SC-5002: Secure Azure Services and Workloads with Microsoft Defender for Cloud

In today's cloud-first world, securing Azure services and workloads is essential to maintaining regulatory compliance and protecting sensitive data. Microsoft Defender for Cloud provides a unified security management system that helps organizations strengthen their security posture across hybrid and multi-cloud environments.

Key framing question: "How can you proactively secure your cloud workloads and meet compliance requirements with confidence?"

0. Introduction

- Welcome and agenda.
- Why Copilot Studio matters: extending Microsoft Copilot with custom AI agents.
- Framing question: "What if your business processes could talk back and take action?"

1. Examine Defender for Cloud regulatory compliance standards

- Learn how to use compliance dashboard and recommendations to improve posture.
- Explore compliance standards and how to assess your Azure environment against them.
- Understand how Microsoft Defender for Cloud maps to regulatory compliance frameworks.

2. Enable Defender for Cloud on your Azure subscription

- Understand pricing tiers and feature availability.
- Configure environment settings and auto-provisioning of agents.
- Enable Microsoft Defender for Cloud across subscriptions and management groups.

3. Create a Log Analytics workspace

- Connect resources to the workspace for centralized logging.
- Create and configure a workspace to collect and analyze security data.
- Learn the role of Log Analytics in Defender for Cloud monitoring.

4. Collect guest operating system monitoring data from Azure and hybrid virtual machines using Azure Monitor Agent

- Collect guest OS telemetry for security and performance insights.
- Deploy and configure the agent on Azure and hybrid VMs.
- Understand the Azure Monitor Agent and its capabilities.

5. Explore just-in-time virtual machine access

- Monitor and audit JIT access requests and approvals.
- Configure JIT policies in Defender for Cloud.
- Learn how JIT VM access reduces exposure to brute-force attacks.

6. Closing and Q&A

- Recap of modules and key concepts.
- Open Q&A session with instructor.
- Final thoughts on Securing Azure workloads and services with Microsoft Defender for Cloud.