

Name: Anne Musau

Program Details: Data Protection Specialist - C1 – 2025

Admission: adc-dp01-25032

Week 2 Lab Assignment: SC-900 Lab 2

Capabilities of Microsoft Security Solution.

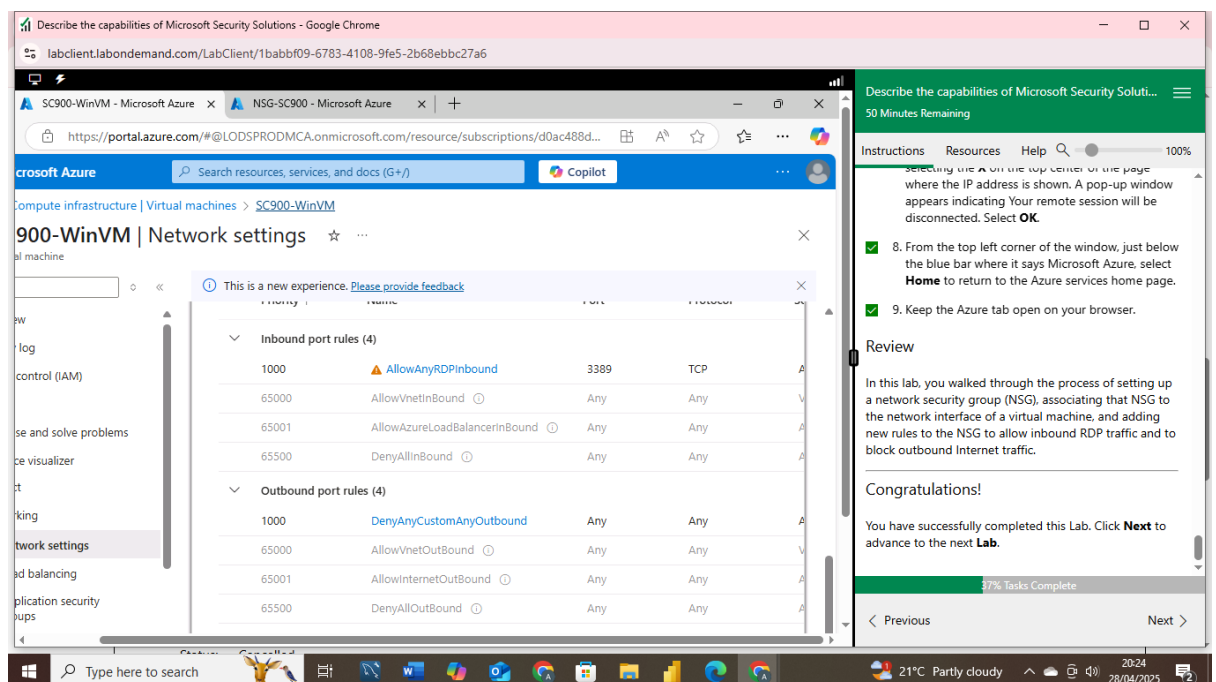
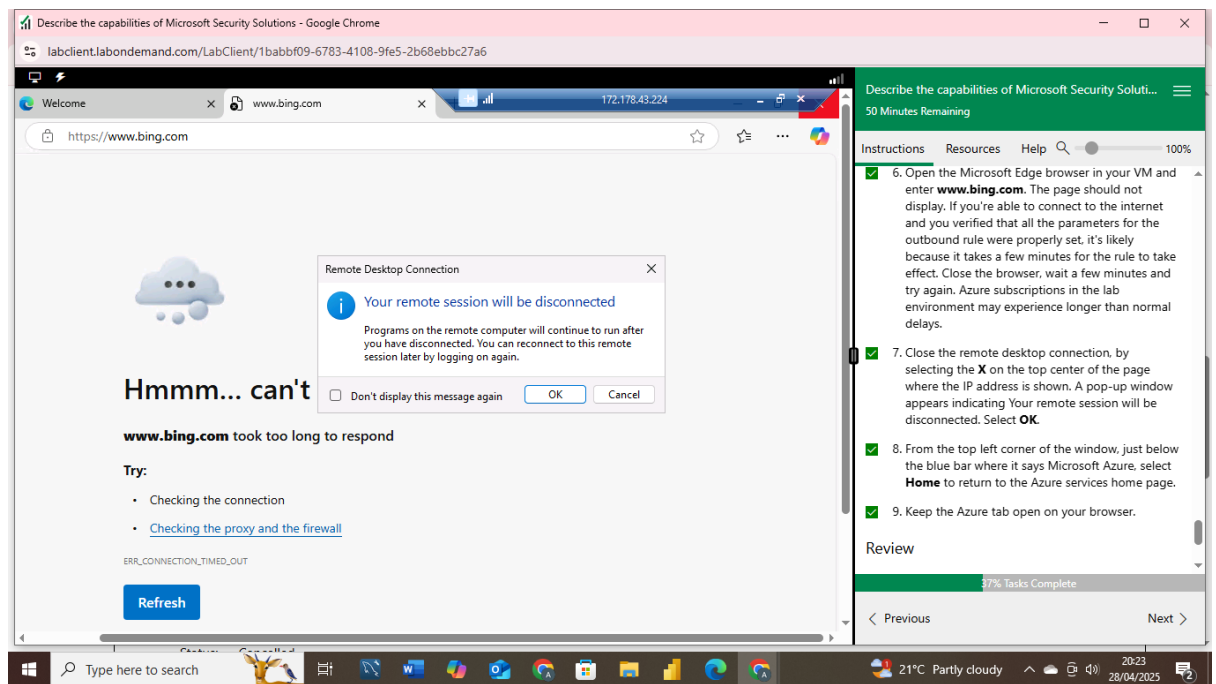
1. Lab: Explore Azure Network Security Groups (NSGs)
2. Lab: Explore Microsoft Defender for Cloud
3. Lab: Explore Microsoft Sentinel
4. Lab: Explore Microsoft Defender for Cloud Apps
5. Lab: Explore the Microsoft Defender portal

1. Lab: Explore Azure Network Security Groups (NSGs)

The screenshot displays the Microsoft Azure portal interface. The main content area shows 'Azure services' with icons for 'Create a resource', 'Virtual machines', 'Network security groups', 'Quickstart Center', 'Azure AI services', 'Kubernetes services', 'App Services', and 'Storage accounts'. Below this is a 'Resources' section with a table of recent resources.

Name	Type	Last Viewed
SC900-WinVM	Virtual machine	9 minutes ago
sc900-winv37	Network interface	9 minutes ago
NSG-SC900	Network security group	31 minutes ago
LabsSC900	Resource group	31 minutes ago

The right sidebar contains a 'Describe the capabilities of Microsoft Security Solutions' lab page. It includes a progress bar showing '48 Minutes Remaining' and a '37% Tasks Complete' status. The sidebar also features a 'Review' section with a congratulatory message and a 'Next' button.



In this lab, I explored the process of creating a Network Security Group (NSG) in Azure and attaching it to a virtual machine's network interface. I learned how to configure inbound and outbound security rules, including setting up a rule to allow inbound RDP traffic for remote access and another to block outbound internet traffic, enhancing the VM's network security posture.

2. Lab: Explore Microsoft Defender for Cloud

The screenshot shows the Microsoft Azure portal home page in a web browser. The page displays various Azure services like Virtual machines, Network security groups, and Storage accounts. A sidebar on the right contains lab instructions for 'Lab: Explore Microsoft Defender for Cloud'. The sidebar includes a progress bar showing '46% Tasks Complete' and a 'Task 1' section.

Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/1babbf09-6783-4108-9fe5-2b68ebbc27a6

Microsoft Azure
Search resources, services, and docs (G+)

Azure services

- Create a resource
- Microsoft Defender for...
- Virtual machines
- Network security groups
- Quickstart Center
- Azure AI services
- Kubernetes services
- App Services
- Storage accounts
- More services

Resources

Recent Favorite

Name	Type	Last Viewed
Virtual machines	Virtual machines	47 minutes ago

Describe the capabilities of Microsoft Security Solutions - Google Chrome
25 Minutes Remaining

Instructions Resources Help 100%

Lab: Explore Microsoft Defender for Cloud

This lab maps to the following Learn content:

- Learning Path: Describe the capabilities of Microsoft security solutions
- Module: Describe the security management capabilities of Azure
- Unit: Describe cloud security posture management

Lab scenario

In this lab, you'll explore Microsoft Defender for Cloud. NOTE: the Azure subscription provided by the Authorized Lab Host (ALH) limits access and may experience longer than normal delays.

Estimated Time: 30 minutes

Task 1
46% Tasks Complete

< Previous Next >

The screenshot shows the 'Settings | Defender plans' page in the Microsoft Azure portal. The page displays the 'Settings & monitoring' section for the 'MOC Subscription-Iod50503388'. It includes a warning about the Defender for Storage classic per-transaction plan and a section for 'Cloud Security Posture Management (CSPM)'. A sidebar on the right contains lab instructions for 'Lab: Explore Microsoft Defender for Cloud'. The sidebar includes a progress bar showing '45% Tasks Complete' and a 'Review' section.

Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/1babbf09-6783-4108-9fe5-2b68ebbc27a6

Microsoft Azure
Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud | Environment settings >

Settings | Defender plans
MOC Subscription-Iod50503388

Save Settings & monitoring

After February 5, 2025, The Defender for Storage classic per-transaction plan will no longer be available for new storage accounts and subscriptions. Learn more here

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

Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at \$5/Billable resource/month. Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

Pricing* Resource quantity Monitoring coverage Status

Describe the capabilities of Microsoft Security Solutions - Google Chrome
12 Minutes Remaining

Instructions Resources Help 100%

Environment settings from the left navigation panel.

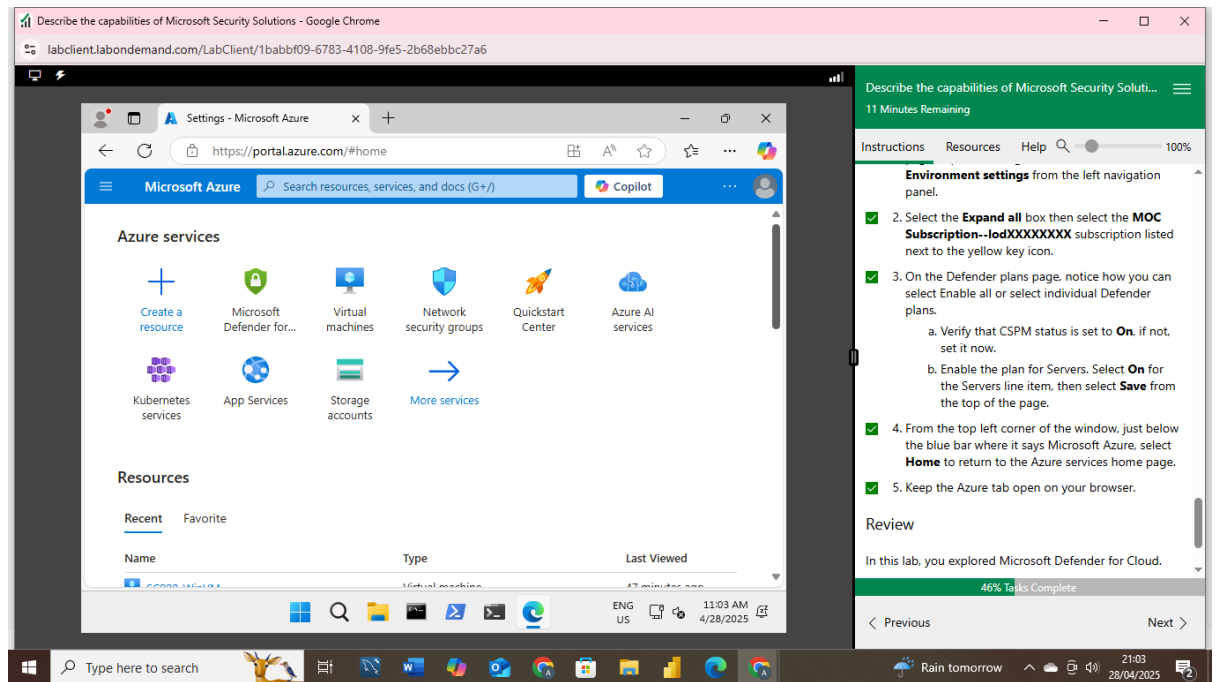
- 2. Select the **Expand all** box then select the **MOC Subscription-IodXXXXXXX** subscription listed next to the yellow key icon.
- 3. On the Defender plans page, notice how you can select Enable all or select individual Defender plans.
 - a. Verify that CSPM status is set to **On**, if not, set it 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.

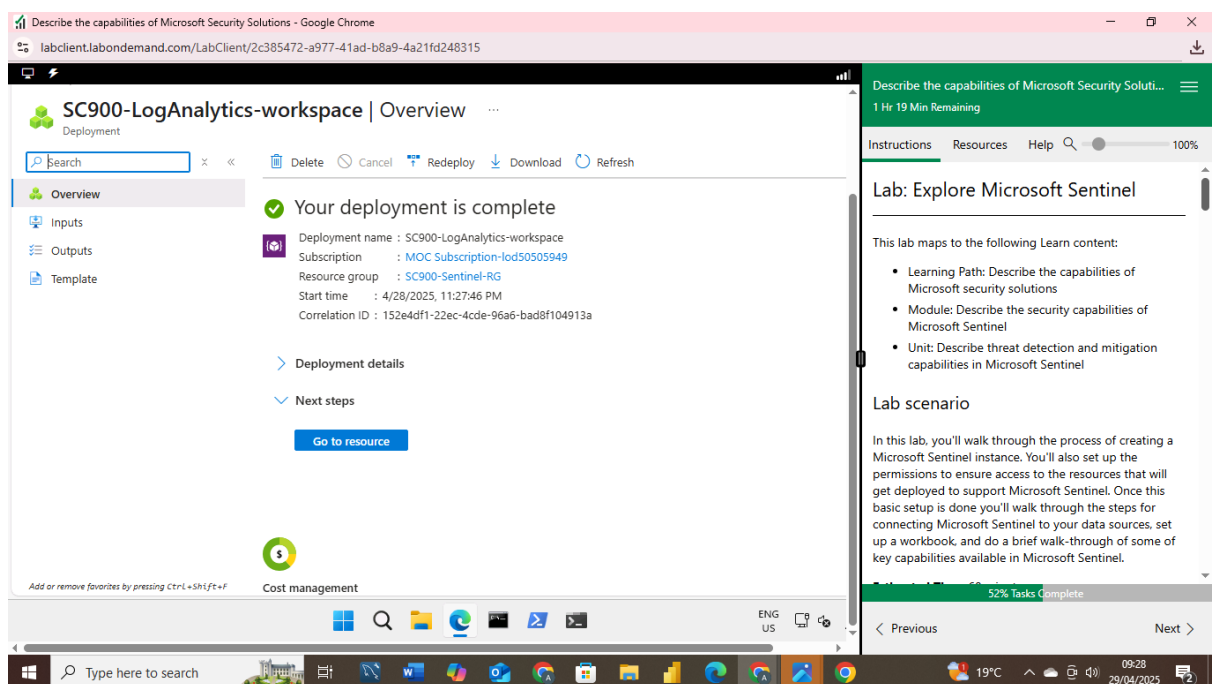
45% Tasks Complete

< Previous Next >



In this lab, I explored Microsoft Defender for Cloud, focusing on the content available on the landing page, including insights from Identity Threat Detection and Response (ITDR) Deployment Health. I also examined the Microsoft Secure Score, gaining an understanding of how it provides actionable recommendations to help organizations continuously assess and improve their overall security posture.

3. Lab: Explore Microsoft Sentinel



Describe the capabilities of Microsoft Security Solutions - Google Chrome

labclient.labondemand.com/LabClient/2c385472-a977-41ad-b8a9-4a21fd248315

Microsoft Azure

Selected workspace: 'sc900-loganalytics-workspace'

2 Active rules

Rules by severity

High (1) Medium (1) Low (0) Informational (0)

Active rules Rule templates Anomalies

Search by ID, name, tactic or technique

Severity	Name	Rule t...	Status	Tactics	Techniques
Medium	Detect CoreBac...	Scd	Enabled	Impact	T1496
High	Advanced Multi...	Fu:	Enabled	Collection +11	

68% Tasks Complete

Previous Next

24 Minutes Remaining

Instructions Resources Help

a. select **Analytics**. There should be two active rules, one that is available by default and the rule you created in the previous task. Select the default rule **Advanced Multistage Attack Detection**. Review the detailed information. **Note:** You may need to select the "<<" at the far-right side of the window to see the information panel.

b. From the left navigation panel, select **Automation**. Here you can create simple automation rules, integrate with existing playbooks, or create new playbooks. Select **+ Create** then select **Automation rule**. Note the window that opens on the right side of the screen and the options available to create conditions and actions. Select **Cancel** from the bottom of the screen.

4. Close the window by selecting the **X** on the top-right corner of the window.

5. From the top left corner of the window, in the blue banner, select **Microsoft Azure** to return to the home page of the Azure portal.

Describe the capabilities of Microsoft Security Solutions - Google Chrome

labclient.labondemand.com/LabClient/2c385472-a977-41ad-b8a9-4a21fd248315

Microsoft Azure

Create a resource

Microsoft Sentinel

Monitor

Quickstart Center

Azure AI services

Kubernetes services

Virtual machines

App Services

Storage accounts

More services

Resources

Recent Favorite

Name	Type	Last Viewed
SC900-LogAnalytics-workspace	Log Analytics workspace	16 minutes ago
SC900-Sentinel-RG	Resource group	23 minutes ago

69% Tasks Complete

Previous Next

23 Minutes Remaining

Instructions Resources Help

4. Close the window by selecting the **X** on the top-right corner of the window.

5. From the top left corner of the window, in the blue banner, select **Microsoft Azure** to return to the home page of the Azure portal.

6. Sign out and close all the open browser tabs.

Review

In this IV you walked through the steps for connecting Microsoft Sentinel to data sources, you set up a workbook, and walked several options available in Microsoft Sentinel.

Congratulations!

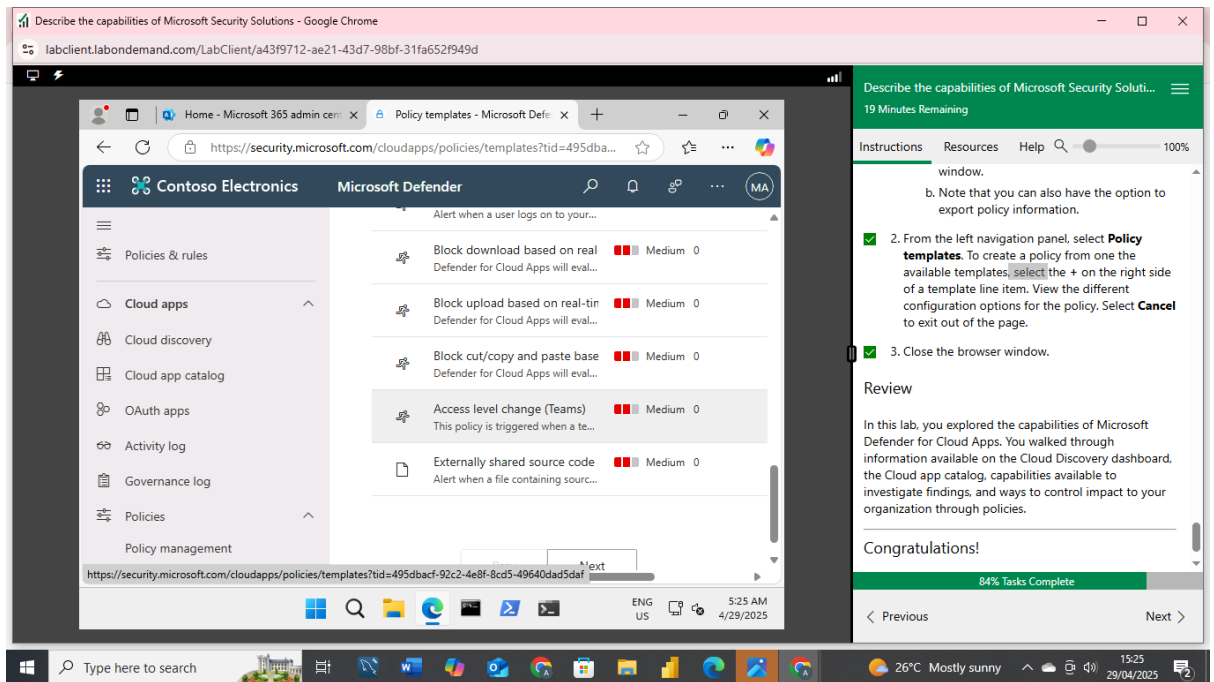
You have successfully completed this Lab. Click **Next** to advance to the next **Lab**.

In this lab, I set up an Analytics Workspace in Microsoft Sentinel and explored its various security monitoring and incident management features. I also walked through the process of creating an automation rule, a mechanism used to automatically manage and respond to incidents and alerts based on predefined criteria. The automated responses help to streamline security operations by reducing manual intervention and ensuring timely incident handling.

4. Lab: Explore Microsoft Defender for Cloud Apps

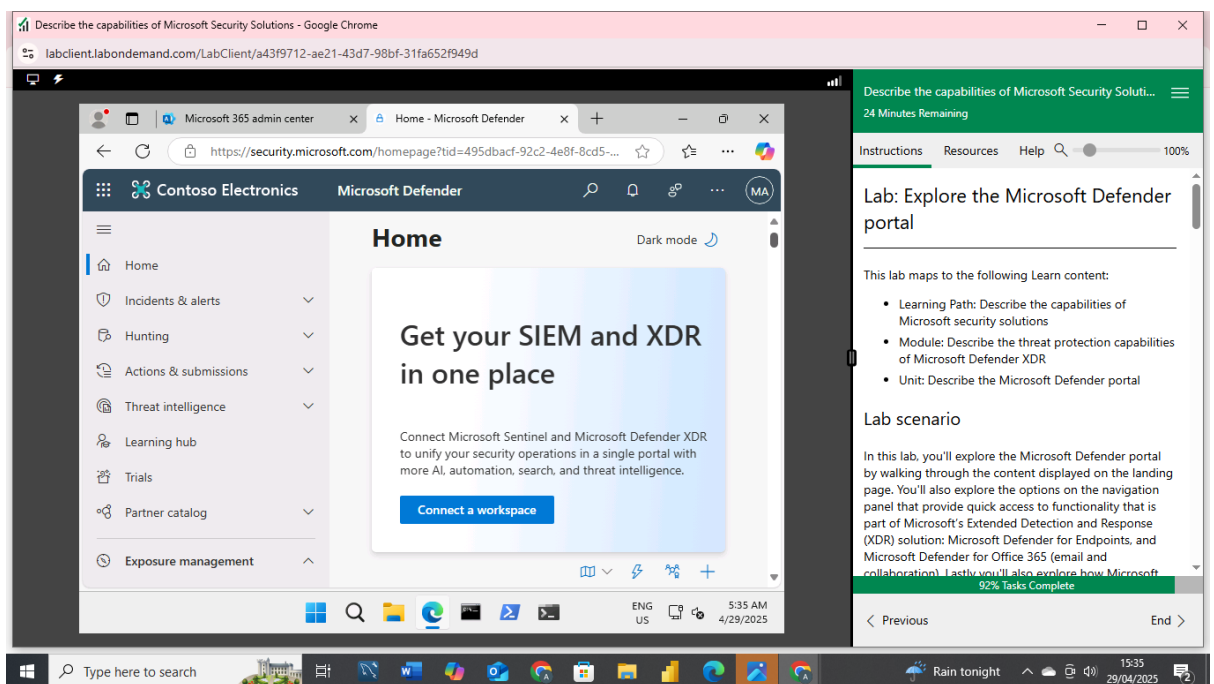
The screenshot shows the Microsoft 365 admin center interface. The header includes the 'Contoso Electronics' logo and the 'Microsoft 365 admin center' title. Below the header, there's a navigation bar with options like 'Simplified view', 'Add a user', 'Reset password', and 'Add a group'. The main content area displays a welcome message: 'Good afternoon, MOD Administrator' and a task card titled 'Set up email with a custom domain'. The task card instructs the user to 'Connect a domain that you own, or get a new one.' The right sidebar shows a progress bar for 'Describe the capabilities of Microsoft Security Solutions' with '20 Minutes Remaining' and a '71% Tasks Complete' status.

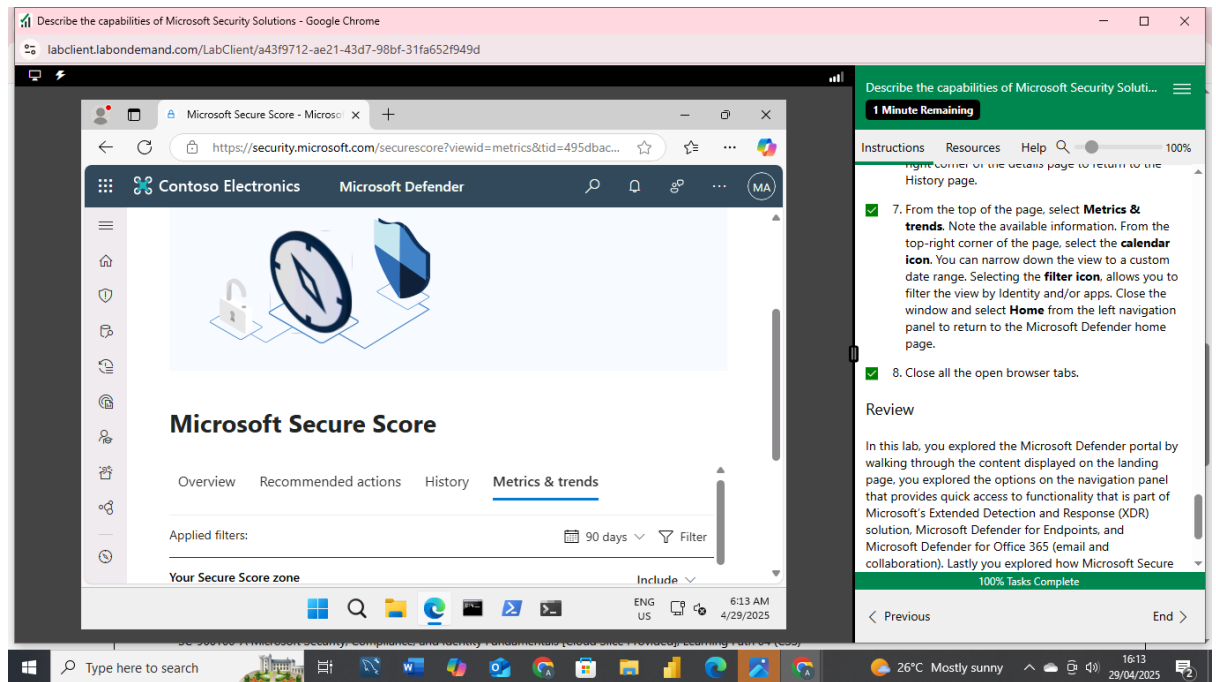
The screenshot shows the Microsoft Defender Cloud Apps settings page. The header includes the 'Contoso Electronics' logo and the 'Microsoft Defender' title. The main content area displays the 'Cloud apps' section with a 'Basic filter' toggle and a list of apps. The list includes 'Microsoft 365' and 'Microsoft Azure'. The right sidebar shows a progress bar for 'Describe the capabilities of Microsoft Security Solutions' with '49 Minutes Remaining' and a '77% Tasks Complete' status.



In this lab, I explored the capabilities of Microsoft Defender for Cloud Apps, focusing on key features such as policy management, the cloud app catalog, and the activity log. Additionally, I examined the Cloud Discovery dashboard, which provides visibility into cloud application usage, user activities, and potential risks. These tools are essential for monitoring, controlling, and securing cloud app environments within an organization.

5. Lab: Explore the Microsoft Defender portal





In this lab, I explored the Microsoft Defender Portal and its available features. I focused on understanding the functionality of Microsoft's Extended Detection and Response (XDR) solution, including the key components such as Exposure Management and the Microsoft Secure Score. These tools provide a comprehensive visibility into an organization's security posture, helping to identify vulnerabilities and track improvements in security configurations and practices.