

MICROSOFT OFFICIAL CURRICULUM

Secure AI solutions in the cloud using Microsoft Defender for Cloud and Microsoft Entra

Official Microsoft Learn-aligned instructor-led program for Secure AI solutions in the cloud using Microsoft Defender for Cloud and Microsoft Entra.

Microsoft

SC-5009

DURATION

1 day

LEVEL

Intermediate

FORMAT

Virtual, On-site, or Hybrid

CERTIFICATION

SC-5009

AUDIENCE PROFILE

Built for these roles

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.

OVERVIEW

Executive overview

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

[View official source](#)

READINESS

Prerequisites

- Relevant foundational experience in the target technology area.
- Comfort with hands-on labs in a cloud or GPU-accelerated environment.

PROGRAM OUTCOMES

Capabilities your teams will gain

- Strengthen capability in security engineer scenarios
- Strengthen capability in azure scenarios

ENTERPRISE CUSTOMIZATION

Enterprise customization

Tailor this program to your organization's priorities: Builds current Microsoft credential readiness for Secure AI solutions in the cloud using Microsoft Defender for Cloud and Microsoft Entra using the official Microsoft Learn outline.

- Align labs to your production environment and platform priorities
- Add readiness reviews and instructor-led practice sessions

- Extend into project-specific architecture or delivery coaching

CURRICULUM

Curriculum roadmap

1 **MODULE 1** **Protect Microsoft Foundry solutions by using Microsoft Defender for Cloud**

Learn how to secure Microsoft Foundry workloads by using Microsoft Defender for Cloud. Discover AI resources across Azure, assess their security posture, protect against runtime threats, and configure model guardrails in Microsoft Foundry to prevent unsafe or policy-violating content.

- Understand how Microsoft Defender for Cloud supports AI security and governance in Azure
- Protect AI workloads with Microsoft Defender for Cloud
- Configure and manage guardrails in Microsoft Foundry
- Secure Microsoft Foundry environments

2 **MODULE 2** **Secure AI identity infrastructure with Microsoft Entra**

Learn how to secure identities used by AI workloads in Azure. Build skills in workload identity architecture, access management, Conditional Access, and identity risk response by using Microsoft Entra.

- Understand identity architecture for AI workloads
- Implement access management for Azure resources
- Plan, implement, and administer Conditional Access
- Manage Microsoft Entra Identity Protection

PRIVATE DELIVERY

Plan a private cohort for your team

Scope delivery format, role mix, and rollout timeline with our solutions team.

[Plan Private Delivery](#)

[Book advisory call](#)