SC-5009-A: Secure AI solutions in the cloud using Microsoft Defender for Cloud and Microsoft Entra

Length: 1 day

Level: Intermediate

Course Overview

About this course

Secure AI solutions in the cloud by configuring AI workloads, applying cloud-native protections, and reinforcing security outcomes with identity controls. Learn how AI workloads authenticate, how trust boundaries are established, and how security posture and workload protection reduce risk using Microsoft Defender for Cloud and Microsoft Foundry. Extend these protections by using Microsoft Entra to design and apply identity and access controls that explain and harden earlier security decisions. Learning outcomes:

- Apply security posture management and workload protection for AI services using Microsoft Defender for Cloud
- Configure and secure Microsoft Foundry environments using cloud-native security controls
- Design and apply identity and access controls for AI workloads using Microsoft Entra

Audience Profile

This course is intended for professionals responsible for securing and operating AI workloads in the cloud. The audience includes cloud security engineers, platform engineers, and application teams working with AI services who need to understand how workload protection, security posture, and identity controls apply to AI environments. Familiarity with Azure, cloud-native security concepts, and basic identity and access principles is recommended.

Course Details

Learning Path 1: Protect Microsoft Foundry solutions by using Microsoft Defender for Cloud

As AI workloads become central to business operations, they introduce new security challenges that traditional cloud tools don't fully address.

In this learning path, you learn how to:

- Understand AI workload risks and how Microsoft Defender for Cloud identifies and protects AI assets
- Enable the AI Workloads plan and use Cloud Security Posture Management (CSPM) to discover and remediate misconfigurations
- Use Cloud Workload Protection (CWP) to detect runtime threats targeting AI components
- Investigate AI security alerts in Microsoft Defender XDR
- Configure and manage guardrails in Microsoft Foundry to prevent unsafe or policy-violating model behavior

Prerequisite

- Experience managing Azure subscriptions, workloads, and Defender for Cloud plans
- Familiarity with Microsoft Foundry and how AI workloads are deployed in Azure
- Understanding of basic cloud security principles, including posture management, access control, and incident investigation

Units

- Introduction
- Understand AI services in Azure
- Understand AI security risks in Azure
- AI guardrails and protections in Azure
- How Azure security and governance tools support AI workloads
- Module Assessment
- Summary

Learning Path 2: Secure AI identity infrastructure with Microsoft Entra

Learn how to secure identities used by AI workloads in Azure. Understand workload identity architecture, configure access to Azure resources, apply Conditional Access policies, and investigate identity risk by using Microsoft Entra.

Prerequisite

- Experience with Microsoft Entra ID fundamentals
- Familiarity with Azure role-based access control (RBAC)
- Basic understanding of Azure subscriptions, resource groups, and resources
- General understanding of identity and access management concepts

Units

- Introduction
- Identity as the control layer for AI solutions
- Management plane and data plane access in AI workloads
- Authentication flows for AI endpoints in Microsoft Foundry
- Human and workload identities in AI workloads
- Role assignments and scope in AI environments
- Common identity misconfigurations in AI deployments
- Module Assessment
- Summary