SC-100T00: Microsoft Cybersecurity Architect

Course Duration: 32 Hours (4 Days)

Overview

The SC-100T00: Microsoft Cybersecurity Architect course is an in-depth training program designed to equip learners with the skills necessary to design and implement a robust cybersecurity architecture within their organizations. Module 1 lays the foundation, focusing on creating a comprehensive security strategy that aligns with the Zero Trust model, encompassing Security operations, and Identity security strategies, including considerations for Hybrid and multi-cloud environments. Module 2 dives into Governance Risk Compliance (GRC), where participants learn to design Regulatory compliance strategies and assess security postures to effectively manage risk. Module 3 targets infrastructure security, teaching learners to develop protective strategies for server, client endpoints, and cloud services (SaaS, PaaS, IaaS). Finally, Module 4 concentrates on safeguarding data and applications, guiding through the specification of Security requirements for applications and the formulation of Data security strategies. This comprehensive course ensures that learners emerge with the capability to architect and oversee a strong cybersecurity framework, addressing current and evolving threats and compliance needs.

Audience Profile

The SC-100T00: Microsoft Cybersecurity Architect course equips professionals with advanced skills in designing and implementing cybersecurity strategies. Targeted job roles and audience for the course include:

- Cybersecurity Architects
- Security Engineers
- IT Security Consultants
- Information Security Analysts
- Infrastructure Architects with a focus on security
- Cloud Security Specialists
- Compliance Officers
- Risk Management Analysts
- System Administrators with a focus on security
- Network Security Engineers
- Security Operations Center (SOC) personnel
- Enterprise Architects
- IT Professionals aiming to specialize in cybersecurity architecture
- Technical Decision Makers with a responsibility for security solutions

Course Syllabus

Module 1: Design a Zero Trust strategy and architecture

Build an overall security strategy and architecture

- Identify the integration points in an architecture by using Microsoft Cybersecurity Reference Architecture (MCRA)
- Translate business goals into security requirements
- Translate security requirements into technical capabilities, including security services, security products, and security processes
- Design security for a resiliency strategy
- Integrate a hybrid or multi-tenant environment into a security strategy
- Develop a technical and governance strategy for traffic filtering and segmentation

Design a security operations strategy

- Design a logging and auditing strategy to support security operations
- Develop security operations to support a hybrid or multi-cloud environment
- Design a strategy for SIEM and SOAR
- Evaluate security workflows
- Evaluate a security operations strategy for incident management lifecycle
- Evaluate a security operations strategy for sharing technical threat intelligence

Design an identity security strategy

Note: includes hybrid and multi-cloud

- Design a strategy for access to cloud resources
- Recommend an identity store (tenants, B2B, B2C, hybrid)
- Recommend an authentication strategy
- Recommend an authorization strategy
- Design a strategy for conditional access
- Design a strategy for role assignment and delegation
- Design security strategy for privileged role access to infrastructure including identity-based firewall rules, Azure PIM
- Design security strategy for privileged activities including PAM, entitlement management, cloud tenant administration

Module 2: Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies

Design a regulatory compliance strategy

- Interpret compliance requirements and translate into specific technical capabilities (new or existing)
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
- Interpret compliance scores and recommend actions to resolve issues or improve security
- Design implementation of Azure Policy
- Design for data residency requirements
- Translate privacy requirements into requirements for security solutions

Evaluate security posture and recommend technical strategies to manage risk

- Evaluate security posture by using benchmarks (including Azure security benchmarks, ISO 2701, etc.)
- Evaluate security posture by using Microsoft Defender for Cloud
- Evaluate security posture by using Secure Scores
- Evaluate security posture 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 3: Design security for infrastructure

Design a strategy for securing server and client endpoints

NOTE: includes hybrid and multi-cloud

- Specify security baselines for server and client endpoints
- Specify security requirements for servers, including multiple platforms and operating systems
- Specify security requirements for mobile devices and clients, including endpoint protection, hardening, and configuration
- Specify requirements to secure Active Directory Domain Services
- Design a strategy to manage secrets, keys, and certificates
- Design a strategy for secure remote access

Design a strategy 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 data workloads, including SQL, Azure SQL Database, Azure <Synapse, and Azure Cosmos DB
- Specify security requirements for web workloads, including Azure App Service
- Specify security requirements for storage workloads, including Azure Storage
- Specify security requirements for containers

- Specify security requirements for container orchestration

Module 4: Design a strategy for data and applications

Specify security requirements for applications

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

Design a strategy for securing data

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