# Microsoft Cybersecurity Architect – Intensive Training («SC100»)

This course prepares students with the background to design and evaluate cybersecurity strategies in the following areas: Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps), and data and applications.

**Duration:** 4 days
**Price:** 3'400.–
**Course documents:** Official Microsoft Courseware and Microsoft Learn
**Vendor code:** SC-100

## Content

The content of this intensive training is derived from the exam «SC-100: Microsoft Cybersecurity Architect». Start preparing for the course on Microsoft Learn now and use the Learning Support if you have any questions. During the intensive training days with the instructor you will work with the official Microsoft course material (more information under «Methodology & didactics»).

**Module 1: Build an overall security strategy and architecture**
**Lessons**

- Zero Trust overview
- Develop Integration points in an architecture
- Develop security requirements based on business goals
- Translate security requirements into technical capabilities
- Design security for a resiliency strategy
- Design a security strategy for hybrid and multi-tenant environments
- Design technical and governance strategies for traffic filtering and segmentation
- Understand security for protocols
- **Exercise: Build an overall security strategy and architecture**

**Module 2: Design a security operations strategy**
**Lessons**

- Understand security operations frameworks, processes, and procedures
- Design a logging and auditing security strategy
- Develop security operations for hybrid and multi-cloud environments
- Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration,
- Evaluate security workflows
- Review security strategies for incident management
- Evaluate security operations strategy for sharing technical threat intelligence
- Monitor sources for insights on threats and mitigations

**Module 3: Design an identity security strategy**
**Lessons**

- Secure access to cloud resources
- Recommend an identity store for security
- Recommend secure authentication and security authorization strategies
- Secure conditional access
- Design a strategy for role assignment and delegation
- Define Identity governance for access reviews and entitlement management

- Design a security strategy for privileged role access to infrastructure
- Design a security strategy for privileged activities
- Understand security for protocols

**Module 4: Evaluate a regulatory compliance strategy**
**Lessons**

- Interpret compliance requirements and their technical capabilities
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
- Interpret compliance scores and recommend actions to resolve issues or improve security
- Design and validate implementation of Azure Policy
- Design for data residency Requirements
- Translate privacy requirements into requirements for security solutions

**Module 5: Evaluate security posture and recommend technical strategies to manage risk**
**Lessons**

- Evaluate security postures by using benchmarks
- Evaluate security postures by using Microsoft Defender for Cloud
- Evaluate security postures by using Secure Scores
- Evaluate security hygiene of Cloud Workloads
- Design security for an Azure Landing Zone
- Interpret technical threat intelligence and recommend risk mitigations
- Recommend security capabilities or controls to mitigate identified risks

**Module 6: Understand architecture best practices and how they are changing with the Cloud**
**Lessons**

- Plan and implement a security strategy across teams
- Establish a strategy and process for proactive and continuous evolution of a security strategy
- Understand network protocols and best practices for network segmentation and traffic filtering

**Module 7: Design a strategy for securing server and client endpoints**
**Lessons**

- Specify security baselines for server and client endpoints
- Specify security requirements for servers
- Specify security requirements for mobile devices and clients
- Specify requirements for securing Active Directory Domain Services
- Design a strategy to manage secrets, keys, and certificates
- Design a strategy for secure remote access
- Understand security operations frameworks, processes, and procedures
- Understand deep forensics procedures by resource type

**Module 8: Design a strategy for securing PaaS, IaaS, and SaaS services**
**Lessons**

- Specify security baselines for PaaS, IaaS, and SaaS services
- Specify security requirements for IoT, data, web, and storage workloads
- Specify security requirements for containers and container orchestration

**Module 9: Specify security requirements for applications**
**Lessons**

- Understand application threat modeling
- Specify priorities for mitigating threats to applications
- Specify a security standard for onboarding a new application
- Specify a security strategy for applications and APIs

**Module 10: Design a strategy for securing data**
**Lessons**

- Prioritize mitigating threats to data
- Design a strategy to identify and protect sensitive data
- Specify an encryption standard for data at rest and in motion

## Key Learnings

- Designing a Zero Trust strategy and architecture
- Evaluating Governance Risk Compliance (GRC) technical strategies and security operations strategies
- Designing security for infrastructure
- Designing a strategy for data and applications

## Target audience

IT professionals with advanced experience and knowledge in a wide range of security engineering areas, including identity and access, platform protection, security operations, securing data, and securing applications. They should also have experience with hybrid and cloud implementations.

## Requirements

- Advanced experience and knowledge in identity and access, platform protection, security operations, securing data and securing applications
- Experience with hybrid and cloud implementations

- Microsoft Identity and Access Administrator – Intensive Training («SC300»)
- Microsoft Azure Security Technologies – Intensive Training («AZ500»)
- Microsoft Security Operations Analyst – Intensive Training («SC200»)

## Certification

This intensive training prepares you for:

- **Exam:** «SC-100: Microsoft Cybersecurity Architect» for the
- **Certification:** «Microsoft Certified: Cybersecurity Architect Expert»

## Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-microsoft-technology/microsoft-security-compliance-and-identity/microsoft-certified-cybersecurity-architect-expert/course-microsoft-cybersecurity-architect-intensive-training-sc-100