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

Duration: 1 Day **Course Code: M-SC5009** **Delivery Method: Virtual Learning**

Overview:

Secure AI workloads in Azure using cloud native protection and identity controls.
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.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

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.

Objectives:

- **After this course participants should be able to:**
- 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

Prerequisites:

Learners should have:

- Familiarity with Microsoft Azure and cloud-native security concepts, including workload protection and security posture management.
- Basic understanding of identity and access management concepts, such as authentication and authorization principles.
- Experience or exposure to securing cloud workloads, especially in Azure environments.

Testing and Certification

None

Follow-on-Courses:

None

Content:

Module 1: Protect Microsoft Foundry solutions by using Microsoft Defender for Cloud

- 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

Module 2:Secure AI identity infrastructure with 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

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/