Azure Security Center Compliance Lab Instructions

1. Lab Overview

This lab guides you through using Microsoft Defender for Cloud to assess and remediate the security posture of a virtual machine (VM) in Azure. You will deploy a Windows Server VM, configure its network security, enable Defender for Cloud, review security recommendations, and take remediation steps to improve its secure score.

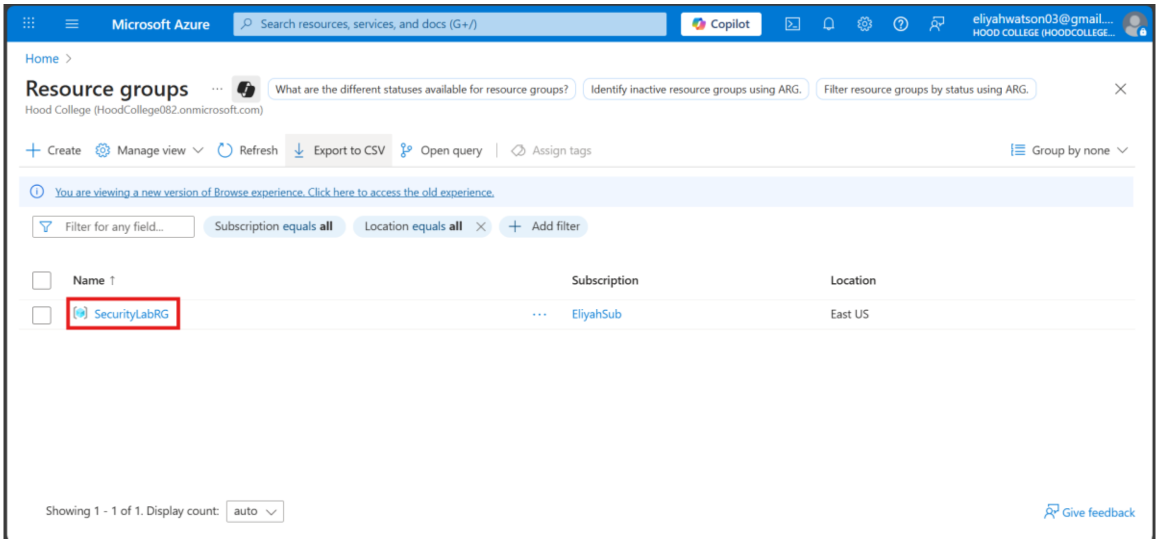
2. Prerequisites

Ensure you have the following before starting:

- An active Azure subscription (Pay-As-You-Go with free tier access)
- An active storage account
- Contributor or Owner permissions on the subscription
- -Optional: Familiarity with Azure Portal or Azure CLI

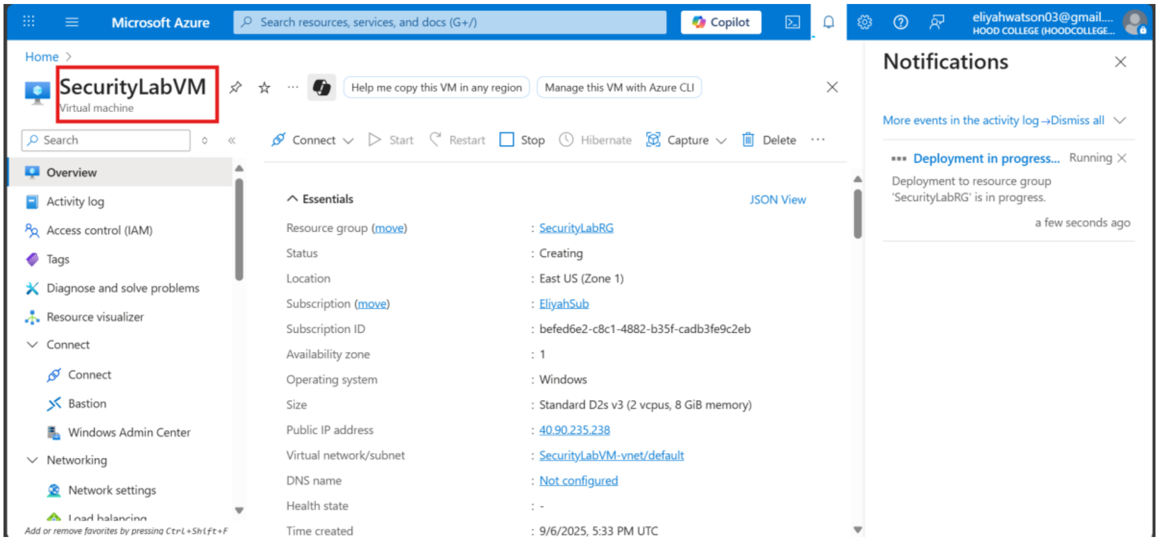
3. Step-by-Step Instructions

1. Create a Resource Group:
   - Navigate to Azure Portal > Resource Groups > Create.
   - Name: 'SecurityLabRG', Region: your preferred region.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
eliyahwatson03@gmail....
HOOD COLLEGE (HOODCOLLEGE...
Home >
Resource groups
Hood College (HoodCollege082.onmicrosoft.com)
What are the different statuses available for resource groups?
Identify inactive resource groups using ARG.
Filter resource groups by status using ARG.
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Group by none
You are viewing a new version of Browse experience. Click here to access the old experience.
Filter for any field...
Subscription equals all
Location equals all
Add filter
Showing 1 - 1 of 1. Display count: auto
Give feedback

Name ↑	Subscription	Location
SecurityLabRG	EliyahSub	East US

2. Deploy a VM:
   - Go to Azure Portal > Virtual Machines > Create.
   - Name: 'SecurityLabVM', Size: B1s, Image: Windows Server 2025.
   - Set administrator account's username and password.
   - Use default settings for disk and networking.



SecurityLabVM
Virtual machine

Essentials

Resource group (move) : SecurityLabRG
Status : Creating
Location : East US (Zone 1)
Subscription (move) : EliyahSub
Subscription ID : befed6e2-c8c1-4882-b35f-cadb3fe9c2eb
Availability zone : 1
Operating system : Windows
Size : Standard D2s v3 (2 vcpus, 8 GiB memory)
Public IP address : 40.90.235.238
Virtual network/subnet : SecurityLabVM-vnet/default
DNS name : Not configured
Health state : -
Time created : 9/6/2025, 5:33 PM UTC

Notifications

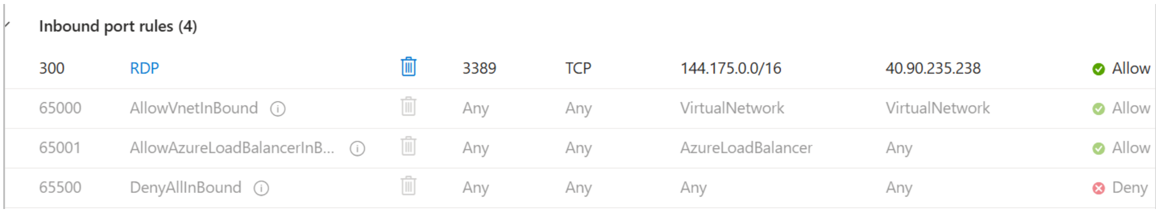
More events in the activity log → Dismiss all

Deployment in progress... Running

Deployment to resource group 'SecurityLabRG' is in progress.

a few seconds ago

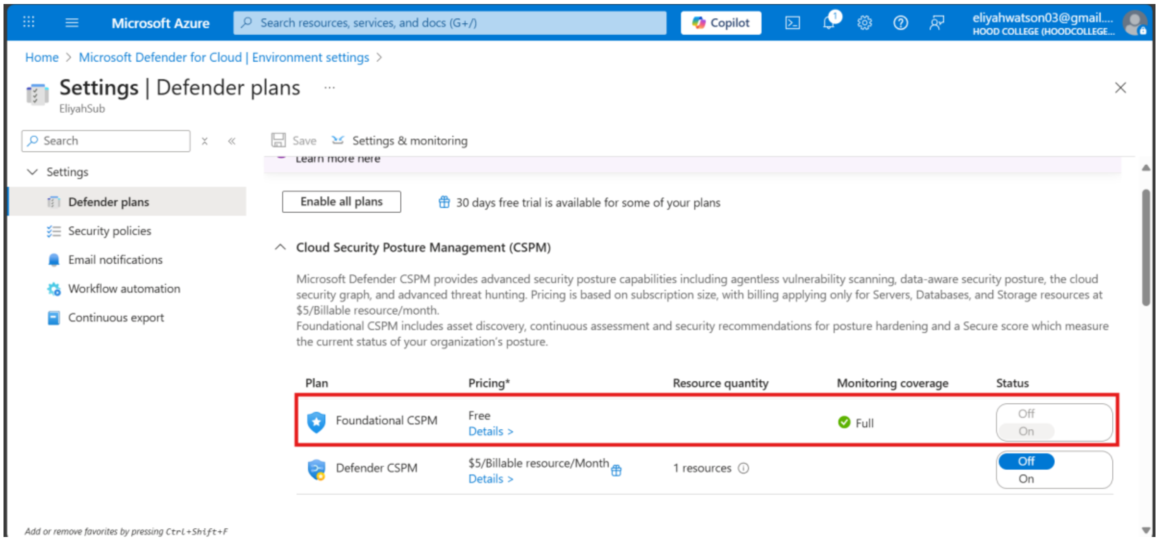
3. Configure NSG:
   - Go to your VM > Networking > Network settings.
   - Edit the Network Security Group attached to the VM.
   - Allow inbound RDP (port 3389) only from your public IP address.



Inbound port rules (4)

300	RDP	3389	TCP	144.175.0.0/16	40.90.235.238	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

4. Enable Defender for Cloud:
   - Go to Microsoft Defender for Cloud > Environment Settings.
   - Select your subscription and enable Cloud Security Posture Management (CSPM).



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
eliyahwatson03@gmail....
HOOD COLLEGE (HOODCOLLEGE...

Home > Microsoft Defender for Cloud | Environment settings >

Settings | Defender plans

EliyahSub

30 days free trial is available for some of your plans

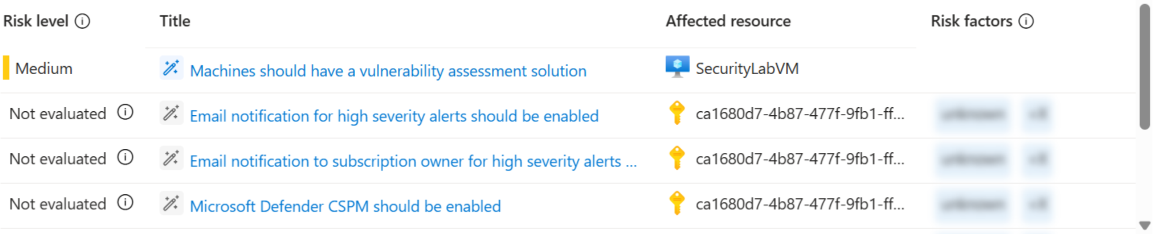
Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at $5/Billable resource/month.
Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

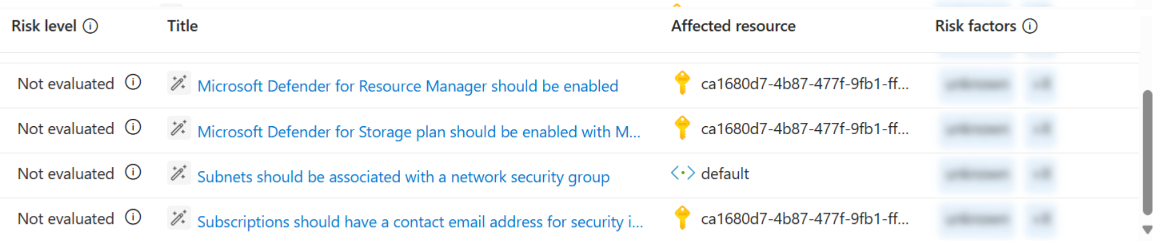
Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free Details >		Full	Off On
Defender CSPM	$5/Billable resource/Month Details >	1 resources		Off On

Add or remove favorites by pressing Ctrl+Shift+F

5. Review Security Recommendations:
   - In Defender for Cloud, navigate to Recommendations.
   - Review issues related to guest configuration, diagnostics, and NSG rules.

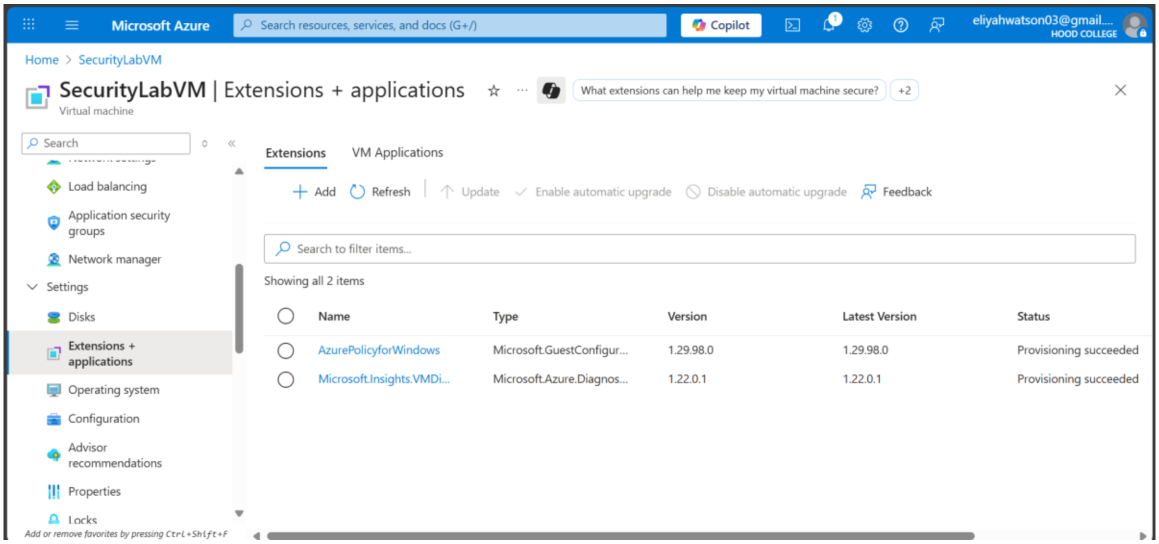


Risk level	Title	Affected resource	Risk factors
Medium	Machines should have a vulnerability assessment solution	SecurityLabVM	
Not evaluated	Email notification for high severity alerts should be enabled	ca1680d7-4b87-477f-9fb1-ff...	[redacted]
Not evaluated	Email notification to subscription owner for high severity alerts ...	ca1680d7-4b87-477f-9fb1-ff...	[redacted]
Not evaluated	Microsoft Defender CSPM should be enabled	ca1680d7-4b87-477f-9fb1-ff...	[redacted]



Risk level	Title	Affected resource	Risk factors
Not evaluated	Microsoft Defender for Resource Manager should be enabled	ca1680d7-4b87-477f-9fb1-ff...	[redacted]
Not evaluated	Microsoft Defender for Storage plan should be enabled with M...	ca1680d7-4b87-477f-9fb1-ff...	[redacted]
Not evaluated	Subnets should be associated with a network security group	default	[redacted]
Not evaluated	Subscriptions should have a contact email address for security i...	ca1680d7-4b87-477f-9fb1-ff...	[redacted]

6. Remediate Issues:
   - Enable Azure Machine configuration extension for Windows Extension on the VM.



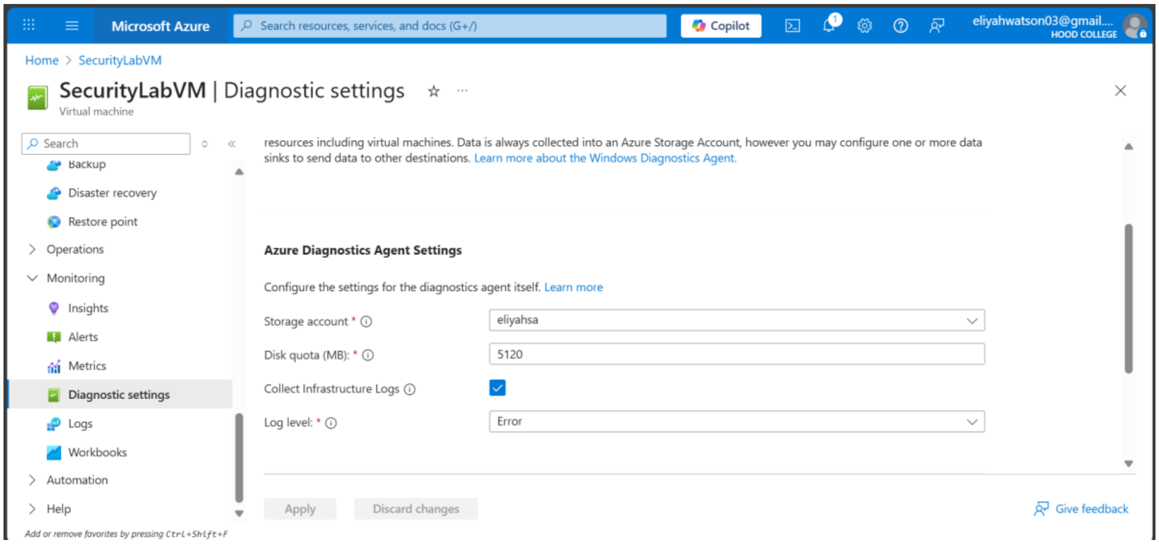
SecurityLabVM | Extensions + applications

Virtual machine

Showing all 2 items

Name	Type	Version	Latest Version	Status
AzurePolicyforWindows	Microsoft.GuestConfigur...	1.29.98.0	1.29.98.0	Provisioning succeeded
Microsoft.Insights.VMDi...	Microsoft.Azure.Diagnos...	1.22.0.1	1.22.0.1	Provisioning succeeded

- Enable diagnostic settings for logging.



SecurityLabVM | Diagnostic settings

Virtual machine

resources including virtual machines. Data is always collected into an Azure Storage Account, however you may configure one or more data sinks to send data to other destinations. Learn more about the Windows Diagnostics Agent.

Azure Diagnostics Agent Settings

Configure the settings for the diagnostics agent itself. Learn more

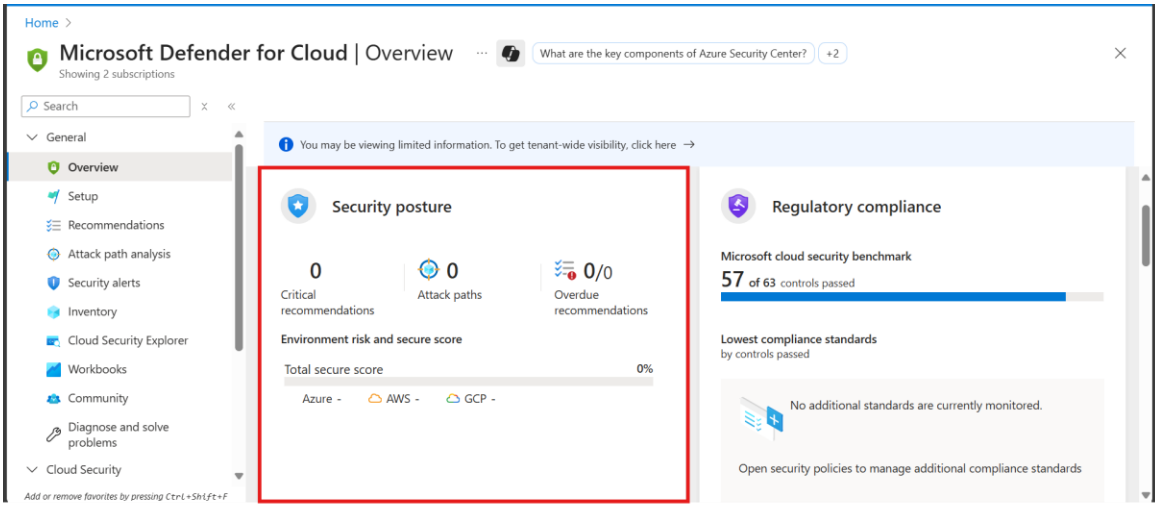
Storage account * : eliyahsa

Disk quota (MB): * : 5120

Collect Infrastructure Logs: ☑

Log level: * : Error

7. See Secure Score



Microsoft Defender for Cloud | Overview

Showing 2 subscriptions

You may be viewing limited information. To get tenant-wide visibility, click here →

Security posture

0 Critical recommendations

0 Attack paths

0/0 Overdue recommendations

Environment risk and secure score

Total secure score 0%

Azure - AWS - GCP -

Regulatory compliance

Microsoft cloud security benchmark

57 of 63 controls passed

Lowest compliance standards by controls passed

No additional standards are currently monitored.

Open security policies to manage additional compliance standards

4. Lessons Learned

- Secure Deployment Matters: I successfully deployed a virtual machine in Azure using hardened NSG rules, diagnostic logging, and Guest Configuration — all within the free-tier limits.
- Defender for Cloud Is Powerful (and Tricky): I learned how to navigate Microsoft Defender for Cloud’s posture tools, distinguish between free and paid features, and avoid surprise charges while still improving security.
- Secure Score Isn’t Everything: A low or zero Secure Score doesn’t always mean poor security — it can reflect pending evaluations or missing premium features. I learned to interpret posture data critically and document real remediation steps.
- Cost Awareness Is a Skill: Avoiding paid Defender plans while still achieving compliance goals taught me how to balance security with budget constraints — a key skill for any IT professional.
- Documentation Is Key: I captured before/after screenshots, summarized remediation actions, and built a clear lab narrative that reflects both technical execution and strategic decision-making.