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.

A screenshot of a computer

AI-generated content may be incorrect.

1. 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.

A screenshot of a computer

AI-generated content may be incorrect.

1. 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.

A white background with black text

AI-generated content may be incorrect.

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

A screenshot of a computer

AI-generated content may be incorrect.

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

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

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

A screenshot of a computer

AI-generated content may be incorrect.

- Enable diagnostic settings for logging.

A screenshot of a computer

AI-generated content may be incorrect.

- Tighten NSG rules to reduce exposure.

1. Export Secure Score or Compliance Report:  
    - In Defender for Cloud, go to Secure Score.  
    - Use the Export option to download the report.

# 4. Screenshots

Include the following screenshots in your final report:

A screenshot of a computer

AI-generated content may be incorrect.

* NSG Configuration
* Defender for Cloud Recommendations
* VM Overview Page

# 5. 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.