SC-5009: Secure AI Solutions in the Cloud using Microsoft Defender for Cloud and Microsoft Entra

Course Overview

This course explores how to secure AI workloads in Azure using Microsoft Defender for Cloud and Microsoft Entra. It covers AI security risks, governance strategies, identity architecture, and access controls required to protect modern AI solutions. Learners will gain practical knowledge to implement guardrails, secure environments, and manage identities for AI workloads.

Prerequisites

- Basic understanding of Azure services
- Familiarity with AI/ML workloads in cloud environments
- Foundational knowledge of security concepts (identity, access control, networking)

Learning Path 1: Protect Microsoft Foundry Solutions using Microsoft Defender for Cloud

Module 1: Introduction to AI Security in Azure

- Introduction to AI services in Azure
- Understanding AI security risks
- AI guardrails and protections
- Azure security and governance tools for AI workloads

Module 2: Protect AI Workloads with Microsoft Defender for Cloud

- Overview of AI workload protection
- Enable AI workloads protection plan
- Data & AI security dashboard insights
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection (CWP)
- Incident investigation using Defender XDR

Module 3: Configure and Manage Guardrails in Microsoft Foundry

- Introduction to guardrails and content safety
- Safety controls in Microsoft Foundry
- Built-in guardrails and testing
- Create and manage blocklists
- Configure and apply guardrails
- Optimize and refine guardrails

Module 4: Secure Microsoft Foundry Environments

- Access control with Microsoft Entra ID
- Role-based access within Foundry projects
- Secure secrets using Azure Key Vault
- Network isolation (VNet and Private Link)
- Diagnostic logging and monitoring

Learning Path 2: Secure AI Identity Infrastructure using Microsoft Entra

Module 5: Identity Architecture for AI Workloads

- Identity as a control layer
- Management vs data plane access
- Authentication flows for AI endpoints
- Human vs workload identities
- Role assignments and scope
- Common identity misconfigurations

Module 6: Implement Access Management for Azure Resources

- Azure role-based access control (RBAC)
- Custom roles configuration
- Managed identities (creation & usage)
- Access Azure resources securely
- Azure Key Vault RBAC policies

Module 7: Plan, Implement, and Administer Conditional Access

- Security defaults planning
- Conditional Access policy design
- Policy implementation and assignments
- Testing and troubleshooting
- Application controls
- Session management & continuous access evaluation
- Conditional Access Optimization agent

Module 8: Manage Microsoft Entra Identity Protection

- Identity protection fundamentals
- User risk and sign-in risk policies
- MFA registration policies
- Monitoring and remediation of risky users
- Security for workload identities
- Microsoft Defender for Identity overview
- Identity Risk Management agent