Microsoft Cybersecurity Architect (SC-100)

Modality: Virtual Classroom

Duration: 4 Days

If you enroll in this course at the listed price, you receive a Free Official Exam Voucher for the SC-100 Exam. This course does not include Exam Voucher if enrolled within the Master Subscription, however, you can request to purchase the Official Exam Voucher separately.

About this Course:

This is an advanced, expert-level course. Although not required to attend, students are strongly encouraged to have taken and passed another associate level certification in the security, compliance and identity portfolio (such as AZ-500, SC-200 or SC-300) before attending this class. This course prepares students with the expertise 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).

Course Objectives:

- Introduction to Zero Trust and best practice frameworks
- Design solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)
- Design solutions that align with the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB)
- Design a resiliency strategy for common cyberthreats like ransomware
- Case study: Design solutions that align with security best practices and priorities
- Design solutions for regulatory compliance
- Design solutions for identity and access management
- Design solutions for securing privileged access
- Design solutions for security operations
- Case study: Design security operations, identity and compliance capabilities
- Design solutions for securing Microsoft 365
- Design solutions for securing applications
- Design solutions for securing an organization's data
- Case study: Design security solutions for applications and data
- Specify requirements for securing SaaS, PaaS, and IaaS services
- Design solutions for security posture management in hybrid and multicloud environments
- Design solutions for securing server and client endpoints
- Design solutions for network security
- Case study: Design security solutions for infrastructure

Audience:

This course is for experienced cloud security engineers who have taken a previous certification in the security, compliance and identity portfolio. Specifically, students should have 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. Beginning students should instead take the course SC-900: Microsoft Security, Compliance, and Identity Fundamentals.

Prerequisites:

Before attending this course, students must have:

- Highly recommended to have attended and passed one of the associate level certifications in the security, compliance and identity portfolio (such as AZ-500, SC-200 or SC-300)
- Advanced experience and knowledge in identity and access, platform protection, security operations, securing data and securing applications.
- Experience with hybrid and cloud implementations.

Course Outline:

Module 1: Introduction to Zero Trust and best practice frameworks

- Understand how to use best practices as a cybersecurity architect.
- Understand the concept of Zero Trust and how it can be used to modernize an organizations cybersecurity.
- Understand when to use different best practice frameworks like MCRA, CAF and WAF.

Module 2: Design solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)

- Understand the Cloud Adoption Framework and how it can be used to accelerate and secure an organizations move to the cloud.
- Understand the Well-Architected Framework and how it can be used to design solutions in the cloud that adhere to sound design principles including security.

Module 3: Design solutions that align with the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB)

- Understand how to use Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB) to design more secure solutions.

Module 4: Design a resiliency strategy for common cyberthreats like ransomware

- Understand common cyberthreats like ransomware.
- Understand how to support business resiliency.
- Design configurations for secure backup and restore.
- Design solutions for managing security updates.

Module 5: Case study: Design solutions that align with security best practices and priorities

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

Module 6: Design solutions for regulatory compliance

- Translate compliance requirements into a security solution
- Address compliance requirements with Microsoft Purview
- Design a solution to address privacy requirements with Microsoft Priva
- Design Azure Policy solutions to address security and compliance requirements
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud

Module 7: Design solutions for identity and access management

- Design cloud, hybrid and multicloud access strategies
- Design a solution for Azure Active Directory (Azure AD), part of Microsoft Entra
- Design a solution for external identities
- Design modern authentication and authorization strategies
- Specify requirements to secure Active Directory Domain Services
- Design a solution to manage secrets, keys, and certificates

Module 8: Design solutions for securing privileged access

- Understand privileged access and the Enterprise Access Model
- Design identity governance solutions
- Design a solution for securing administration of cloud tenants
- Design for cloud infrastructure entitlement management

Module 9: Design solutions for security operations

- Design security operations capabilities in hybrid and multicloud environments
- Design centralized logging and auditing
- Design Security Event Management (SIEM) solutions
- Design a solution for detection and response that includes Extended Detection and Response (XDR)
- Design a solution for security orchestration, automation and response (SOAR)
- Design security workflows
- Design and evaluate threat detection with the MITRE ATT&CK framework

Module 10: Case study: Design security operations, identity and compliance capabilities

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

Module 11: Design solutions for securing Microsoft 365

- Evaluate security posture for collaboration and productivity workloads

- Design a Microsoft 365 Defender solution
- Design configurations and operational practices for Microsoft 365

Module 12: Design solutions for securing applications

- Evaluate security posture of existing application portfolios
- Evaluate threats to business-critical applications by using threat modeling
- Design and implement a full lifecycle strategy for application security
- Design and implement standards and practices for securing the application development process
- Design a solution for workload identity to authenticate and access Azure cloud resources
- Design a solution for API management and security
- Design a solution for secure access to applications

Module 13: Design solutions for securing an organization's data

- Design a solution for data discovery and classification using Microsoft Purview
- Specify priorities for mitigating threats to data
- Design a solution for protection of data at rest, data in motion, and data in use
- Design a security solution for data in Azure workloads
- Design a security solution for data in Azure Storage
- Design a security solution that includes Microsoft Defender for SQL and Microsoft Defender for Storage

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

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

Module 15: Specify requirements for securing SaaS, PaaS, and IaaS services

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

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

- Evaluate security posture by using Microsoft Cloud Security Benchmark, Microsoft Defender for Cloud, and Secure Scores
- Design integrated security posture management and workload protection solutions in hybrid and multicloud environments
- Design cloud workload protection solutions that use Microsoft Defender for Cloud

Module 17: Design solutions for securing server and client endpoints

- Specify security requirements for servers
- Specify security requirements for mobile devices and clients
- Specify security requirements for IoT devices and embedded systems
- Design a solution for securing operational technology (OT) and industrial control systems (ICS) by using Microsoft Defender for IoT
- Specify security baselines for server and client endpoints
- Design a solution for secure remote access

Module 18: Design solutions for network security

- Design solutions for network segmentation
- Design solutions for filtering traffic with network security groups
- Design solutions for network posture measurement
- Design solutions for network monitoring

Module 19: Case study: Design security solutions for infrastructure

- How to analyze business requirements
- How to match technical capabilities to meet those needs

How to design cohesive solutions that incorporate all of the required functions