training code: SC-5009 / ENG DL 1d / EN

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

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

Training recipients

The training is intended for:

- Security Engineers
- Administrators
- Developers
- Identity and Access Administrators

Benefits

Foundation skills acquired include:

- 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

Training program

1.Understand how Microsoft Defender for Cloud supports AI security and governance in Azure

- 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

2.Protect AI workloads with Microsoft Defender for Cloud

- 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

3.Configure and manage guardrails in Microsoft Foundry

- 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

4.Secure Microsoft Foundry environments

- 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

5.Understand identity architecture for AI workloads

- 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

6.Implement access management for Azure resources

- Assign Azure roles
- Configure custom Azure roles
- Create and configure managed identities
- Access Azure resources with managed identities
- Analyze Azure role permissions
- Configure Azure Key Vault RBAC policies

- Retrieve objects from Azure Key Vault

7.Plan, implement, and administer Conditional Access

- Plan security defaults
- Plan Conditional Access policies
- Implement Conditional Access policy controls and assignments
- Test and troubleshoot Conditional Access policies
- Implement application controls
- Implement session management and continuous access evaluation
- Microsoft Entra Conditional Access Optimization agent

8.Manage Microsoft Entra Identity Protection

- Review identity protection basics
- Implement and manage user risk policy
- Monitor, investigate, and remediate elevated risky users
- Implement security for workload identities
- Explore Microsoft Defender for Identity
- Explore the Identity Risk Management Agent

Expected preparation of the participant

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.

Training Includes

- manual in electronic form available on the platform: https://learn.microsoft.com/pl-pl/training/
- access to Altkom Akademia's student portal

Duration

1 days / 7 hours

Language

- Training: English
- Materials: English