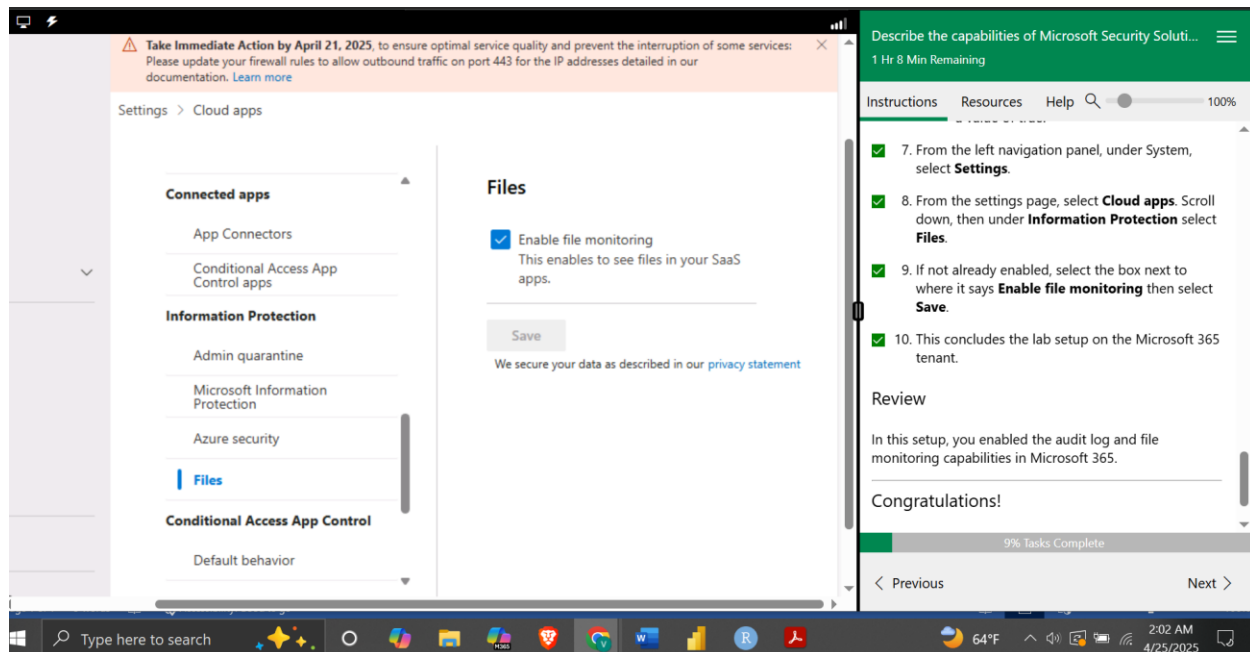


Valerie Kivayiru Jarenga

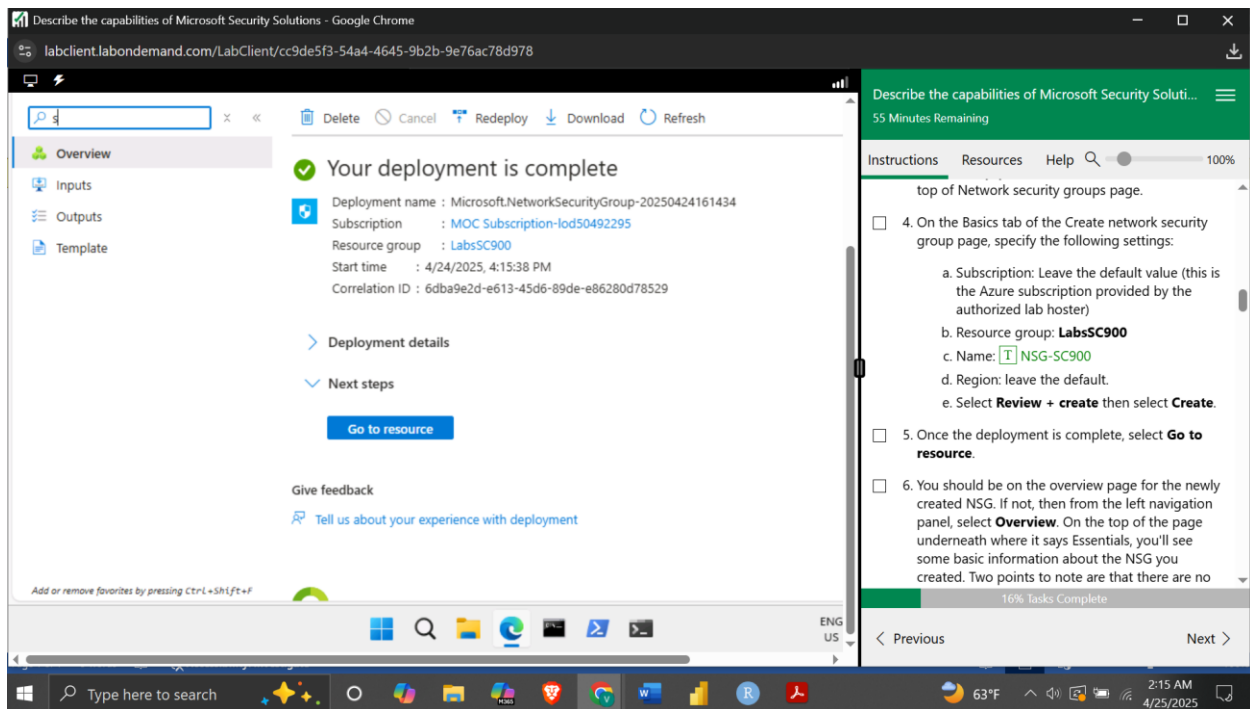
Cloud Security Specialist

1. the lab setup on the Microsoft 365 tenant.

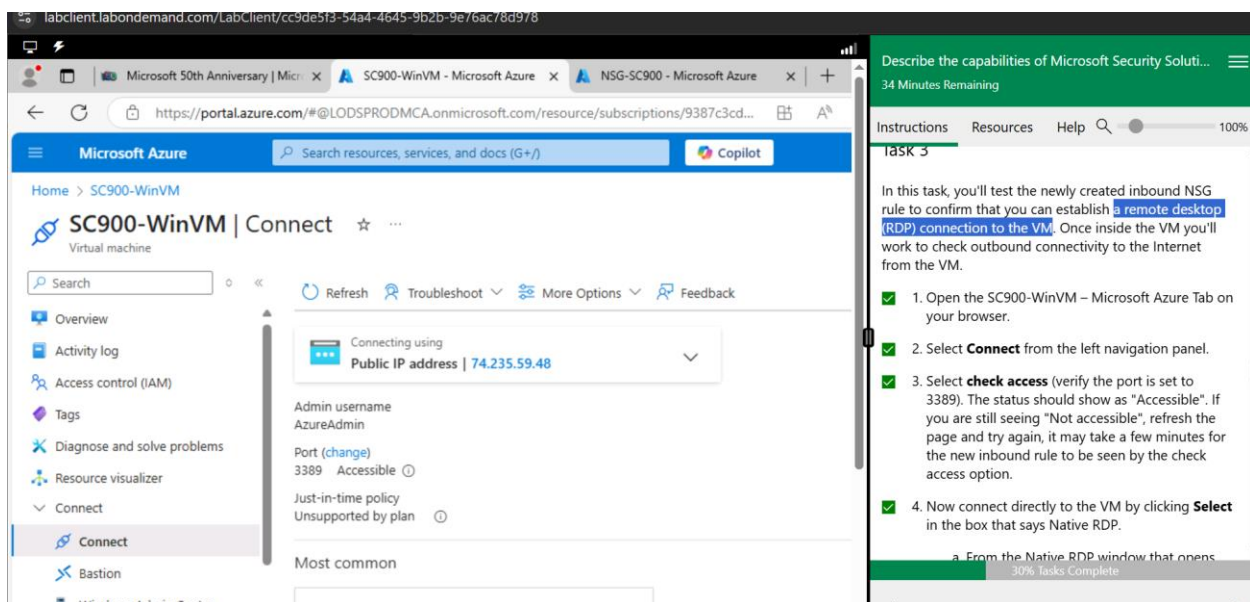


1. In this lab, I walked through the process of setting up a network security group (NSG), associating that NSG to the network interface of a virtual machine, and adding new rules to the NSG to allow inbound RDP traffic and to block outbound Internet traffic.

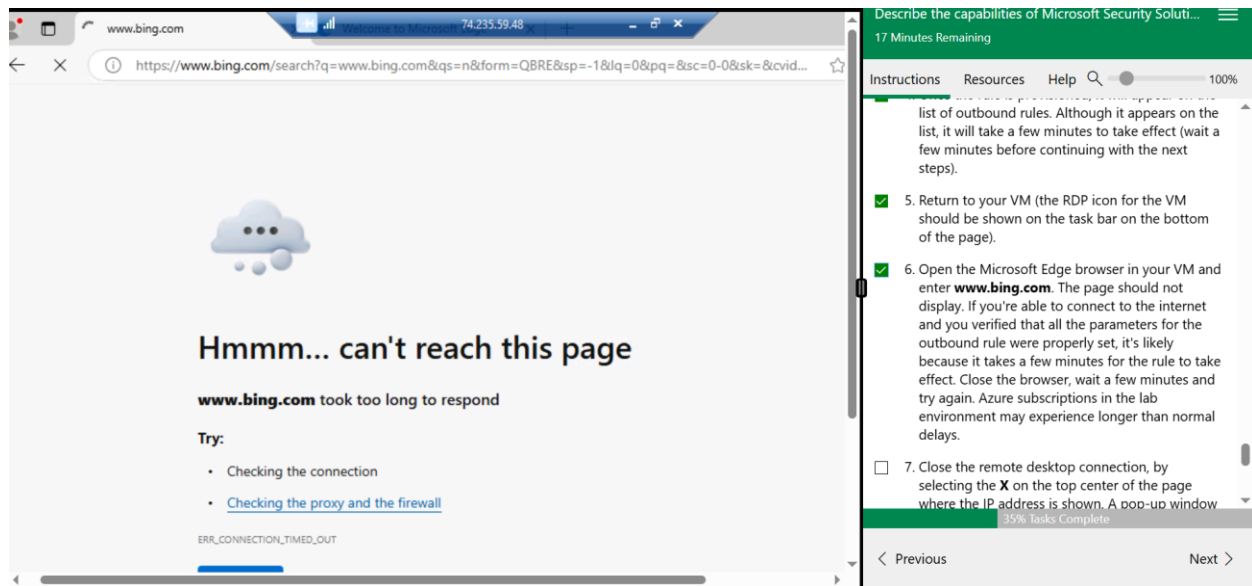
The image below shows deployment of network security group complete



The image below shows a remote desktop (RDP) connection to the VM has been established

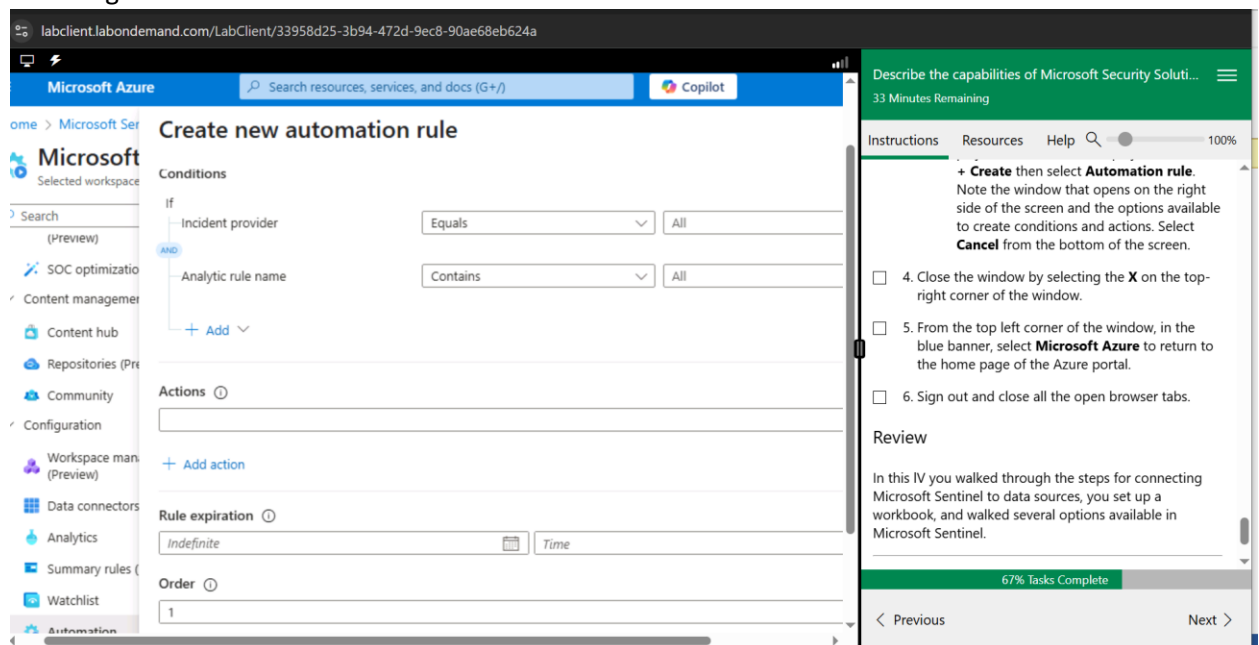


The image below shows the parameters for the outbound rule has been successful



2. Explore Microsoft Defender for Cloud

The image below shows where to create automation rule in Microsoft Sentinel



Explore Microsoft Defender for Cloud Apps

The image below shows configuration options for the policy

The screenshot shows the 'Create activity policy' page in the Microsoft Defender portal. The page has a form with the following fields:

- Policy template ***: A dropdown menu showing 'Administrative activity from a non-corporate IP address'.
- Policy name ***: A text box containing 'Administrative activity from a non-corporate IP address'.
- Policy severity ***: A set of three colored squares (orange, red, dark red).
- Category ***: A dropdown menu showing 'Threat detection'.
- Description**: A text box containing 'Alert when an admin user performs an administrative activity from an IP address that is not included in the corporate IP address range category. You must first configure your corporate IP addresses by going to the Settings page, and selecting IP address ranges.'

On the right side, there is a task pane titled 'Describe the capabilities of Microsoft Security Solutions' with a progress bar at 100%. It contains instructions for creating a policy and a 'Review' section.

Explore the Microsoft Defender portal

The image below shows Microsoft Secure Score as a percentage

The screenshot shows the 'Microsoft Secure Score' page in the Microsoft Defender portal. The page displays the following information:

- Microsoft Secure Score**: The main heading.
- Applied filters**: A section for filtering the score.
- Your secure score**: A section showing the current score.
- Secure Score: 40.3%**: The current score, with a progress bar showing 160/397 points achieved.
- History tab**: A tab for viewing the score history, showing a line graph of the score over time.

On the right side, there is a task pane titled 'Describe the capabilities of Microsoft Security Solutions' with a progress bar at 100%. It contains instructions for exploring the Secure Score and a 'Review' section.

The image below shows the history tab under Microsoft secure score

Microsoft Secure Score

Overview Recommended actions **History** Metrics & trends

▲ 10.73%



Describe the capabilities of Microsoft Security Solutions

17 Minutes Remaining

Instructions Resources Help 100%

- 5. Select the first item from the list and review the available information. In the window that opens, note the status options available. Select the **Implementation** tab to view to view information related to implementation. Select the **X** at the top right corner to close this window.
- 6. Select the **History** tab from the top of the page. For each activity listed there is a brief statement that provides context. Select an item from the history table. On the top-right of the details page, under History, select **X events** (where X is a number). The action history window opens and provides more information. Select **Close** on the bottom of the page, then select the **X** on the top-right corner of the details page to return to the History page.
- 7. From the top of the page, select **Metrics & trends**. Note the available information. From the top-right corner of the page, select the **calendar icon**. You can narrow down the view to a custom date range. Selecting the **filter icon** allows you to

100% Tasks Complete

< Previous

End >