port rules (4)				
1000	AllowAnyRDPInbound	3389	TCP	Any
65000	AllowVnetInBound	Any	Any	Virtua
65001	AllowAzureLoadBalancerInBound	Any	Any	Azure
65500	DenyAllInBound	Any	Any	Any
Outbound port rules (4)				
1000	DenyAnyCustomAnyOutbound	Any	Any	Any
65000	AllowVnetOutBound	Any	Any	Virtua
65001	AllowInternetOutBound	Any	Any	Any
65500	DenyAllOutBound	Any	Any	Any

Describe the capabilities of Microsoft Security Solutions
20 Minutes Remaining

Instructions Resources Help 90%

f. Destination port ranges: ***** (be sure to put an asterisk in the destination port ranges field)

g. Protocol: **Any**

h. Action: **Deny**

i. Priority: **1000**

j. Name: Leave the default name or create your own descriptive name.

k. Select **Add**

☐ 4. Once the rule is provisioned, it will appear on the list of outbound rules. Although it appears on the list, it will take a few minutes to take effect (wait a few minutes before continuing with the next steps).

☐ 5. Return to your VM (the RDP icon for the VM should be shown on the task bar on the bottom of the page).

☐ 6. Open the Microsoft Edge browser in your VM and enter **www.bing.com**. The page should not display. If you're able to connect to the internet and you verified that all the parameters for the outbound rule were properly set, it's likely because it takes a few minutes for the rule to take effect. Close the browser, wait a few minutes and try again. Azure subscriptions in the lab environment may experience longer than normal delays.

☐ 7. Close the remote desktop connection, by selecting the **X** on the top center of the page where the IP address is shown. A pop-up window appears indicating Your remote session will be disconnected. Select **OK**.

☐ 8. From the top left corner of the window, just below the blue bar where it savs Microsoft Azure. select **Home** to return to the Azure services

31% Tasks Complete

< Previous   Next >

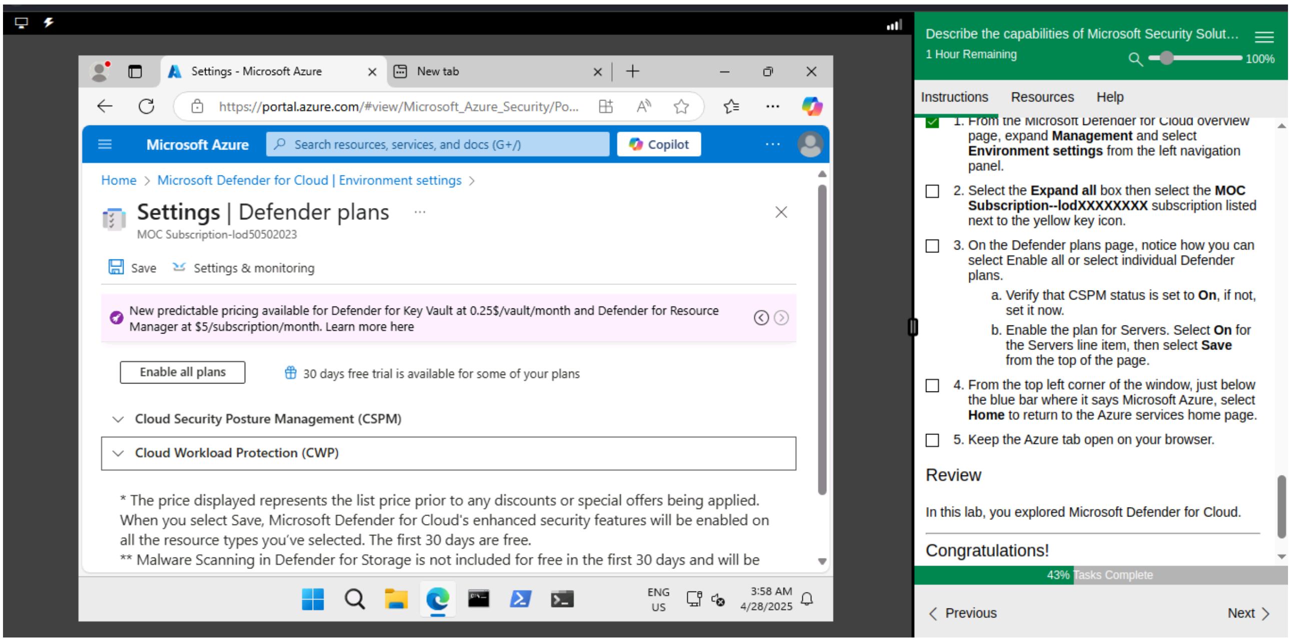
Custom Security Rules added.

3. MICROSOFT DEFENDER FOR CLOUD

This is a cloud-native application protection platform designed to secure cloud workloads and hybrid environments across Microsoft Azure, AWS and Google Cloud Platform.

It combines the features of Cloud Security Posture Management(CSPM) and Cloud Workload Protection(CWP).

CSPM continuously assess an organisation's cloud environment's configuration and security posture. CWP provides threat detection and protection for individual workloads



Settings - Microsoft Azure
New tab
https://portal.azure.com/#view/Microsoft_Azure_Security/Po...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ENG US
3:58 AM 4/28/2025

Home > Microsoft Defender for Cloud | Environment settings >

Settings | Defender plans

MOC Subscription-lod50502023

Save   Settings & monitoring

New predictable pricing available for Defender for Key Vault at 0.25$/vault/month and Defender for Resource Manager at $5/subscription/month. Learn more here

Enable all plans   30 days free trial is available for some of your plans

Cloud Security Posture Management (CSPM)

Cloud Workload Protection (CWP)

* The price displayed represents the list price prior to any discounts or special offers being applied. When you select Save, Microsoft Defender for Cloud's enhanced security features will be enabled on all the resource types you've selected. The first 30 days are free.
** Malware Scanning in Defender for Storage is not included for free in the first 30 days and will be

Describe the capabilities of Microsoft Security Solut...
1 Hour Remaining   100%

Instructions Resources Help

☑ 1. From the Microsoft Defender for Cloud overview page, expand **Management** and select **Environment settings** from the left navigation panel.

☐ 2. Select the **Expand all** box then select the **MOC Subscription--lodXXXXXXXX** subscription listed next to the yellow key icon.

☐ 3. On the Defender plans page, notice how you can select Enable all or select individual Defender plans.

a. Verify that CSPM status is set to **On**, if not, set it now.

b. Enable the plan for Servers. Select **On** for the Servers line item, then select **Save** from the top of the page.

☐ 4. From the top left corner of the window, just below the blue bar where it says Microsoft Azure, select **Home** to return to the Azure services home page.

☐ 5. Keep the Azure tab open on your browser.

Review

In this lab, you explored Microsoft Defender for Cloud.

Congratulations!

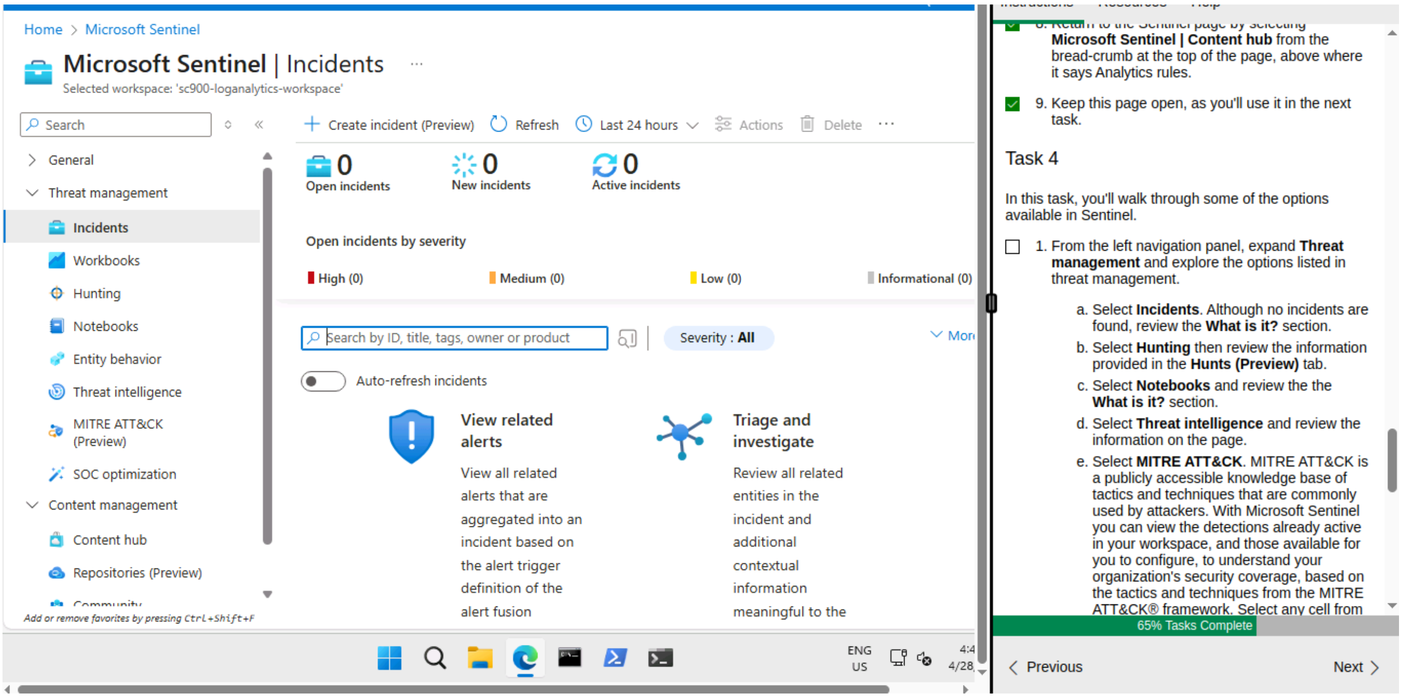
43% Tasks Complete

< Previous   Next >

4. MICROSOFT SENTINEL

Sentinel combines the capabilities of SIEM and SOAR services, which helps organisations detect, investigate, respond to, and prevent threats across their entire IT environment, either on-premises, Azure, or other clouds. Key capabilities include:

- Data collection by connecting to multiple data sources (Microsoft 365, Azure, AWS, on-premise systems)
- Automation and response -automates common tasks and responses.
- Threat Intelligence Integration- ingests threat intel from Microsoft and third parties to enrich detection and investigation.



View all related alerts that are aggregated into an incident based on the alert trigger definition of the alert fusion

Review all related entities in the incident and additional contextual information meaningful to the

☑ **Microsoft Sentinel | Content hub** from the bread-crumb at the top of the page, above where it says Analytics rules.

☑ 9. Keep this page open, as you'll use it in the next task.

Task 4

In this task, you'll walk through some of the options available in Sentinel.

☐ 1. From the left navigation panel, expand **Threat management** and explore the options listed in threat management.

a. Select **Incidents**. Although no incidents are found, review the **What is it?** section.

b. Select **Hunting** then review the information provided in the **Hunts (Preview)** tab.

c. Select **Notebooks** and review the the **What is it?** section.

d. Select **Threat intelligence** and review the information on the page.

e. Select **MITRE ATT&CK**. MITRE ATT&CK is a publicly accessible knowledge base of tactics and techniques that are commonly used by attackers. With Microsoft Sentinel you can view the detections already active in your workspace, and those available for you to configure, to understand your organization's security coverage, based on the tactics and techniques from the MITRE ATT&CK® framework. Select any cell from

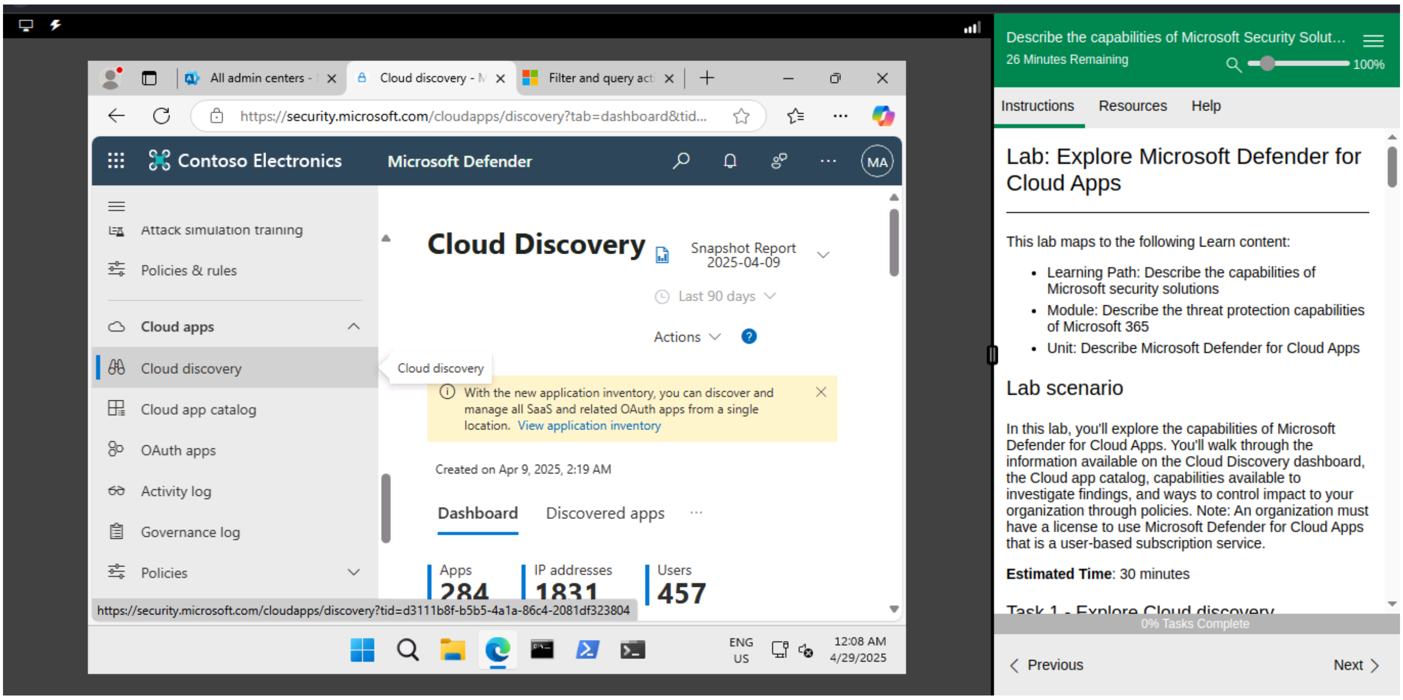
Some tools of Sentinel.

5. MICROSOFT DEFENDER FOR CLOUD APPS

Formerly Microsoft Cloud App Security, Microsoft Defender for Cloud Apps provides rich visibility, control over data travel, and powerful analytics to identify and combat cyber threats across cloud services. Its core features include:

- Cloud App Discovery- helps organisations identify and monitor the use of cloud apps across their network.
- Cloud Apps Catalog - a built-in database within Defender for Cloud Apps that helps security teams evaluate cloud apps based on a wide range of security, compliance, and business readiness criteria.

- Activity log- provides detailed visibility into user and app activity across an organisation's cloud environment.
- OAuth apps- third-party applications users authorise to access corporate cloud data.



With the new application inventory, you can discover and manage all SaaS and related OAuth apps from a single location. View application inventory

Created on Apr 9, 2025, 2:19 AM

Lab: Explore Microsoft Defender for Cloud Apps

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft security solutions
- Module: Describe the threat protection capabilities of Microsoft 365
- Unit: Describe Microsoft Defender for Cloud Apps

Lab scenario

In this lab, you'll explore the capabilities of Microsoft Defender for Cloud Apps. You'll walk through the information available on the Cloud Discovery dashboard, the Cloud app catalog, capabilities available to investigate findings, and ways to control impact to your organization through policies. Note: An organization must have a license to use Microsoft Defender for Cloud Apps that is a user-based subscription service.

Estimated Time: 30 minutes

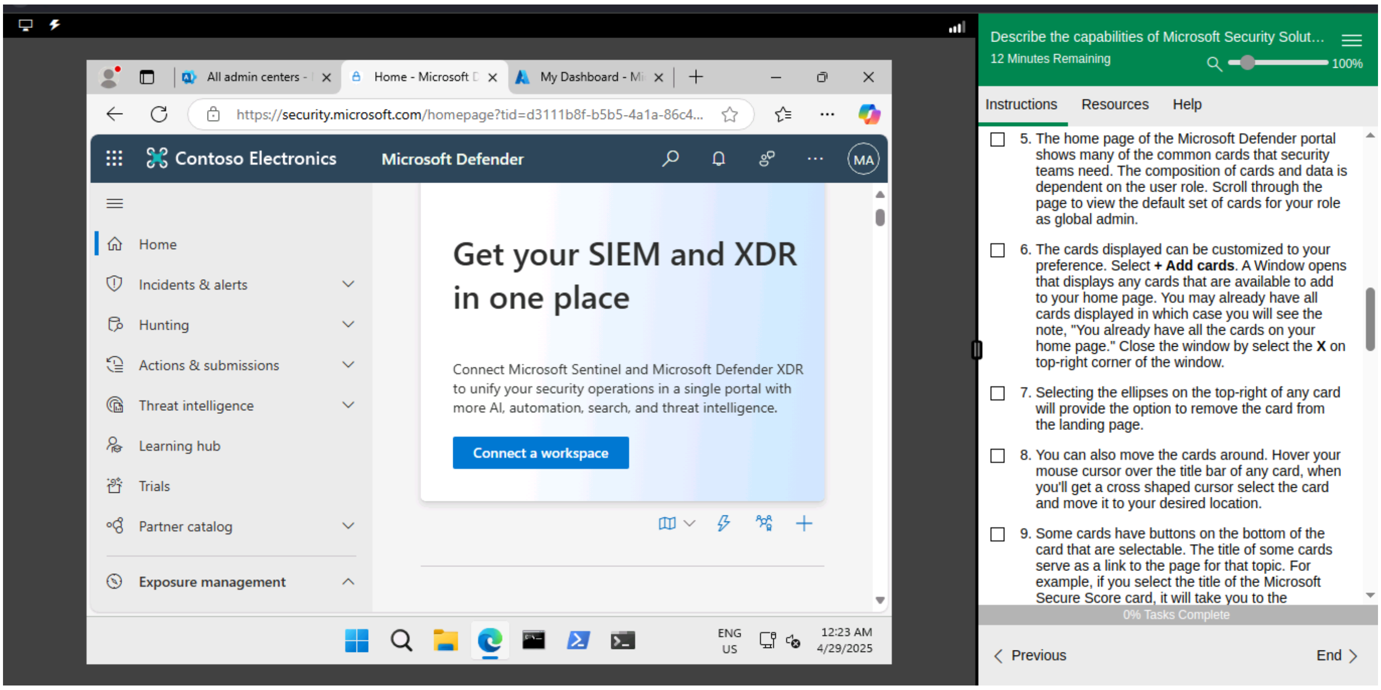
Task 1 - Explore Cloud discovery

6. MICROSOFT DEFENDER PORTAL

Microsoft Defender Portal consolidates various security tools and dashboards into a single card pane. This makes it easier for security teams to manage security for endpoints, identities, emails, applications and cloud resources. Users can add different cards for tools or dashboards depending on what they need to monitor, e.g A security news feed.

Some of its features include:

- Incidents and alerts- allows you to view and investigate alerts from across Microsoft security products.
- Hunting- using KQL to search raw data and track threats across logs from all Defender components.
- Threat Intelligence- provides deep insights into emerging threats, attack behaviour, and context-rich indicators
- Partner catalog- pre-integrated third-party cloud apps and services supported for API-based monitoring and control.



☐ 5. The home page of the Microsoft Defender portal shows many of the common cards that security teams need. The composition of cards and data is dependent on the user role. Scroll through the page to view the default set of cards for your role as global admin.

☐ 6. The cards displayed can be customized to your preference. Select **+ Add cards**. A Window opens that displays any cards that are available to add to your home page. You may already have all cards displayed in which case you will see the note, "You already have all the cards on your home page." Close the window by select the **X** on top-right corner of the window.

☐ 7. Selecting the ellipses on the top-right of any card will provide the option to remove the card from the landing page.

☐ 8. You can also move the cards around. Hover your mouse cursor over the title bar of any card, when you'll get a cross shaped cursor select the card and move it to your desired location.

☐ 9. Some cards have buttons on the bottom of the card that are selectable. The title of some cards serve as a link to the page for that topic. For example, if you select the title of the Microsoft Secure Score card, it will take you to the