training code: SC-500 / ENG DL 4d / EN

Implement end to end security controls for cloud and AI workloads

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. This course is intended for security engineers who are responsible for planning and implementing security controls across cloud, hybrid, and multi-cloud environments using Microsoft security technologies.

Training recipients

The training is intended for:

- Security Engineers

Benefits

By completing this course, students will achieve the following objectives:

- Securing access to resources by using Microsoft Entra ID and Azure Key Vault
- Enforcing security and regulatory compliance
- Securing storage, databases, and networking
- Securing compute
- Securing AI solutions
- Managing and monitoring security posture

Training program

1.Secure access to resources by using Microsoft Entra

- Manage and implement authentication methods in Microsoft Entra ID
- Implement and configure Privileged Identity Management (PIM)
- Authenticate your API plugin for declarative agents with secured APIs

2.Secure Azure Key Vault with defense in depth for the cloud and AI workloads

- Configure and secure Azure Key Vault
- Manage keys and secrets in Azure Key Vault
- Manage certificates and monitor Azure Key Vault
- Protect Azure Key Vault with Microsoft Defender for Cloud

3.Enforce security governance and regulatory compliance

- Enforce governance with Azure Policy and resource locks
- Configure security controls and remediate recommendations in Defender for Cloud
- Evaluate regulatory compliance in Defender for Cloud
- Manage and right-size RBAC role assignments for least privilege
- Protect backup data with Azure Backup security features
- Implement security controls in infrastructure as code

4.Implement security for Azure Storage for the cloud and AI security engineer

- Describe Azure storage services
- Implement security and manage access for Azure Storage
- Configure network security for Azure Storage
- Implement Microsoft Defender for Storage

5.Implement security for Azure SQL databases

- Configure platform-level security for Azure SQL
- Configure auditing for Azure SQL Database and SQL Managed Instance
- Implement Microsoft Defender for Databases

Expected preparation of the participant

- Practical experience in administration of Microsoft Azure and hybrid environments, including compute, networks, and storage
- Strong familiarity with Microsoft Entra ID
- Familiarity with Microsoft 365 administration.

To increase the comfort of work and training’s effectiveness we suggest using an additional monitor. The lack of additional monitor does not exclude participation in the training, however, it significantly influences the comfort of work during classes.

You can find information and requirements of participation in Distance Learning trainings at:

https://www.altkomakademia.pl/en/how-it-works/about-courses/

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

4 days / 28 hours

Language

- Training: English
- Materials: English