

**NAME: BINYANYA DEBORAH NYATICHI**

**CS NO: ADC-CSS02-25051.**

**DESCRIPTION: Week 3 Assignment 5**

**ASSIGNMENT: Lab on Describe the capabilities of Microsoft Security Solutions**

**DATE: 02/05/2025**

## INTRODUCTION

This week, I will be working on a series of labs designed to help me explore the capabilities of Microsoft Security Solutions. I will begin by setting up a Microsoft 365 tenant, which will provide the foundation for testing and configuring various security features. I will then explore tools such as Azure Network Security Groups (NSGs), Microsoft Defender for Cloud, Microsoft Sentinel, Microsoft Defender for Cloud Apps, and the Microsoft Defender portal. Through these labs, I aim to gain hands-on experience in managing cloud security, monitoring threats, and understanding how Microsoft's integrated tools work together to protect enterprise environments.

## 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

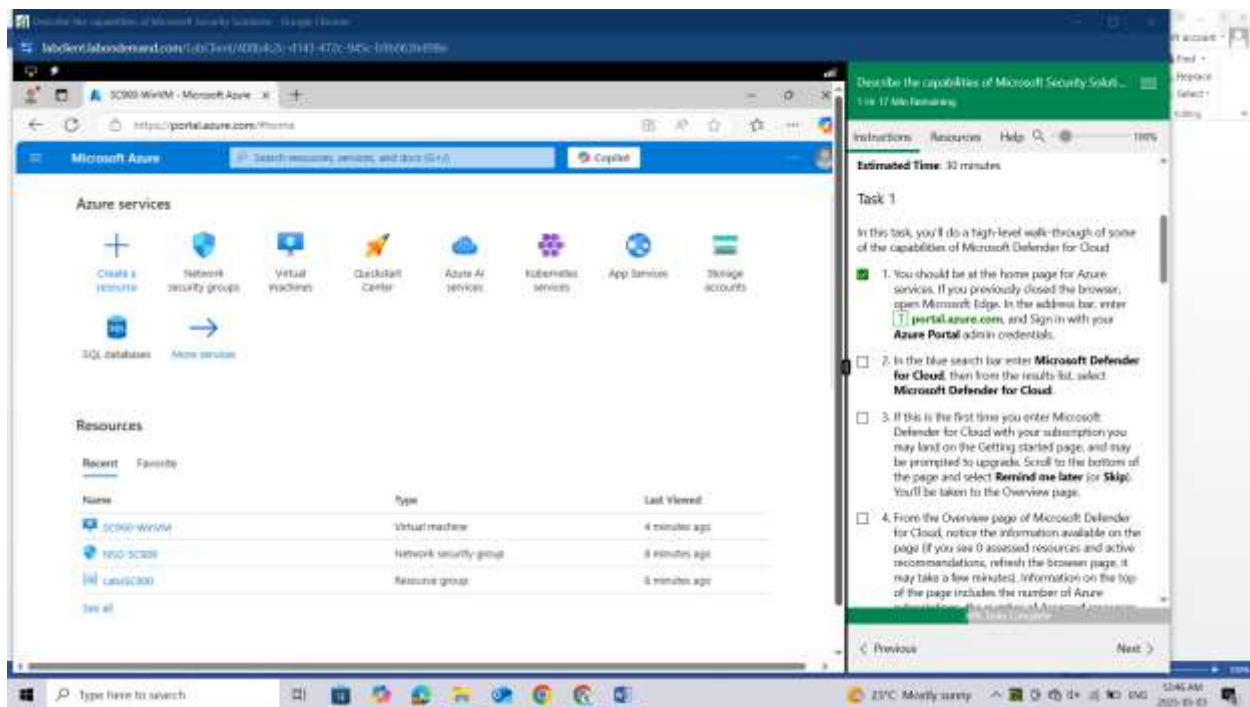
In this lab, you'll explore Microsoft Defender for Cloud.

NOTE: the Azure subscription provided by the Authorized Lab Host (ALH) limits access and may experience longer than normal delays.

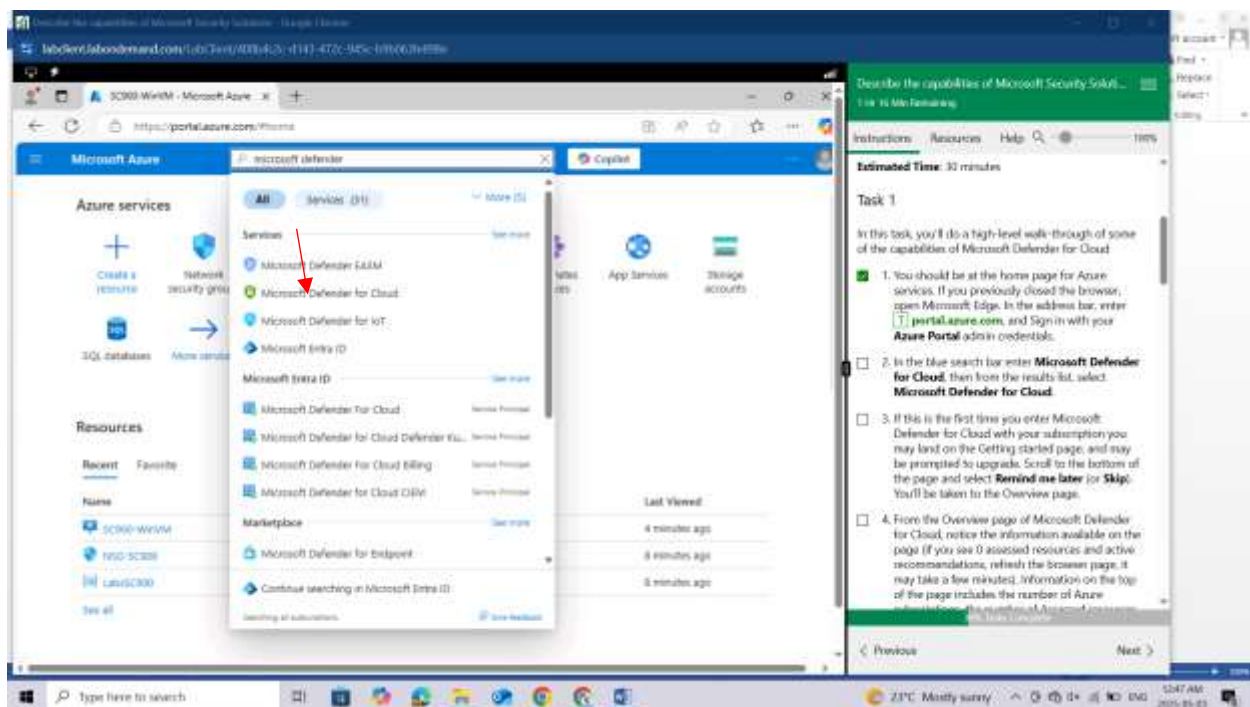
### Task 1

In this task, you'll do a high-level walk-through of some of the capabilities of Microsoft Defender for Cloud

You should be at the home page for Azure services. If you previously closed the browser, open Microsoft Edge. In the address bar, enter [portal.azure.com](https://portal.azure.com), and Sign in with your Azure Portal admin credentials.

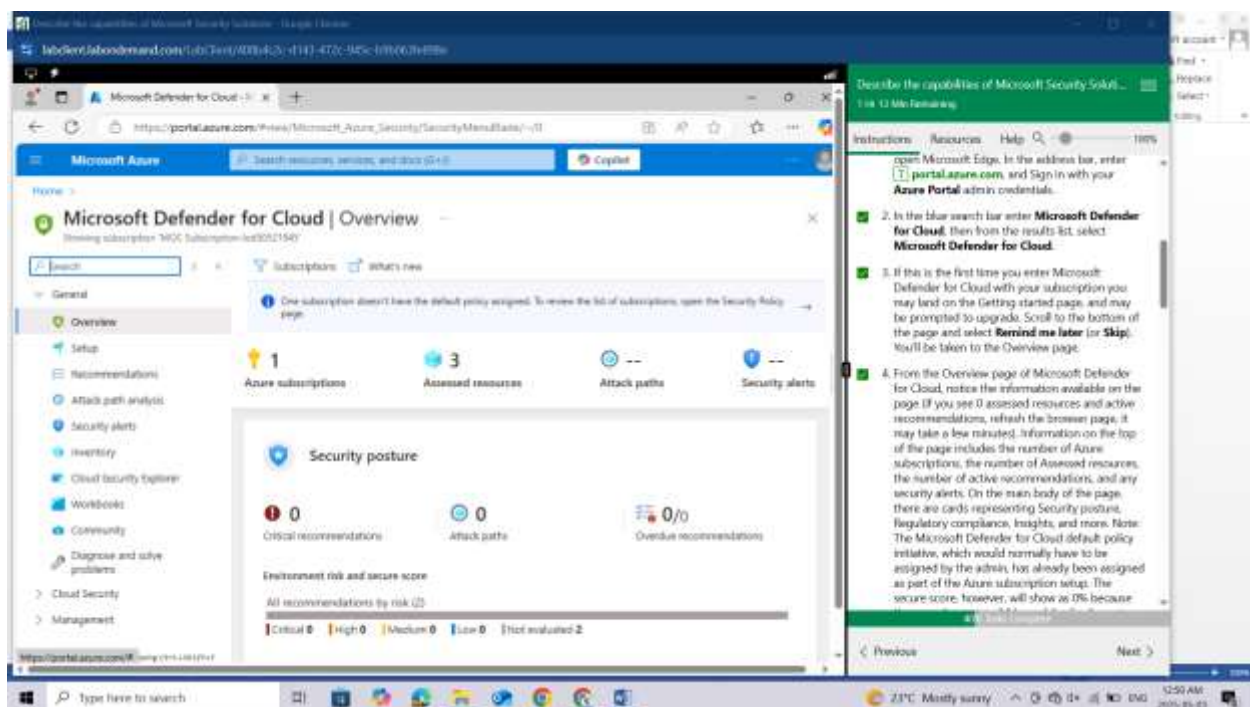


In the blue search bar enter **Microsoft Defender for Cloud**, then from the results list, select **Microsoft Defender for Cloud**.

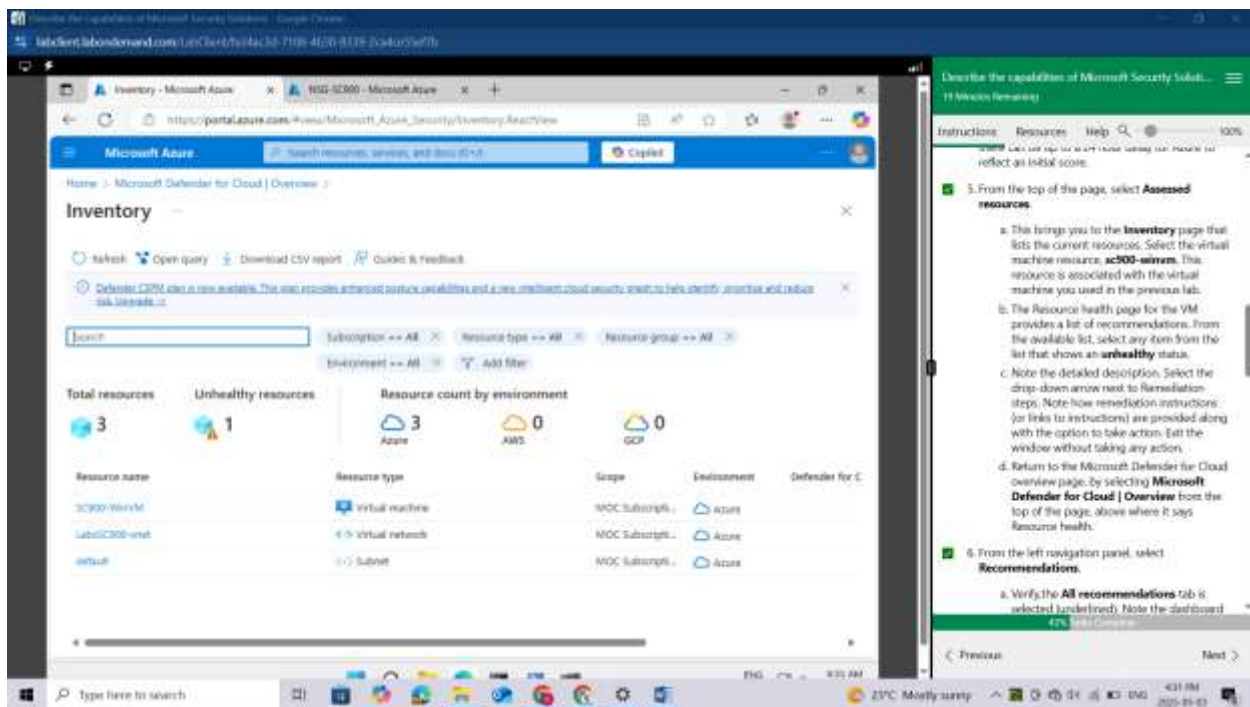


If this is the first time you enter Microsoft Defender for Cloud with your subscription you may land on the Getting started page, and may be prompted to upgrade. Scroll to the bottom of the page and select **Remind me later (or Skip)**. You'll be taken to the Overview page.

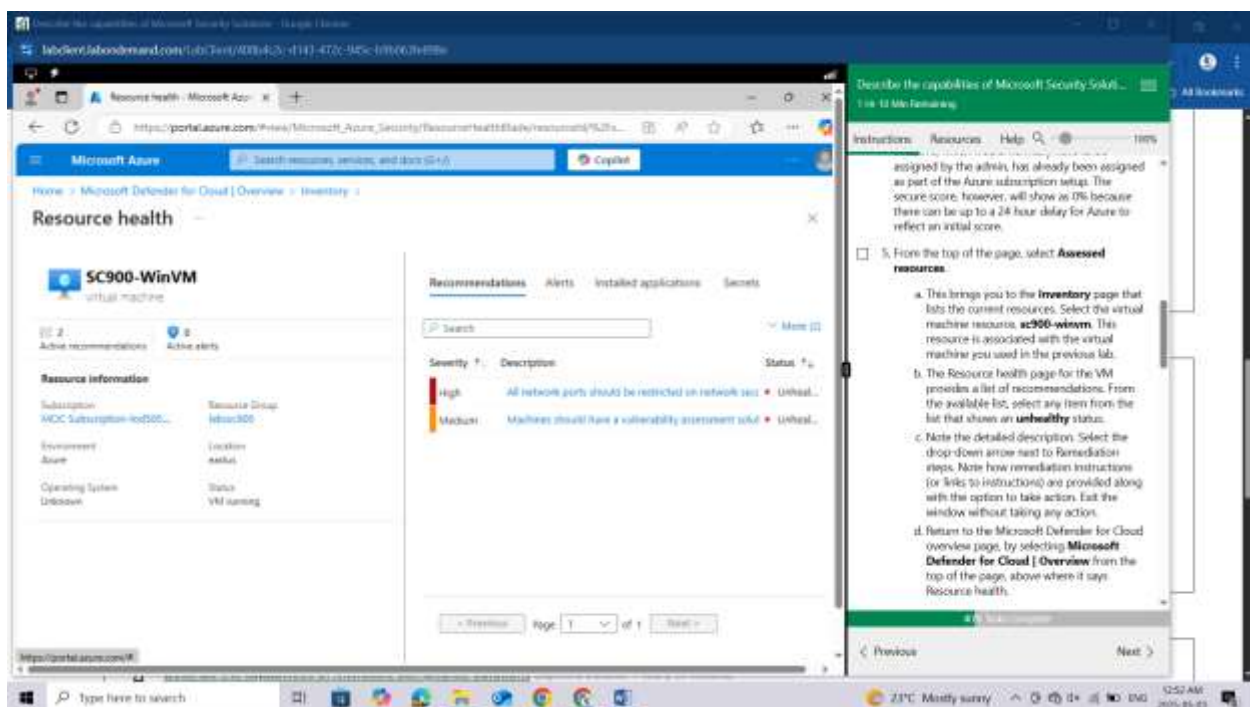
From the Overview page of Microsoft Defender for Cloud, notice the information available on the page (if you see 0 assessed resources and active recommendations, refresh the browser page, it may take a few minutes). Information on the top of the page includes the number of Azure subscriptions, the number of Assessed resources, the number of active recommendations, and any security alerts. On the main body of the page, there are cards representing Security posture, Regulatory compliance, Insights, and more. Note: The Microsoft Defender for Cloud default policy initiative, which would normally have to be assigned by the admin, has already been assigned as part of the Azure subscription setup. The secure score, however, will show as 0% because there can be up to a 24 hour delay for Azure to reflect an initial score.



From the top of the page, select **Assessed resources**.

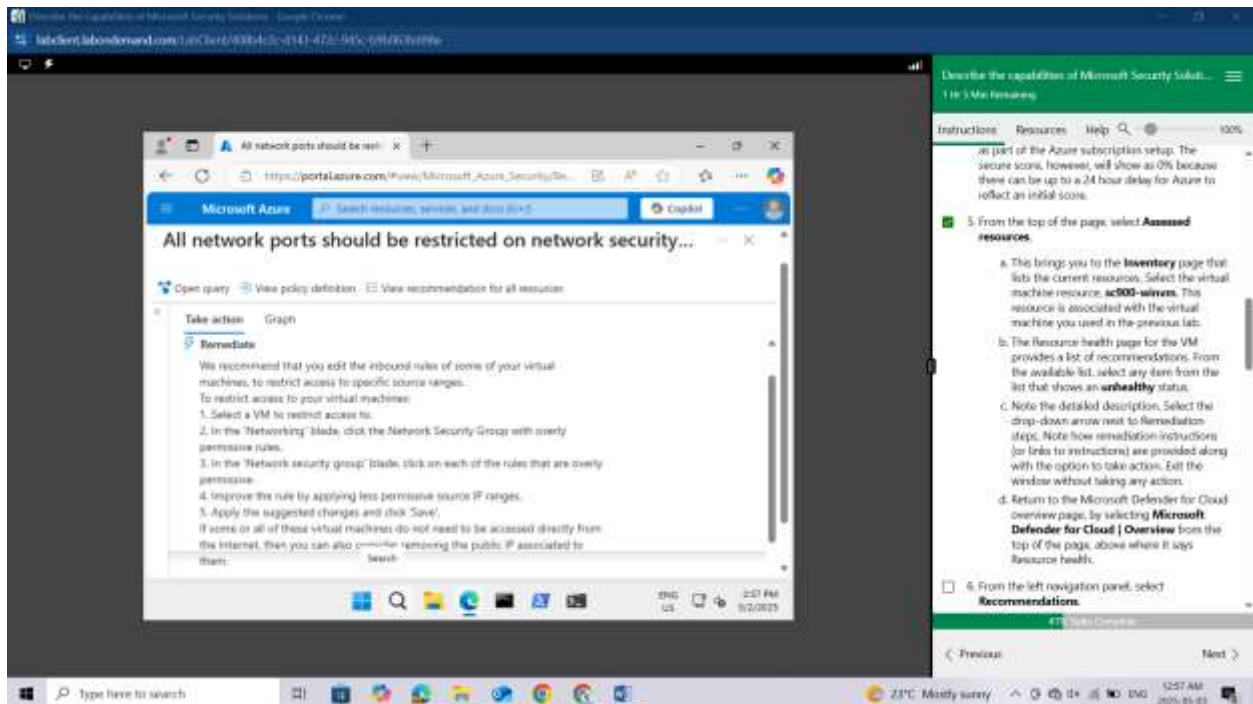


This brings you to the **Inventory** page that lists the current resources. Select the virtual machine resource, **sc900-winvm**. This resource is associated with the virtual machine you used in the previous lab.

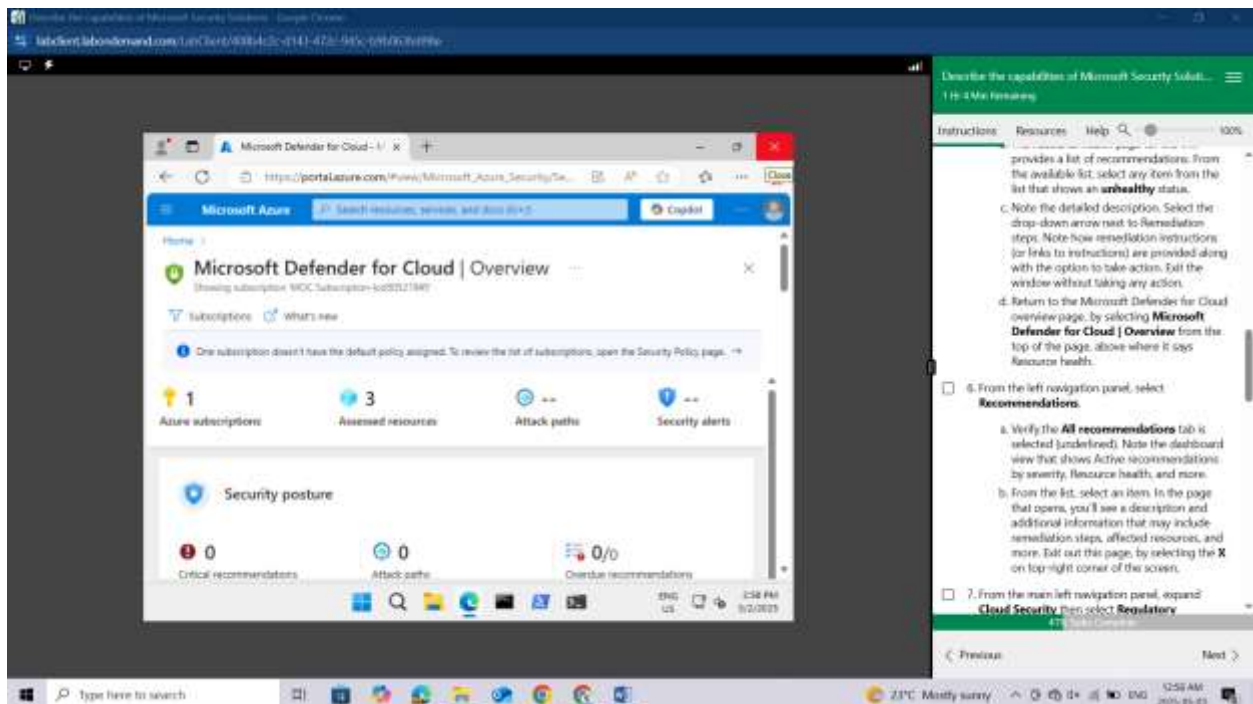


The Resource health page for the VM provides a list of recommendations. From the available list, select any item from the list that shows an **unhealthy** status.

Note the detailed description. Select the drop-down arrow next to Remediation steps. Note how remediation instructions (or links to instructions) are provided along with the option to take action. Exit the window without taking any action.



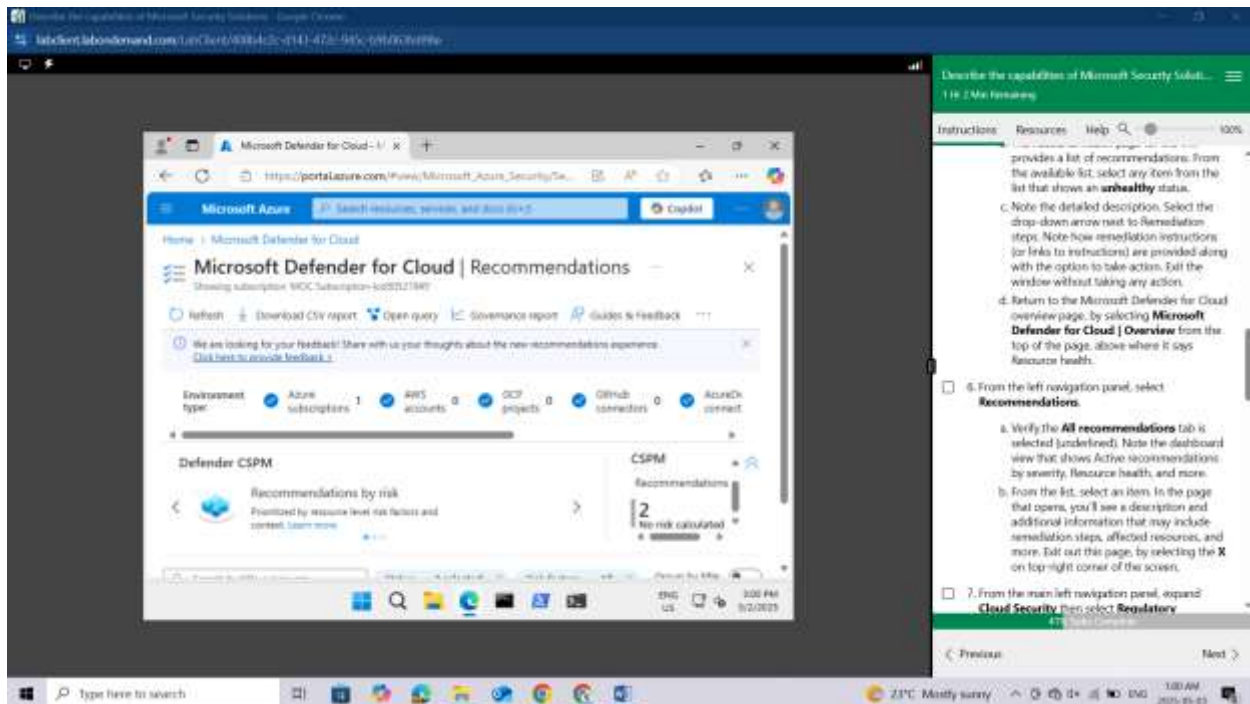
Return to the Microsoft Defender for Cloud overview page, by selecting **Microsoft Defender for Cloud | Overview** from the top of the page, above where it says Resource health.



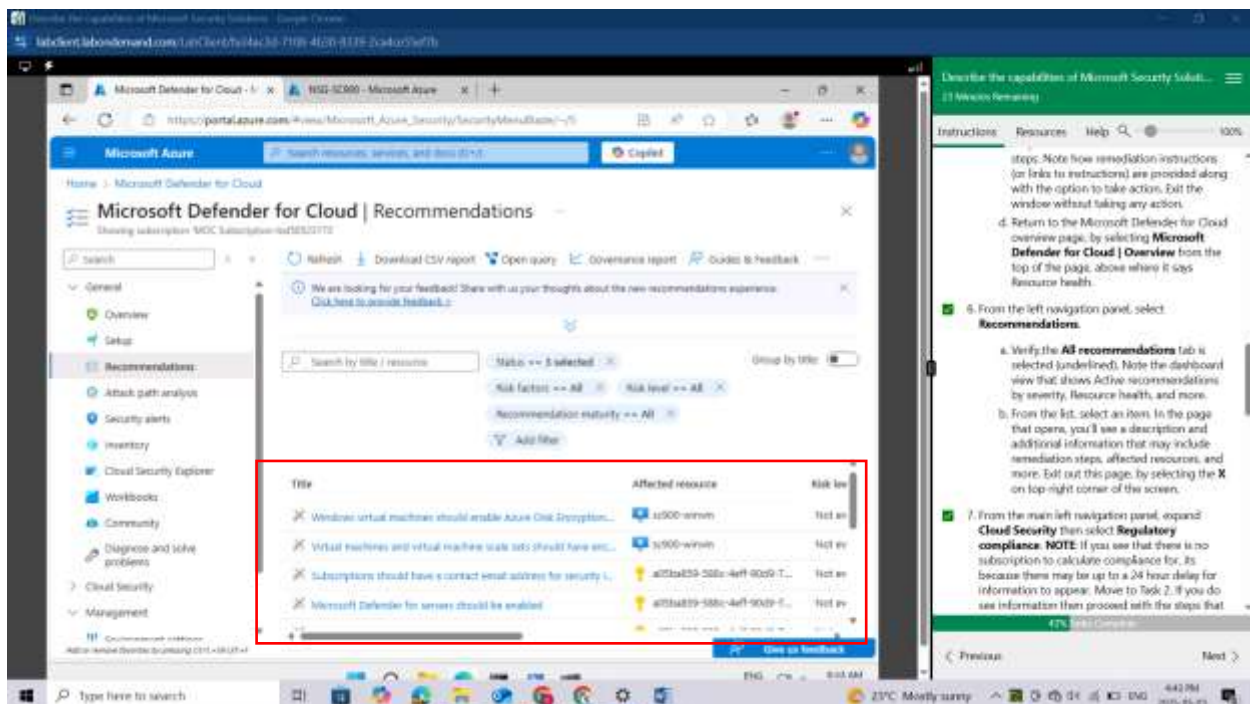


From the left navigation panel, select **Recommendations**.

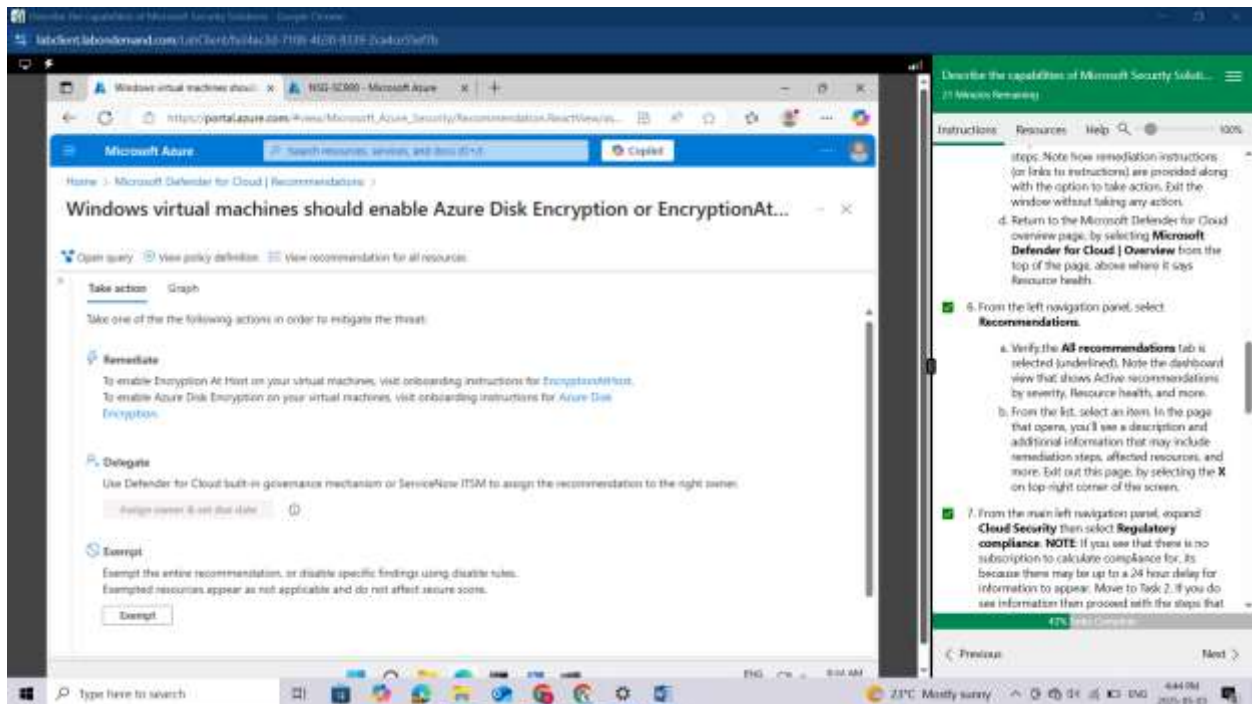
Verify, the **All recommendations** tab is selected (underlined). Note the dashboard view that shows Active recommendations by severity, Resource health, and more.



From the list, select an item.



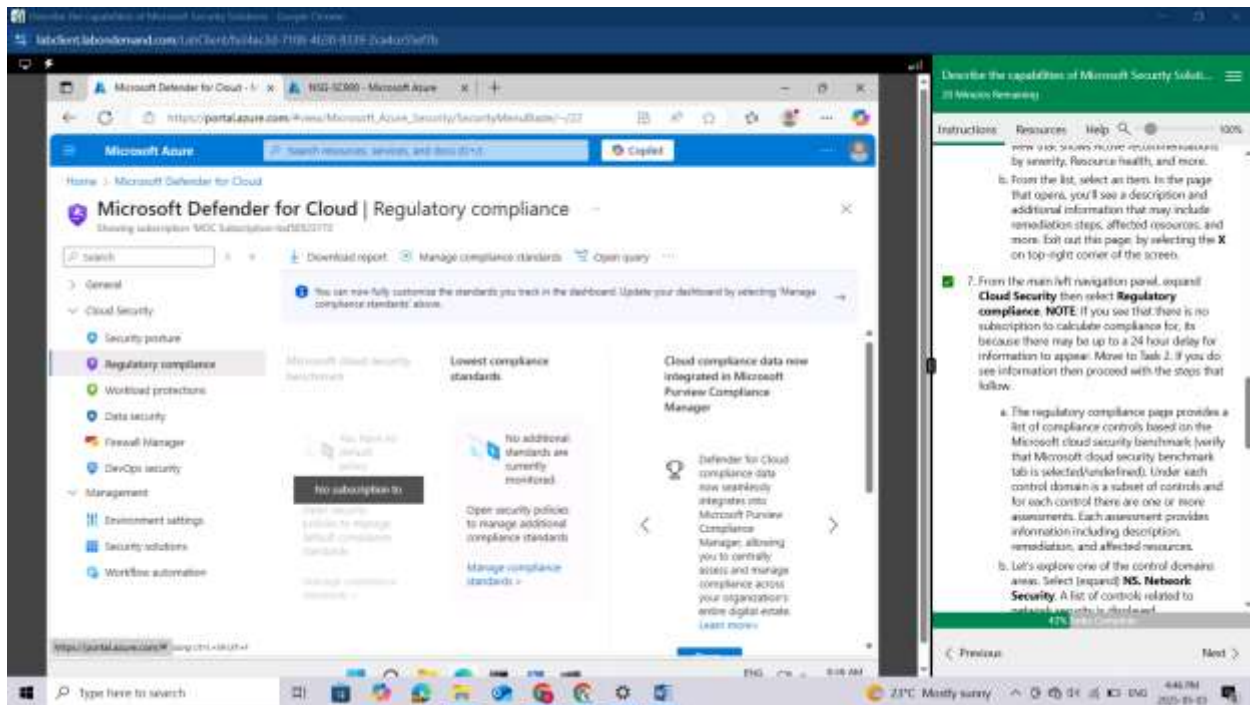
In the page that opens, you'll see a description and additional information that may include remediation steps, affected resources, and more. Exit out this page, by selecting the X on top-right corner of the screen.



From the main left navigation panel, expand **Cloud Security** then select **Regulatory compliance**.

NOTE: If you see that there is no subscription to calculate compliance for, its because there may be up to a 24 hour delay for information to appear. Move to Task 2. If you do see information then proceed with the steps that follow.





The regulatory compliance page provides a list of compliance controls based on the Microsoft cloud security benchmark (verify that Microsoft cloud security benchmark tab is selected/underlined). Under each control domain is a subset of controls and for each control there are one or more assessments. Each assessment provides information including description, remediation, and affected resources.

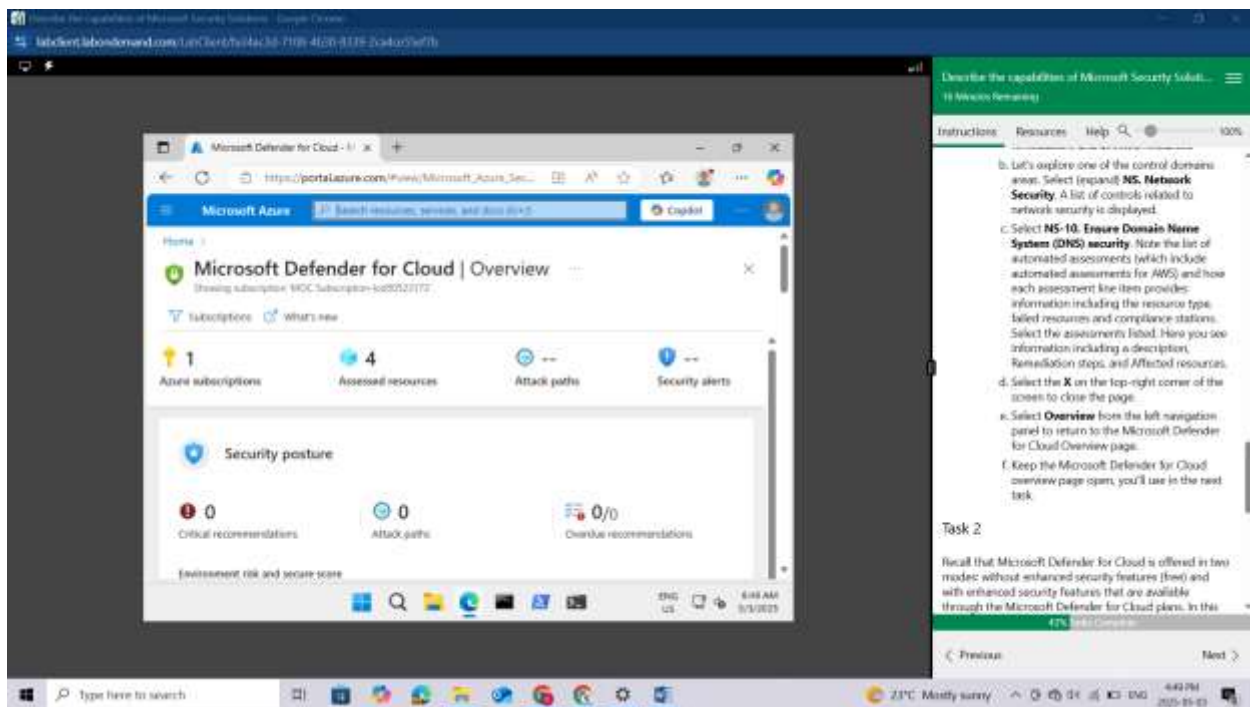
Let's explore one of the control domains areas. Select (expand) **NS. Network Security**. A list of controls related to network security is displayed.

Select **NS-10. Ensure Domain Name System (DNS) security**. Note the list of automated assessments (which include automated assessments for AWS) and how each assessment line item provides information including the resource type, failed resources and compliance stations. Select the assessments listed. Here you see information including a description, Remediation steps, and Affected resources.

Select the **X** on the top-right corner of the screen to close the page.

Select **Overview** from the left navigation panel to return to the Microsoft Defender for Cloud Overview page.

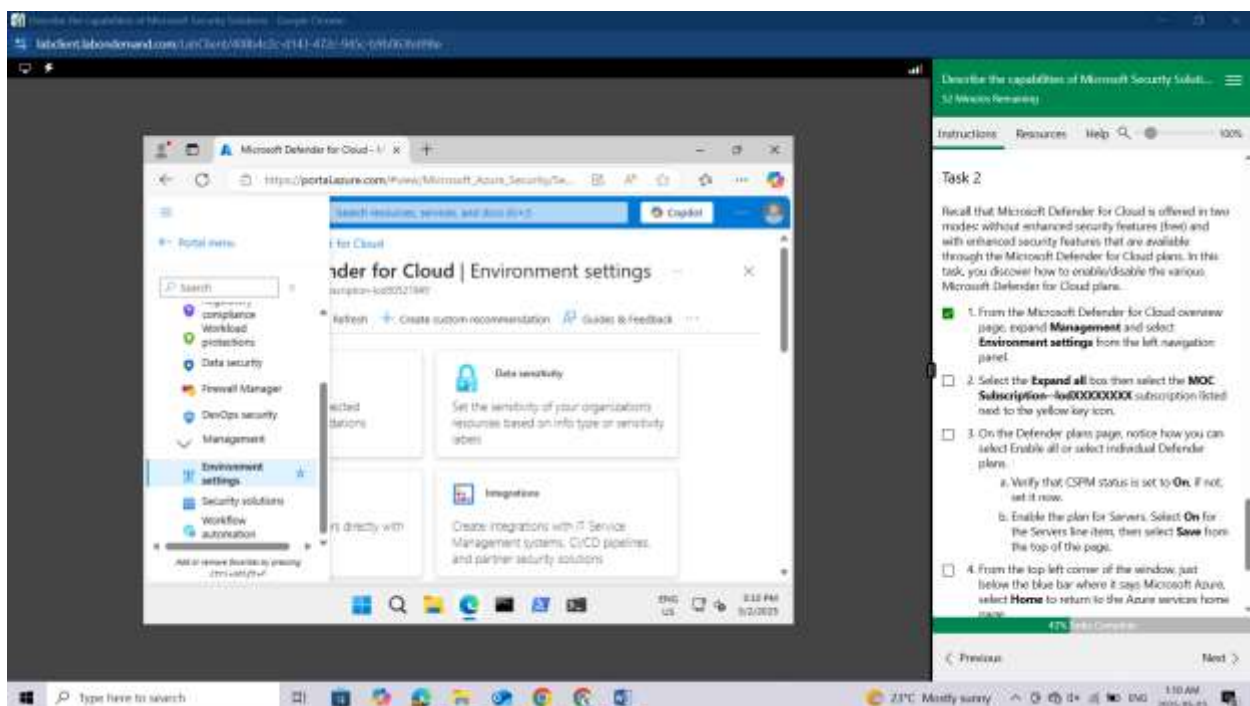
Keep the Microsoft Defender for Cloud overview page open, you'll use in the next task.



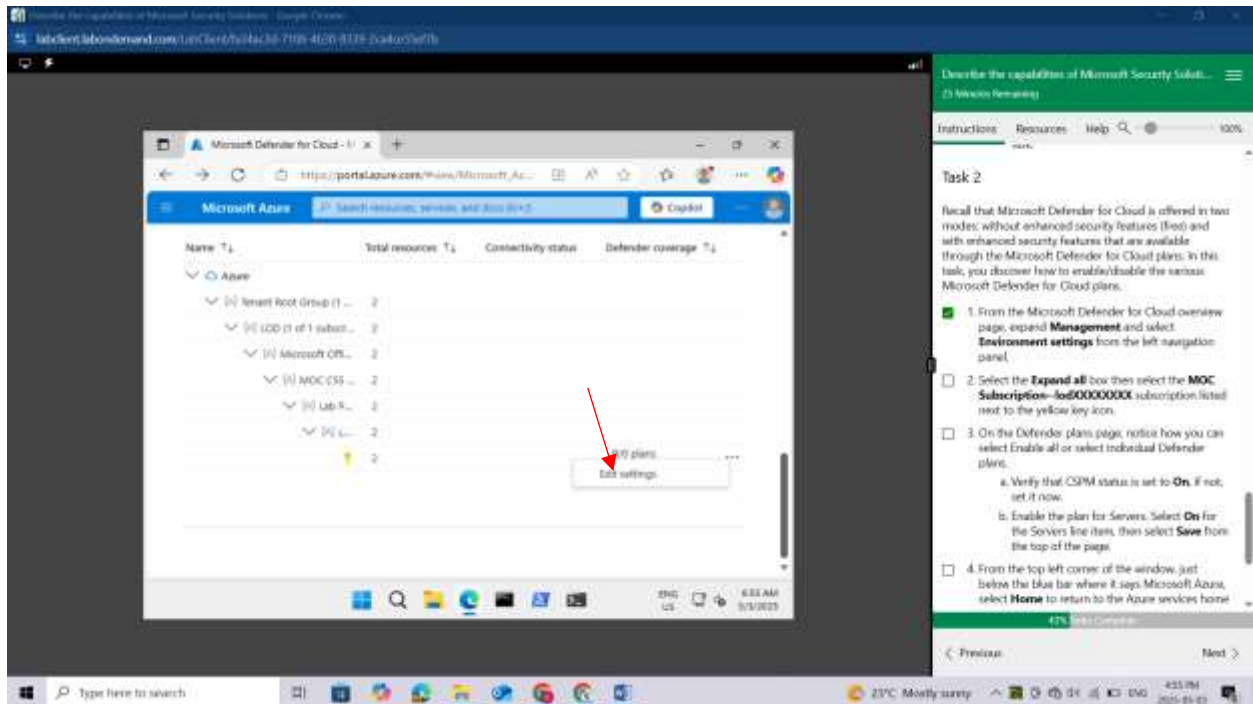
## Task 2

Recall that Microsoft Defender for Cloud is offered in two modes: without enhanced security features (free) and with enhanced security features that are available through the Microsoft Defender for Cloud plans. In this task, you discover how to enable/disable the various Microsoft Defender for Cloud plans.

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

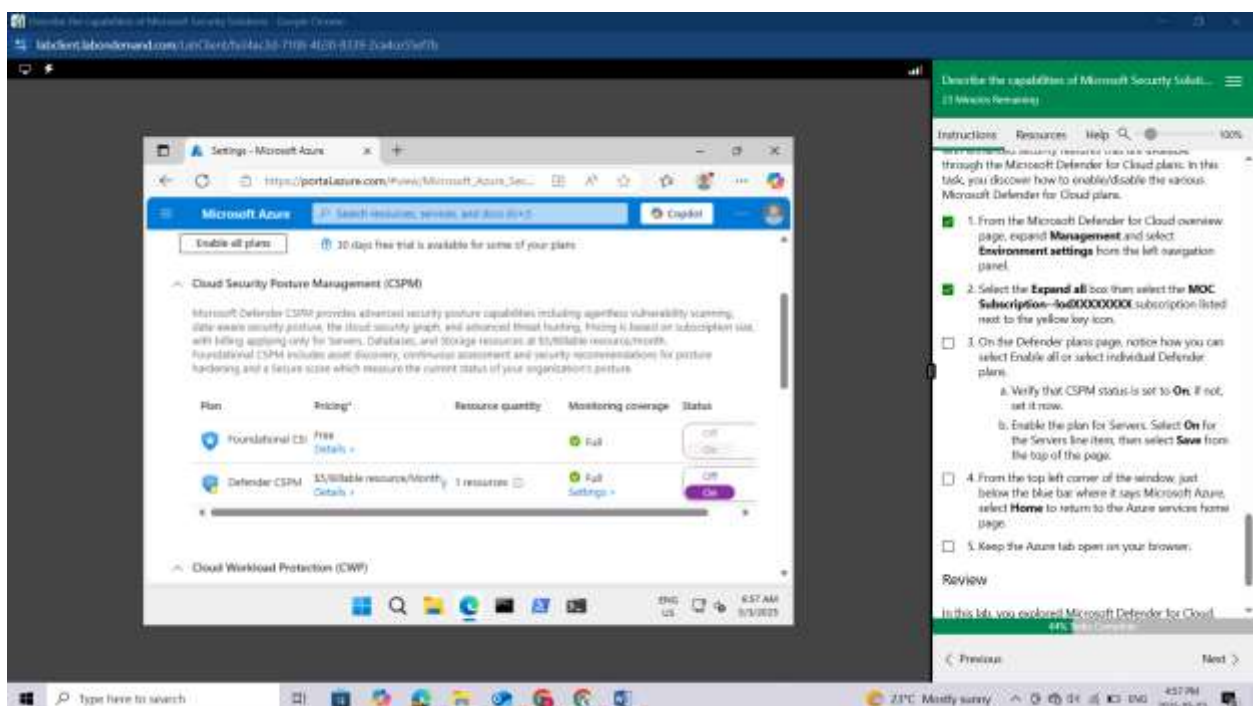


Select the **Expand all** box then select the **MOC Subscription--lodXXXXXXXX** subscription listed next to the yellow key icon.



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

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



The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and a 'Cloud' button. Below that, the 'Cloud Workload Protection (CWP)' section is active. It displays a table of services and their protection status. A red arrow points to the 'On' button for the 'Servers' plan.

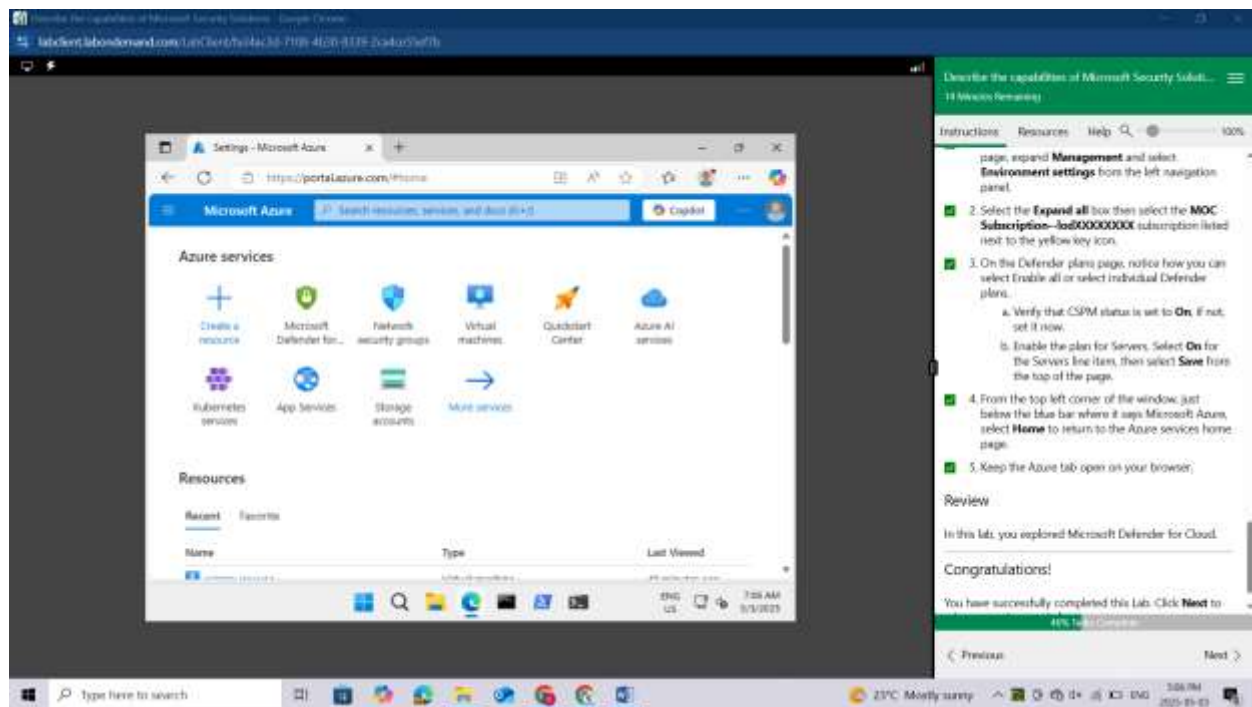
Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (\$15/Server/Month) <a href="#">Change plan &gt;</a>	1 servers	Full <a href="#">Settings &gt;</a>	Off <a href="#">On</a>
App Service	\$15/Instance/Month <a href="#">Details &gt;</a>	0 instances	Full	Off <a href="#">On</a>
Databases	Selected \$94 <a href="#">Select types &gt;</a>	0 instances	Full <a href="#">Settings &gt;</a>	Off <a href="#">On</a>
Storage	\$10/Storage account/month \$0.15/GB scanned for On-Disk <a href="#">Details &gt;</a>	0 storage accounts	Full <a href="#">Settings &gt;</a>	Off <a href="#">On</a>
Containers	\$0.888/VM core/Month <a href="#">Details &gt;</a>	0 container registered	Full <a href="#">Settings &gt;</a>	Off <a href="#">On</a>
AI Services	\$0.002/1K tokens/month <a href="#">Details &gt;</a>	0 AI resources	Full <a href="#">Settings &gt;</a>	Off <a href="#">On</a>

The bottom of the screen shows the Windows taskbar with various application icons and the system clock indicating 7:00 AM on 9/19/2023.

The screenshot shows the 'Settings | Defender plans' page in the Azure portal. A red arrow points to the 'Save' button located at the top left of the settings card. The page displays a notification about predictable pricing for Key Vault and Defender for Resource Manager. Below this, there is an 'Enable all plans' button and a note about a 30-day free trial. The 'Cloud Security Posture Management (CSPM)' and 'Cloud Workload Protection (CWP)' plans are listed. The CWP plan description states: 'Microsoft Defender for Cloud provides comprehensive, cloud-native protection from development to runtime in multi-cloud environments.' At the bottom, there is a table with columns: Plan, Pricing\*, Resource quantity, Monitoring coverage, and Status.

Keep the Azure tab open on your browser.





## Review

In this lab, you explored Microsoft Defender for Cloud.

## LAB: EXPLORE MICROSOFT SENTINEL

This lab maps to the following Learn content:

Learning Path: Describe the capabilities of Microsoft security solutions

Module: Describe the security capabilities of Microsoft Sentinel

Unit: Describe threat detection and mitigation capabilities in Microsoft Sentinel

## Lab scenario

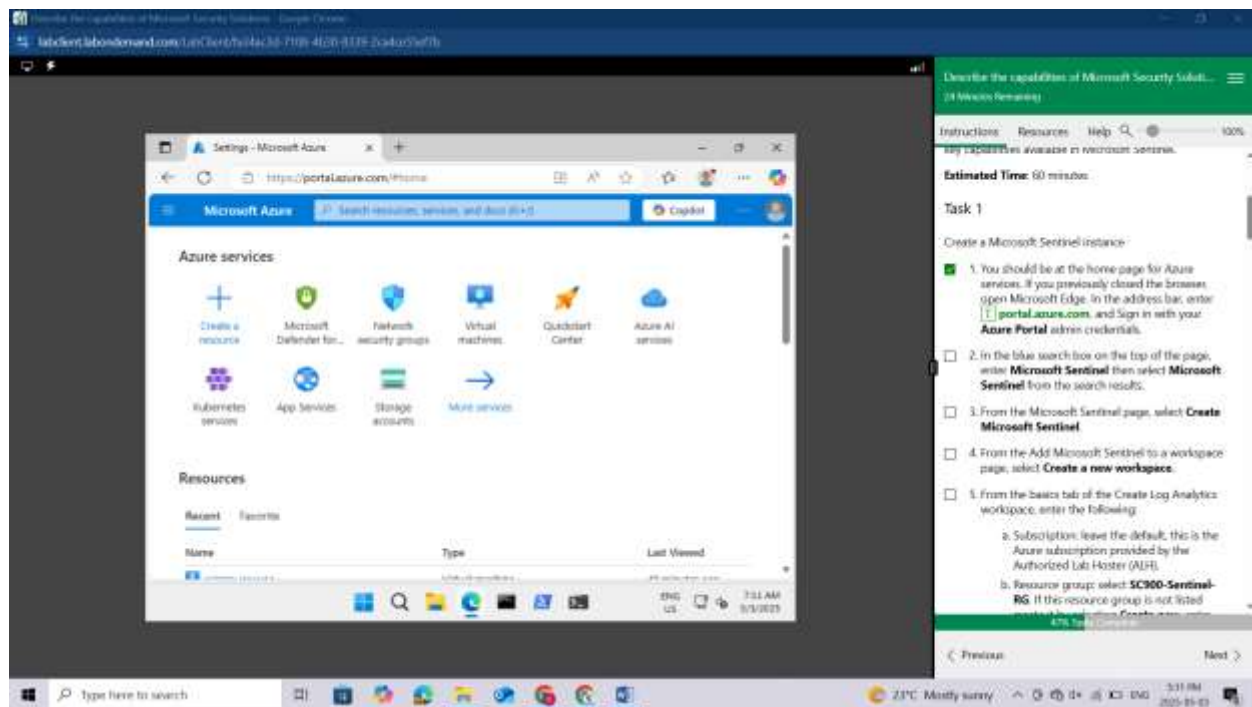
In this lab, you'll walk through the process of creating a Microsoft Sentinel instance. You'll also set up the permissions to ensure access to the resources that will get deployed to support Microsoft Sentinel. Once this basic setup is done you'll walk through the steps for connecting Microsoft Sentinel to your data sources, set up a workbook, and do a brief walk-through of some of key capabilities available in Microsoft Sentinel.

## Task 1

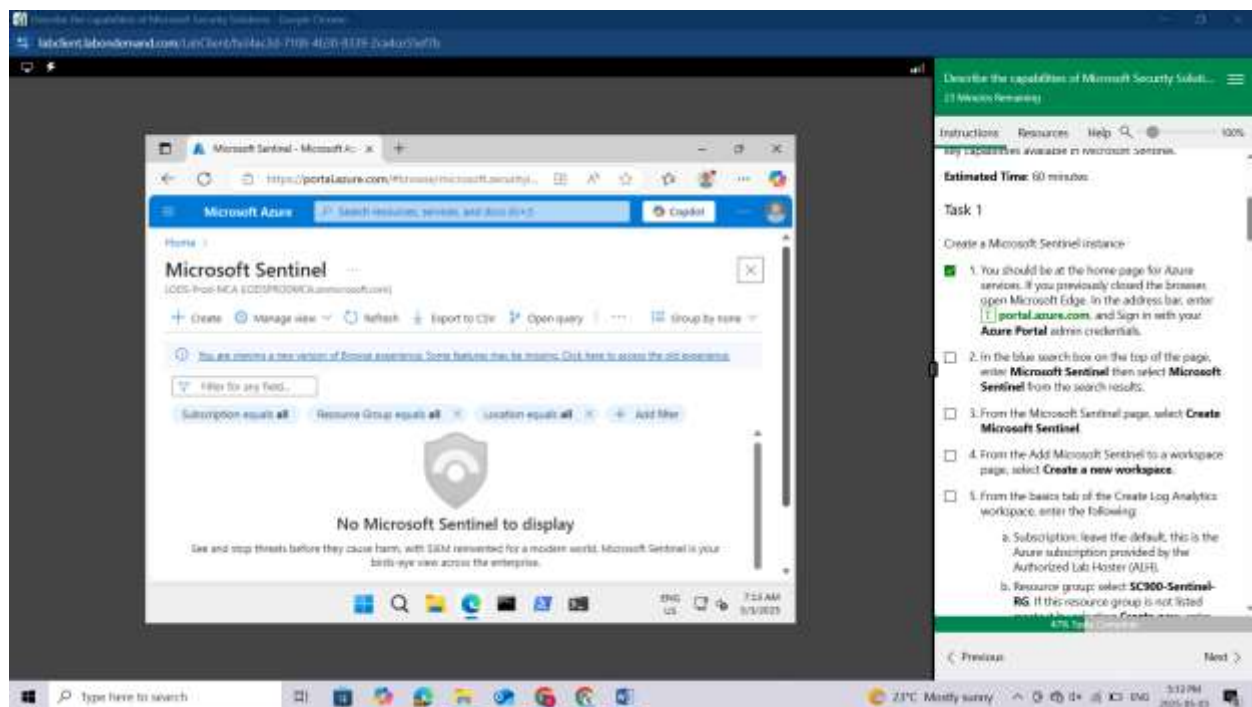
Create a Microsoft Sentinel instance

You should be at the home page for Azure services. If you previously closed the browser, open Microsoft Edge. In the address bar, enter portal.azure.com, and Sign in with your Azure Portal admin credentials.

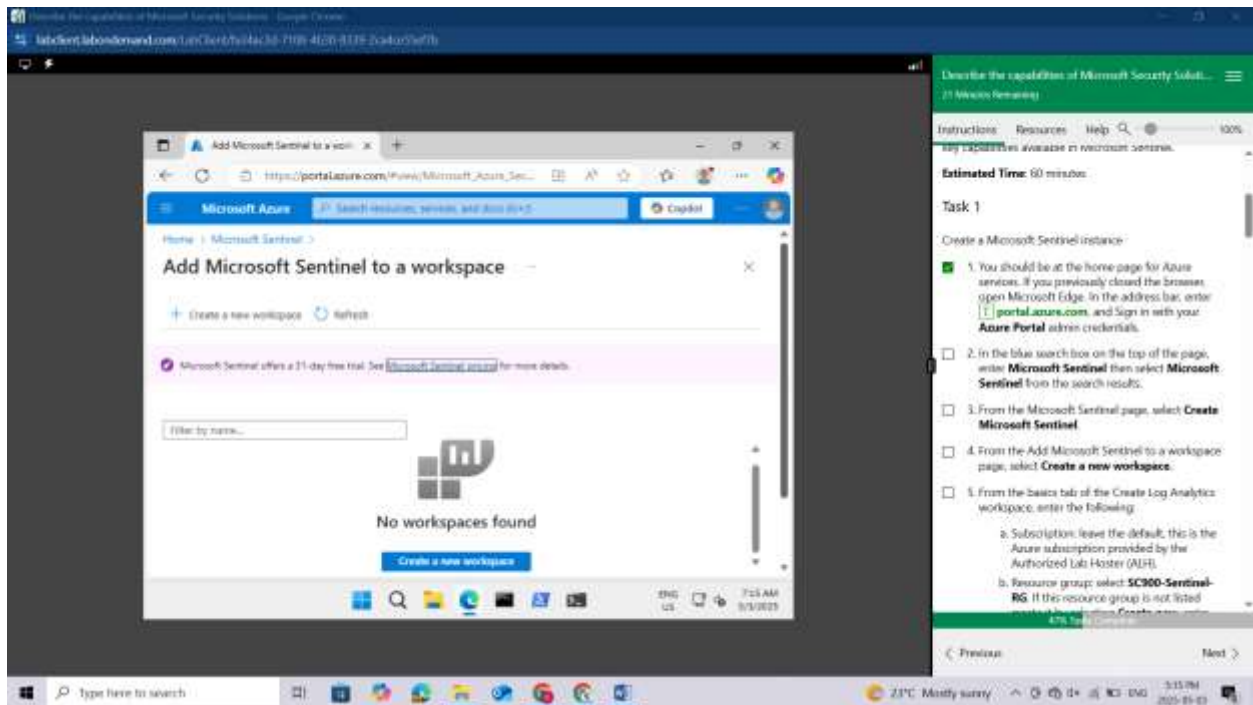




In the blue search box on the top of the page, enter **Microsoft Sentinel** then select **Microsoft Sentinel** from the search results.



From the Microsoft Sentinel page, select **Create Microsoft Sentinel**.

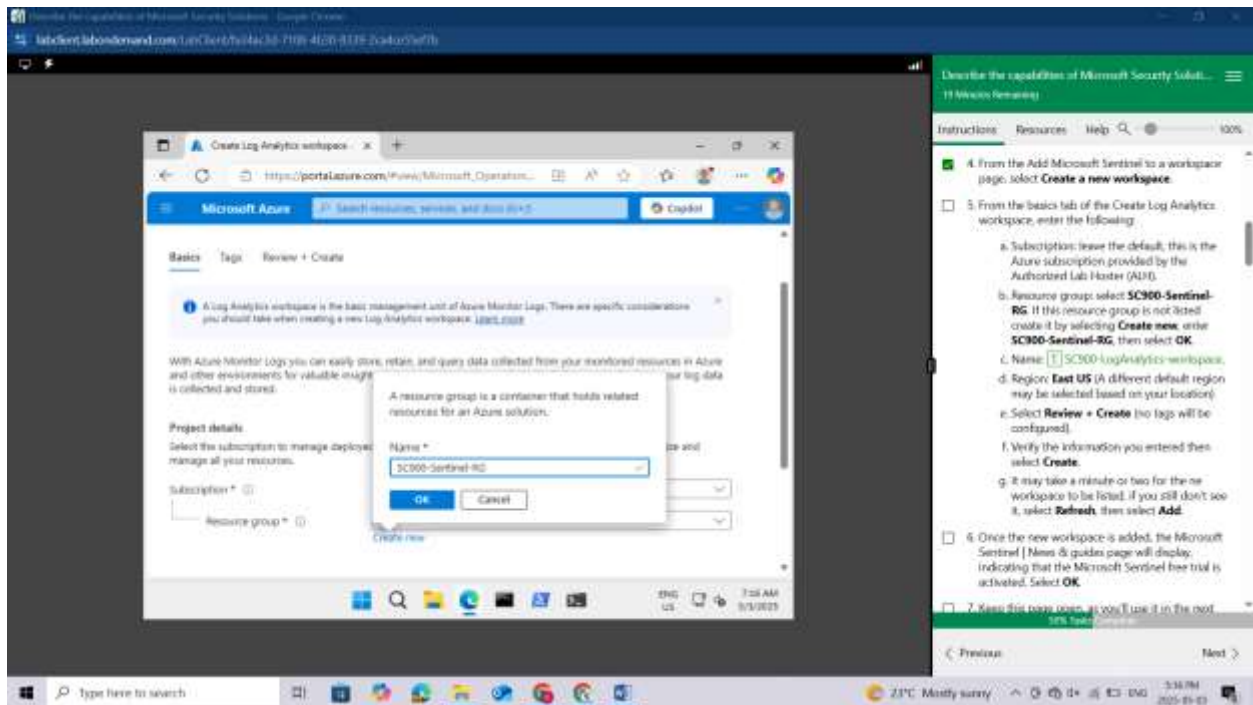


From the Add Microsoft Sentinel to a workspace page, select **Create a new workspace**.

From the basics tab of the Create Log Analytics workspace, enter the following:

Subscription: leave the default, this is the Azure subscription provided by the Authorized Lab Hosters (ALH).

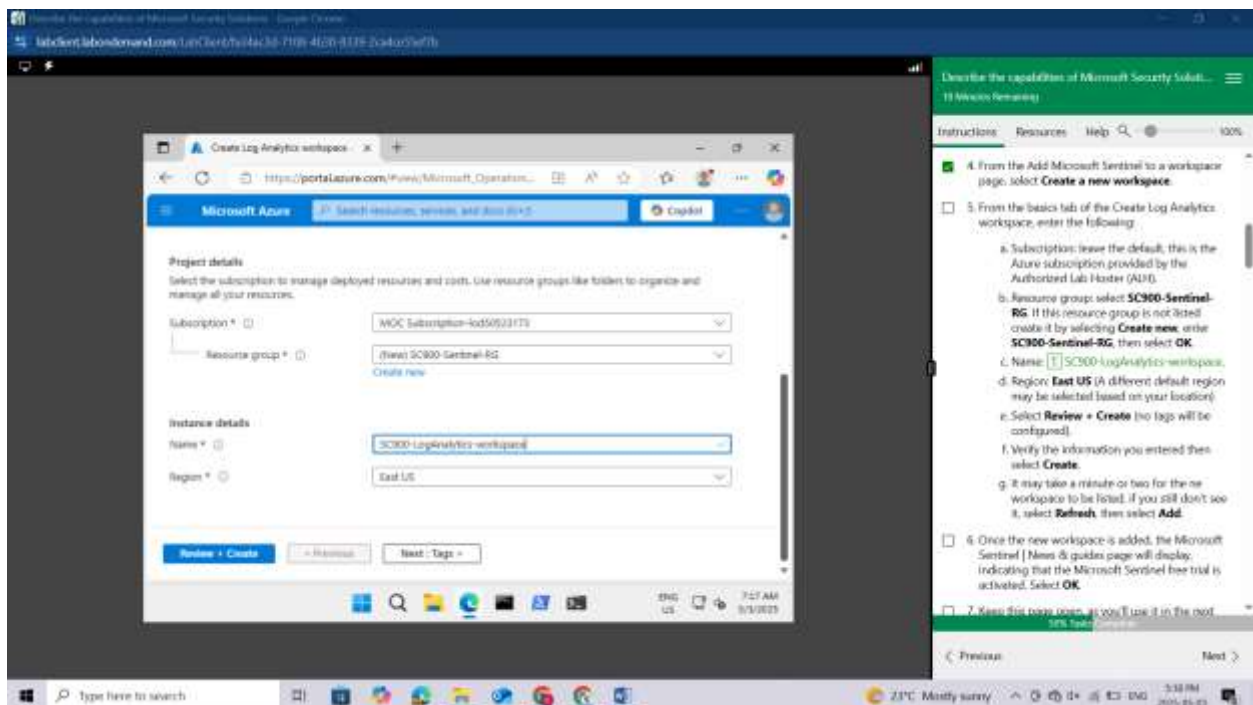
Resource group: select **SC900-Sentinel-RG**. If this resource group is not listed create it by selecting **Create new**, enter **SC900-Sentinel-RG**, then select **OK**.



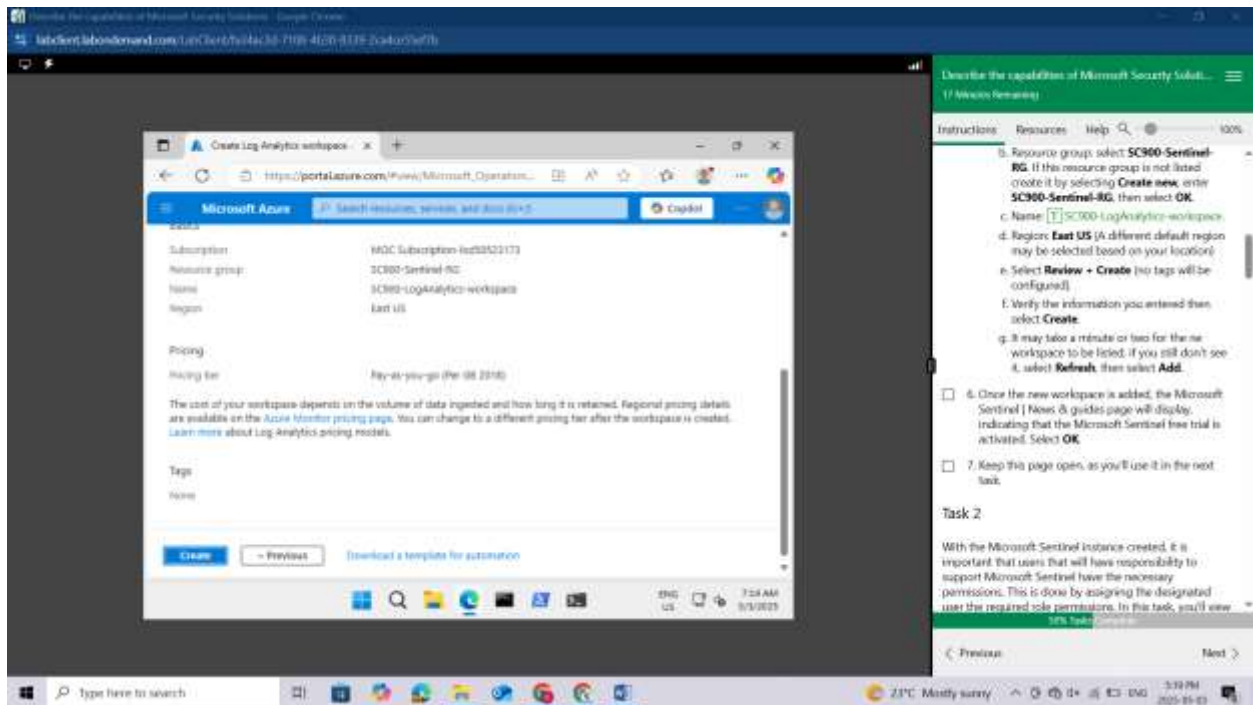
Name: SC900-LogAnalytics-workspace.

Region: East US (A different default region may be selected based on your location)

Select **Review + Create** (no tags will be configured).

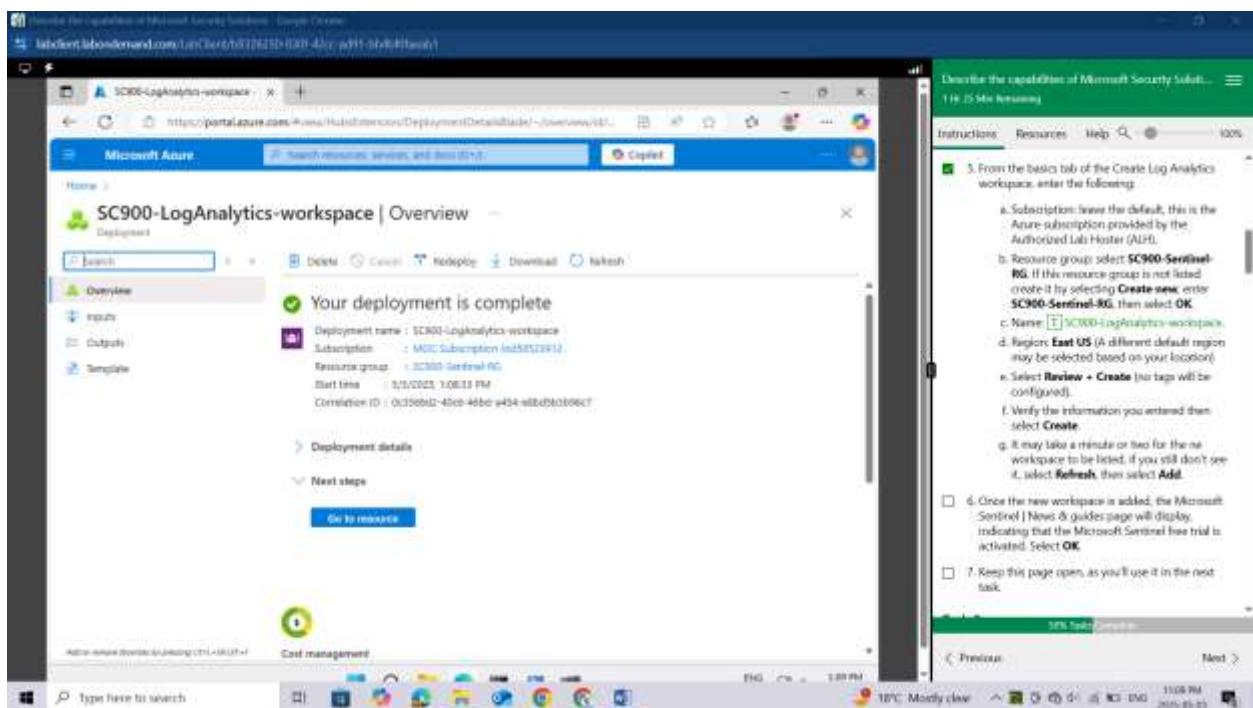


Verify the information you entered then select **Create**.



It may take a minute or two for the new workspace to be listed, if you still don't see it, select **Refresh**, then select **Add**.

Once the new workspace is added, the Microsoft Sentinel | News & guides page will display, indicating that the Microsoft Sentinel free trial is activated. Select **OK**.



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

## Task 2

With the Microsoft Sentinel instance created, it is important that users that will have responsibility to support Microsoft Sentinel have the necessary permissions. This is done by assigning the designated user the required role permissions. In this task, you'll view the available, built-in Microsoft Sentinel roles.

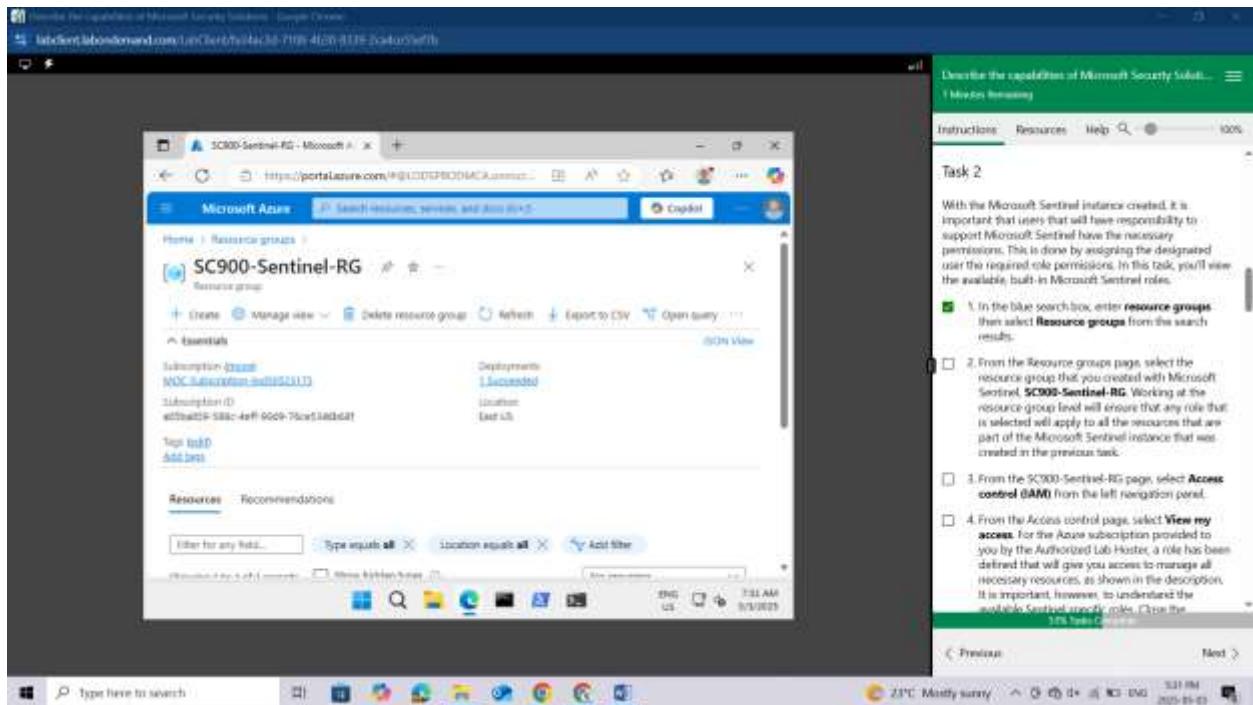
In the blue search box, enter **resource groups** then select **Resource groups** from the search results.

The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'Resource groups' page for the subscription 'LabSC900'. The page includes a search bar, a filter bar, and a table of resource groups. The table has columns for 'Name', 'Subscription', and 'Location'. The resource groups listed are 'LabSC900', 'NetworkWatcherRG', and 'SC900-Sentinel-RG'. The 'SC900-Sentinel-RG' resource group is highlighted. To the right, a sidebar shows 'Task 2' instructions, which include steps for selecting the resource group and viewing access control.

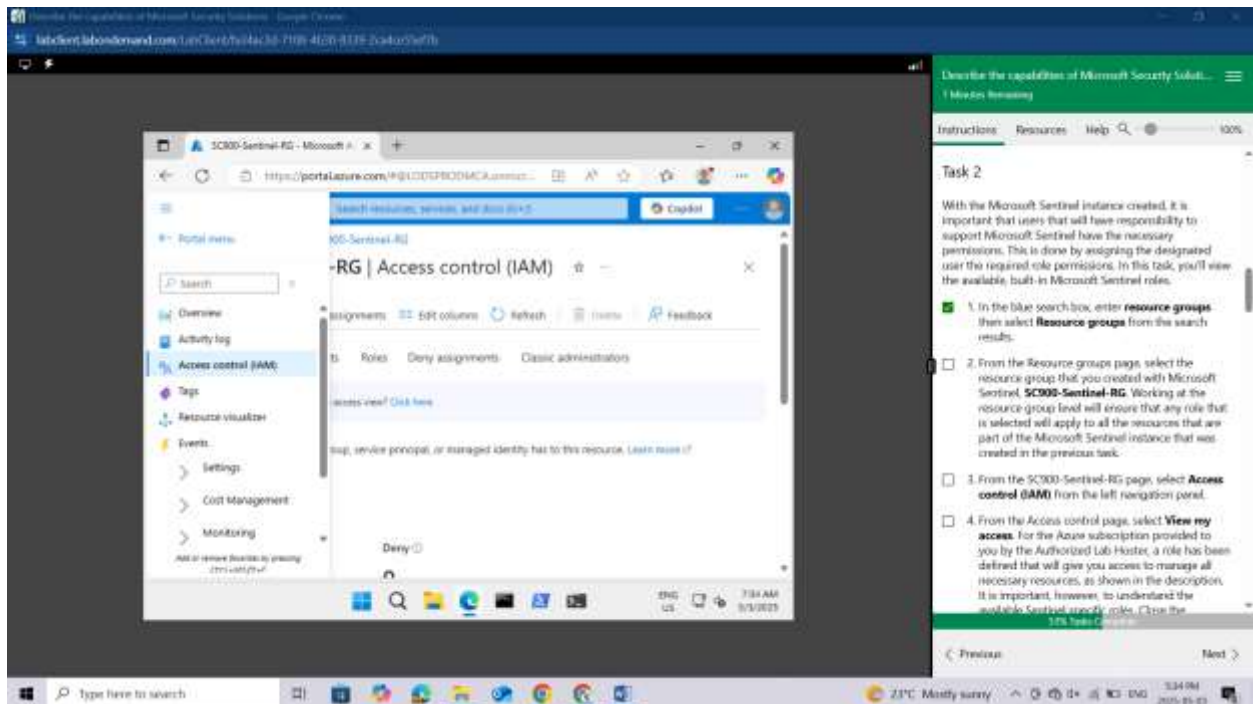
Name	Subscription	Location
LabSC900	MDSC Subscription test...	East US
NetworkWatcherRG	MDSC Subscription test...	East US
SC900-Sentinel-RG	MDSC Subscription test...	East US

From the Resource groups page, select the resource group that you created with Microsoft Sentinel, **SC900-Sentinel-RG**. Working at the resource group level will ensure that any role that is selected will apply to all the resources that are part of the Microsoft Sentinel instance that was created in the previous task.

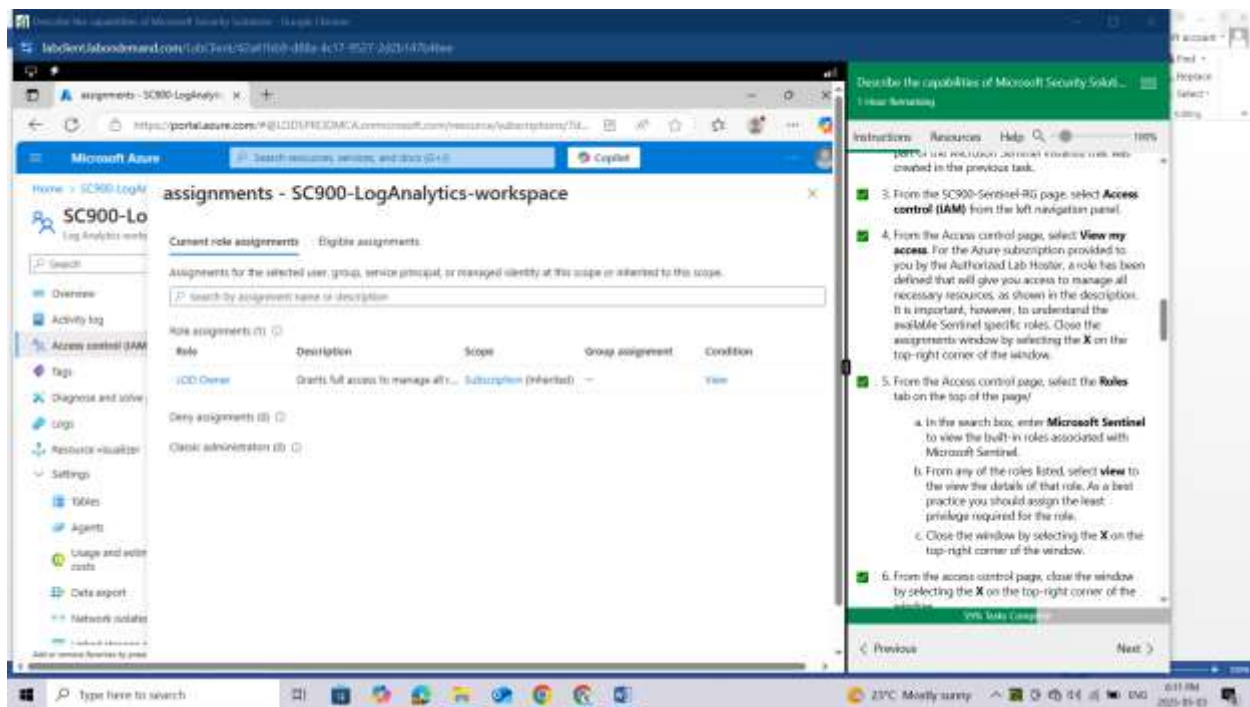




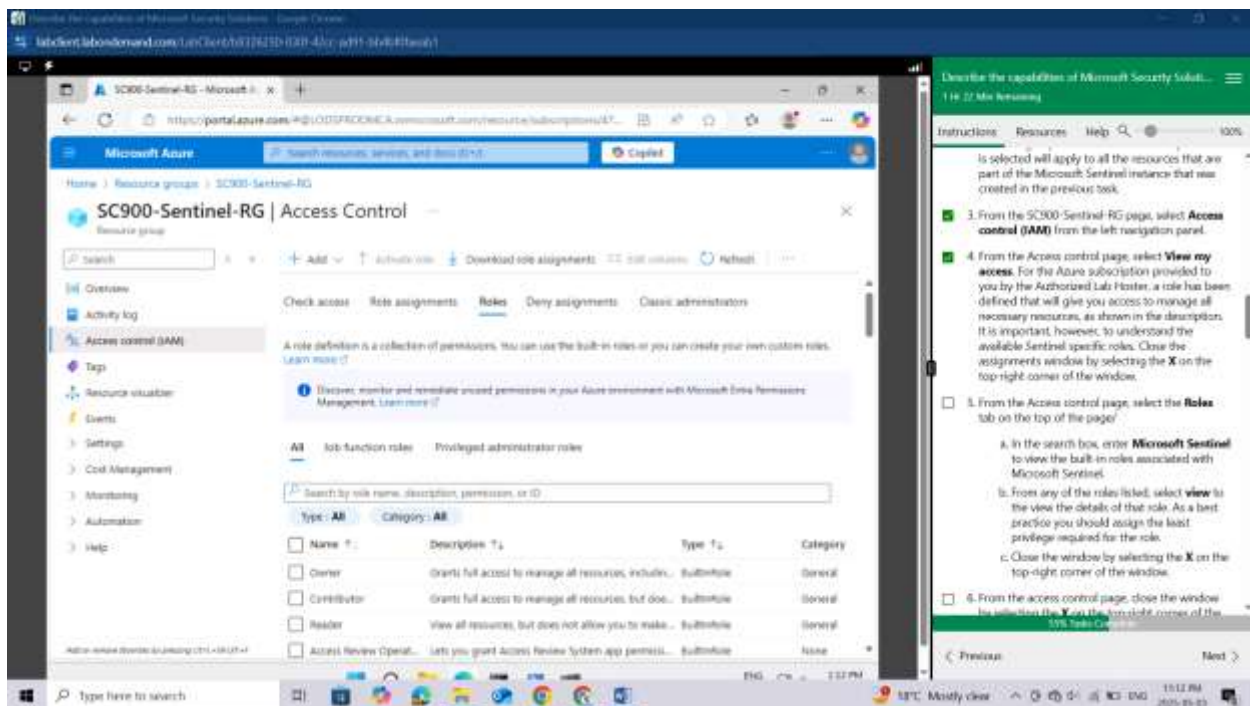
From the **SC900-Sentinel-RG** page, select **Access control (IAM)** from the left navigation panel.



From the Access control page, select **View my access**. For the Azure subscription provided to you by the Authorized Lab Host, a role has been defined that will give you access to manage all necessary resources, as shown in the description. It is important, however, to understand the available Sentinel specific roles. Close the assignments window by selecting the X on the top-right corner of the window.



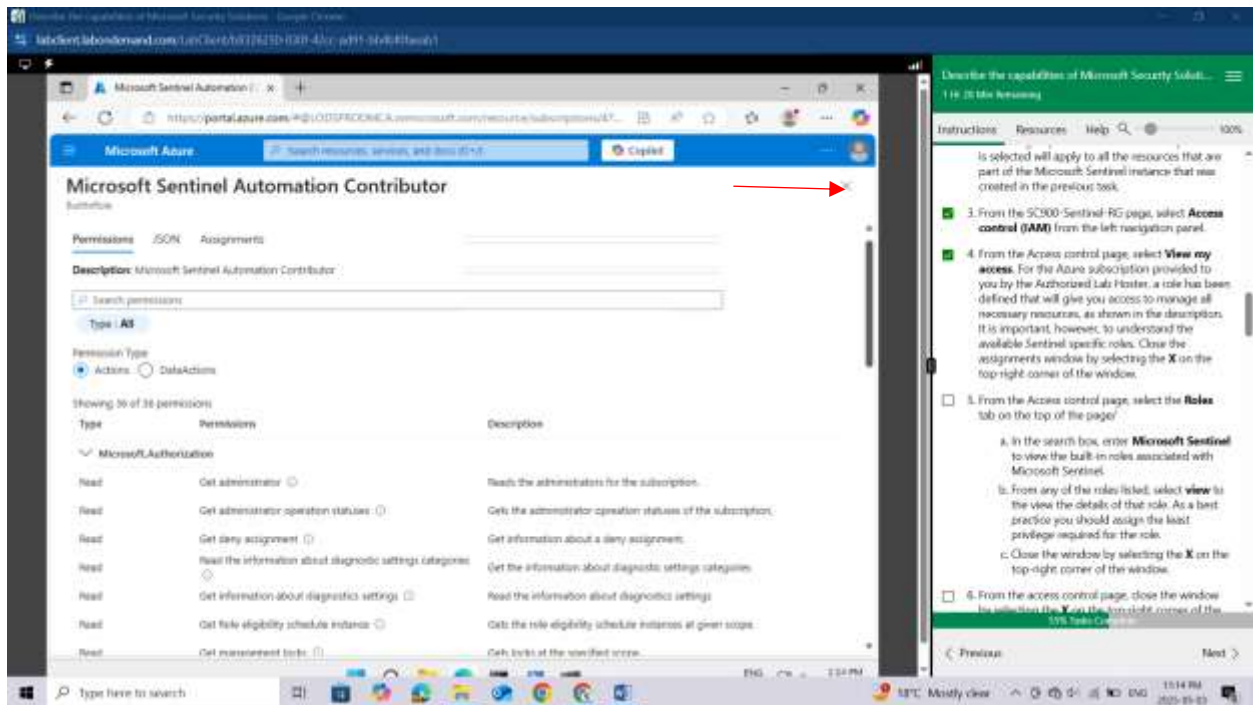
From the Access control page, select the **Roles** tab on the top of the page



In the search box, enter **Microsoft Sentinel** to view the built-in roles associated with Microsoft Sentinel.



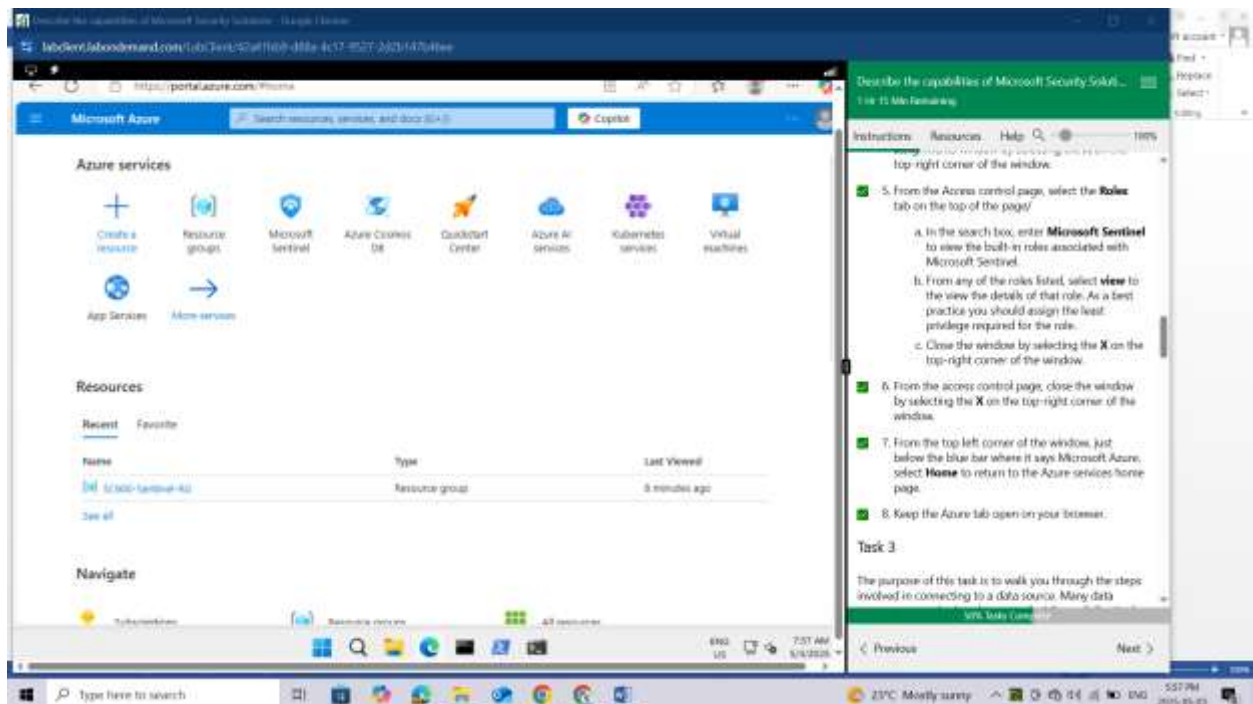




From the access control page, close the window by selecting the **X** on the top-right corner of the window.

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.

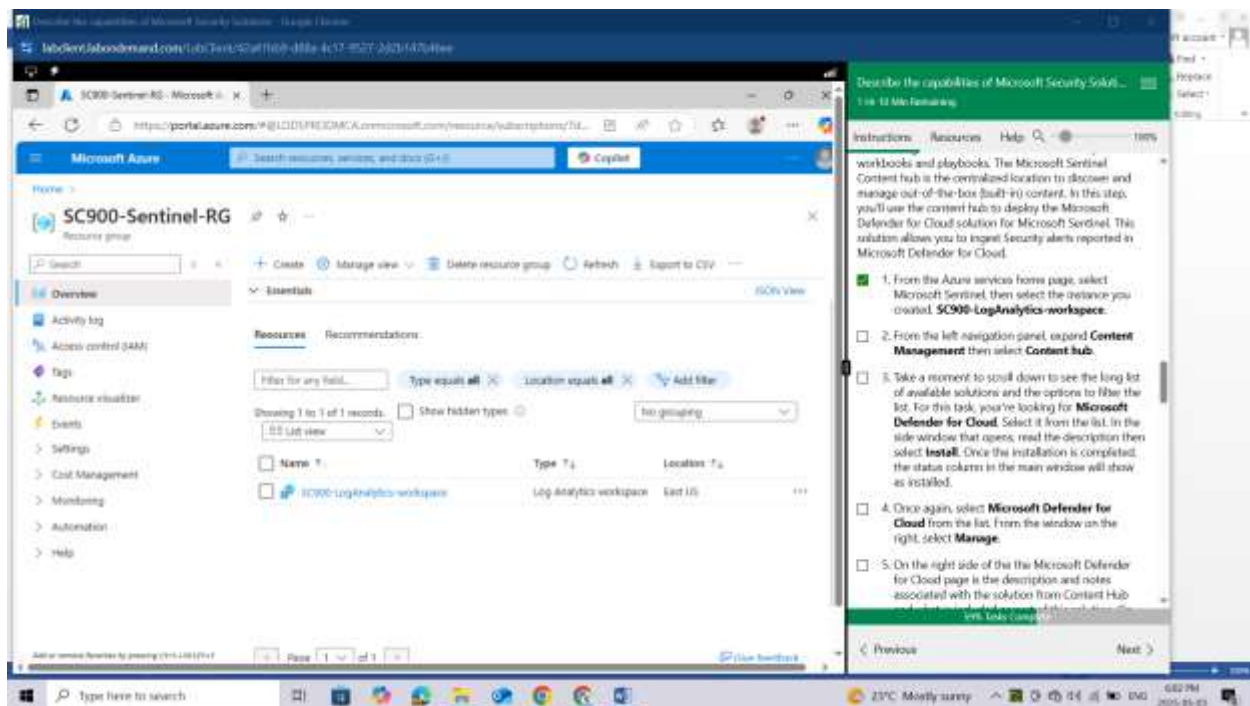
Keep the Azure tab open on your browser.



### Task 3

The purpose of this task is to walk you through the steps involved in connecting to a data source. Many data connectors are deployed as part of a Microsoft Sentinel solution together with related content like analytics rules, workbooks and playbooks. The Microsoft Sentinel Content hub is the centralized location to discover and manage out-of-the-box (built-in) content. In this step, you'll use the content hub to deploy the Microsoft Defender for Cloud solution for Microsoft Sentinel. This solution allows you to ingest Security alerts reported in Microsoft Defender for Cloud.

From the Azure services home page, select **Microsoft Sentinel**, then select the instance you created, **SC900-LogAnalytics-workspace**.



The screenshot displays the Microsoft Sentinel Content Hub interface within the Azure portal. The main window shows the 'SC900-Sentinel-RG' resource group. A table lists available solutions, including 'SC900-LogAnalytics-workspace'. The table has columns for Name, Type, and Location. The 'SC900-LogAnalytics-workspace' solution is listed with Type 'Log Analytics workspace' and Location 'East US'. On the right, a sidebar titled 'Describe the capabilities of Microsoft Security Solutions' provides instructions for installing the solution. The instructions include steps for selecting the solution, filtering the list, and installing the solution.

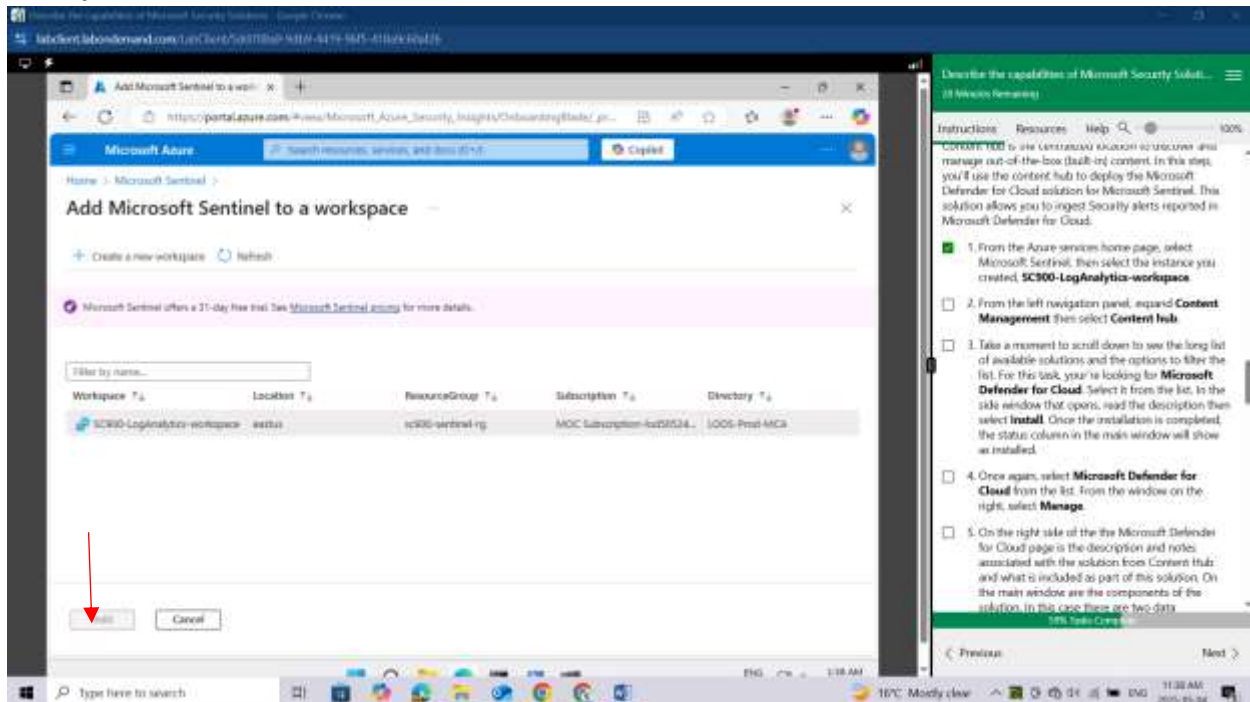
Name	Type	Location
SC900-LogAnalytics-workspace	Log Analytics workspace	East US

Instructions: Describe the capabilities of Microsoft Security Solutions...

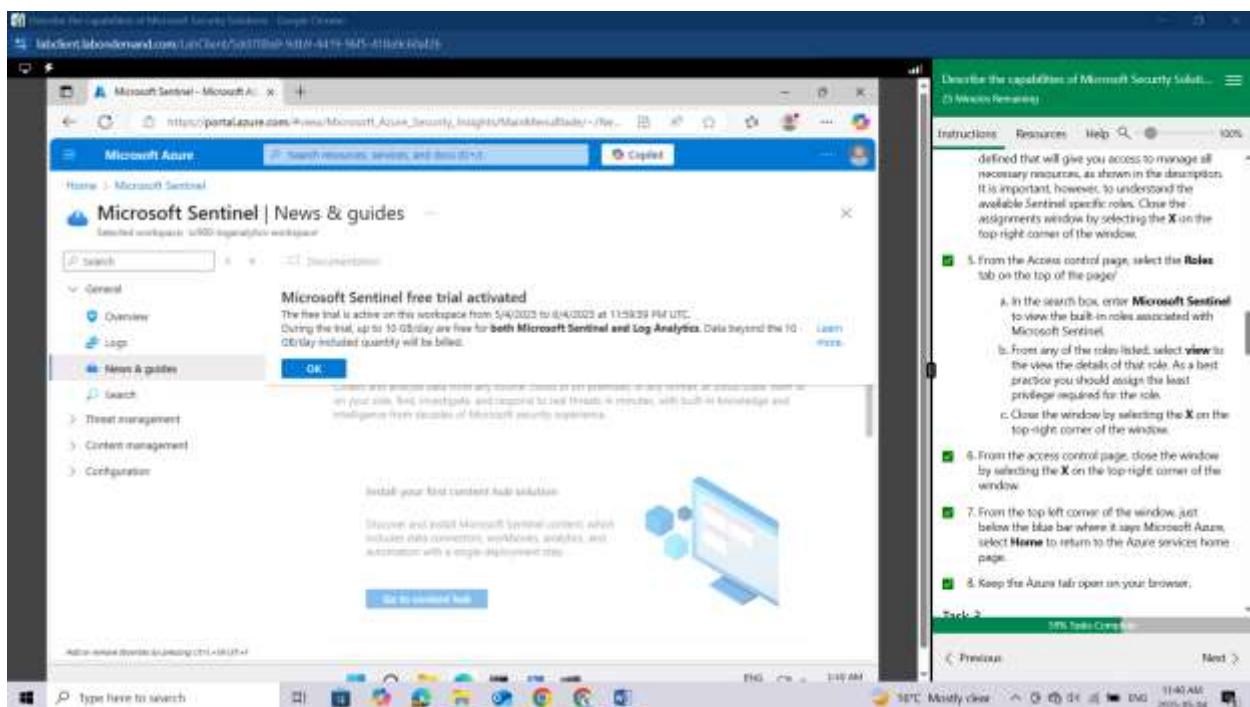
1. From the Azure services home page, select Microsoft Sentinel, then select the instance you created, **SC900-LogAnalytics-workspace**.
2. From the left navigation panel, expand **Content Management** then select **Content hub**.
3. Take a moment to scroll down to see the long list of available solutions and the options to filter the list. For this task, you're looking for **Microsoft Defender for Cloud**. Select it from the list. In the side window that opens, read the description then select **Install**. Once the installation is completed, the status column in the main window will show as installed.
4. Once again, select **Microsoft Defender for Cloud** from the list. From the window on the right, select **Manage**.
5. On the right side of the the Microsoft Defender for Cloud page is the description and notes associated with the solution from Content Hub.



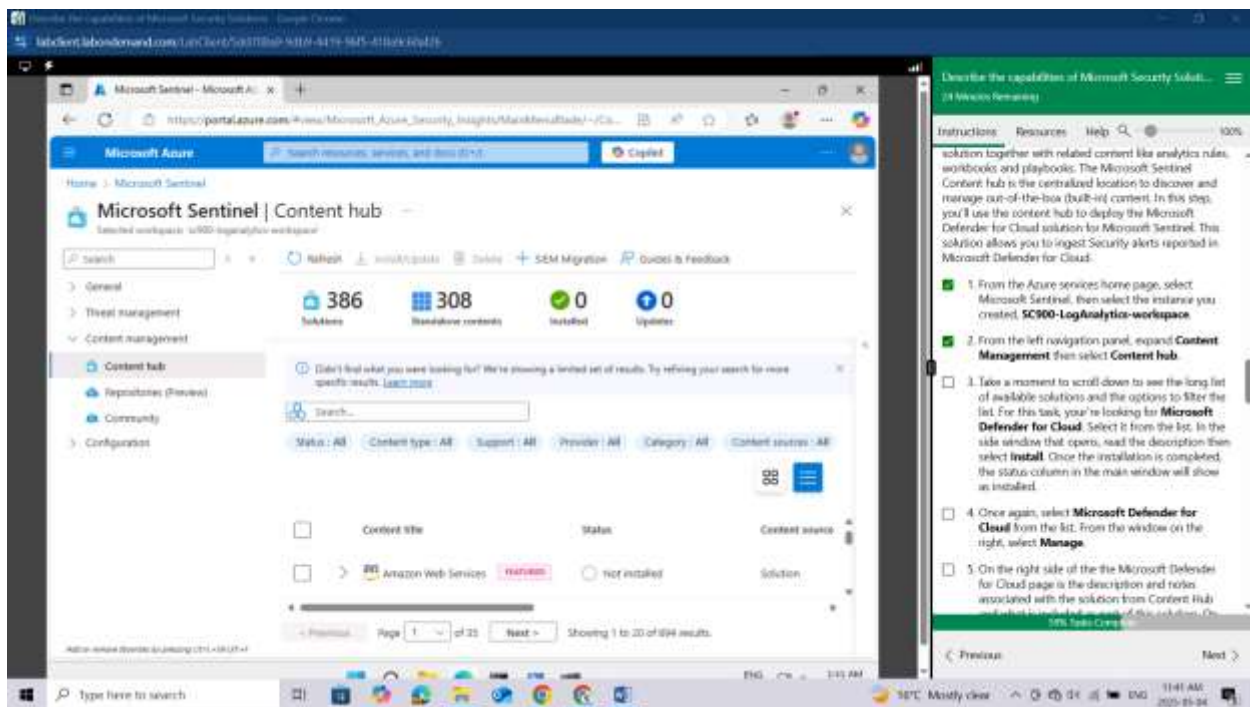
First you have to add the log analytics workspace to Microsoft sentinel by: Click on your **LogAnalytics workspace** and then click on **Add**



After adding you will see this message

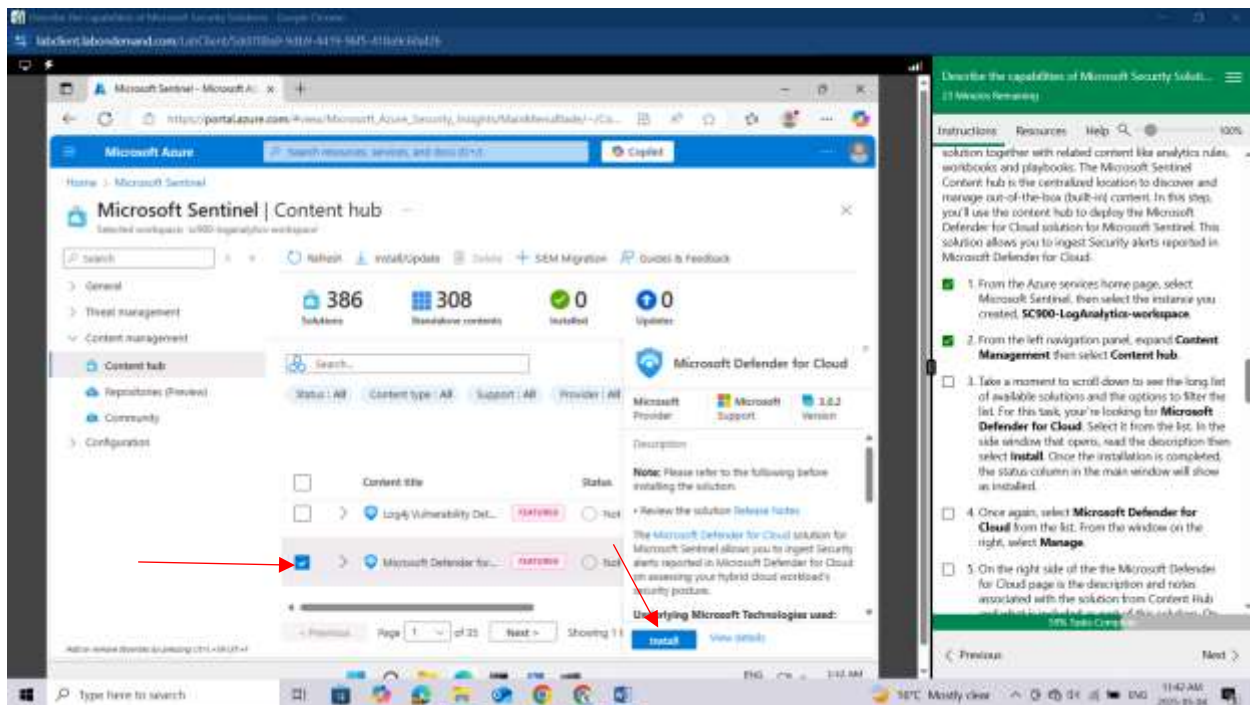


From the left navigation panel, expand **Content Management** then select **Content hub**.



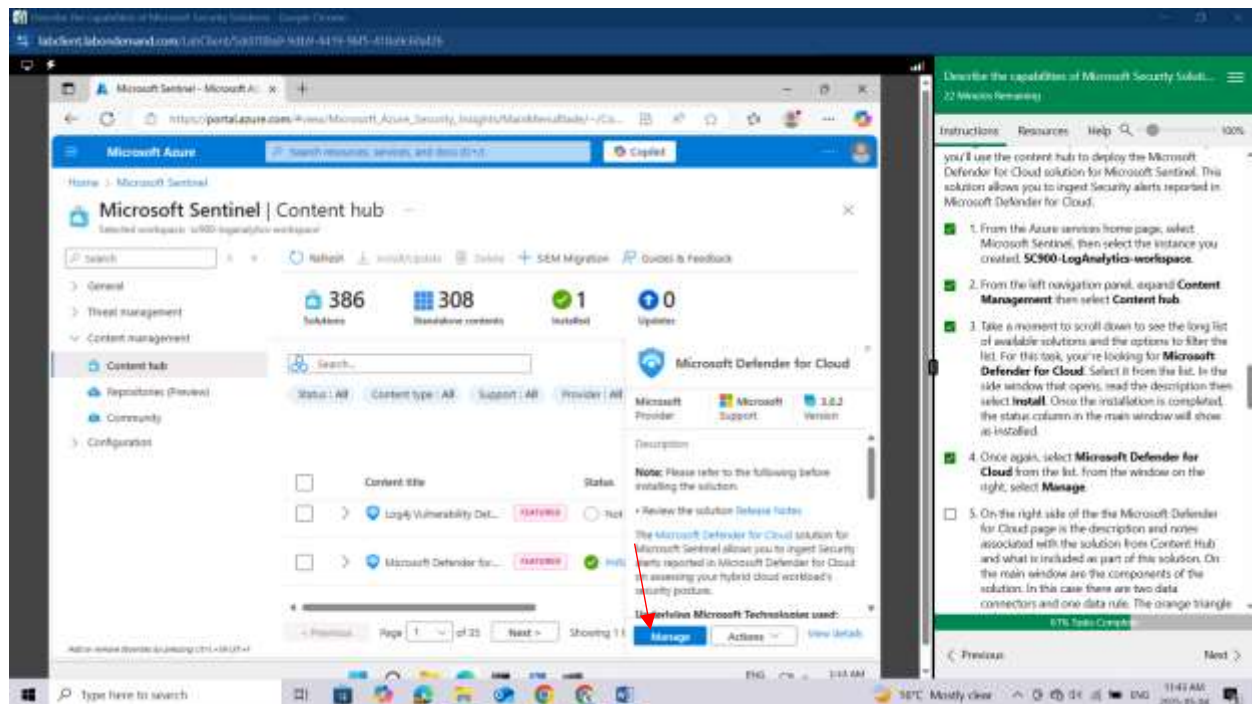
Take a moment to scroll down to see the long list of available solutions and the options to filter the list.

For this task, you're looking for **Microsoft Defender for Cloud**. Select it from the list. In the side window that opens, read the description then select **Install**.

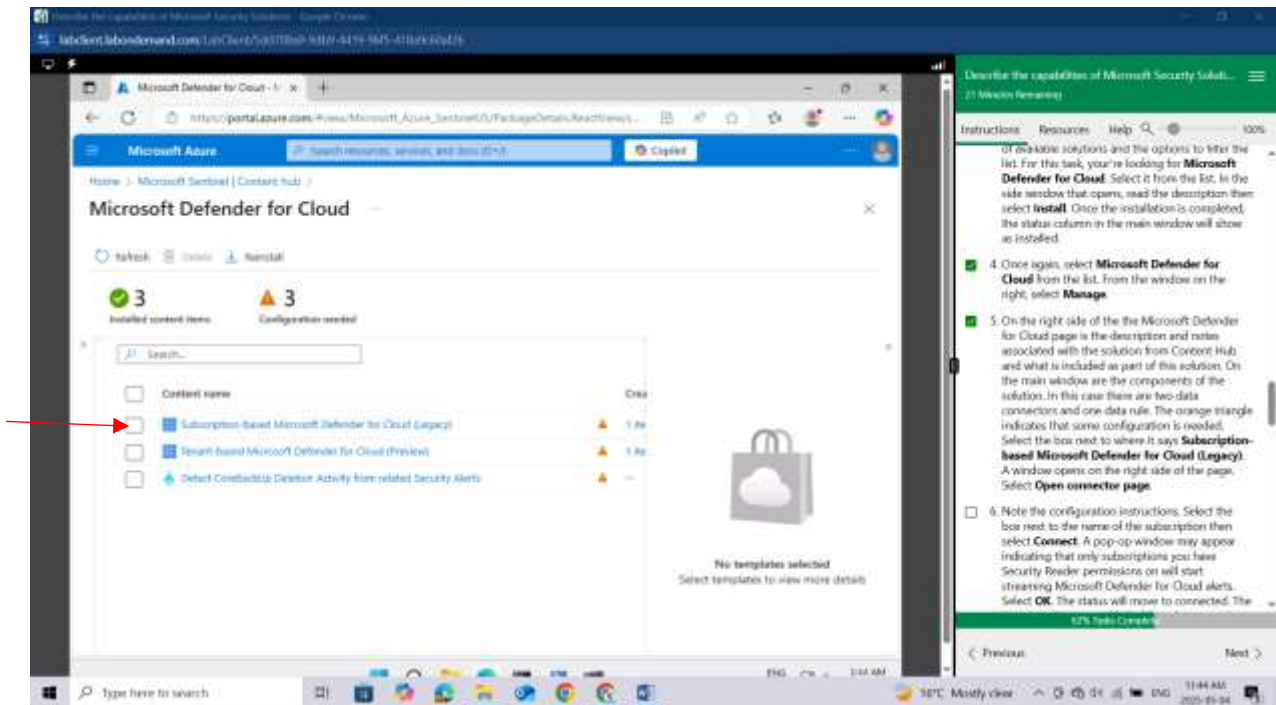


Once the installation is completed, the status column in the main window will show as installed.

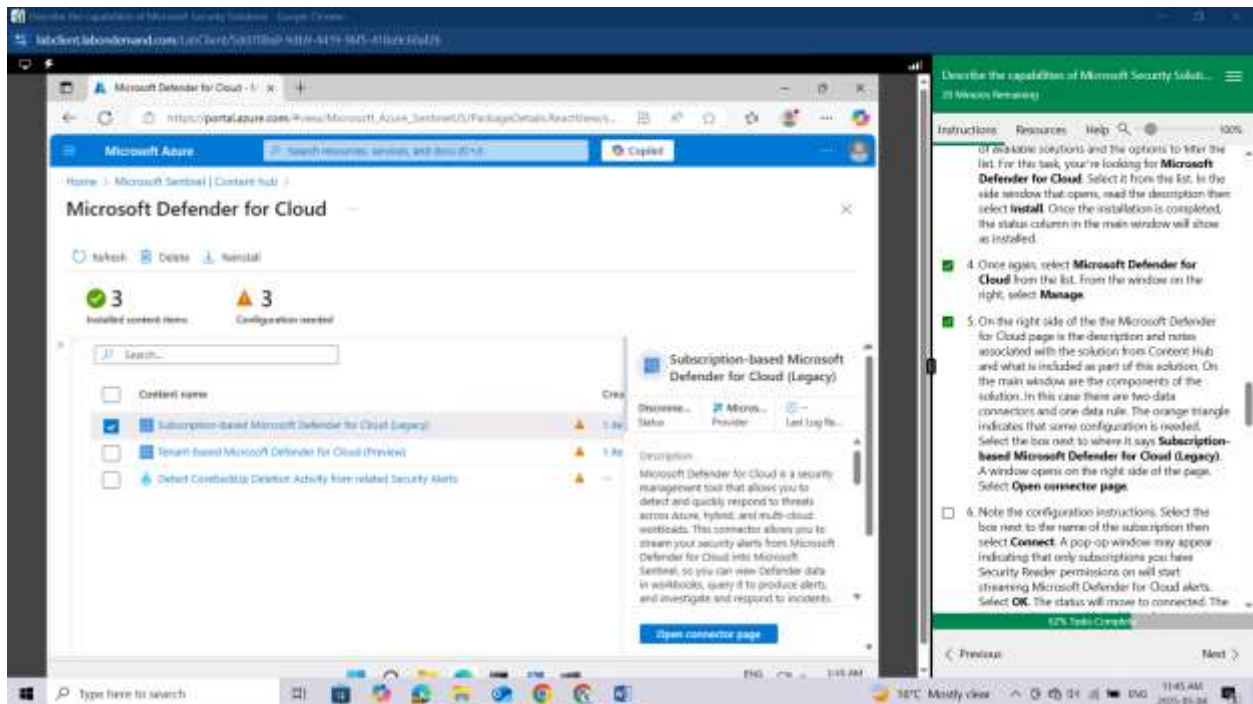
Once again, select **Microsoft Defender for Cloud** from the list. From the window on the right, select **Manage**.



On the right side of the the Microsoft Defender for Cloud page is the description and notes associated with the solution from Content Hub and what is included as part of this solution. On the main window are the components of the solution. In this case there are two data connectors and one data rule. The orange triangle indicates that some configuration is needed. Select the box next to where it says **Subscription-based Microsoft Defender for Cloud (Legacy)**.



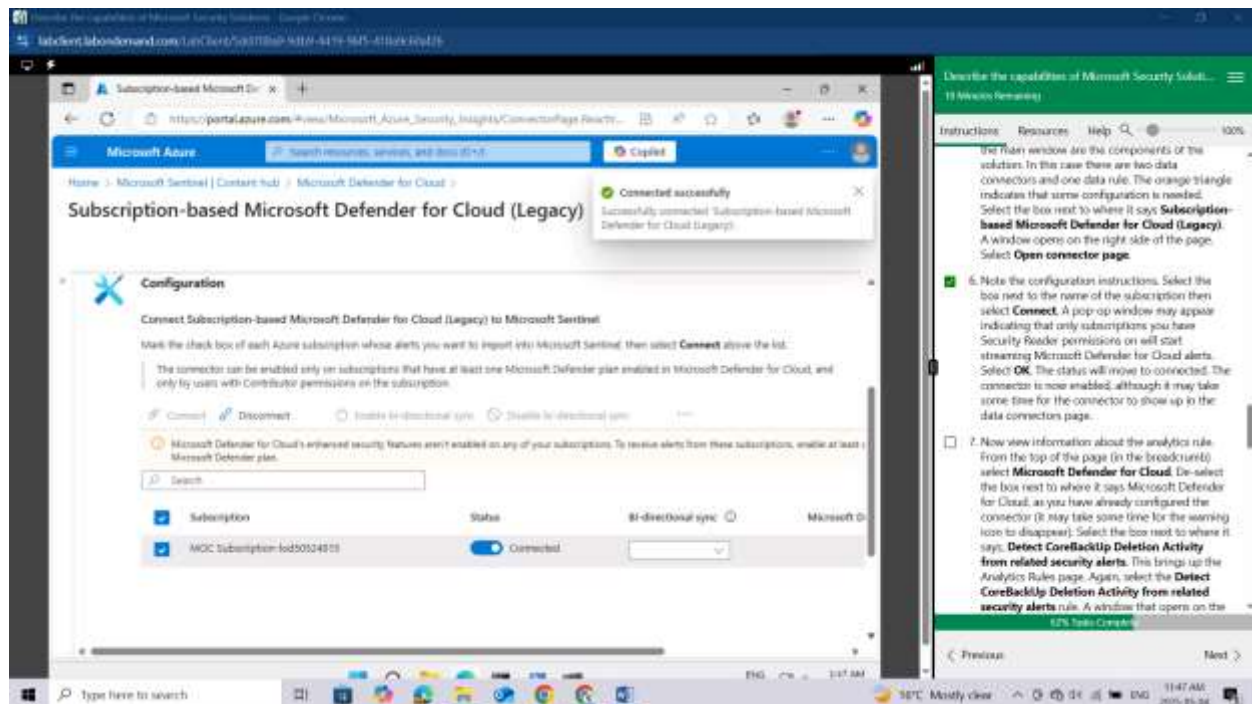
A window opens on the right side of the page. Select **Open connector page**.



Note the configuration instructions. Select the box next to the name of the subscription then select **Connect**. A pop-up window may appear indicating that only subscriptions you have Security Reader permissions on will start streaming Microsoft Defender for Cloud alerts. Select **OK**. The status will move

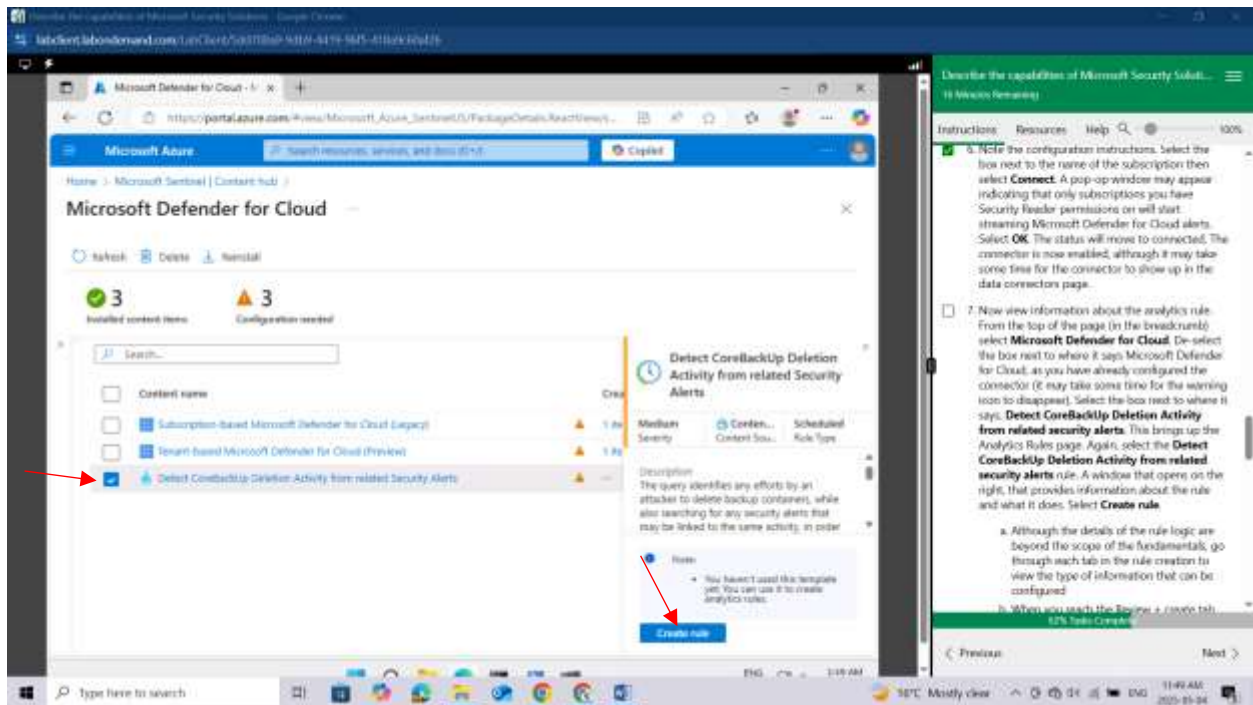


to connected. The connector is now enabled, although it may take some time for the connector to show up in the data connectors page.



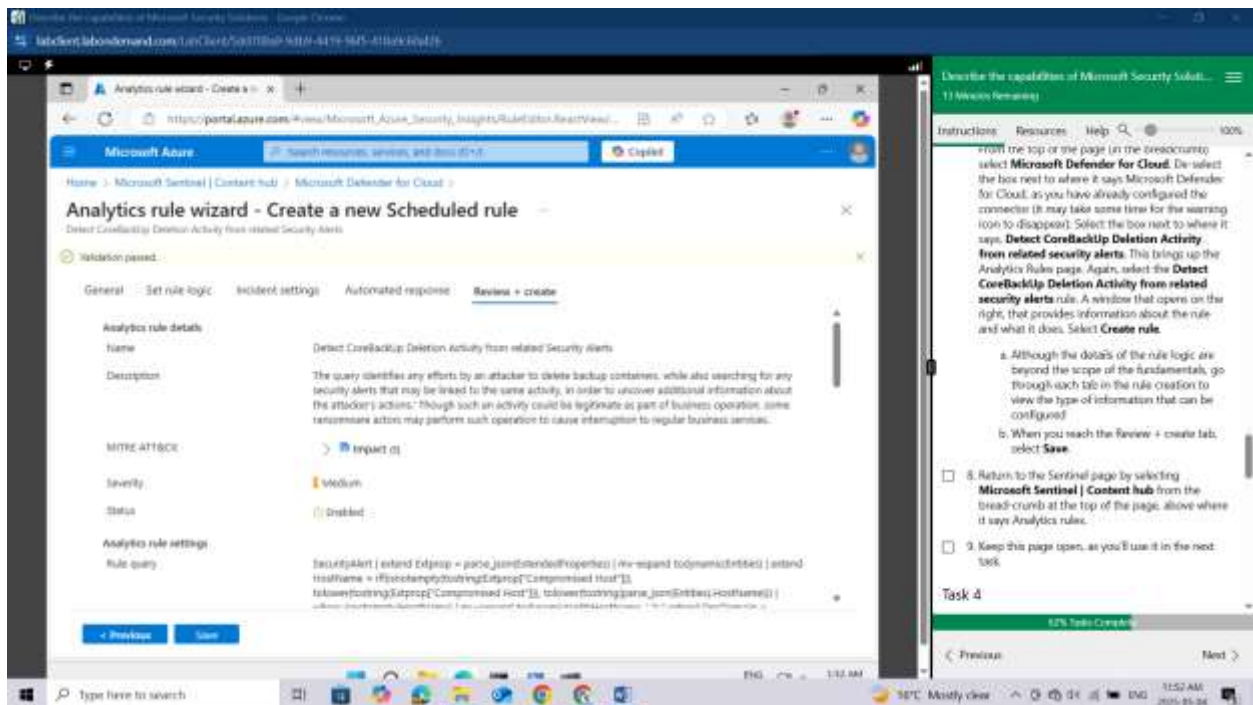
Now view information about the analytics rule. From the top of the page (in the breadcrumb) select Microsoft Defender for Cloud. De-select the box next to where it says Microsoft Defender for Cloud, as you have already configured the connector (it may take some time for the warning icon to disappear). Select the box next to where it says, Detect CoreBackUp Deletion Activity from related security alerts. This brings up the Analytics Rules page. Again, select the **Detect CoreBackUp Deletion Activity from related security alerts rule**. A window that opens on the right, that provides information about the rule and what it does. Select **Create rule**.





Although the details of the rule logic are beyond the scope of the fundamentals, go through each tab in the rule creation to view the type of information that can be configured

When you reach the **Review + create** tab, select **Save**.



Return to the Sentinel page by selecting **Microsoft Sentinel | Content hub** from the bread-crumbs at the top of the page, above where it says Analytics rules.

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

The screenshot shows the Microsoft Sentinel Content hub interface. The left navigation pane has 'Threat management' expanded, showing options like Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization, Content management, and Content hub. The main content area displays a list of solutions, including 'Log4j Vulnerability De...' and 'Microsoft Defender for...'. A right-hand sidebar contains instructions for a task, including steps 8 and 9, and a 'Task 4' section.

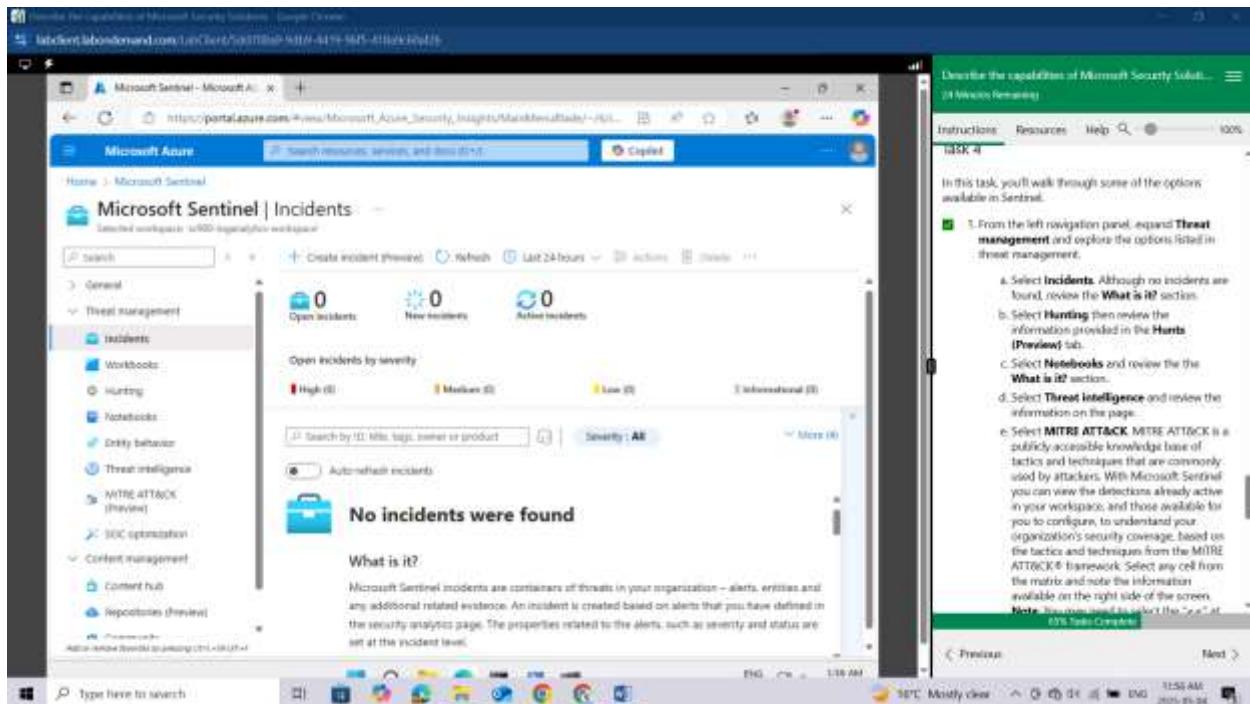
## Task 4

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

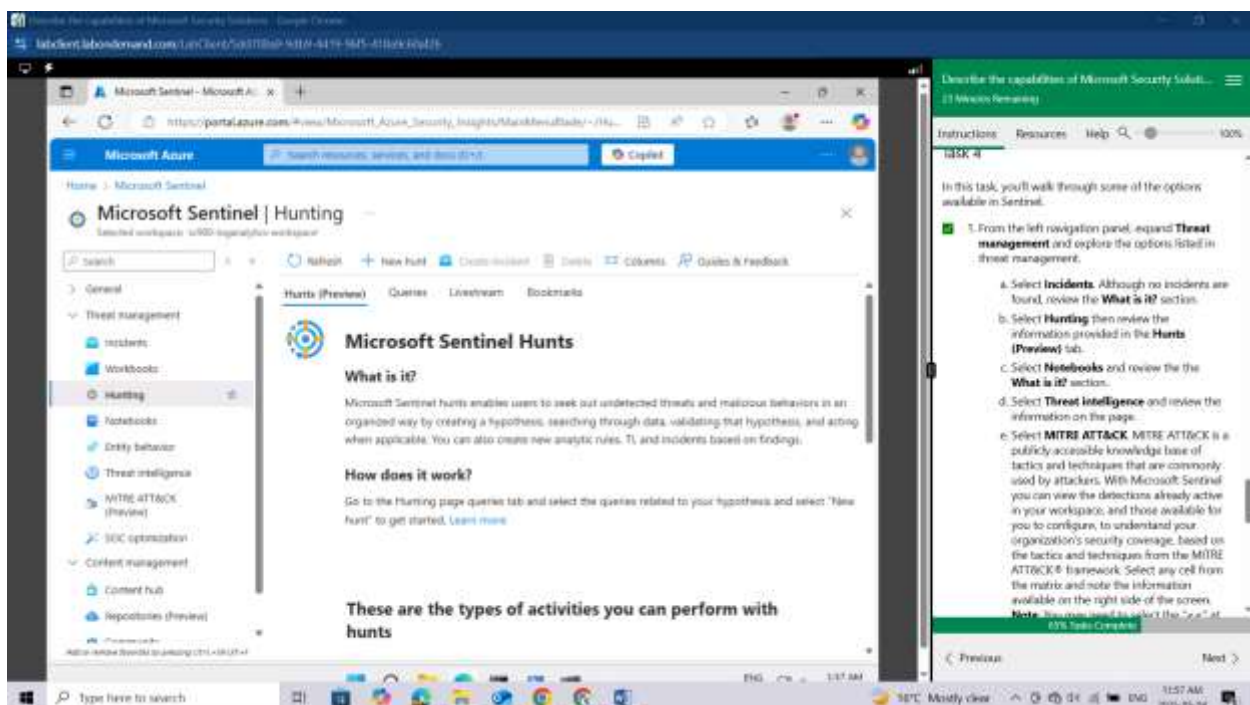
From the left navigation panel, expand **Threat management** and explore the options listed in threat management.

The screenshot shows the Microsoft Sentinel Content hub interface, with 'Threat management' expanded in the left navigation pane. The main content area displays a list of solutions, including 'Log4j Vulnerability De...' and 'Microsoft Defender for...'. A right-hand sidebar contains instructions for a task, including steps 8 and 9, and a 'Task 4' section.

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

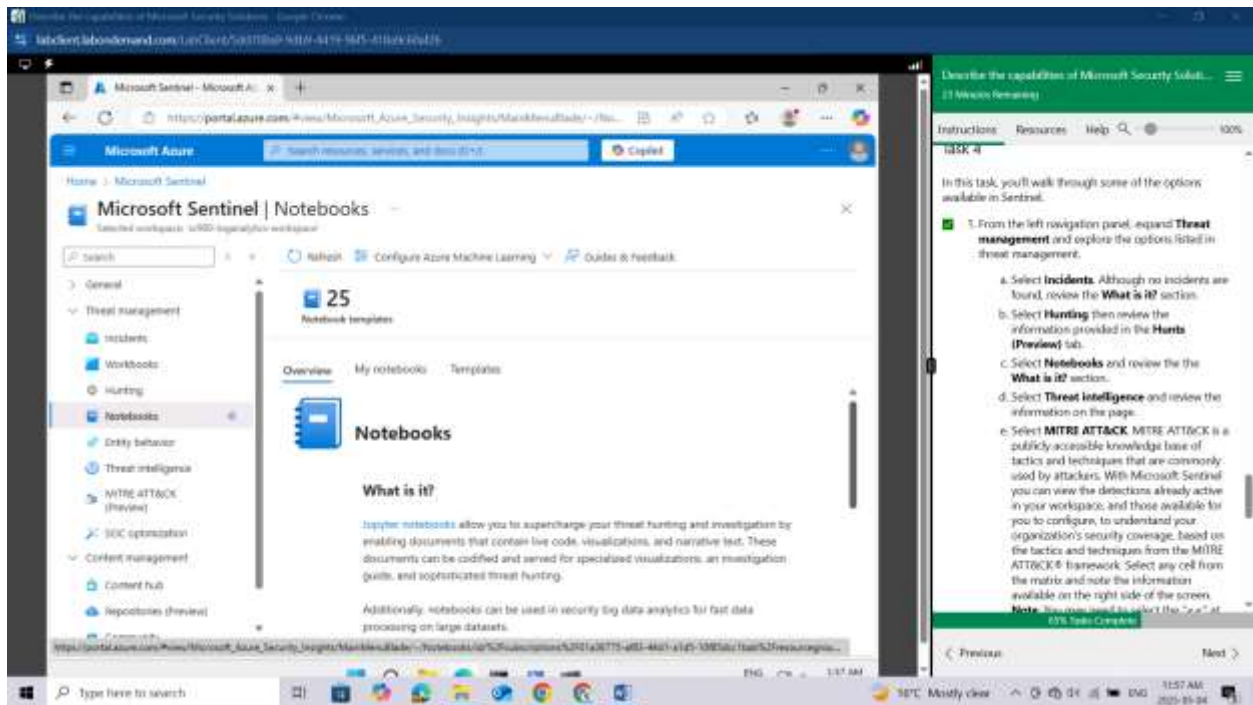


Select **Hunting** then review the information provided in the **Hunts (Preview)** tab.

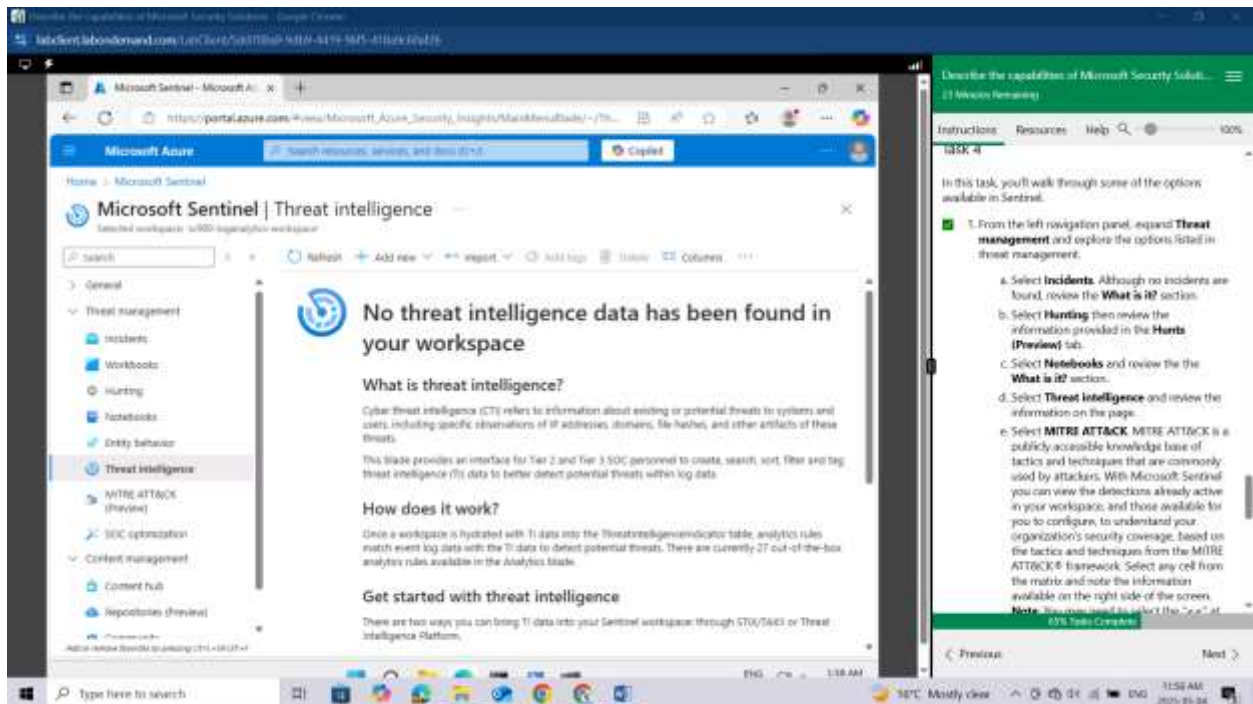


Select **Notebooks** and review the the **What is it?** section.



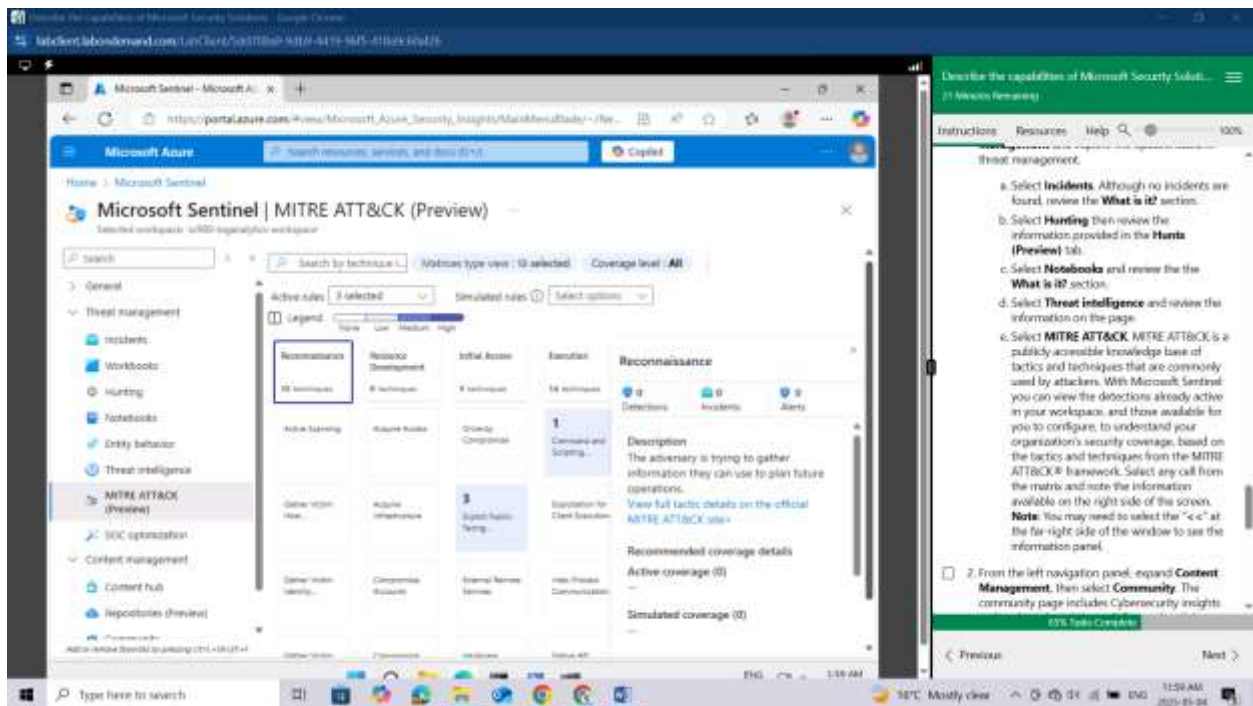


Select **Threat intelligence** and review the information on the page.

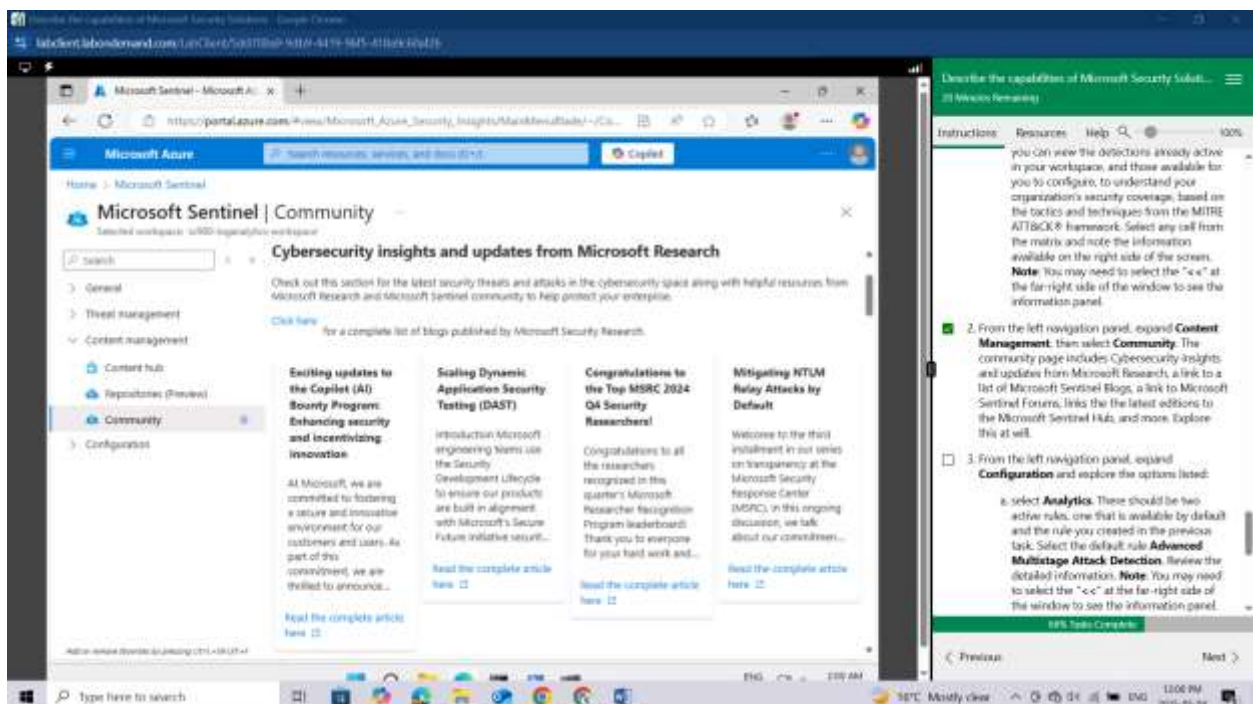


Select **MITRE ATT&CK**. MITRE ATT&CK is a publicly accessible knowledge base of tactics and techniques that are commonly used by attackers. With Microsoft Sentinel you can view the detections already active in your workspace, and those available for you to configure, to understand your organization's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

rk. Select any cell from the matrix and note the information available on the right side of the screen. Note: You may need to select the "<<" at the far-right side of the window to see the information panel.



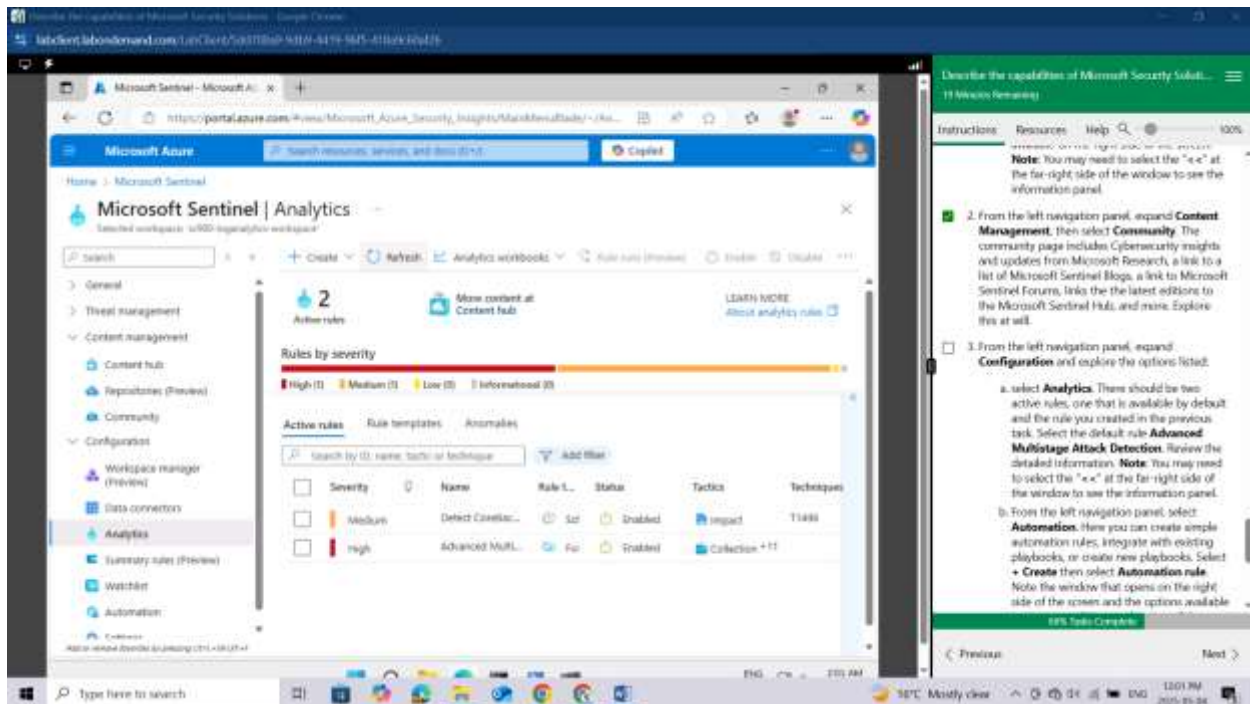
From the left navigation panel, expand **Content Management**, then select **Community**. The community page includes Cybersecurity insights and updates from Microsoft Research, a link to a list of Microsoft Sentinel Blogs, a link to Microsoft Sentinel Forums, links the the latest editions to the Microsoft Sentinel Hub, and more. Explore this at will.



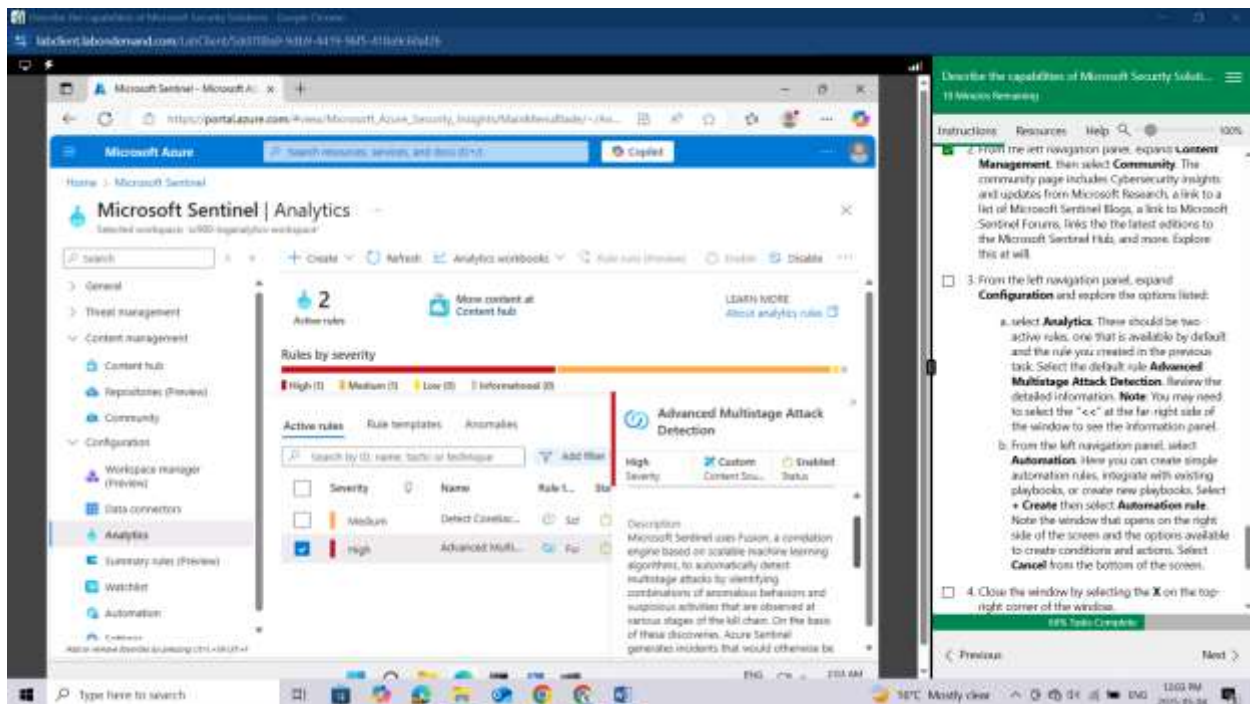


From the left navigation panel, expand **Configuration** and explore the options listed:

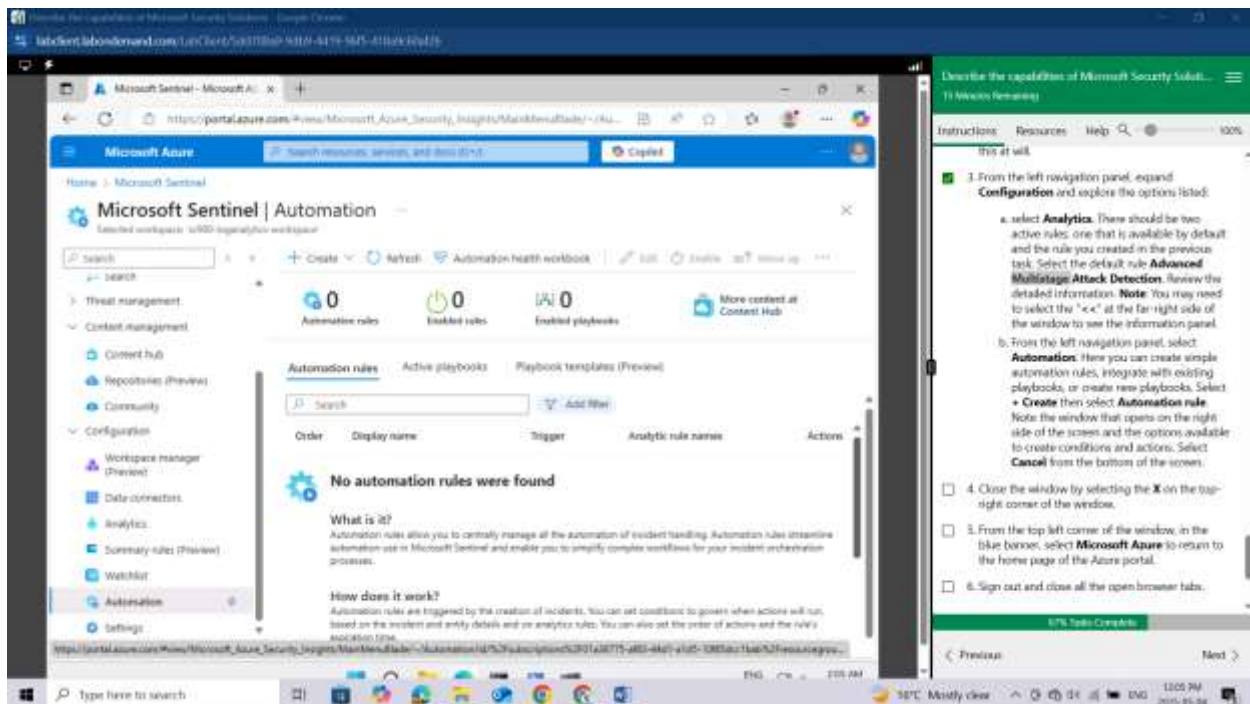
select **Analytics**. There should be two active rules, one that is available by default and the rule you created in the previous task.



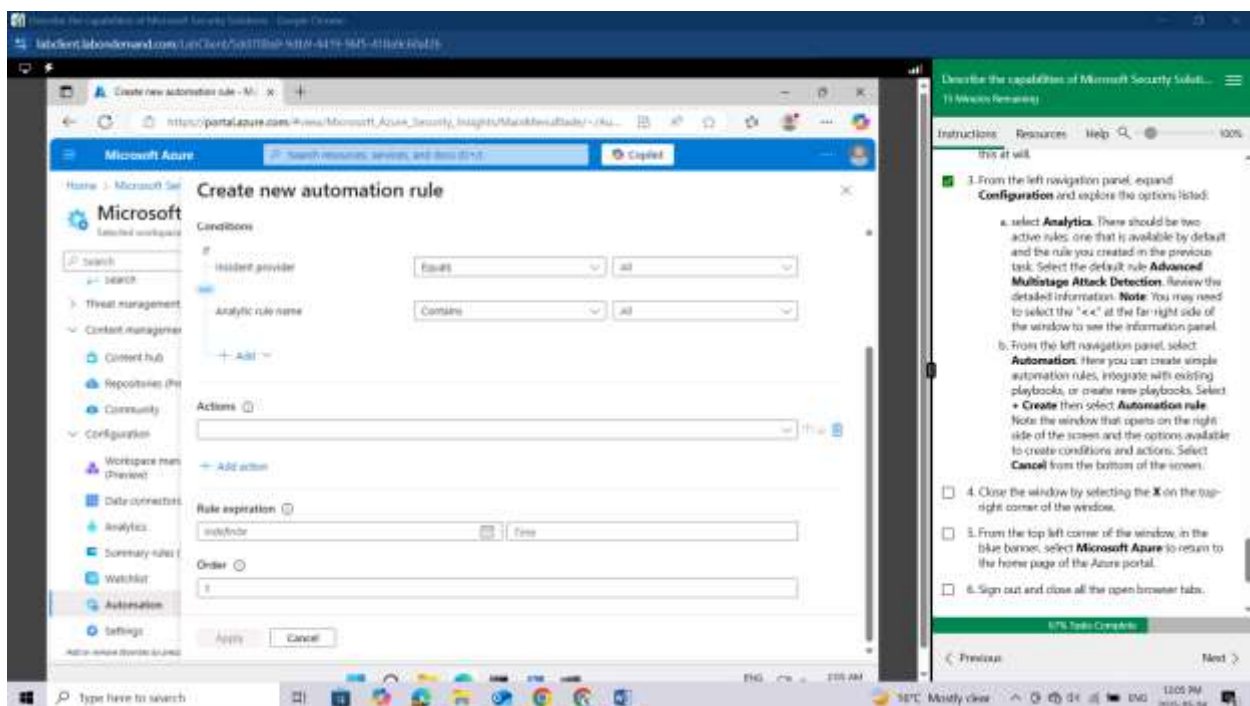
Select the default rule **Advanced Multistage Attack Detection**. Review the detailed information. Note: You may need to select the "<<" at the far-right side of the window to see the information panel.



From the left navigation panel, select **Automation**. Here you can create simple automation rules, integrate with existing playbooks, or create new playbooks.



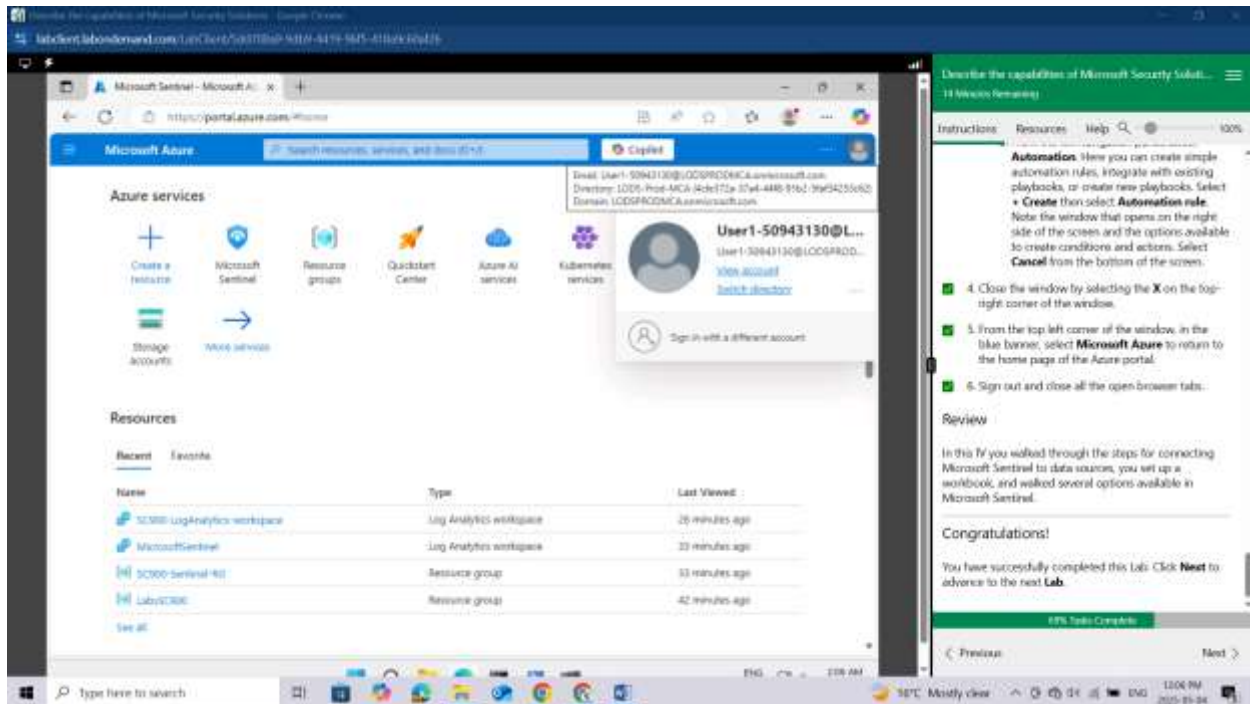
Select **+ Create** then select **Automation rule**. Note the window that opens on the right side of the screen and the options available to create conditions and actions. Select **Cancel** from the bottom of the screen.



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

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.

Sign out and close all the open browser tabs.



## Conclusion

Through these two labs, I've now got a much better handle on Microsoft's cloud security tools. In the **Explore Microsoft Defender for Cloud** lab, I got to see how it helps manage security and protect things across Azure and even hybrid setups. I explored how it gives recommendations, shows alerts, and helps keep an eye on the overall security health. Then, with the **Explore Microsoft Sentinel** lab, I jumped into Microsoft's cloud SIEM and SOAR. I learnt how to connect different data sources, and specifically, I connected Microsoft Defender for Cloud so its security info could flow into Sentinel. I also got to learn around the key parts of Sentinel, like the **Content hub** for finding ready-made security stuff, Incidents for dealing with threats, Hunting to proactively look for trouble, **Analytics rules** to automatically spot threats, and Automation to set up automatic responses. Basically, these labs have shown me how Microsoft Defender for Cloud and Microsoft Sentinel team up to make the cloud environment more secure, help find threats, and even automate how we respond to them.