Azure Security Center

What is Azure Security Center?

- Azure Security Center (now part of Microsoft Defender for Cloud) is a unified security management system that:

- Protects Azure, hybrid, and on-premises workloads.

- Detects threats with AI-driven security analytics.

- Provides security recommendations to improve compliance and protection.

Key Features of Azure Security Center

1 Secure Score (Security Posture Management)

- Provides a numerical score for your security posture.
- Recommends actions to enhance security, such as enabling MFA, limiting network access.

- Example: Check Secure Score in Azure CLI
  az security secure-score list --output table

2 Threat Protection & Alerts

- Microsoft Defender XDR detects cyber threats in real time.
- Alerts for suspicious activities, such as brute-force attacks or unauthorized changes to the firewall.

- Example: View Security Alerts
  az security alert list --output table

Key Features of Azure Security Center

3 Compliance & Regulatory Standards

- PCI-DSS, ISO 27001, and Azure CIS Benchmarks compliance.
- Detects misconfigurations in NSGs, storage, and identity settings.

Example: Check Compliance Assessment in CLI

az security regulatory-compliance-standards list --output table

4 Just-in-Time (JIT) VM Access

- Reduces attack surface by allowing VM access only when required.
- Prevents unnecessary open RDP & SSH ports.

Example: Enable JIT Access for a VM

```
az security jit-policy update \
    --name MyVM \
    --resource-group SecurityRG \
    --add properties.virtualMachines
name=MyVM ports=22,3389
```

5 Adaptive Application Controls

- Uses AI to create allow-lists for applications.
- Blocks unauthorized malware or ransomware execution.

Example: Create an Adaptive Application Control Policy:

az security adaptive-application-controls list

Hands-On Scenario: Enhancing Security in Azure Security Center

Scenario: A company aims to enhance the security posture for its Azure environment by:

1️⃣ Activating Microsoft Defender for Cloud.
2️⃣ Enabling Just-in-Time (JIT) VM Access.
3️⃣ Setting up Threat Protection for Azure Storage.

Solution Steps:

✅ 1. Enable Microsoft Defender for Cloud

```
az security pricing create \
    --name VirtualMachines \
    --tier Standard
```

✅ 2. Restrict VM Access with Just-in-Time (JIT)

```
az security jit-policy update
--name WebServerVM \
    --resource-group SecurityRG \
    --add properties.virtualMachines name=WebServerVM
ports=22
```

✅3. Storage Threat Protection

```
az security setting update \
    --name "AzureStorage" \
    --enabled true
```

Comparison: Azure Security Center vs Other Cloud Security Services

Feature	Azure Security Center	AWS Security Hub	GCP Security Command Center
Threat Detection	✅ Yes	✅ Yes	✅ Yes
Regulatory Compliance	✅ PCI, ISO, CIS	✅ CIS, GDPR	✅ CIS, GDPR
Just-in-Time VM Access	✅ Yes	❌ No	❌ No
AI-Based Threat Prevention	✅ Yes	❌ Limited AI	✅ Yes