SC 100- Microsoft Cybersecurity Architect

Days: 4

Prerequisites: Before attending this course, students must 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); have taken Microsoft Azure Administrator (AZ-104T00), Microsoft 365 Administrator (MS-102T00) and Defend against cyberthreats with Microsoft's security operations platform (SC-200T00) or possess an equivalent knowledge; have advanced experience and knowledge in identity and access, platform protection, security operations, securing data and securing applications; and have experience with hybrid and cloud implementations.

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.

Description: 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).

OUTLINE:

MODULE 1: SC-100: DESIGN SOLUTIONS THAT ALIGN WITH SECURITY BEST PRACTICES AND PRIORITIES

- 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 ransomware and other attacks based on Microsoft Security Best Practices
- Case study: Design solutions that align with security best practices and priorities

MODULE 2: SC-100: DESIGN SECURITY OPERATIONS, IDENTITY, AND COMPLIANCE CAPABILITIES

- 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

MODULE 3: SC-100: DESIGN SECURITY SOLUTIONS FOR APPLICATIONS AND DATA

- Design solutions for securing Microsoft 365

SC 100- Microsoft Cybersecurity Architect

- Design solutions for securing applications
- Design solutions for securing an organization's data
- Case study: Design security solutions for applications and data

MODULE 4: SC-100: DESIGN SECURITY SOLUTIONS FOR INFRASTRUCTURE

- 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