SC-100T00 Microsoft Cybersecurity Architect

Overview

Course Duration: 4 Days

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).*

Audience Profile

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.

Course Outline

Module 1: Introduction to Zero Trust and best practice frameworks
Module 2: Design solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)
Module 3: Design solutions that align with the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB)
Module 4: Design a resiliency strategy for common cyberthreats like ransomware
Module 5: Case study: Design solutions that align with security best practices and priorities
Module 6: Design solutions for regulatory compliance
Module 7: Design solutions for identity and access management
Module 8: Design solutions for securing privileged access
Module 9: Design solutions for security operations
Module 10: Case study: Design security operations, identity and compliance capabilities
Module 11: Design solutions for securing Microsoft 365
Module 12: Design solutions for securing applications
Module 13: Design solutions for securing an organization's data
Module 14: Case study: Design security solutions for applications and data
Module 15: Specify requirements for securing SaaS, PaaS, and IaaS services
Module 16Design solutions for security posture management in hybrid and multicloud environments
Module 17: Design solutions for securing server and client endpoints
Module 18: Design solutions for network security
Module 19: Case study: Design security solutions for infrastructure

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.