# Secure Microsoft AI Solutions in the Cloud

***Duration: 1 Day***

In this course, 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

**Prerequisites**

- 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

**Module 1: Understand how Microsoft Defender for Cloud supports AI security and governance in Azure**

In this module, you learn to:

- Identify the layers that make up AI workloads in Azure
- Recognize security risks unique to AI, including prompt injection, data leakage, and model misuse
- Explain how Microsoft Foundry provides guardrails and observability for AI models
- Describe how Microsoft Defender for Cloud, Microsoft Purview, and Microsoft Entra ID work together to secure and govern AI workloads
- Summarize how these services align to create a unified, defense-in-depth strategy for AI security in Azure.

**Lessons:**

- 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 2: Protect AI workloads with Microsoft Defender for Cloud**

In this module, you learn to:

- Enable and configure the AI workloads plan in Microsoft Defender for Cloud
- Review AI resource insights in the Data & AI security dashboard
- Assess and improve AI posture with Cloud Security Posture Management (CSPM)
- Detect and respond to runtime threats using Cloud Workload Protection (CWP)
- Investigate AI-related alerts and incidents in Microsoft Defender XDR

Lessons:

- Introduction
- Enable the AI workloads plan
- Review insights in the Data & AI security dashboard
- Assess and improve AI security posture with Cloud Security Posture Management (CSPM)
- Detect AI threats at runtime with Cloud Workload Protection (CWP)

- Investigate AI security alerts with prompt evidence in Microsoft Defender XDR

**Module 3: Configure and manage guardrails in Microsoft Foundry**

In this module, you learn to:

- Explain how guardrails secure model interactions in Microsoft Foundry
- Describe safety controls such as content filters, blocklists, and Prompt Shields
- Configure and validate custom guardrails for different workload types
- Evaluate guardrail effectiveness and refine configurations for continuous assurance

Lessons:

- Introduction
- Understand guardrails and Microsoft Content Safety
- Understand safety controls in Microsoft Foundry
- Try out built-in guardrails
- Create and manage blocklists in Microsoft Foundry
- Configure and apply guardrails in Microsoft Foundry
- Choose and refine the right guardrails for your AI workloads

**Module 4: Secure Microsoft Foundry environments**

In this module, you learn to:

- Define access boundaries using Microsoft Entra ID and role-based access control (RBAC)
- Manage project-level permissions within shared environments
- Secure secrets with Key Vault and managed identities
- Isolate workloads with managed virtual networks and Private Link
- Enable diagnostic logging for centralized visibility and investigation

Lessons:

- Introduction
- Control access to Microsoft Foundry with Microsoft Entra ID
- Manage access within Microsoft Foundry projects
- Secure Microsoft Foundry secrets with Azure Key Vault (preview)
- Isolate networks with managed virtual network and Private Link
- Enable diagnostic logging in Microsoft Foundry