Training: Microsoft

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

TRAINING GOALS:

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.

CONSPECT:

- Protect Microsoft Foundry solutions by using Microsoft Defender for Cloud
  - Module 1: Understand how Microsoft Defender for Cloud supports AI security and governance in Azure
  - Module 2: Protect AI workloads with Microsoft Defender for Cloud
  - Module 3: Configure and manage guardrails in Microsoft Foundry
  - Module 4: Secure Microsoft Foundry environments
- Secure AI identity infrastructure with Microsoft Entra

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Module 1: Understand identity architecture for AI workloads
- Module 2: Implement access management for Azure resources
- Module 3: Plan, implement, and administer Conditional Access
- Module 4: Manage Microsoft Entra Identity Protection

REQUIREMENTS:

- Experience managing Azure subscriptions, workloads, and Defender for Cloud plans (from LP1)
- Familiarity with Microsoft Foundry and how AI workloads are deployed in Azure (from LP1)
- Understanding of basic cloud security principles (from LP1)
- Experience with Microsoft Entra ID fundamentals (from LP2)
- Familiarity with Azure RBAC (from LP2)

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Microsoft (course completion). This course is not directly mapped to a Microsoft certification exam.

TRAINER:

Microsoft Certified Trainer (MCT)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007