Microsoft ADC Cybersecurity Skilling Program

Week 3 Lab Assignment

Student Name: Vincent Onchieku Collins

Student ID: ADC-CSS02-25052

Introduction

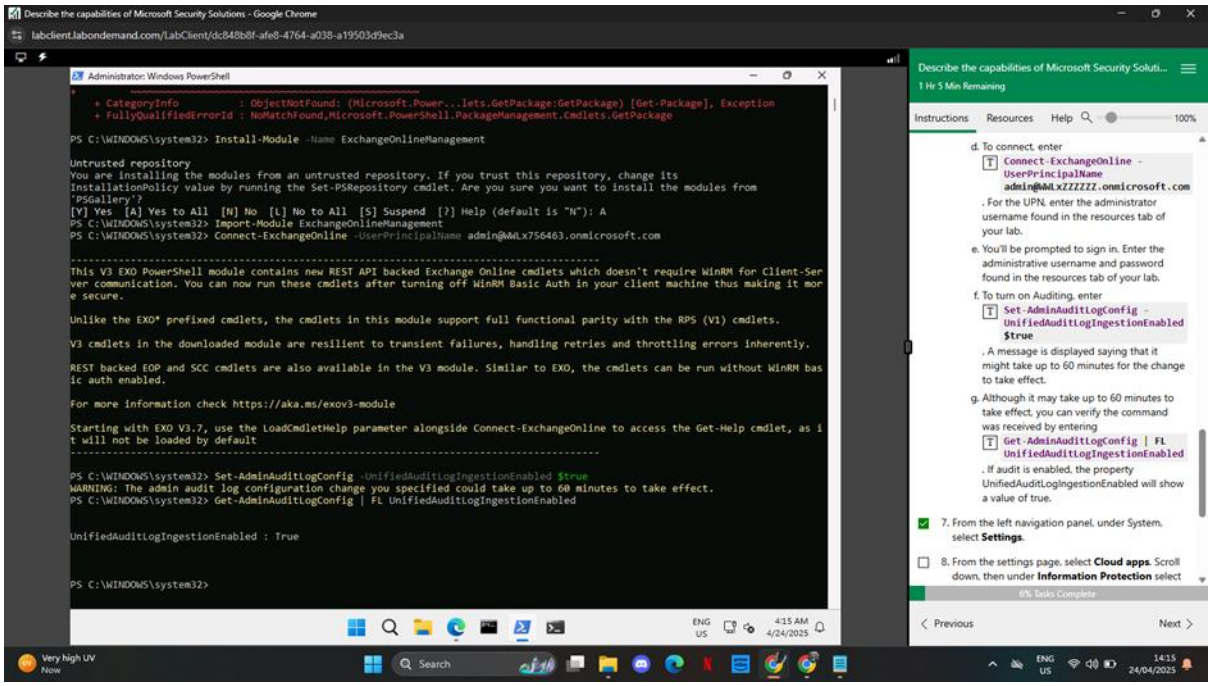
The following report presents a comprehensive overview of six hands-on labs that explore core components of Microsoft security and compliance solutions. Each lab focused on practical tasks within the Microsoft 365 and Azure ecosystems, offering a guided experience in configuring and managing enterprise-grade security tools. From setting up tenant auditing in Microsoft 365 to exploring threat detection through Microsoft Sentinel and posture management with Defender for Cloud, these labs provided valuable insights into how Microsoft's integrated security solutions work together to enhance visibility, compliance, and protection across cloud environments.

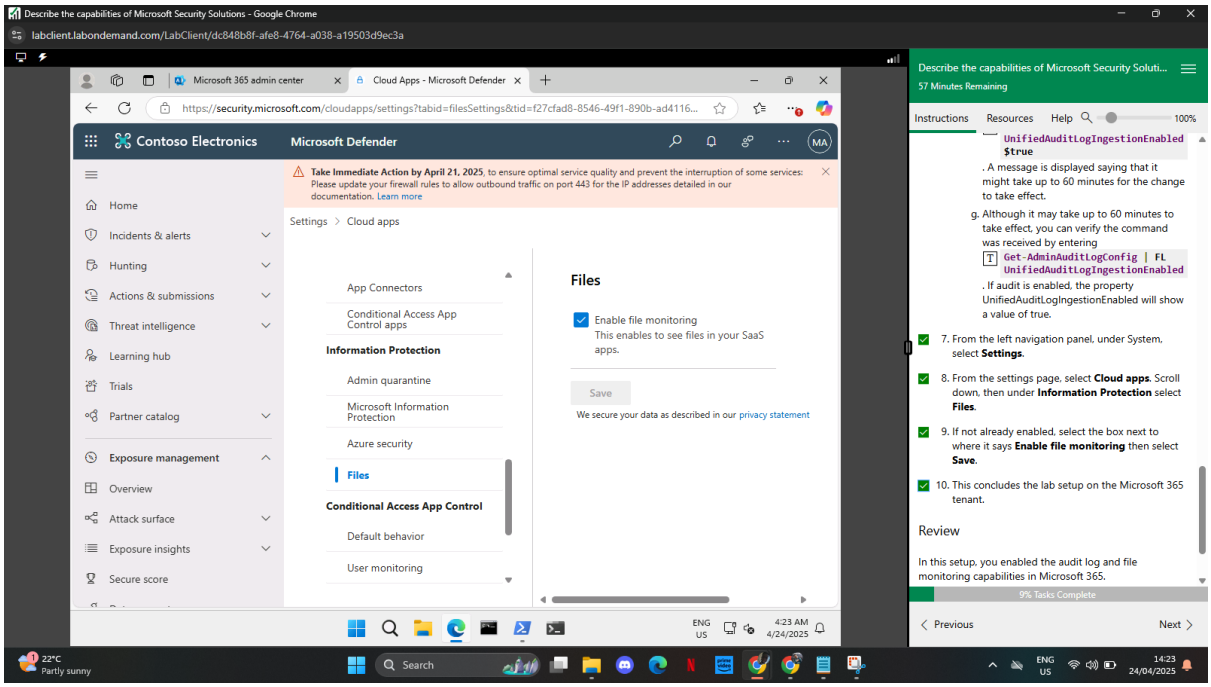
This week, we will be completing the second lab that explores the Describe the capabilities of Microsoft Security Solutions. The labs you need to complete will include:

1. Lab: Setup of the Microsoft 365 tenant
2. Lab: Explore Azure Network Security Groups (NSGs)
3. Lab: Explore Microsoft Defender for Cloud
4. Lab: Explore Microsoft Sentinel
5. Lab: Explore Microsoft Defender for Cloud Apps
6. Lab: Explore the Microsoft Defender portal

Lab 1: Setup of the Microsoft 365 tenant

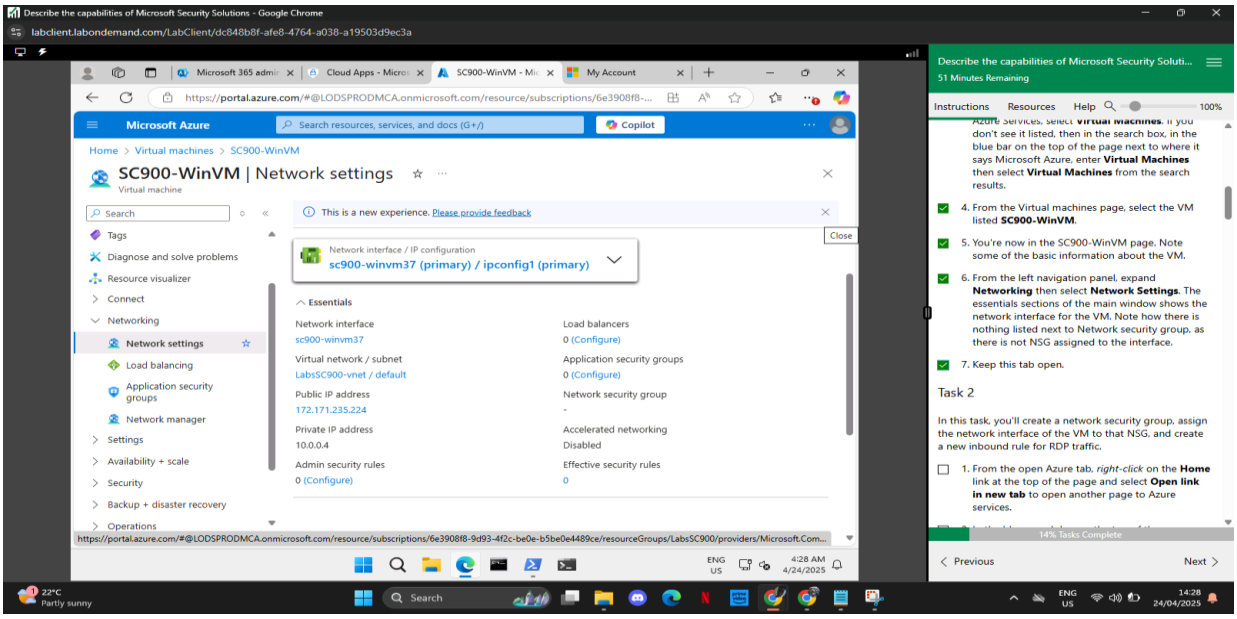
In this lab, I successfully configured the Microsoft 365 tenant by enabling key auditing and file monitoring features. I began by accessing the Microsoft 365 admin center and navigating to the Microsoft Defender portal. From there, I verified whether auditing was already enabled. Since it was not, I initiated the process of recording user and admin activities. In cases where the graphical interface failed to confirm audit status, I used PowerShell commands to manually enable the unified audit log ingestion. Once activated, I confirmed that the UnifiedAuditLogIngestionEnabled property was set to true. Lastly, I enabled file monitoring under the Cloud apps settings, specifically under the Information Protection section. This lab provided foundational exposure to tenant setup and reinforced the importance of audit logging and file tracking for effective security monitoring within the Microsoft 365 environment.

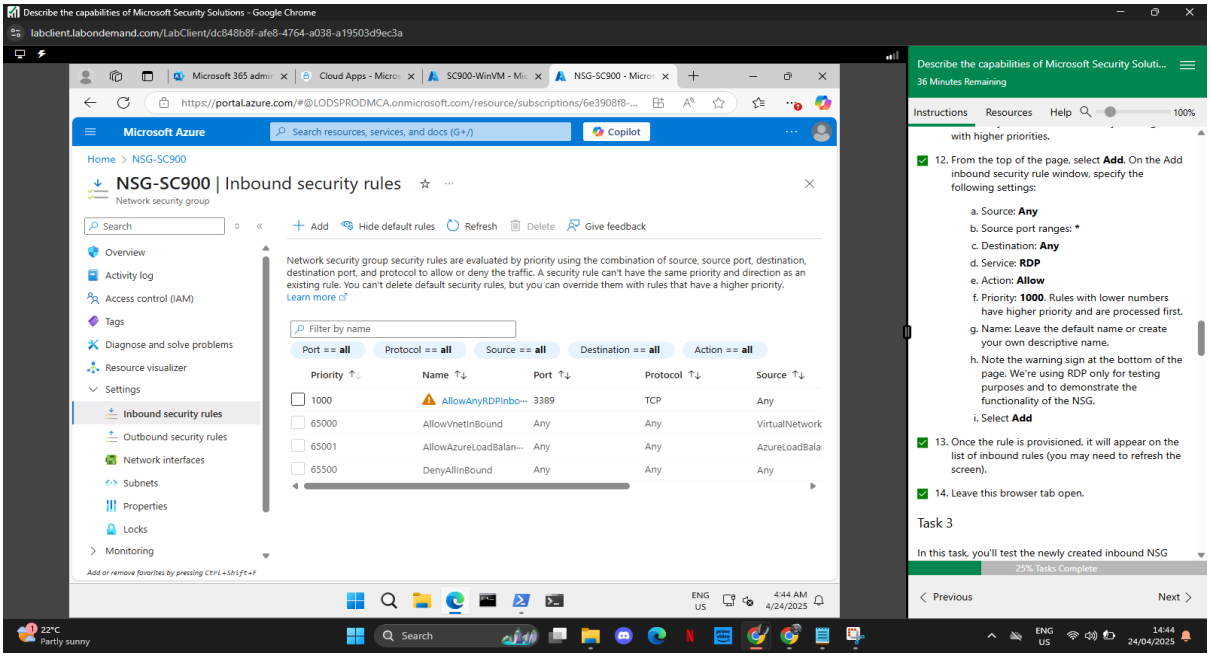

Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/dc848b8f-afe8-4764-a038-a19503d9ec3a
Administrator: Windows PowerShell
+ CategoryInfo : ObjectNotFound: (Microsoft.Power...lets.GetPackage:GetPackage) [Get-Package], Exception
+ FullyQualifiedErrorId : NoMatchFound,Microsoft.PowerShell.PackageManagement.Cmdlets.GetPackage
PS C:\WINDOWS\system32> Install-Module -Name ExchangeOnlineManagement
Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\WINDOWS\system32> Import-Module ExchangeOnlineManagement
PS C:\WINDOWS\system32> Connect-ExchangeOnline -UserPrincipalName admin@WWLx756463.onmicrosoft.com
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't require WinRM for Client-Ser
ver communication. You can now run these cmdlets after turning off WinRM Basic Auth in your client machine thus making it mor
e secure.
Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with the RPS (V1) cmdlets.
V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and throttling errors inherently.
REST backed EOP and SCC cmdlets are also available in the V3 module. Similar to EXO, the cmdlets can be run without WinRM bas
ic auth enabled.
For more information check https://aka.ms/exov3-module
Starting with EXO V3.7, use the LoadCmdletHelp parameter alongside Connect-ExchangeOnline to access the Get-Help cmdlet, as i
t will not be loaded by default
PS C:\WINDOWS\system32> Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
WARNING: The admin audit log configuration change you specified could take up to 60 minutes to take effect.
PS C:\WINDOWS\system32> Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled
UnifiedAuditLogIngestionEnabled : True
PS C:\WINDOWS\system32>
Describe the capabilities of Microsoft Security Soluti...
1 Hr 5 Min Remaining
Instructions
Resources
Help
100%
d. To connect, enter
Connect-ExchangeOnline -UserPrincipalName admin@WWLx222222.onmicrosoft.com
. For the UPN, enter the administrator username found in the resources tab of your lab.
e. You'll be prompted to sign in. Enter the administrative username and password found in the resources tab of your lab.
f. To turn on Auditing, enter
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
. A message is displayed saying that it might take up to 60 minutes for the change to take effect.
g. Although it may take up to 60 minutes to take effect, you can verify the command was received by entering
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled
. If audit is enabled, the property UnifiedAuditLogIngestionEnabled will show a value of true.
7. From the left navigation panel, under System, select Settings.
8. From the settings page, select Cloud apps. Scroll down, then under Information Protection select
6% Tasks Complete
Previous
Next
Very high UV
Now
Search
ENG US
4:15 AM
4/24/2025
14:15
24/04/2025

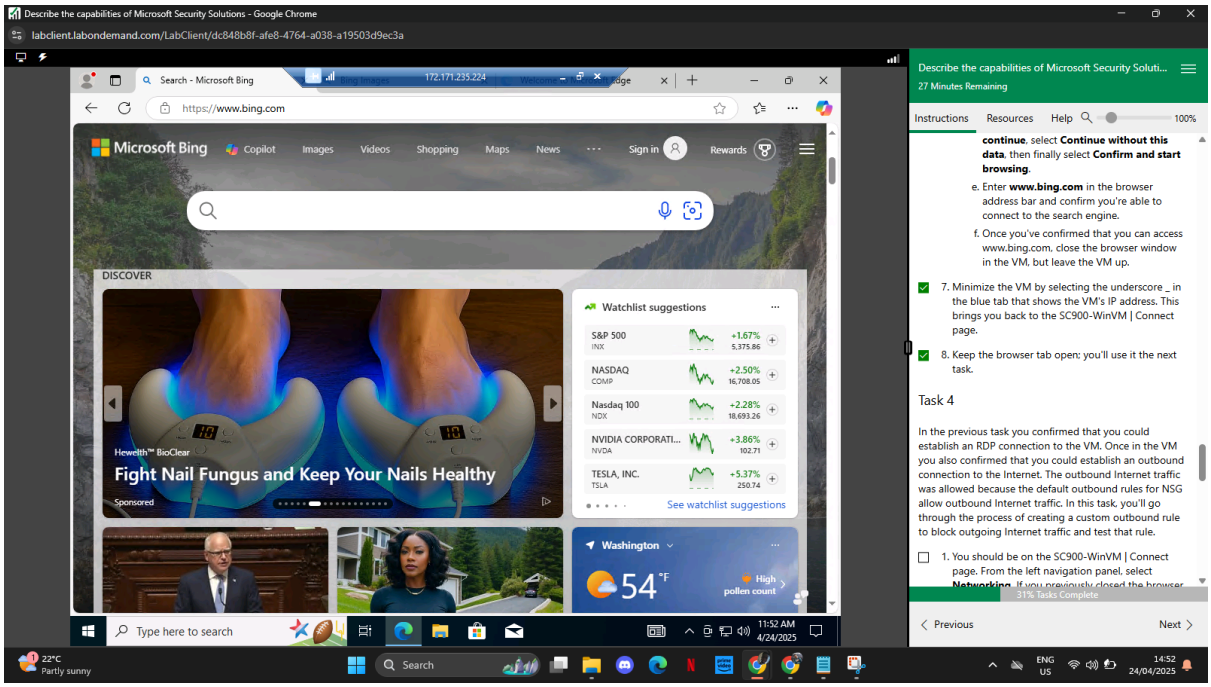

Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/dc848b8f-afe8-4764-a038-a19503d9ec3a
Microsoft 365 admin center
Cloud Apps - Microsoft Defender
https://security.microsoft.com/cloudapps/settings?tabid=filesSettings&tid=f27cfad8-8546-49f1-890b-ad4116...
Contoso Electronics
Microsoft Defender
MA
Take Immediate Action by April 21, 2025, to ensure optimal service quality and prevent the interruption of some services: Please update your firewall rules to allow outbound traffic on port 443 for the IP addresses detailed in our documentation. Learn more
Home
Incidents & alerts
Hunting
Actions & submissions
Threat intelligence
Learning hub
Trials
Partner catalog
Exposure management
Overview
Attack surface
Exposure insights
Secure score
Settings > Cloud apps
App Connectors
Conditional Access App Control apps
Information Protection
Admin quarantine
Microsoft Information Protection
Azure security
Files
Conditional Access App Control
Default behavior
User monitoring
Files
Enable file monitoring
This enables to see files in your SaaS apps.
Save
We secure your data as described in our privacy statement
Describe the capabilities of Microsoft Security Soluti...
57 Minutes Remaining
Instructions
Resources
Help
100%
UnifiedAuditLogIngestionEnabled $true
. A message is displayed saying that it might take up to 60 minutes for the change to take effect.
g. Although it may take up to 60 minutes to take effect, you can verify the command was received by entering
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled
. If audit is enabled, the property UnifiedAuditLogIngestionEnabled will show a value of true.
7. From the left navigation panel, under System, select Settings.
8. From the settings page, select Cloud apps. Scroll down, then under Information Protection select Files.
9. If not already enabled, select the box next to where it says Enable file monitoring then select Save.
10. This concludes the lab setup on the Microsoft 365 tenant.
Review
In this setup, you enabled the audit log and file monitoring capabilities in Microsoft 365.
9% Tasks Complete
Previous
Next
22°C
Partly sunny
Search
ENG US
4:23 AM
4/24/2025
14:23
24/04/2025

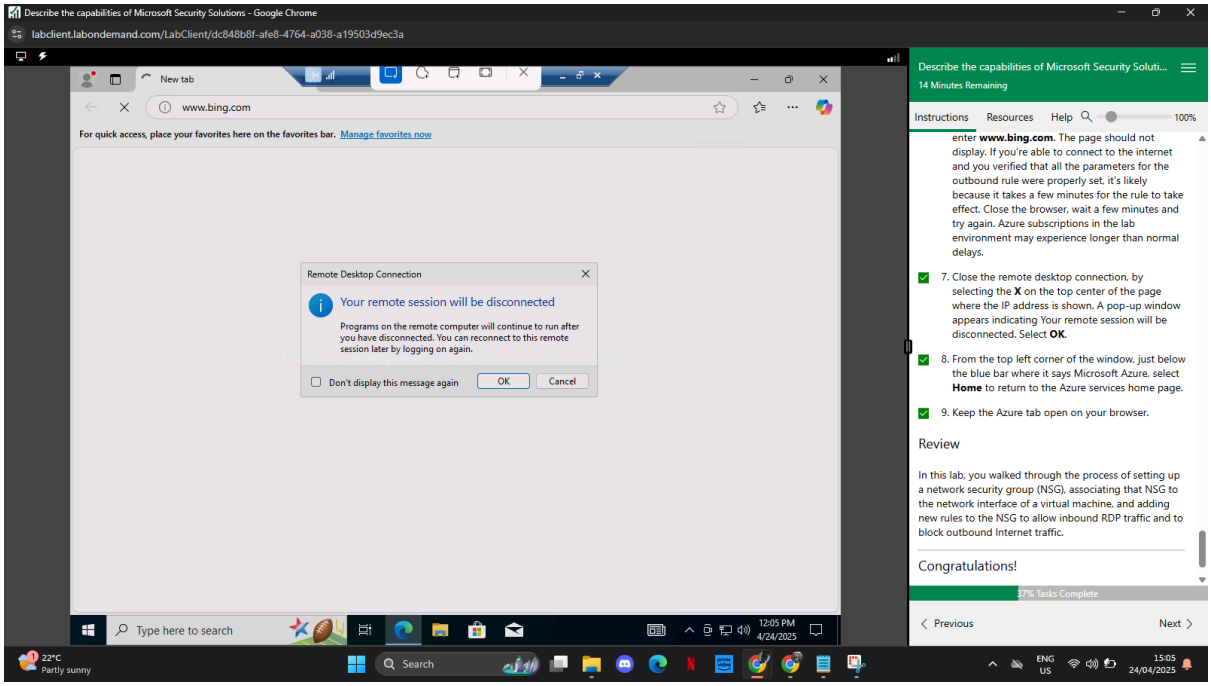
Lab 2: Explore Azure Network Security Groups (NSGs)

In Lab 2, I explored the functionality of Azure Network Security Groups (NSGs) by creating an NSG and associating it with the network interface of a pre-existing virtual machine (VM). I reviewed the default inbound and outbound security rules, then created a custom inbound rule to allow Remote Desktop Protocol (RDP) traffic on port 3389. After verifying that the RDP connection was accessible, I connected to the VM and confirmed outbound internet access by navigating to www.bing.com. Next, I created a custom outbound rule to block all internet traffic by denying all outbound connections to the "Internet" service tag. After waiting for the rule to take effect, I tested the VM's outbound connectivity again and confirmed that access to www.bing.com was successfully blocked. This lab demonstrated how NSGs can be used to control traffic flow to and from Azure resources.



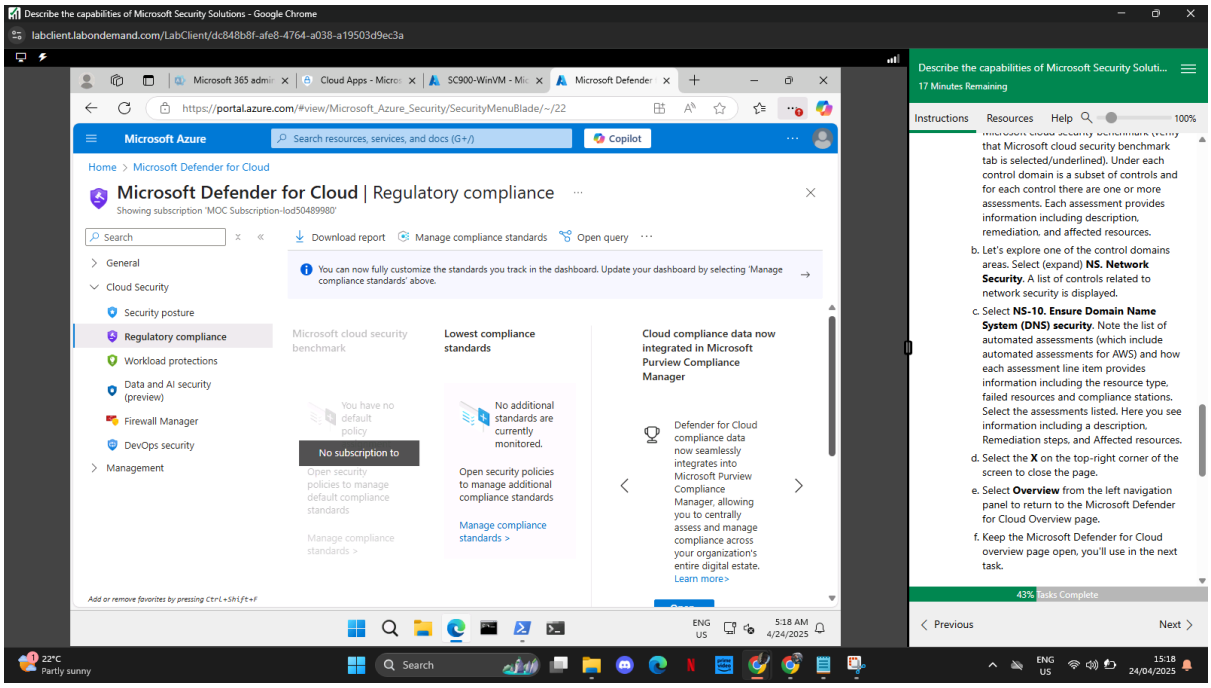


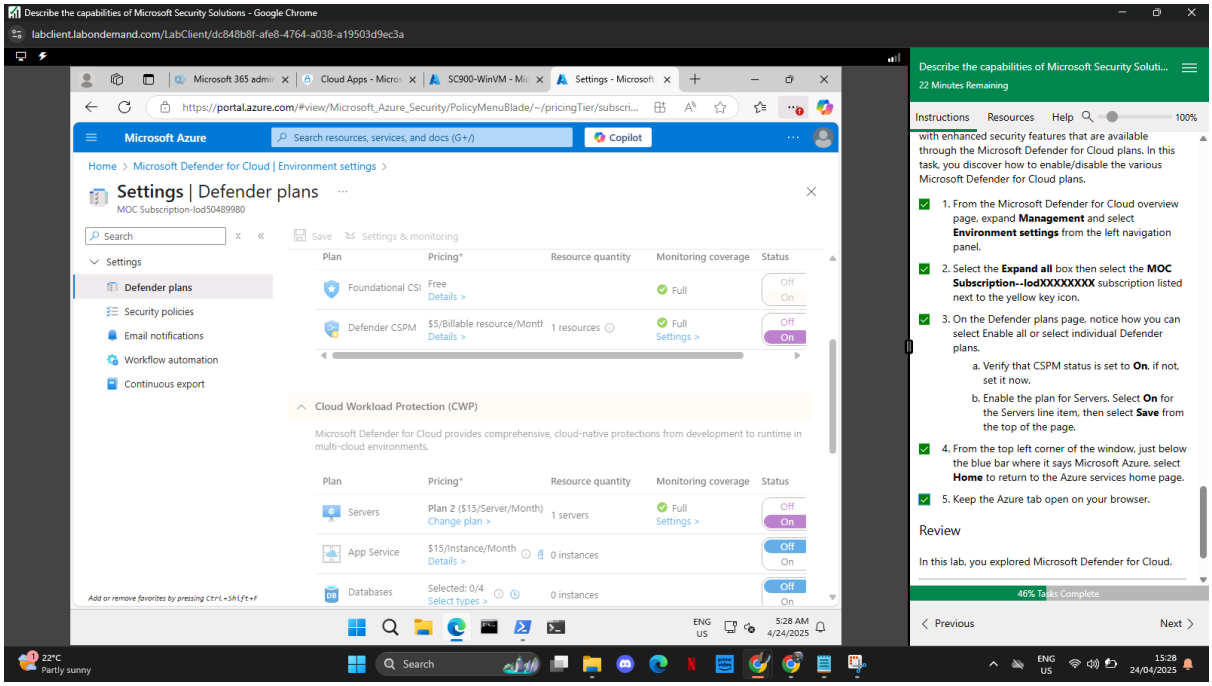

Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/dc848b8f-afe8-4764-a038-a19503d9ec3a
Search - Microsoft Bing
https://www.bing.com
Microsoft Bing
Copilot
Images
Videos
Shopping
Maps
News
Sign in
Rewards
DISCOVER
Fight Nail Fungus and Keep Your Nails Healthy
Sponsored
Watchlist suggestions
S&P 500
NASDAQ
Nasdaq 100
NVIDIA CORPORATI...
TESLA, INC.
See watchlist suggestions
Washington
54 °F
Type here to search
Describe the capabilities of Microsoft Security Soluti...
27 Minutes Remaining
Instructions
Resources
Help
100%
continue, select Continue without this data, then finally select Confirm and start browsing.
e. Enter www.bing.com in the browser address bar and confirm you're able to connect to the search engine.
f. Once you've confirmed that you can access www.bing.com, close the browser window in the VM, but leave the VM up.
7. Minimize the VM by selecting the underscore _ in the blue tab that shows the VM's IP address. This brings you back to the SC900-WinVM | Connect page.
8. Keep the browser tab open; you'll use it the next task.
Task 4
In the previous task you confirmed that you could establish an RDP connection to the VM. Once in the VM you also confirmed that you could establish an outbound connection to the Internet. The outbound Internet traffic was allowed because the default outbound rules for NSG allow outbound Internet traffic. In this task, you'll go through the process of creating a custom outbound rule to block outgoing Internet traffic and test that rule.
1. You should be on the SC900-WinVM | Connect page. From the left navigation panel, select
Previous
Next
22°C
Partly sunny
Search
ENG
US
14:52
24/04/2025


Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/dc848b8f-afe8-4764-a038-a19503d9ec3a
New tab
www.bing.com
For quick access, place your favorites here on the favorites bar. Manage favorites now
Remote Desktop Connection
Your remote session will be disconnected
Programs on the remote computer will continue to run after you have disconnected. You can reconnect to this remote session later by logging on again.
Don't display this message again
OK
Cancel
Type here to search
Describe the capabilities of Microsoft Security Soluti...
14 Minutes Remaining
Instructions
Resources
Help
100%
enter www.bing.com. The page should not display. If you're able to connect to the internet and you verified that all the parameters for the outbound rule were properly set, it's likely because it takes a few minutes for the rule to take effect. Close the browser, wait a few minutes and try again. Azure subscriptions in the lab environment may experience longer than normal delays.
7. Close the remote desktop connection, by selecting the X on the top center of the page where the IP address is shown. A pop-up window appears indicating Your remote session will be disconnected. Select OK.
8. 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.
9. Keep the Azure tab open on your browser.
Review
In this lab, you 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.
Congratulations!
37% Tasks Complete
Previous
Next
22°C
Partly sunny
Search
ENG
US
15:05
24/04/2025

Lab 3: Explore Microsoft Defender for Cloud

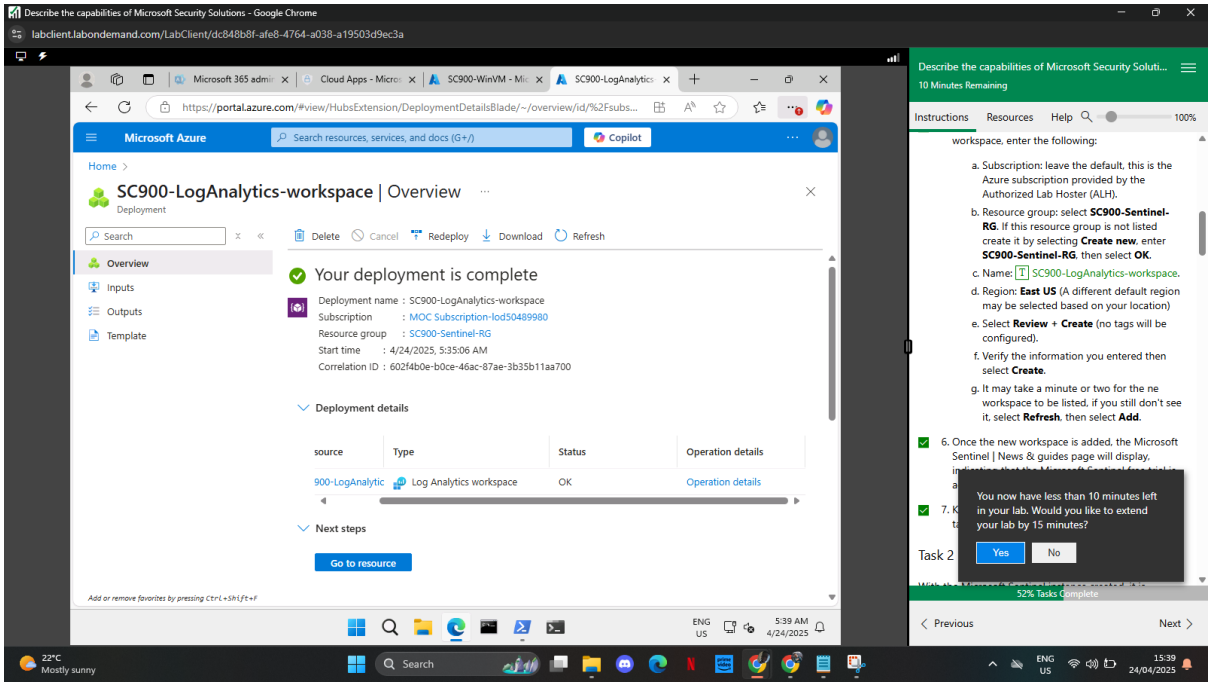
In Lab 3, I explored Microsoft Defender for Cloud, focusing on its capabilities for security posture management within Azure. I accessed the Microsoft Defender for Cloud from the Azure portal and reviewed the Overview page, which displayed information such as the number of Azure subscriptions, assessed resources, active recommendations, and security alerts. I navigated to the Inventory page to examine a virtual machine resource (sc900-winvm) and reviewed specific unhealthy status recommendations and their remediation steps. I also viewed the Recommendations tab and analyzed active recommendations by severity. Under the Regulatory compliance section, I explored compliance controls based on the Microsoft cloud security benchmark, specifically reviewing the Network Security domain (NS-10) related to DNS security. Lastly, I examined the Environment settings under Management to manage Defender plans, verifying that Cloud Security Posture Management (CSPM) was enabled and enabling the plan for Servers. This lab provided hands-on experience with monitoring and managing cloud security using Microsoft Defender for Cloud.

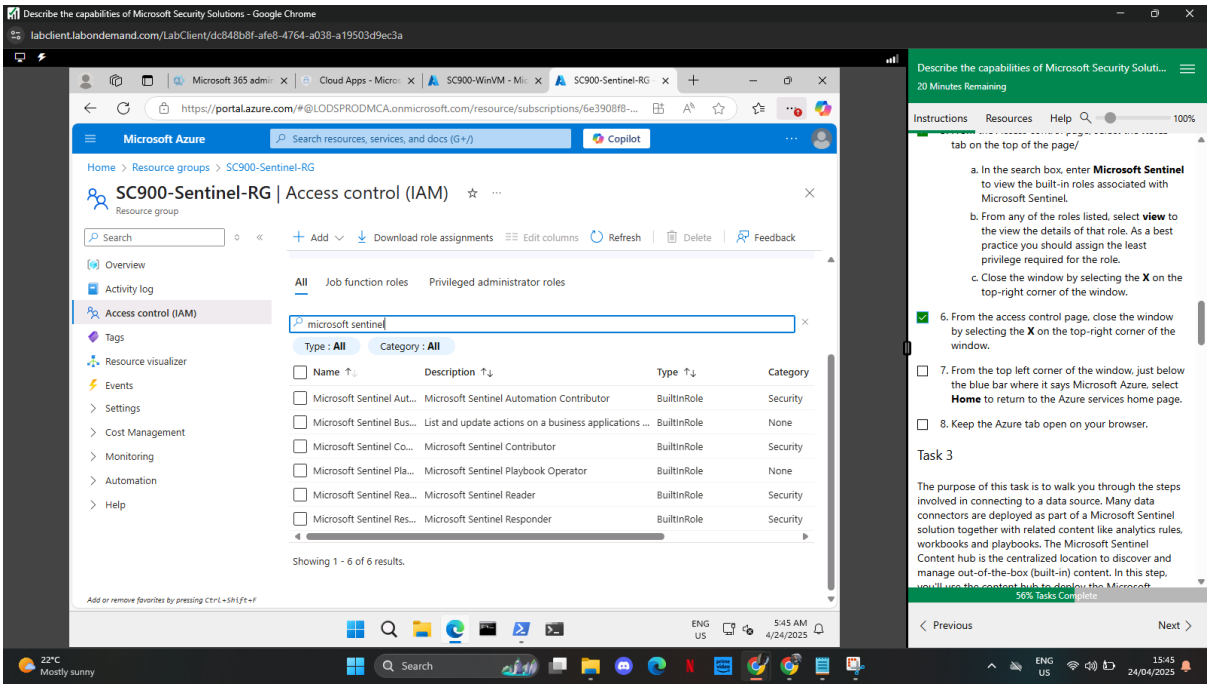


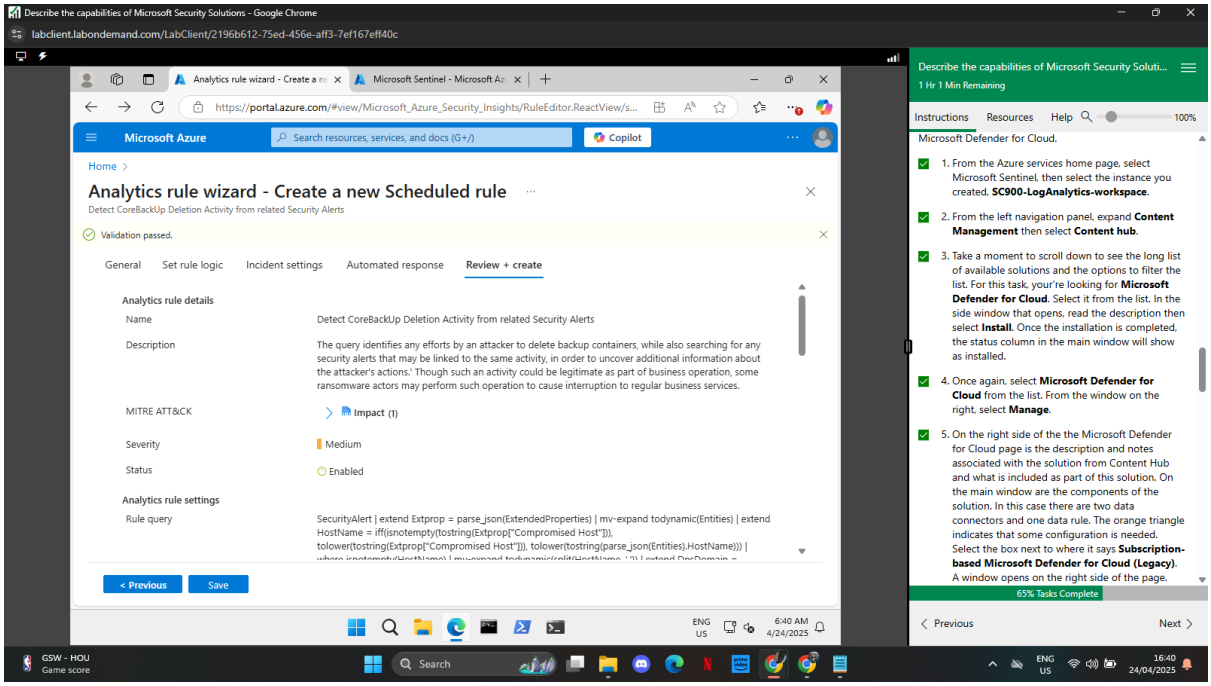


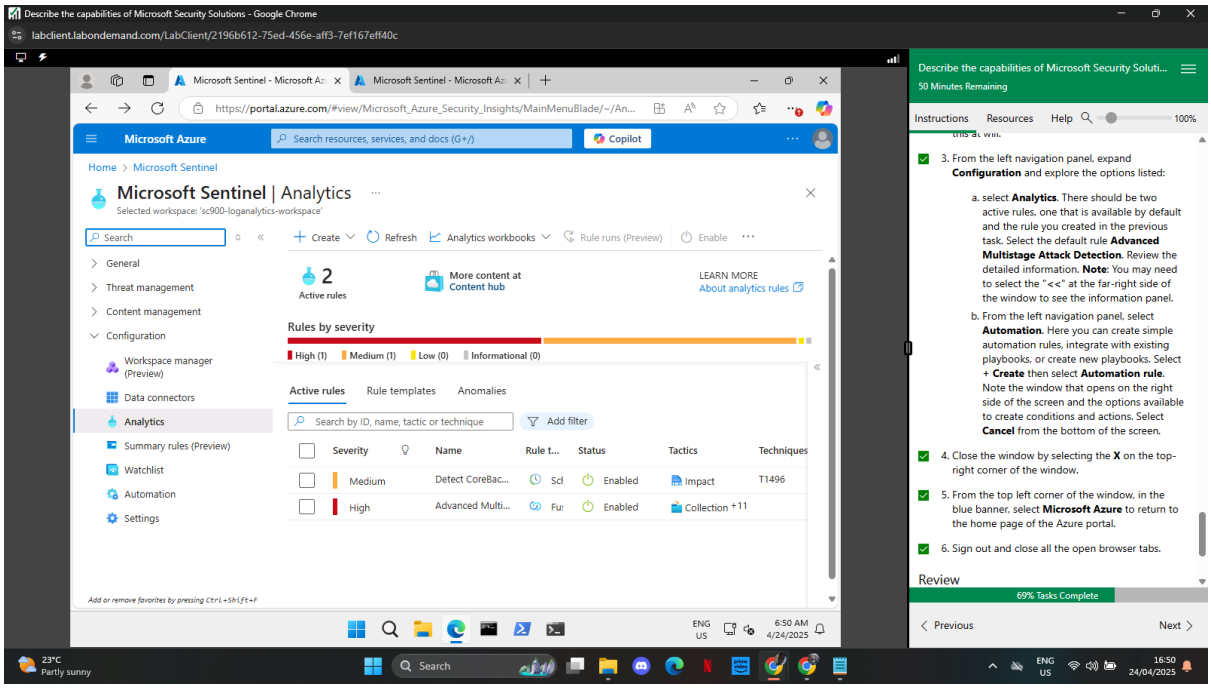
Lab 4: Explore Microsoft Sentinel

In Lab 4, I explored the capabilities of Microsoft Sentinel by first creating a Sentinel instance and setting up a Log Analytics workspace named SC900-LogAnalytics-workspace. I ensured appropriate access control by reviewing and understanding built-in Microsoft Sentinel roles and assigning them at the resource group level. Next, I connected Sentinel to a data source by deploying the Microsoft Defender for Cloud solution via the Content Hub and configured its connector and an associated analytics rule. Finally, I explored various Sentinel features, including Incidents, Hunting, Notebooks, Threat Intelligence, MITRE ATT&CK, Analytics, Automation, and the Community section, gaining hands-on experience in threat detection and security operations management within the Microsoft Sentinel environment.


Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/dc848b8f-afe8-4764-a038-a19503d9ec3a
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
SC900-LogAnalytics-workspace | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name : SC900-LogAnalytics-workspace
Subscription : MOC Subscription-lod50489980
Resource group : SC900-Sentinel-RG
Start time : 4/24/2025, 5:35:06 AM
Correlation ID : 602f4b0e-b0ce-46ac-87ae-3b35b11aa700
Deployment details
source
Type
Status
Operation details
900-LogAnalytic
Log Analytics workspace
OK
Operation details
Next steps
Go to resource
Describe the capabilities of Microsoft Security Soluti...
10 Minutes Remaining
Instructions
Resources
Help
100%
workspace, enter the following:
a. Subscription: leave the default, this is the Azure subscription provided by the Authorized Lab Hoster (ALH).
b. 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.
c. Name: SC900-LogAnalytics-workspace.
d. Region: East US (A different default region may be selected based on your location)
e. Select Review + Create (no tags will be configured).
f. Verify the information you entered then select Create.
g. It may take a minute or two for the ne workspace to be listed, if you still don't see it, select Refresh, then select Add.
6. Once the new workspace is added, the Microsoft Sentinel | News & guides page will display,
You now have less than 10 minutes left in your lab. Would you like to extend your lab by 15 minutes?
Yes
No
Task 2
52% Tasks Complete
Previous
Next
22°C
Mostly sunny
Search
ENG
US
15:39
24/04/2025

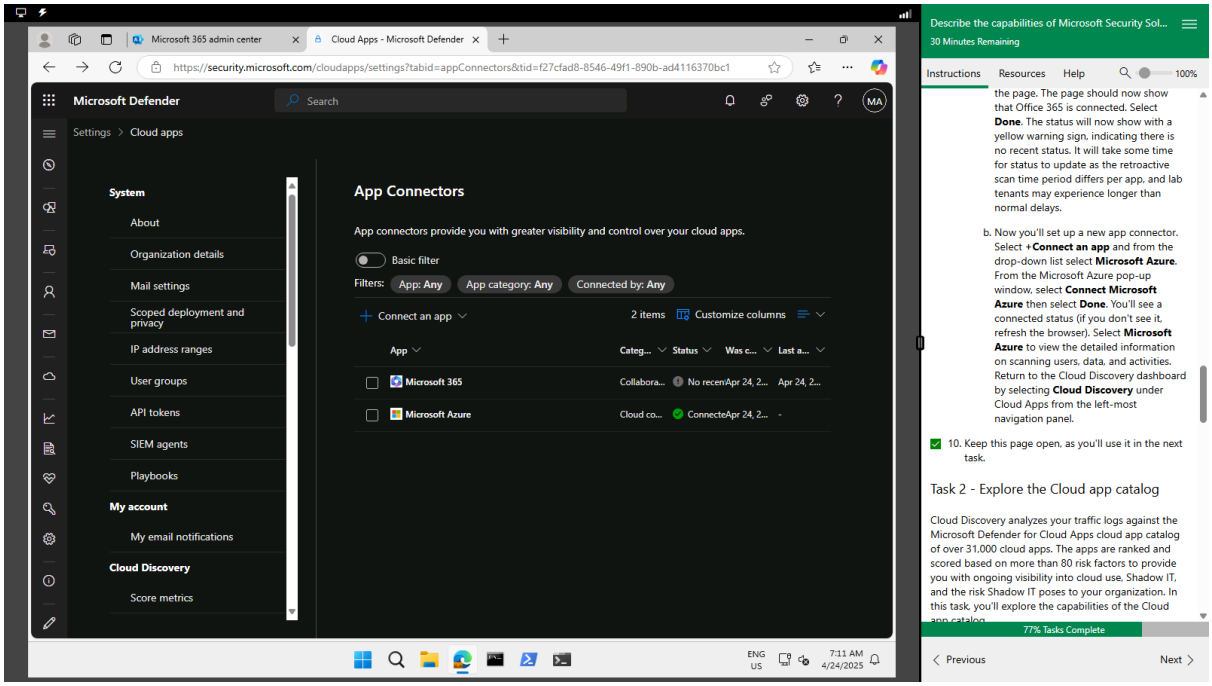

Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/dc848b8f-afe8-4764-a038-a19503d9ec3a
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Resource groups > SC900-Sentinel-RG
SC900-Sentinel-RG | Access control (IAM)
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Monitoring
Automation
Help
Add
Download role assignments
Edit columns
Refresh
Delete
Feedback
All
Job function roles
Privileged administrator roles
microsoft sentinel
Type : All
Category : All
Name
Description
Type
Category
Microsoft Sentinel Aut... Microsoft Sentinel Automation Contributor BuiltInRole Security
Microsoft Sentinel Bus... List and update actions on a business applications ... BuiltInRole None
Microsoft Sentinel Co... Microsoft Sentinel Contributor BuiltInRole Security
Microsoft Sentinel Pla... Microsoft Sentinel Playbook Operator BuiltInRole None
Microsoft Sentinel Rea... Microsoft Sentinel Reader BuiltInRole Security
Microsoft Sentinel Res... Microsoft Sentinel Responder BuiltInRole Security
Showing 1 - 6 of 6 results.
Describe the capabilities of Microsoft Security Soluti...
20 Minutes Remaining
Instructions
Resources
Help
100%
tab on the top of the page/
a. In the search box, enter Microsoft Sentinel to view the built-in roles associated with Microsoft Sentinel.
b. From any of the roles listed, select view to the view the details of that role. As a best practice you should assign the least privilege required for the role.
c. Close the window by selecting the X on the top-right corner of the window.
6. From the access control page, close the window by selecting the X on the top-right corner of the window.
7. 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.
8. 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,
56% Tasks Complete
Previous
Next
22°C
Mostly sunny
Search
ENG
US
15:45
24/04/2025

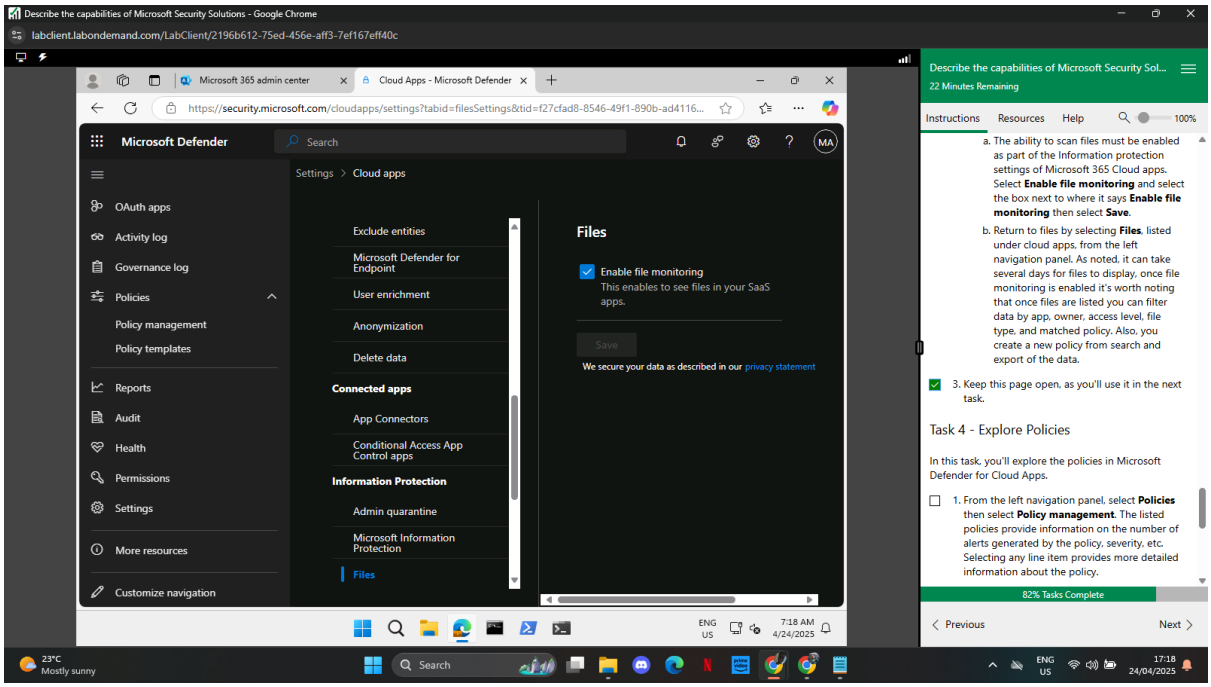

Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/2196b612-75ed-456e-aff3-7ef167eff40c
Analytics rule wizard - Create a new Scheduled rule
Detect CoreBackUp Deletion Activity from related Security Alerts
Validation passed.
General
Set rule logic
Incident settings
Automated response
Review + create
Analytics rule details
Name
Detect CoreBackUp Deletion Activity from related Security Alerts
Description
The query identifies any efforts by an attacker to delete backup containers, while also searching for any security alerts that may be linked to the same activity, in order to uncover additional information about the attacker's actions.' Though such an activity could be legitimate as part of business operation, some ransomware actors may perform such operation to cause interruption to regular business services.
MITRE ATT&CK
Impact (1)
Severity
Medium
Status
Enabled
Analytics rule settings
Rule query
SecurityAlert | extend Extprop = parse_json(ExtendedProperties) | mv-expand todynamic(Entities) | extend HostName = iff(isnotempty(tostring(Extprop["Compromised Host"])), tolower(tostring(Extprop["Compromised Host"])), tolower(tostring(parse_json(Entities).HostName))) |
< Previous
Save
Describe the capabilities of Microsoft Security Soluti...
1 Hr 1 Min Remaining
Instructions
Resources
Help
100%
Microsoft Defender for Cloud.
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, your'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 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.
65% Tasks Complete
Previous
Next

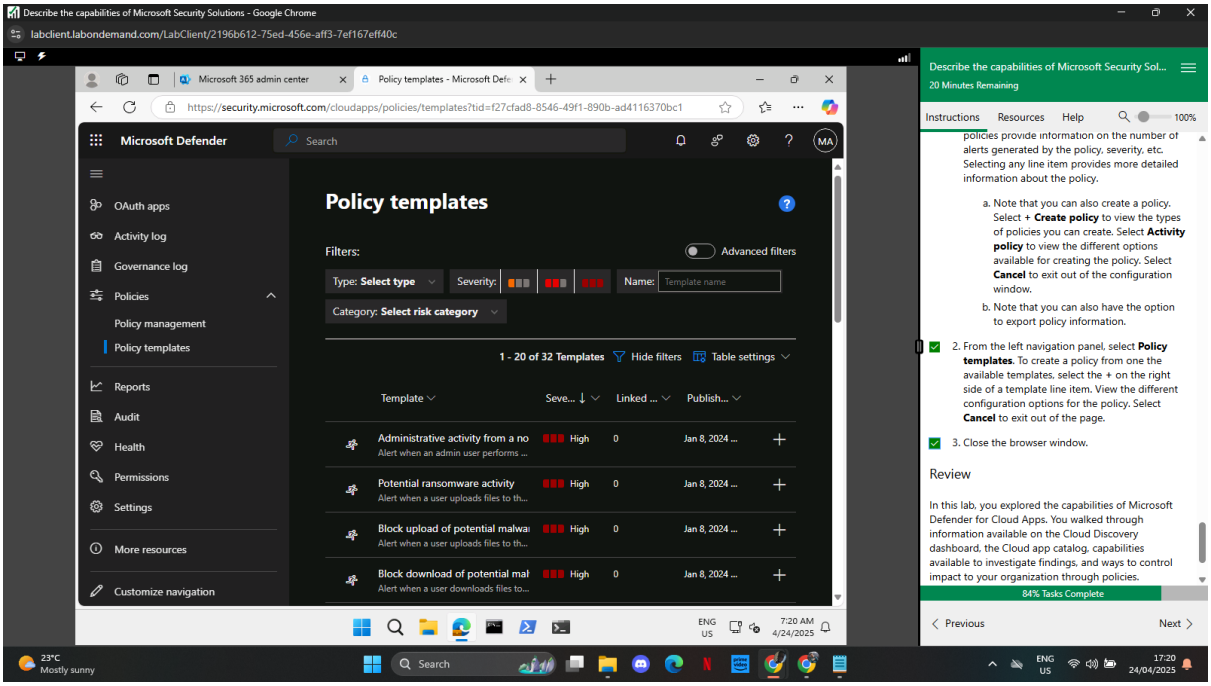

Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/2196b612-75ed-456e-aff3-7ef167eff40c
Microsoft Sentinel | Analytics
Selected workspace: 'sc900-loganalytics-workspace'
Create
Refresh
Analytics workbooks
Rule runs (Preview)
Enable
General
Threat management
Content management
Configuration
Workspace manager (Preview)
Data connectors
Analytics
Summary rules (Preview)
Watchlist
Automation
Settings
2
Active rules
More content at Content hub
LEARN MORE
About analytics rules
Rules by severity
High (1)
Medium (1)
Low (0)
Informational (0)
Active rules
Rule templates
Anomalies
Search by ID, name, tactic or technique
Add filter
Severity
Name
Rule t...
Status
Tactics
Techniques
Medium
Detect CoreBac...
Scl
Enabled
Impact
T1496
High
Advanced Multi...
Fu:
Enabled
Collection +11
Add or remove favorites by pressing Ctrl+Shift+F
Describe the capabilities of Microsoft Security Soluti...
50 Minutes Remaining
Instructions
Resources
Help
100%
3. From the left navigation panel, expand Configuration and explore the options listed:
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.
6. Sign out and close all the open browser tabs.
Review
69% Tasks Complete
Previous
Next

Lab 5: Explore Microsoft Defender for Cloud Apps

In this lab, I explored the capabilities of Microsoft Defender for Cloud Apps. I navigated the Cloud Discovery dashboard to view detailed information about discovered apps, IP addresses, and users, as well as options for uploading snapshot traffic reports and configuring automatic uploads. I examined app connectors, including how to connect Microsoft Azure and Office 365, and reviewed data visibility provided through connected apps. I also explored the Cloud app catalog, using filters like compliance risk factor and category to assess app risk and suitability. In the Activity log and Files sections, I learned how to investigate app activity and enable file monitoring for enhanced data protection. Finally, I examined policy management and templates, including how to create and configure policies to help control cloud app usage and mitigate risk.

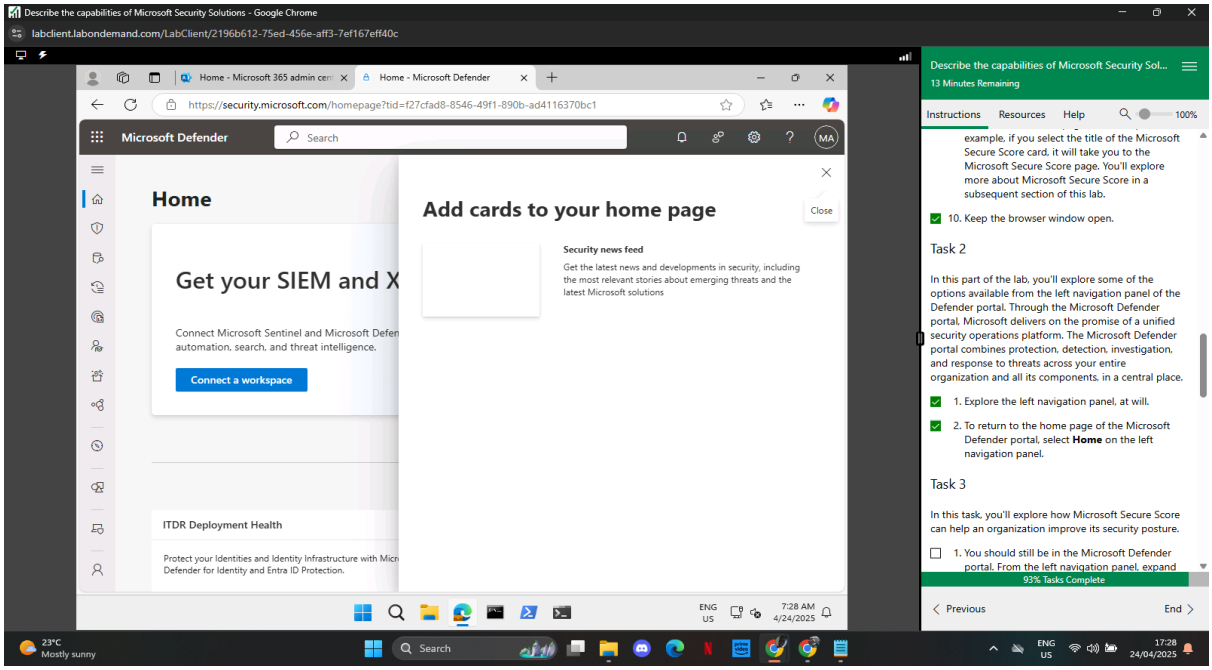


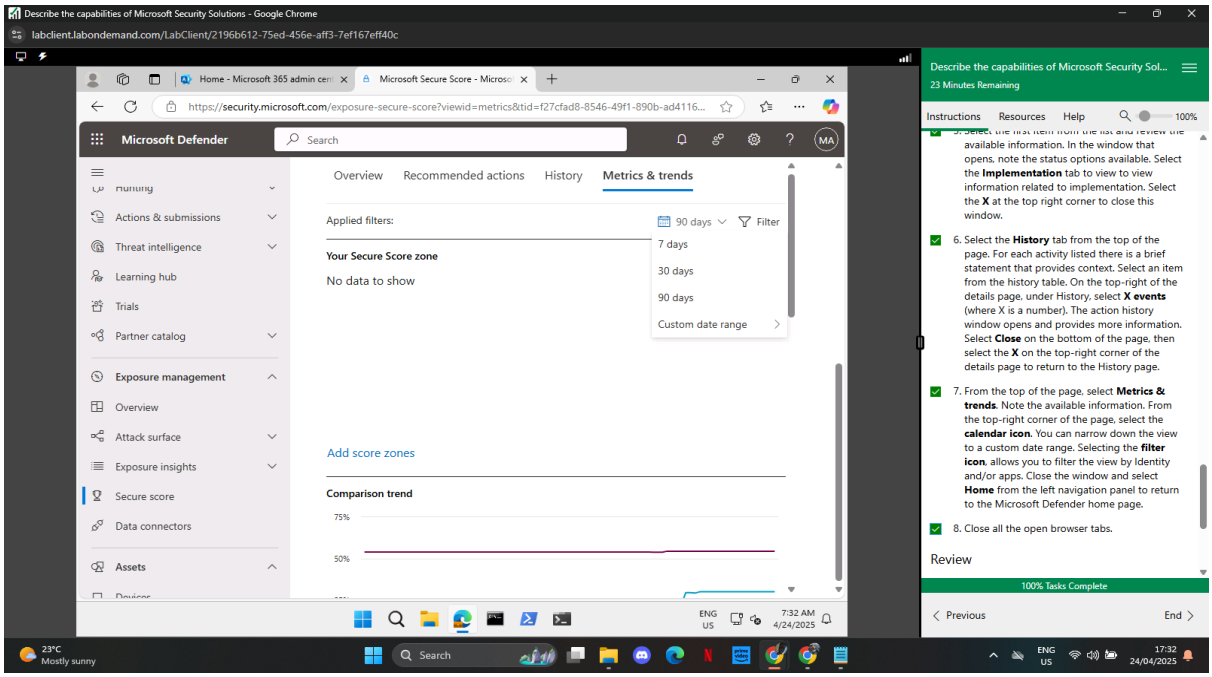

Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/2196b612-75ed-456e-aff3-7ef167eff40c
Microsoft 365 admin center
Cloud Apps - Microsoft Defender
https://security.microsoft.com/cloudapps/settings?tabid=filesSettings&tid=f27cfad8-8546-49f1-890b-ad4116...
Microsoft Defender
Search
Settings > Cloud apps
OAuth apps
Activity log
Governance log
Policies
Policy management
Policy templates
Reports
Audit
Health
Permissions
Settings
More resources
Customize navigation
Exclude entities
Microsoft Defender for Endpoint
User enrichment
Anonymization
Delete data
Connected apps
App Connectors
Conditional Access App Control apps
Information Protection
Admin quarantine
Microsoft Information Protection
Files
Files
Enable file monitoring
This enables to see files in your SaaS apps.
Save
We secure your data as described in our privacy statement
Describe the capabilities of Microsoft Security Sol...
22 Minutes Remaining
Instructions
Resources
Help
100%
a. The ability to scan files must be enabled as part of the Information protection settings of Microsoft 365 Cloud apps. Select Enable file monitoring and select the box next to where it says Enable file monitoring then select Save.
b. Return to files by selecting Files, listed under cloud apps, from the left navigation panel. As noted, it can take several days for files to display, once file monitoring is enabled it's worth noting that once files are listed you can filter data by app, owner, access level, file type, and matched policy. Also, you create a new policy from search and export of the data.
3. Keep this page open, as you'll use it in the next task.
Task 4 - Explore Policies
In this task, you'll explore the policies in Microsoft Defender for Cloud Apps.
1. From the left navigation panel, select Policies then select Policy management. The listed policies provide information on the number of alerts generated by the policy, severity, etc. Selecting any line item provides more detailed information about the policy.
82% Tasks Complete
Previous
Next
23°C
Mostly sunny
Search
ENG
US
7:18 AM
4/24/2025
17:18
24/04/2025


Describe the capabilities of Microsoft Security Solutions - Google Chrome
labclient.labondemand.com/LabClient/2196b612-75ed-456e-aff3-7ef167eff40c
Microsoft 365 admin center
Policy templates - Microsoft Defe
https://security.microsoft.com/cloudapps/policies/templates?tid=f27cfad8-8546-49f1-890b-ad4116370bc1
Microsoft Defender
Search
OAuth apps
Activity log
Governance log
Policies
Policy management
Policy templates
Reports
Audit
Health
Permissions
Settings
More resources
Customize navigation
Policy templates
Filters:
Advanced filters
Type: Select type
Severity:
Name:
Template name
Category: Select risk category
1 - 20 of 32 Templates
Hide filters
Table settings
Template
Seve...
Linked ...
Publish...
Administrative activity from a no
Alert when an admin user performs ...
High
0
Jan 8, 2024 ...
Potential ransomware activity
Alert when a user uploads files to th...
High
0
Jan 8, 2024 ...
Block upload of potential malwa
Alert when a user uploads files to th...
High
0
Jan 8, 2024 ...
Block download of potential mal
Alert when a user downloads files to...
High
0
Jan 8, 2024 ...
Describe the capabilities of Microsoft Security Sol...
20 Minutes Remaining
Instructions
Resources
Help
100%
policies provide information on the number of alerts generated by the policy, severity, etc. Selecting any line item provides more detailed information about the policy.
a. Note that you can also create a policy. Select + Create policy to view the types of policies you can create. Select Activity policy to view the different options available for creating the policy. Select Cancel to exit out of the configuration window.
b. Note that you can also have the option to export policy information.
2. From the left navigation panel, select Policy templates. To create a policy from one the available templates, select the + on the right side of a template line item. View the different configuration options for the policy. Select Cancel to exit out of the page.
3. Close the browser window.
Review
In this lab, you explored the capabilities of Microsoft Defender for Cloud Apps. You walked through information available on the Cloud Discovery dashboard, the Cloud app catalog, capabilities available to investigate findings, and ways to control impact to your organization through policies.
84% Tasks Complete
Previous
Next
23°C
Mostly sunny
Search
ENG
US
7:20 AM
4/24/2025
17:20
24/04/2025

Lab 6: Explore the Microsoft Defender portal

In Lab 6, I explored the Microsoft Defender portal by first examining the landing page and its customizable card layout. I learned how to add, remove, and rearrange cards based on my preferences as a global admin. I then navigated through the options on the left panel, which provided centralized access to Microsoft's Extended Detection and Response (XDR) solutions like Defender for Endpoints and Defender for Office 365. Lastly, I explored the Microsoft Secure Score feature, which evaluates an organization's security posture and provides actionable recommendations to improve it. I reviewed score breakdowns, implementation steps, historical data, and metrics and trends, gaining insights into how Secure Score can guide security improvements.





Conclusion

Completing these six labs offered a practical and holistic understanding of Microsoft's cloud security landscape. I gained hands-on experience with tools that support governance, risk mitigation, and advanced threat detection. The labs demonstrated how to effectively monitor and manage user activity, secure network traffic, enforce policy compliance, and proactively respond to security threats using Microsoft 365 Defender, Defender for Cloud, Sentinel, and related portals. These exercises not only strengthened my technical skills but also emphasized the importance of an integrated, layered security approach in today’s cloud-first environments.