**Name:** Anne Musau

**Program Details:** Data Protection Specialist - C1 – 2025

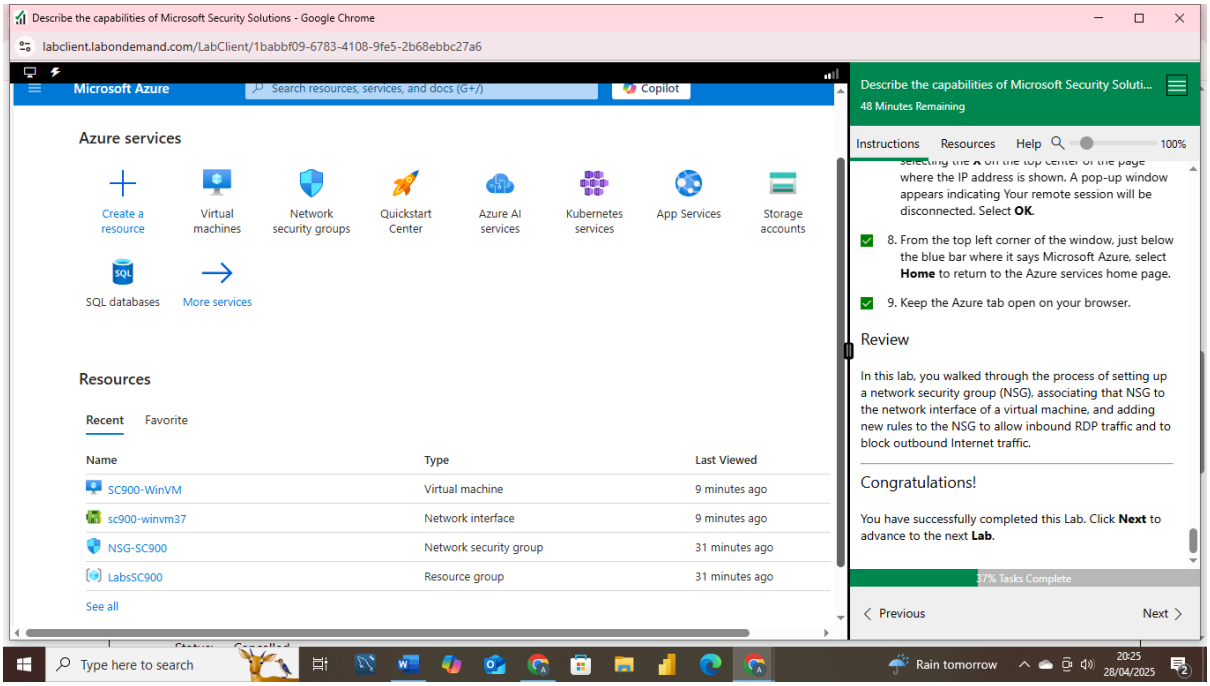
**Admission:** adc-dp01-25032

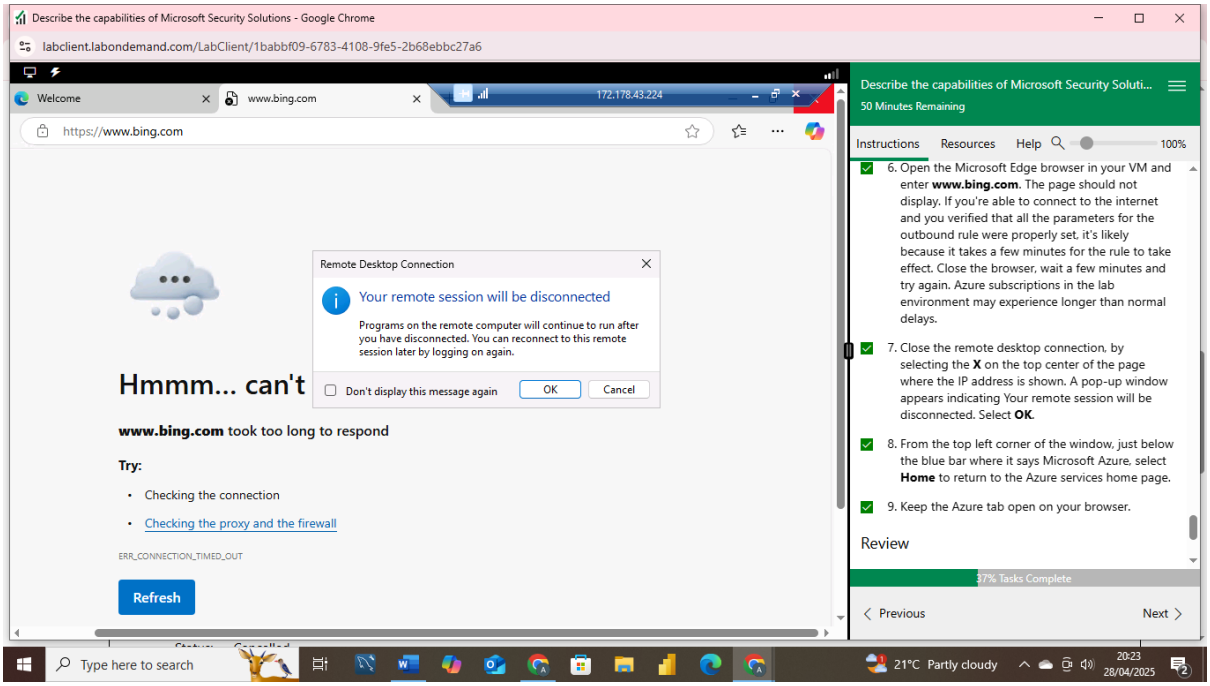
**Week 2 Lab Assignment:** SC-900 Lab 2

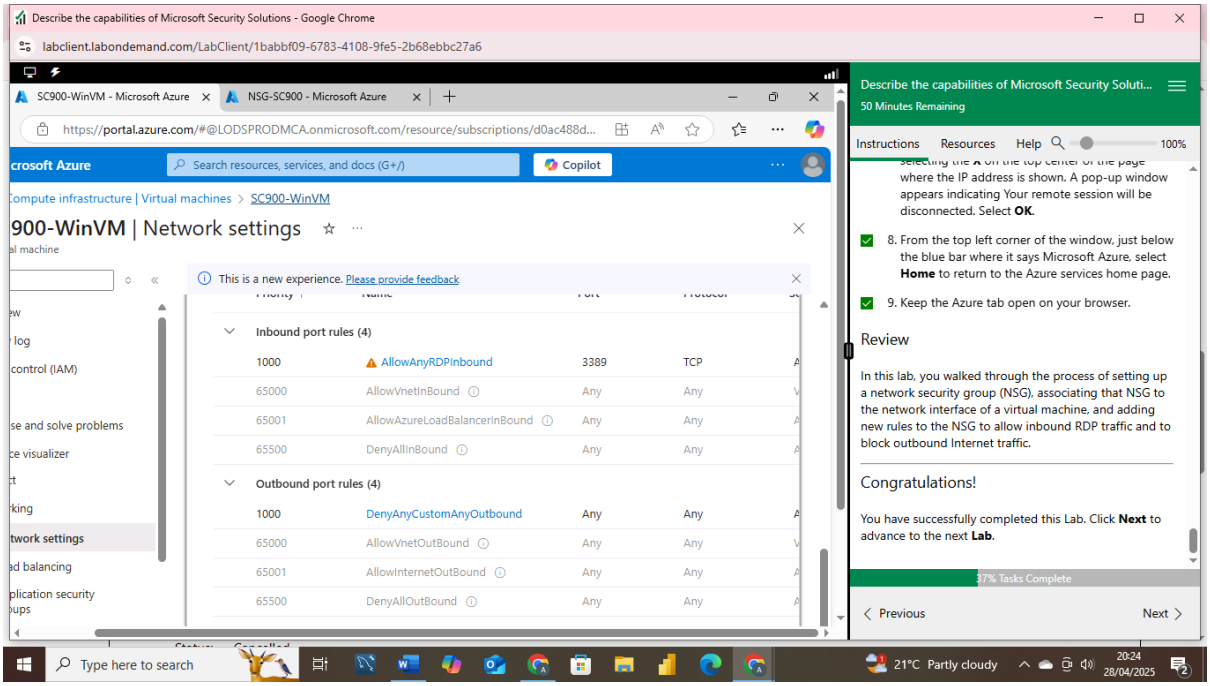
## Capabilities of Microsoft Security Solution.

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)

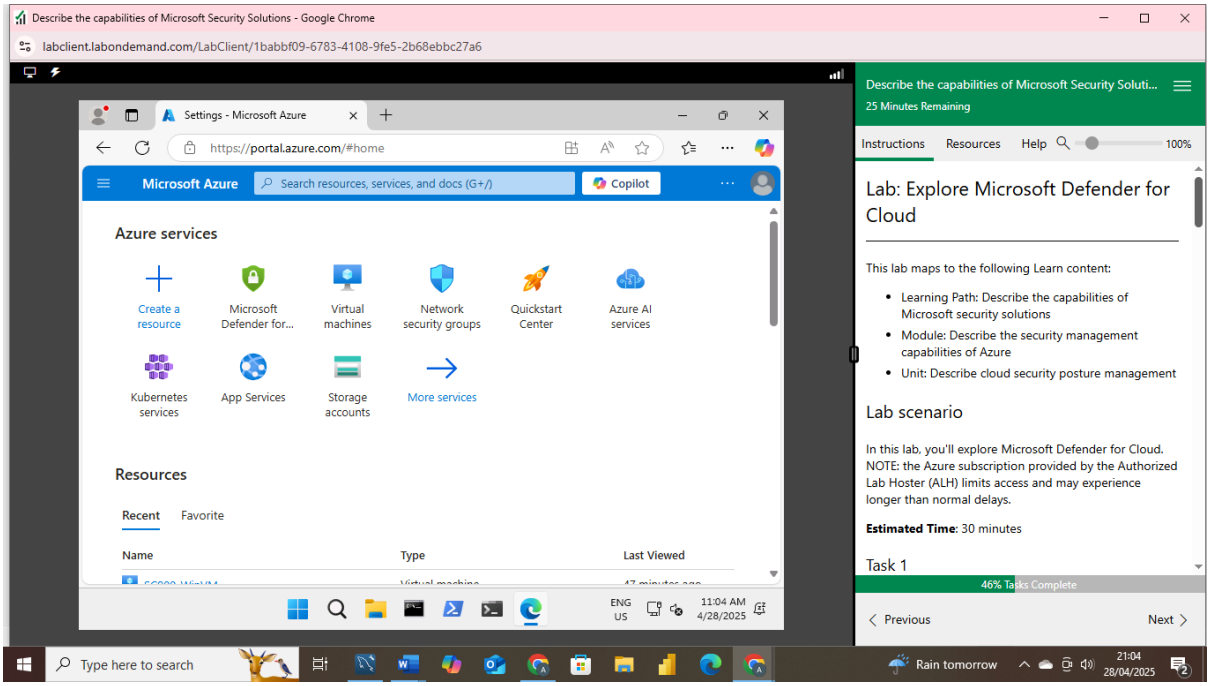


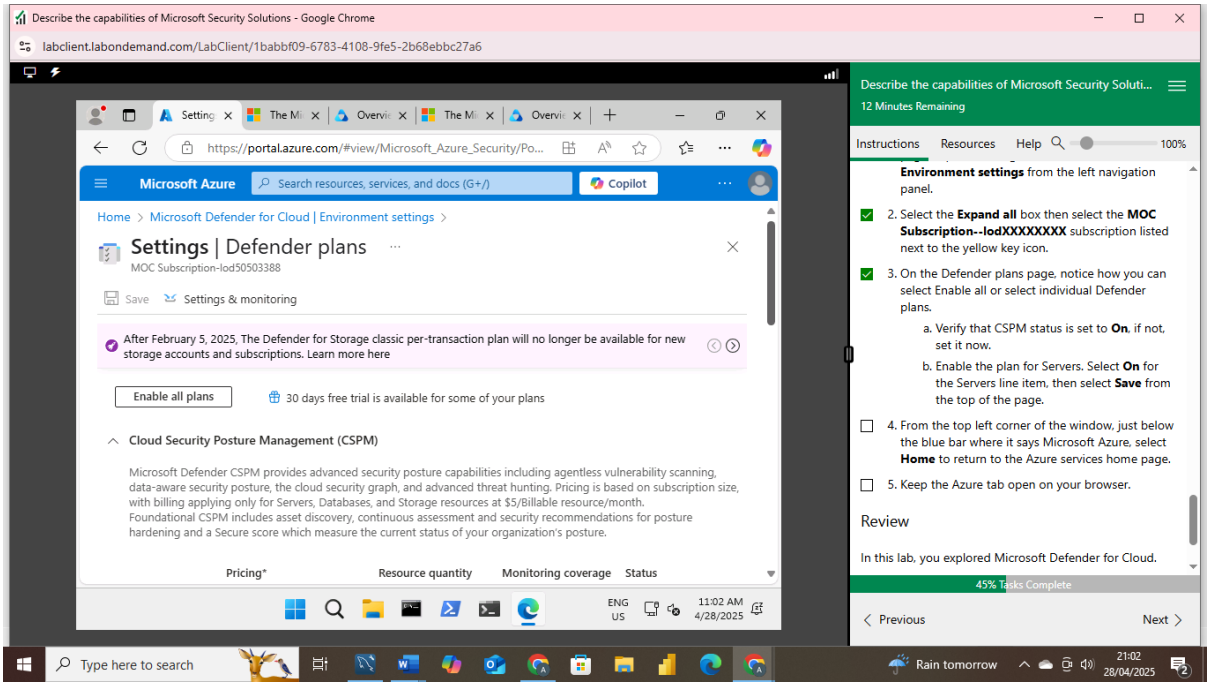


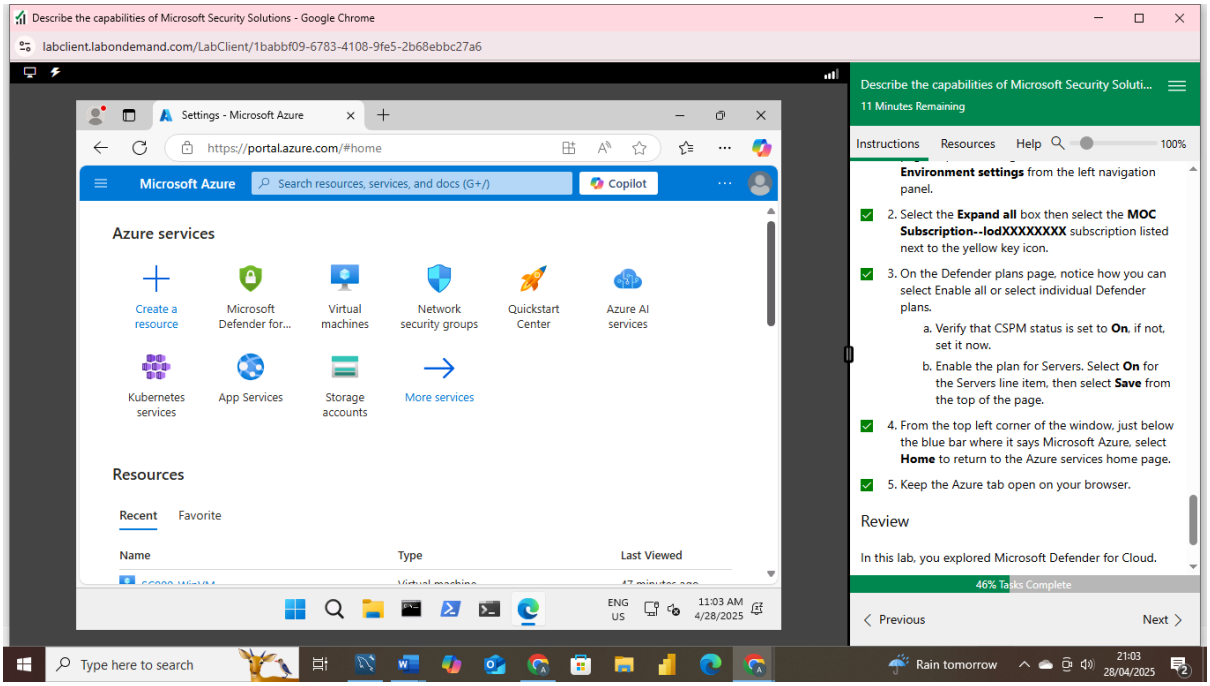




In this lab, I explored the process of creating a Network Security Group (NSG) in Azure and attaching it to a virtual machine's network interface. I learned how to configure inbound and outbound security rules, including setting up a rule to allow inbound RDP traffic for remote access and another to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

2. Lab: Explore Microsoft Defender for Cloud

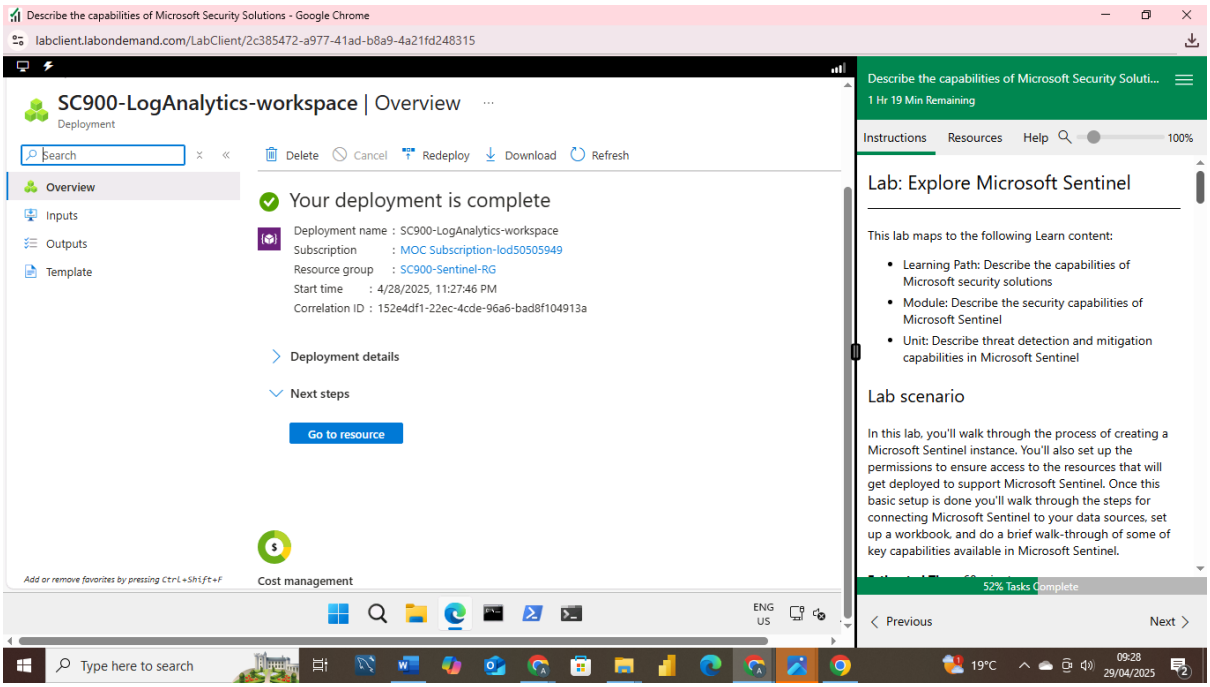


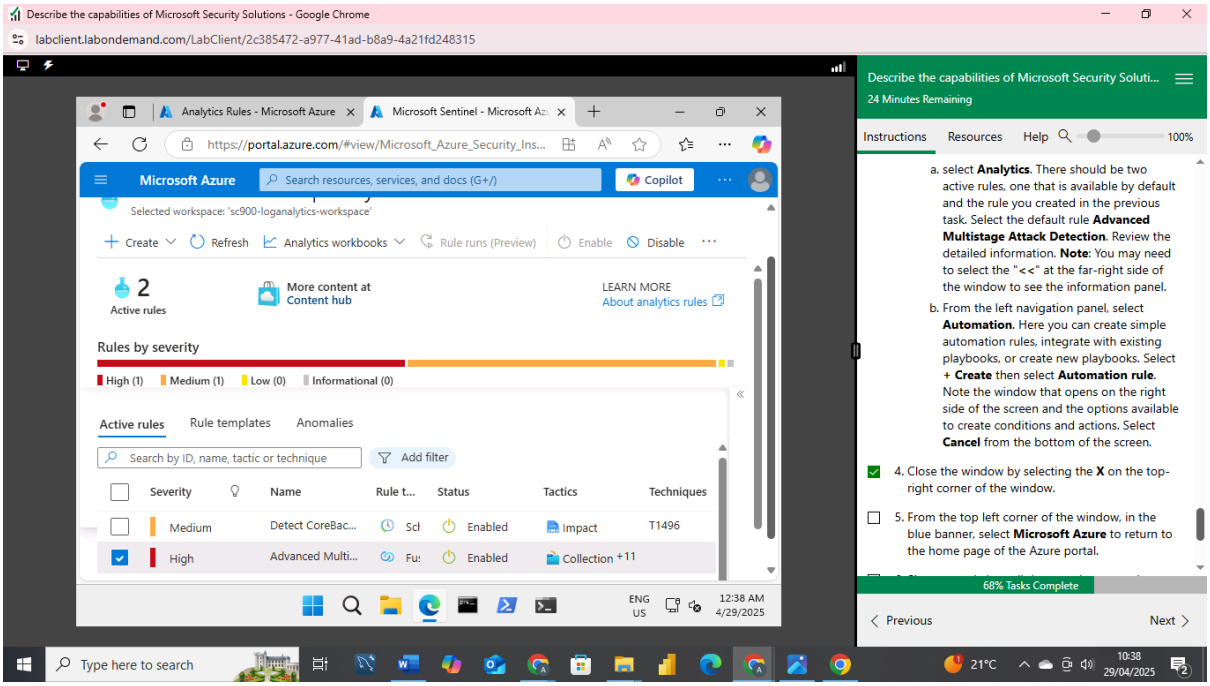



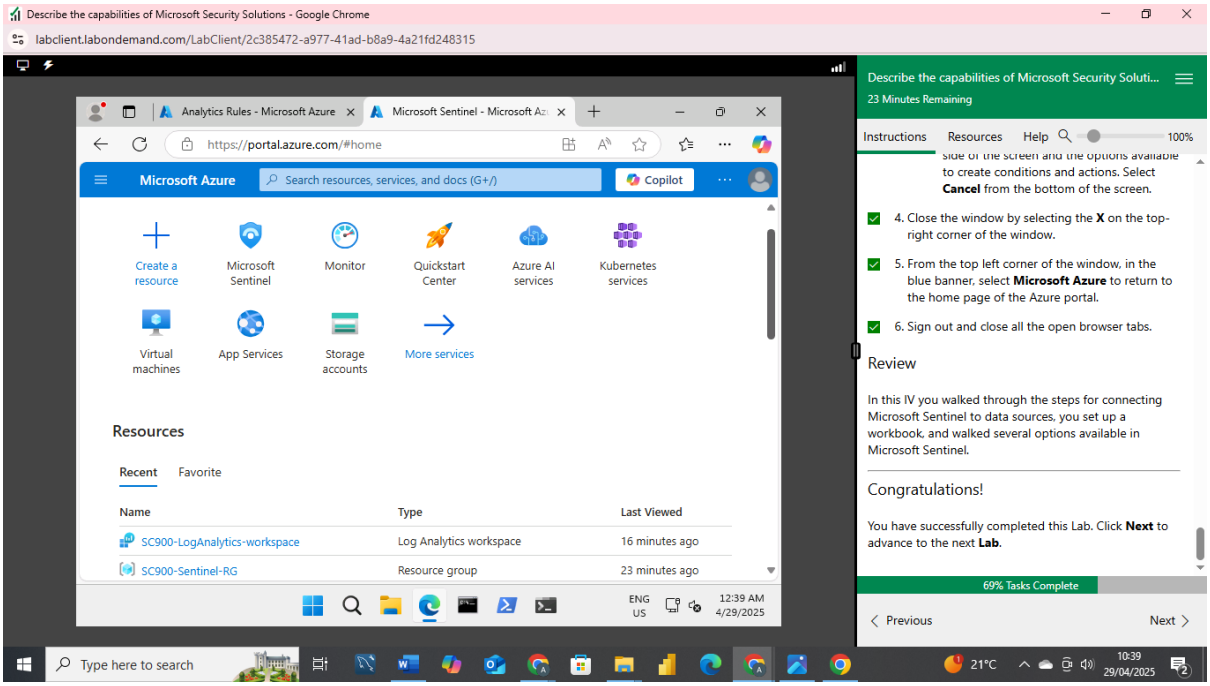



In this lab, I explored Microsoft Defender for Cloud, focusing on the content available on the landing page, including insights from Identity Threat Detection and Response (ITDR) Deployment Health. I also examined the Microsoft Secure Score, gaining an understanding of how it provides actionable recommendations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

3. Lab: Explore Microsoft Sentinel

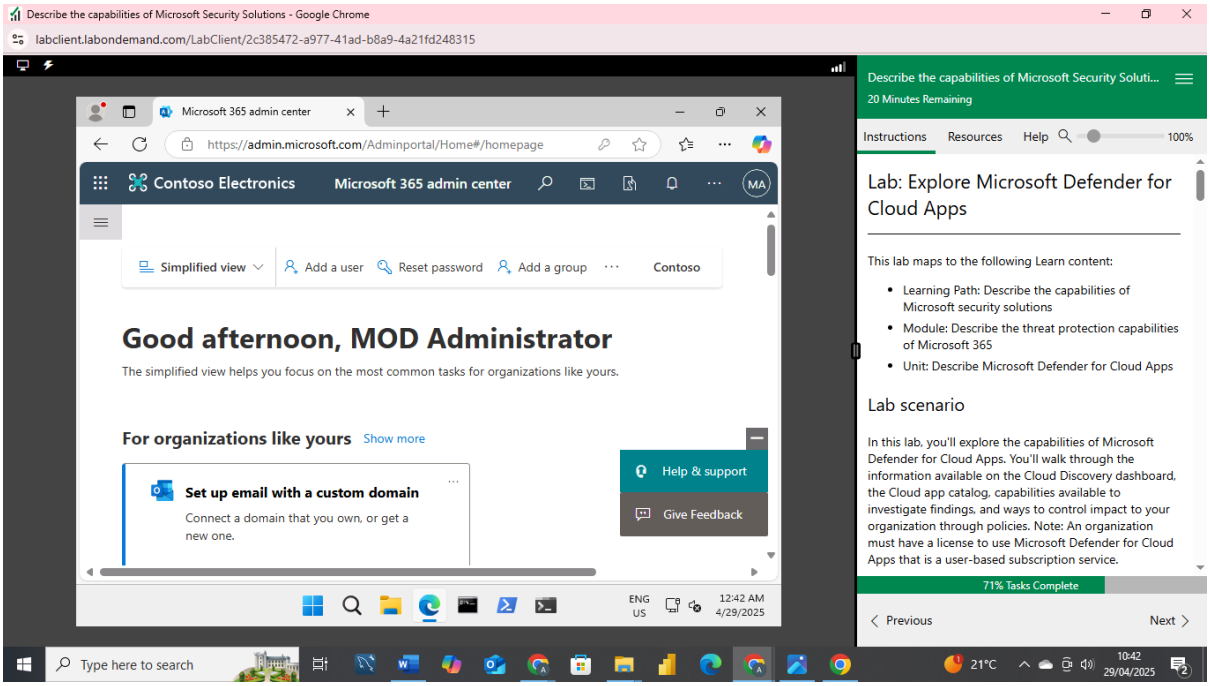


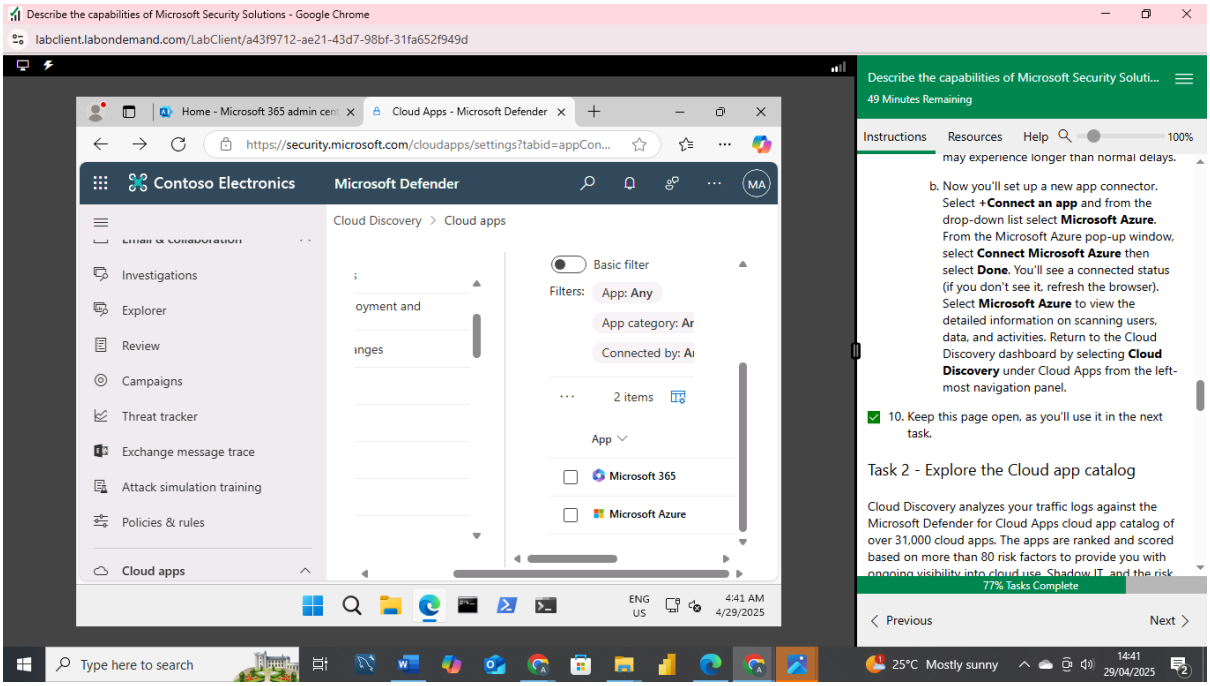


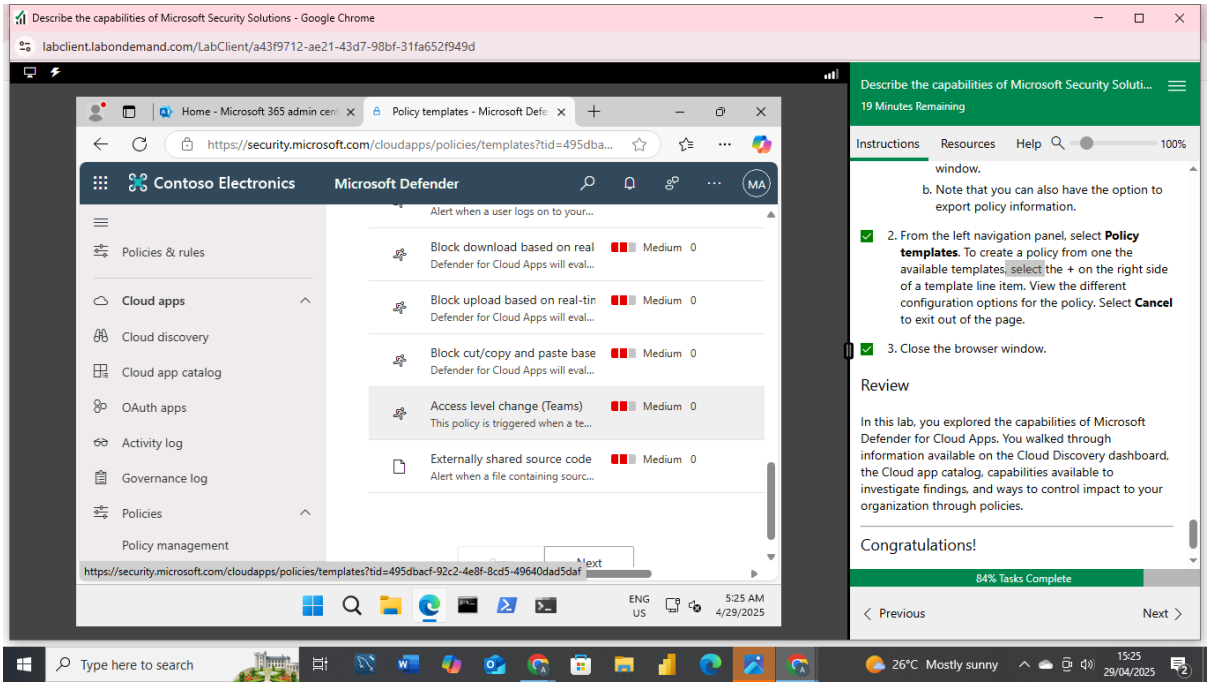




In this lab, I set up an Analytics Workspace in Microsoft Sentinel and explored its various security monitoring and incident management features. I also walked through the process of creating an automation rule, a mechanism used to automatically manage and respond to incidents and alerts based on predefined 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

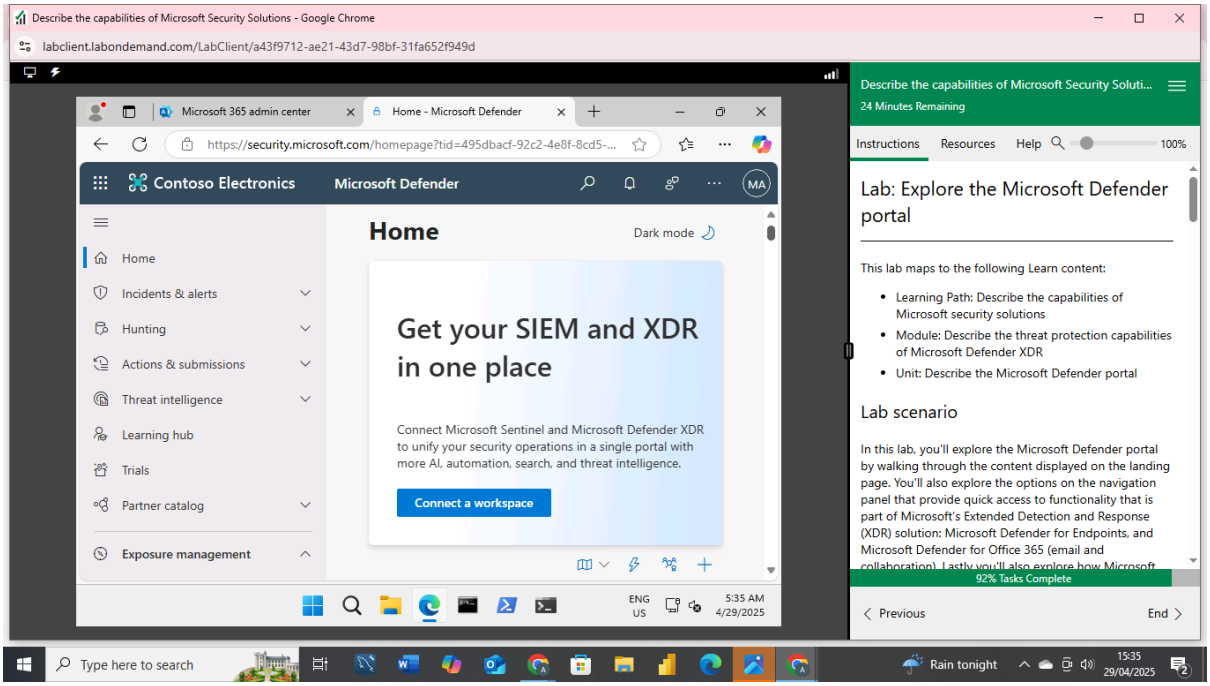


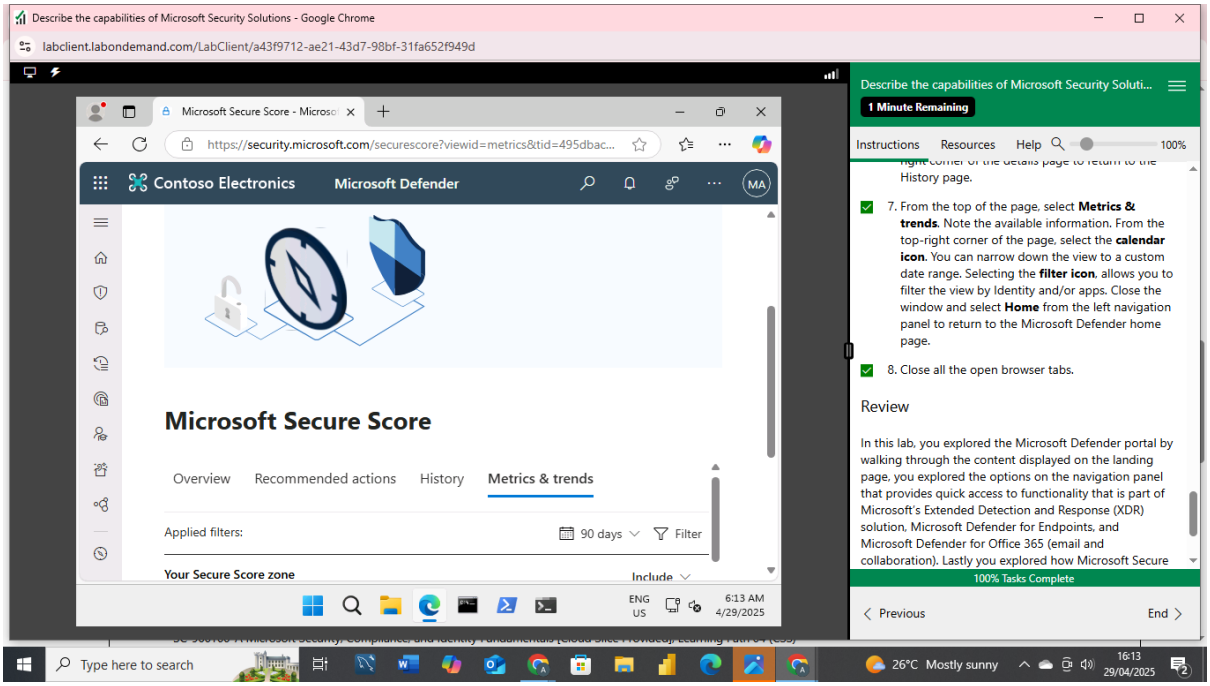






In this lab, I explored the capabilities of Microsoft Defender for Cloud Apps, focusing on key features such as policy management, the cloud app catalog, and the activity log. Additionally, I examined the Cloud Discovery dashboard, which provides visibility into cloud application usage, user activities, 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.