SC-500

Implement End-to-End Security Controls for Cloud and AI Workloads

Description:

This course prepares you to design, implement, and manage end-to-end security controls across Microsoft Azure and Microsoft 365 environments — including the emerging landscape of AI workloads and autonomous agents. Through a combination of instructor-led sessions and hands-on labs, you build practical skills in identity security, cloud infrastructure protection, threat detection, and posture management.

Students will be able to:

- Secure identity and access across users, applications, and agents.
- Protect secrets, keys, certificates, storage, and databases.
- Apply governance, policy, and least-privilege controls across Azure.
- Secure network access to Azure resources and services.
- Assess and protect AI workloads, agents, and data exposure paths.
- Secure compute, container, and application platforms.
- Manage cloud security posture across Azure, hybrid, and multicloud environments.

Course requirements:

- Foundational Azure knowledge
- Basic identity and access knowledge
- General security fundamentals
- Basic cloud networking knowledge
- Basic data and workload awareness
- Familiarity with Microsoft security tools
- Introductory AI awareness
- Hands-on Azure portal experience

This course is intended for:

This course is for the Information Security Administrator who plan and implement information security for sensitive data using Microsoft Purview and related services. You're responsible for mitigating risks by protecting data within Microsoft 365 collaboration environments from internal and external threats, as well as safeguarding data used by AI services. Your role involves implementing information protection, data loss prevention (DLP), retention, and insider risk management. You also manage security alerts and respond to incidents by investigating activities, responding to DLP alerts, and managing insider risk cases. In this role, you collaborate with other roles responsible for governance, data, and security to develop policies that address your organization's information security and risk reduction goals. You work with workload administrators, business application owners, and governance stakeholders to implement technology solutions that support these policies and controls.

Literature:

All participants will receive original Microsoft student materials and access to labs.

Hardware:

Classrooms are equipped with high-performance computers with Internet access and the possibility of wireless connection.

Syllabus:

Module 1: Secure access to resources by using Microsoft Entra

Module 2: Secure Azure Key Vault with defense in depth

Module 3: Enforce security governance and regulatory compliance

Module 4: Implement security for Azure Storage

Module 5: Implement security for Azure SQL databases

Module 6: Implement network security controls in Azure

Module 7: Implement security for servers and virtual machines

Module 8: Implement security for AI

Module 9: Secure Azure application platform services

Module 10: Manage security posture by using Microsoft Defender for Cloud

Module 11: Implement activity and event collection in Microsoft Sentinel

Module 12: Deploy and operate Microsoft Security Copilot

Contact us
OKsystem a.s., Na Pankráci 1690/125, 140 00 Prague 4
(+420) 236 072 111 skoleni@oksystem.cz www.okskoleni.cz

OKškolení
by OKsystem