Microsoft Cybersecurity Architect (SC-100)

Description

Mastering Microsoft Cybersecurity Architecture

In a digital world where threats are constantly evolving, the cybersecurity architect plays a crucial role. The Microsoft Cybersecurity Architect (SC-100) training prepares you to design robust strategies tailored to modern environments. This expert-level program is designed to give you an advanced understanding of zero trust principles, risk governance, security operations, and the protection of data and applications.

Built around Microsoft best practices, this course is an essential asset for any expert seeking to deepen their skills. You will learn how to align security strategies with key reference frameworks while mastering the specific requirements of SaaS, PaaS, and IaaS infrastructures. Through a methodological and practical approach, you will be able to design comprehensive, resilient security architectures that meet regulatory standards.

Become an expert in cloud and hybrid security architectures

Designing, evaluating, and enhancing robust cybersecurity architectures is a strategic challenge for all modern organizations. With the Microsoft Cybersecurity Architect (SC-100) training, you will be ready to meet this challenge and help organizations achieve optimal security. This comprehensive course will enable you to master all aspects of a security architecture, from initial design to compliance validation, including advanced protection of data and applications in hybrid and multicloud environments.

Course Content
Module 1: Introduction to Zero Trust frameworks and best practices

- Introduction to Zero Trust
- Zero Trust initiatives
- Zero Trust technology pillars Part 1
- Zero Trust technology pillars Part 2

Module 2: Designing security solutions aligned with the Cloud Adoption Framework (CAF) and the Well-Architected Framework (WAF)

- Define a security strategy
- Introduction to the Cloud Adoption Framework
- Cloud Adoption Framework secure methodology
- Introduction to Azure landing zones
- Designing security with Azure landing zones
- Introduction to the Well-Architected Framework
- Well-Architected Framework security pillar

Module 3: Designing solutions aligned with MCRA (Microsoft Cybersecurity Reference Architecture) and MCSB (Microsoft Cloud Security Benchmark)

- Introduction to Microsoft Cybersecurity Reference Architecture and Cloud Security Benchmark
- Designing solutions using best practices for features and controls

- Designing solutions using best practices to protect against insider, external, and supply chain attacks

Module 4: Designing a resilience strategy against ransomware and other attacks following Microsoft security best practices

- Common cyberthreats and attack patterns
- Supporting business resilience
- Designing solutions to mitigate ransomware attacks, including BCDR and privileged access prioritization
- Designing solutions for business continuity and disaster recovery (BCDR), including secure backup and restore
- Designing solutions for security patching

Module 5: Case study: Designing solutions aligned with security best practices and priorities

- Case study description
- Case study responses
- Conceptual step-by-step procedure
- Technical step-by-step procedure

Module 6: Designing regulatory compliance solutions

- Introduction to regulatory compliance
- Translating compliance requirements into security controls
- Designing a solution to meet compliance requirements using Microsoft Purview
- Meeting privacy requirements with Microsoft Priva
- Meeting security and compliance requirements with Azure Policy
- Assessing and validating alignment with regulatory standards and benchmarks using Microsoft Defender for Cloud

Module 7: Designing identity and access management solutions

- Introduction to identity and access management
- Designing access strategies for cloud, hybrid, and multicloud solutions (including Microsoft Entra ID)
- Designing a solution for external identities
- Designing modern authentication and authorization strategies
- Aligning conditional access and Zero Trust
- Specifying requirements to secure Active Directory Domain Services (AD DS)
- Designing a solution for secrets, keys, and certificate management

Module 8: Designing solutions to secure privileged access

- Introduction to privileged access
- Enterprise access model
- Assessing security and governance for Microsoft Entra ID solutions
- Designing a solution to secure tenant administration
- Designing a solution for privileged access workstations and bastion services
- Evaluating an access review management solution
- Assessing security and governance for on-premises Active Directory Domain Services (AD DS), including resistance to common attacks

Module 9: Designing security operations solutions

- Introduction to security operations (SecOps)

- Designing a monitoring solution for hybrid and multicloud environments
- Designing centralized logging and auditing, including Microsoft Purview Audit
- Designing detection and response solutions, including Extended Detection and Response (XDR) and Security Information and Event Management (SIEM)
- Designing a SOAR (Security Orchestration, Automation, and Response) solution
- Designing and evaluating security workflows, including incident response, threat hunting, and incident management
- Designing and evaluating threat detection coverage using MITRE ATT&CK matrices across cloud, enterprise, mobile, and ICS

Module 10: Case study: Designing features related to security operations, identities, and compliance

- Case study description
- Case study responses
- Conceptual step-by-step procedure
- Technical step-by-step procedure

Module 11: Designing solutions to secure Microsoft 365

- Introduction to securing Exchange, SharePoint, OneDrive, and Teams
- Assessing security posture for productivity and collaboration workloads using metrics
- Designing a Microsoft Defender XDR solution
- Designing configurations and operational practices for Microsoft 365
- Evaluating data security and compliance controls in Microsoft Copilot for Microsoft 365 services
- Evaluating data protection solutions in Microsoft 365 using Microsoft Purview

Module 12: Designing application security solutions

- Introduction to application security
- Designing and implementing standards for secure application development
- Assessing security posture for existing application portfolios
- Evaluating application threats using threat modeling
- Designing a security lifecycle strategy for applications
- Securing access for workload identities
- Designing an API management and security solution
- Designing a solution to secure application access

Module 13: Designing solutions to secure organizational data

- Introduction to data security
- Evaluating solutions for data discovery and classification
- Evaluating solutions for data encryption at rest and in transit, including Azure KeyVault and infrastructure encryption
- Designing data security for Azure workloads
- Designing security for Azure Storage
- Designing a security solution with Microsoft Defender for SQL and Microsoft Defender for Storage

Module 14: Case study: Designing security solutions for applications and data

- Case study description
- Case study responses
- Conceptual step-by-step procedure
- Technical step-by-step procedure

Module 15: Specifying requirements to secure SaaS, PaaS, and IaaS services

- Introduction to securing SaaS, PaaS, and IaaS
- Specifying security baselines for SaaS, PaaS, and IaaS services
- Specifying security requirements for IoT workloads
- Specifying security requirements for web workloads
- Specifying security requirements for containers and container orchestration
- Assessing AI services security

Module 16: Designing solutions for security posture management in hybrid and multicloud environments

- Introduction to hybrid and multicloud posture management
- Assessing security posture using Microsoft Cloud Security Benchmark
- Designing integrated posture management and workload protection
- Assessing security posture using Microsoft Defender for Cloud
- Posture assessment with Microsoft Defender for Cloud Secure Score
- Designing cloud workload protection with Microsoft Defender for Cloud
- Integrating hybrid and multicloud environments with Azure Arc
- Designing a solution for external attack surface management
- Posture management using attack path exposure management

Module 17: Designing solutions to secure server and client endpoints

- Introduction to endpoint security
- Specifying server security requirements
- Specifying requirements for mobile devices and clients
- Specifying requirements for IoT and embedded device security
- Securing Operational Technology (OT) and Industrial Control Systems (ICS) with Microsoft Defender for IoT
- Specifying security baselines for server and client endpoints
- Designing a solution to secure remote access
- Evaluating Windows LAPS (Local Administrator Password Solutions)

Module 18: Designing network security solutions

- Designing network segmentation solutions
- Designing traffic filtering solutions using network security groups
- Designing network posture management solutions
- Designing network monitoring solutions
- Evaluating solutions using Microsoft Entra Internet Access
- Evaluating solutions using Microsoft Entra Private Access

Module 19: Case study: Designing infrastructure security solutions

- Case study description
- Case study responses
- Conceptual step-by-step procedure
- Technical step-by-step procedure

Lab / Exercises

- This course provides you with exclusive access to the official Microsoft lab, enabling you to practice your skills in a professional environment.

Documentation

- Access to Microsoft Learn, Microsoft's online learning platform, offering interactive resources and educational content to deepen your knowledge and develop your technical skills.

Exam

- This course prepares you to the SC-100: Microsoft Cybersecurity Architect exam.

Participant profiles

- Cloud security engineers
- Security solutions architects
- Cybersecurity consultants
- IT security managers
- Compliance and data governance experts

Prerequisites

- Master the fundamentals of cybersecurity and compliance
- Understand Microsoft cloud and hybrid environments
- Hold an associate-level certification (AZ-500, SC-200, or SC-300)

Objectives

- Design cybersecurity strategies based on the Zero Trust model
- Develop solutions aligned with the Cloud Adoption Framework standards
- Align security architectures with the Microsoft Cybersecurity Reference Architecture
- Develop resilience strategies against ransomware attacks
- Specify requirements to secure SaaS, PaaS, and IaaS cloud infrastructures
- Manage security posture in hybrid and multicloud environments
- Secure identities, privileged access, and security operations
- Protect an organization's applications, data, and endpoints

Description
Microsoft Cybersecurity Architect (SC-100)
Niveau
Avancé
Classroom Registration Price (CHF)
3200
Virtual Classroom Registration Price (CHF)
3000
Duration (in Days)
4
Reference