

# Microsoft Cybersecurity Architect (SC-100)

Course: **00090**

Filter: **Beginner**

Duration: **20 hours**

Category:: **Software Application Security**

Price: **2500,00 €**

## About Course

This Microsoft Cybersecurity Architect (SC-100) 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. Students will also learn how to design and architect solutions using zero trust principles and specify security requirements for cloud infrastructure in different service models (SaaS, PaaS, IaaS).

## What you'll learn

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

## Pre-requisites

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

## Curriculum

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

- Introduction
- 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
- Understand security operations frameworks, processes, and procedures
- Understand deep forensics procedures by resource type

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

- Introduction
- 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
- After completing this module, students will be able to:
- 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, A.
- Evaluate security workflows.
- Review security strategies for incident management.
- Evaluate security operations for technical threat intelligence.
- Monitor sources for insights on threats and mitigations.

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

- Introduction
- 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
- After completing this module, students will be able to:
- 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 access.

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

- Introduction
- 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**

- Introduction

- Evaluate security postures by using benchmarks
- Evaluate security postures by using Microsoft Defender for Cloud
- Evaluate security postures by using Secure Scores
- 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**

- Introduction
- Plan and implement a security strategy across teams
- Establish a strategy and process for the 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**

- Introduction
- 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