multisoft
Systems

SC-100: Microsoft Cybersecurity Architect Training

COURSE CONTENT

GET IN TOUCH

Multisoft Systems
B - 125, Sector - 2, Noida

(+91) 9810-306-956

info@multisoftsystems.com

www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

The SC-100: Microsoft Cybersecurity Architect training by Multisoft Systems is designed to equip IT professionals with the skills and knowledge necessary to design and implement cybersecurity strategies for cloud and hybrid environments. This course focuses on developing security solutions that align with business goals while safeguarding against cyber threats.

Module 1: Design a Zero Trust strategy and architecture

1. 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

2. 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

3. Design an identity security strategy (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 identitybased 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

1. 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

2. 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

1. Design a strategy for securing server and client endpoints (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

2. 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

1. 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

2. 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