training code: SC-100 / ENG DL 4d / EN

Microsoft Cybersecurity Architect

Authorized Microsoft Cybersecurity Architect SC-100 Distance Learning training.

Target audience:

- Administrator
- IT specialist
- IT security specialist

Training recipients

Training for people who want to familiarize themselves with the principles of designing and assessing cybersecurity strategies in the areas of: Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps) and data and applications. Participants learn how to design solutions using zero trust principles and define security requirements for cloud infrastructure in various service models (SaaS, PaaS, IaaS). The training is particularly aimed at security administrators and IT specialists with advanced experience and knowledge in a wide range of security engineering areas, including identity and access, platform protection, security operations, data security and application security. Experience in hybrid and cloud implementations is also recommended. The course covers topics such as:

- Designing a Zero Trust strategy and architecture,
- Assessing technical strategies and security operations strategies in the field of risk management (GRC),
- Designing security for infrastructure,
- Designing a strategy for data and applications

Benefits

During the training, the participant will gain knowledge and practical skills in security design on the Microsoft platform. The participant will get acquainted with the subject of:

- Zero Trust strategy and architecture design process.
- Evaluating technical and security operations strategies for risk management (GRC).
- The security design process for infrastructure.
- The process of designing strategies for data and applications.

The training helps participants prepare for the SC-100 exam.

Become Microsoft Certified: https://arch-center.azureedge.net/Credentials/Certification-Poster_en-us.pdf

Training program

1: Designing solutions in line with best practices and security priorities

Introduction to Zero Trust and best practices

- Zero Trust RaMP initiatives
- Pillars of Zero Trust technology
- Designing solutions in line with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)
- Defining security strategies

Introduction to the Cloud Adoption Framework

- Cloud Adoption Framework – a secure methodology
- Introduction to Azure Landing Zones
- Designing security with Azure Landing Zones
- Introduction to Well Architected Framework
- Well Architected Framework – a pillar of security
- Solutions with CAF and WAF

Designing solutions that are compliant with Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft Cloud Security Benchmark (MCSB)

- Introduction to MCRA and MCSB
- Designing solutions with best practices for capabilities and controls
- Designing solutions with best practices to protect against attacks
- Strategies for resilience against common cyber threats such as ransomware
- Typical cyber threats and attack patterns
- Supporting business resilience
- Protection against ransomware
- Secure backup and restore configurations
- Security updates

2: Security, identity and compliance design

Designing the solution for compliance

- Introduction to compliance
- Transforming compliance requirements into a security solution
- Meeting compliance requirements with Purview
- Meeting privacy requirements with Priva
- Using Azure Policy to meet security and compliance requirements
- Assessing infrastructure compliance with Microsoft Defender for Cloud

Designing an identity and access management solution

- Designing a solution to manage secrets, keys and certificates
- Introduction to identity and access management
- Designing a cloud, hybrid and multi-cloud access strategy (including Azure AD)
- Designing a solution for external identities
- Designing modern authentication and authorization strategies
- Customizing conditional access and Zero Trust

Designing solutions that provide privileged access

- Introduction to privileged access
- Enterprise access model
- Designing an identity management solution
- Designing a solution to secure tenant administration
- Designing for cloud infrastructure entitlement management (CIEM)
- Designing a solution for privileged access workstations and bastion service

Designing solutions for security operations

- Introduction to security operations (SecOps)
- Designing security operations capabilities in hybrid and multi-cloud environments
- Designing centralized logging and inspection
- Designing SIEM solutions
- Designing a solution for detection and response
- Designing a solution for SOAR
- Designing security workflows
- Designing threat detection coverage

3: Designing a solution to secure applications and data

Designing a solution to secure the Microsoft 365 platform

- Security for Exchange, Sharepoint, OneDrive and Teams (M365)
- Assessing security status for collaboration and productivity workloads
- Designing a Microsoft Defender 365 solution
- Configuration design and operational practices for M365

Designing solutions to secure applications

- Introduction to application security
- Designing and implementing a standard for secure application development
- Assessing the security status of existing applications

- Designing security lifecycle strategies for applications
- Secure identity access
- Designing an API management solution
- Designing a solution to provide secure access to applications

Designing a solution to secure an organization's data

- Introduction to data security
- Designing a solution to detect and classify data using Microsoft Purview
- Designing a solution to protect data at rest, data in motion, and data in use
- Data security in Azure platform workloads
- Securing the Azure Storage service
- Defender for SQL and Defender for storage

4: Designing security solutions for infrastructure

Identify requirements for securing SaaS, PaaS and IaaS services

- Securing SaaS, PaaS and Iaas (shared responsibility model)
- Security baselines for cloud services
- Determining security requirements for web-based workloads
- Determining security requirements for containers and container orchestration

Designing a solution to manage security state in hybrid and multi-cloud environments

- Introduction to hybrid and multi-cloud environments
- Assessing posture with MCSB
- Designing posture management and load protection in hybrid and multi-cloud environments
- A discussion of posture assessment using Defender for Cloud
- Assessing posture using the Microsoft Defender for Cloud secure service score
- Designing a solution to protect cloud workloads that use Microsoft Defender for Cloud service
- Designing a solution to integrate hybrid and multi-cloud environments using the Azure Arc service
- Managing the external attack surface

Designing solutions to secure server and client endpoints

- Introduction to endpoint security
- Determining server and baseline security requirements
- Identify mobile device and client requirements
- Specifying security requirements for IoT and embedded devices
- Microsoft Defender for IoT
- Defining security baselines for server and client endpoints
- Designing a solution for secure remote access

Designing solutions for network security

- Designing a solution for network segmentation
- Designing a solution for traffic filtering with network security groups
- Designing solutions for network health management
- Designing solutions for network monitoring

5: Designing solutions that align with security best practices and priorities

Case study

6: Designing security operations, identity and compliance capabilities
Case study
7: Designing solutions to secure applications and data
Case study
8: Designing security solutions for infrastructure
Case study

Expected preparation of the participant

- At least 2 years' experience with Active Directory infrastructure management
- At least 2 years' experience in managing a cloud environment
- Knowledge and experience in broad areas of security engineering, including identity and access, platform protection, security operations, data security and application security
- Experience in hybrid and cloud deployments is also desirable.
- Familiarity with Microsoft security and compliance technologies.
- Knowledge of information security concepts.
- Intermediate to advanced knowledge of Windows 10/11
- Ability to use English-language materials
- Pre-training: AZ-900, MS-900, SC-900, SC-300, SC-400, SC-200

Training Includes

* electronic handbook available at:
https://learn.microsoft.com/pl-pl/training/

- access to the Altkom Akademia student portal
- training conducted in the form of a presentation
- trainer demonstrations
- practical exercises (case studies)

Training method:

- Distance Learning formula

Language

- **Training**: English
- **Materials**: English

Examination method

Egzamin w formie on-line. Zapis na stronie https://home.pearsonvue.com/Clients/Microsoft.aspx

Duration

4 days / 28 hours

Examination description

Microsoft Certified: Cybersecurity Architect Expert
Exam URL: https://docs.microsoft.com/en-us/learn/certifications/exams/SC-100
Become Microsoft Certified: https://arch-center.azureedge.net/Credentials/Certification-Poster_en-us.pdf