



LAB #2 REPORT [WEEK #2]

BY

EMMANUEL MUTURIA™

ADMISSION NUMBER
[ADC-SE02-25011]

TABLE OF CONTENTS

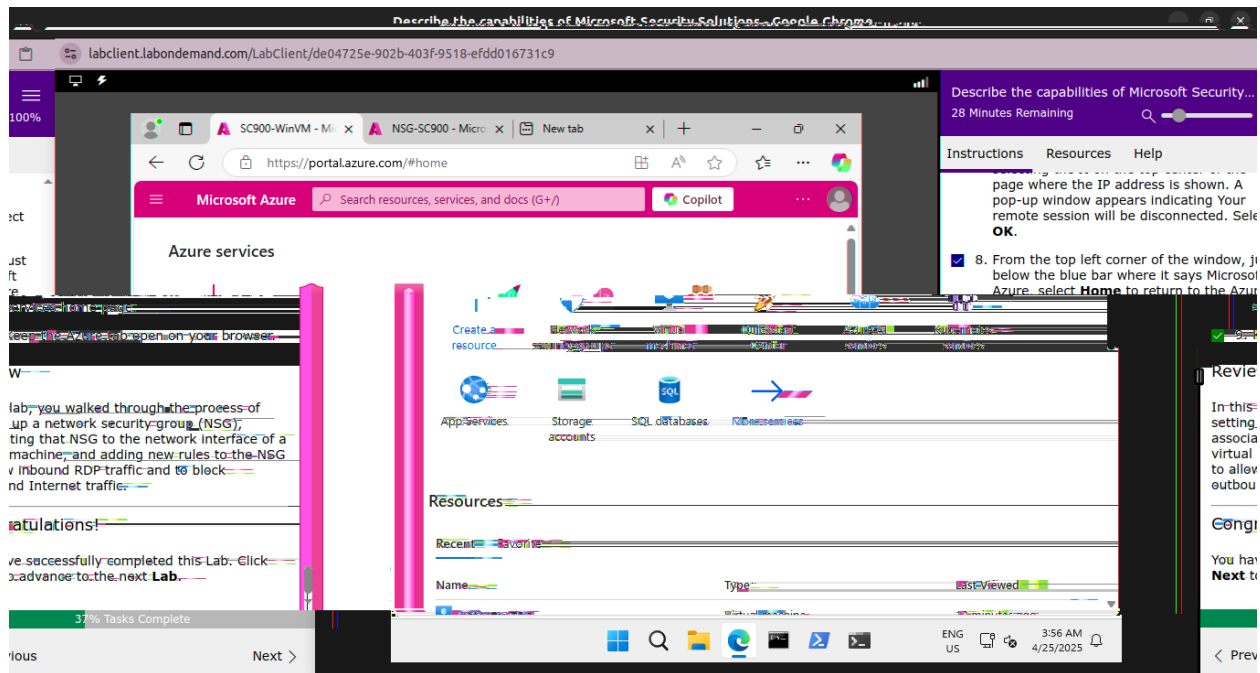
INTRODUCTION.....	
SECTION #1 [Explore Azure Network Security Groups (NSGs)].....	
SECTION #2 [Explore Microsoft Defender for Cloud].....	
SECTION #3 [Explore Microsoft Sentinel].....	
SECTION #4 [Explore Microsoft Defender for Cloud Apps].....	
SECTION #5 [Explore the Microsoft Defender portal].....	
CONCLUSION.....	
REFERENCES.....	



INTRODUCTION

This report documents my continuation of the SC-900 Lab 2: Describe Capabilities of Microsoft Security Solutions as required by the Cyber Shujaa Program [Security Engineer Track]. It contains screenshots and links to the badges to prove the completion of the learning path's modules.

SECTION #1 [Explore Azure Network Security Groups (NSGs)]



In this lab, I walked through the process of setting up a network security group (NSG), associating that NSG to the network interface of a virtual machine, and adding new rules to the NSG to allow inbound RDP traffic and to block outbound Internet traffic.

SECTION #2 [Explore Microsoft Defender for Cloud]

The screenshot displays a web browser window titled "Describe the capabilities of Microsoft Security Solutions - Google Chrome". The address bar shows a URL from "labclient.labondemand.com". The main content area shows the Microsoft Azure portal home page with various service tiles like "Microsoft Defender for...", "Network security groups", "Virtual machines", "Quickstart Center", "Azure AI services", "Kubernetes services", "App Services", and "Storage accounts".

On the right side, there is a sidebar with a green header "Describe the capabilities of Microsoft Security..." and a progress indicator "12 Minutes Remaining" and "100%". Below this, there are sections for "Instructions", "Resources", and "Help". The "Instructions" section contains a list of tasks:

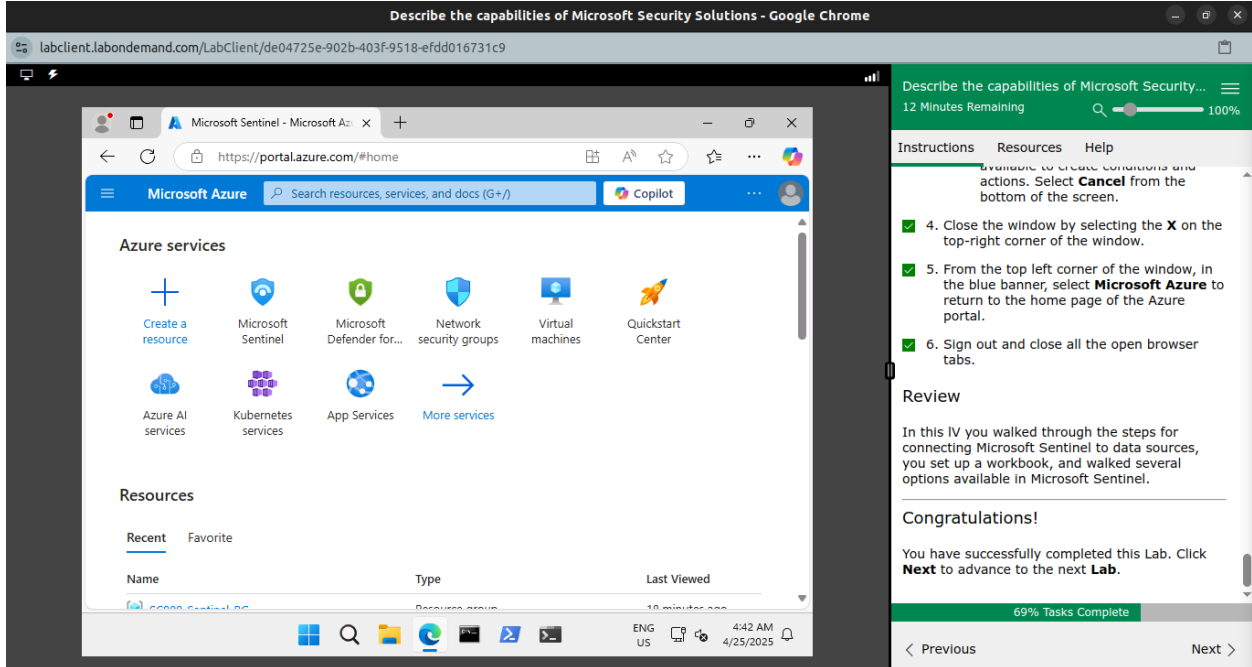
- 3. On the Defender plans page, notice how you can select Enable all or select individual Defender plans.
 - a. Verify that CSPM status is set to **On**, if not, set it now.
 - b. Enable the plan for Servers. Select **On** for the Servers line item, then select **Save** from the top of the page.
- 4. 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.

Below the instructions, there is a "Review" section with the text: "In this lab, you explored Microsoft Defender for Cloud." and a "Congratulations!" section with the text: "You have successfully completed this Lab. Click **Next** to advance to the next Lab."

At the bottom of the sidebar, there is a progress bar showing "46% Tasks Complete" and navigation buttons for "Previous" and "Next".

This lab helped me explore Microsoft Defender for Cloud.

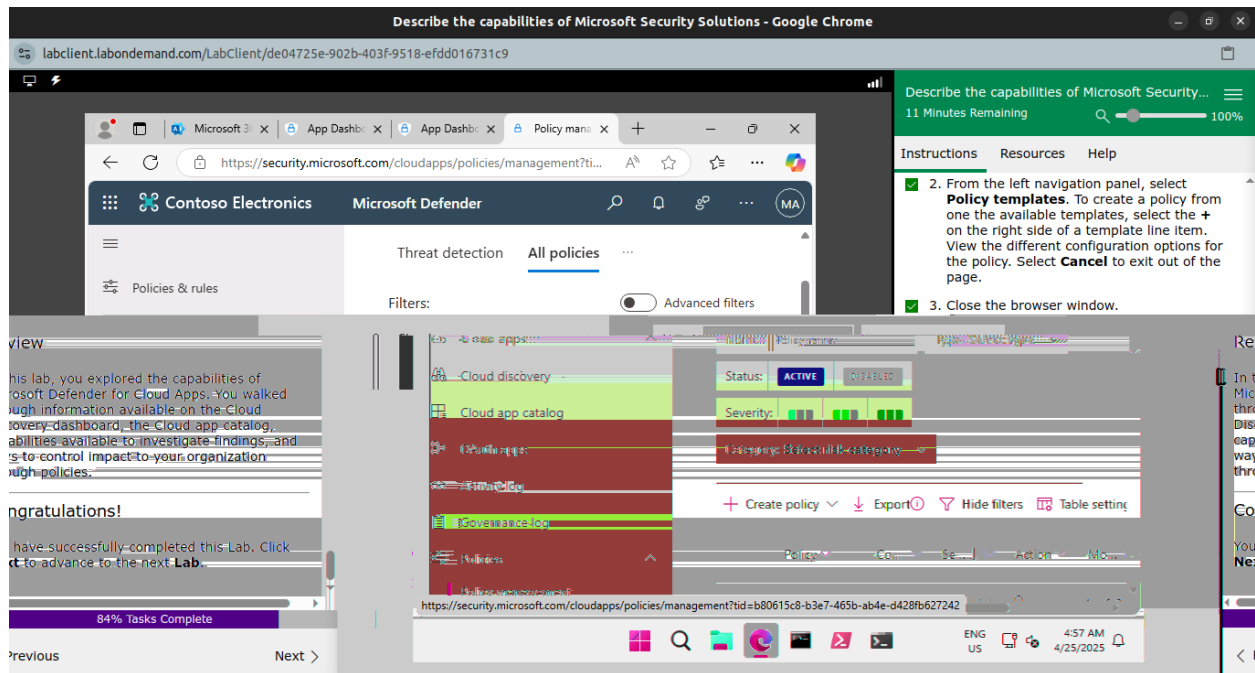
SECTION #3 [Explore Microsoft Sentinel]



The screenshot shows a Google Chrome browser window with the title "Describe the capabilities of Microsoft Security Solutions - Google Chrome". The address bar shows the URL "https://portal.azure.com/#home". The main content area displays the Microsoft Azure portal home page, featuring a search bar, a "Copilot" button, and sections for "Azure services" (including Create a resource, Microsoft Sentinel, Microsoft Defender for..., Network security groups, Virtual machines, Quickstart Center, Azure AI services, Kubernetes services, App Services, and More services) and "Resources" (Recent and Favorite). The sidebar on the right shows a progress bar for "Describe the capabilities of Microsoft Security..." with a "12 Minutes Remaining" timer and a "69% Tasks Complete" status. The sidebar also includes instructions, a review section, and a "Congratulations!" message.

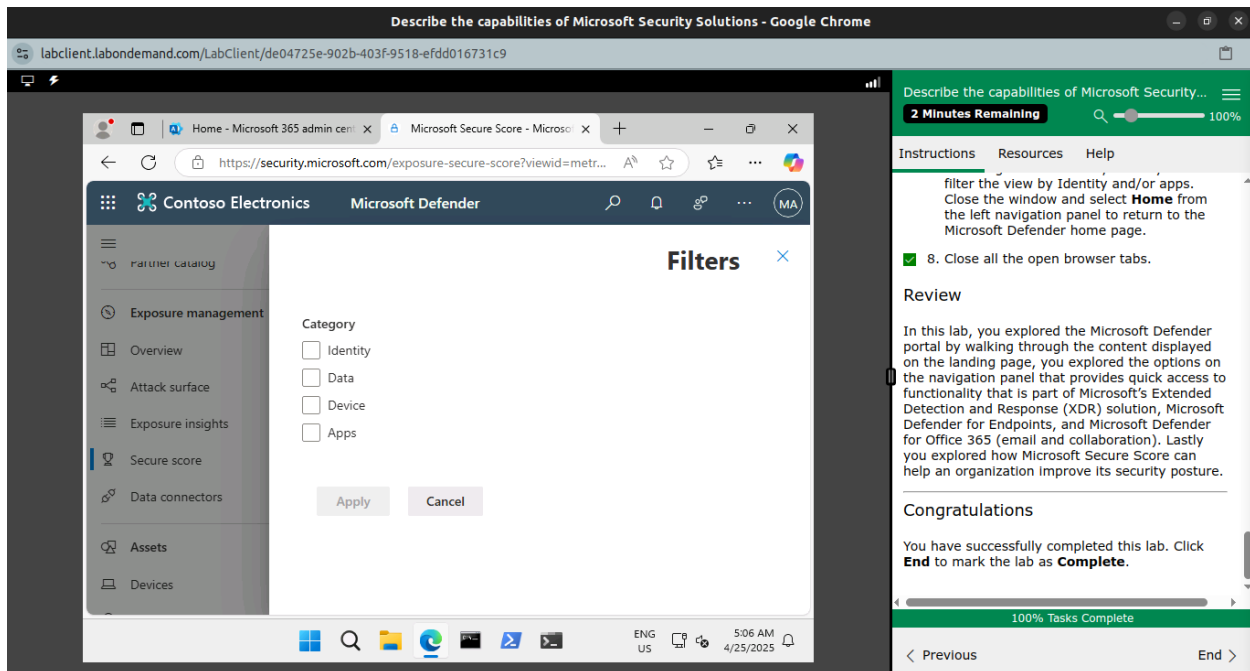
This lab walked me through the steps for connecting Microsoft Sentinel to data sources, you set up a workbook, and walked several options available in Microsoft Sentinel.

SECTION #4 [Explore Microsoft Defender for Cloud Apps]



In this lab, I explored the capabilities of Microsoft Defender for Cloud Apps. I walked through information available on the Cloud Discovery dashboard, the Cloud app catalog, capabilities available to investigate findings, and ways to control impact to my organisation through policies.

SECTION #5 [Explore the Microsoft Defender portal]



In this lab, I explored the Microsoft Defender portal by walking through the content displayed on the landing page, you explored the options on the navigation panel that provides quick access to functionality that is part of Microsoft's Extended Detection and Response (XDR) solution, Microsoft Defender for Endpoints, and Microsoft Defender for Office 365 (email and collaboration). Lastly I explored how Microsoft Secure Score can help an organisation improve its security posture.

CONCLUSION

This report has provided my chronological summary and documentation of the SC-900 Lab 2: Describe Capabilities of Microsoft Security Solutions. It has also included relevant resources that prove the same and serve as a testament to the satisfaction of Week #2's learning requirements as a prerequisite to the following lessons.

REFERENCES

Login - *Skillable* *TMS.* (2024). Learnondemand.net.
[https://msle.learnondemand.net/Lab/62466?
instructionSetLang=en&classId=676662](https://msle.learnondemand.net/Lab/62466?instructionSetLang=en&classId=676662)