SC - 100 : Microsoft Cybersecurity Architect

Course Outline

Module 1: Introduction to Zero Trust and Best Practice Frameworks

- Understand best practices for cybersecurity architecture.
- Learn about Zero Trust and its role in modernizing cybersecurity.
- Explore best practice frameworks such as MCRA, CAF, and WAF.

Module 2: Design Solutions Aligned with CAF and WAF

- Understand and use the Cloud Adoption Framework (CAF) for secure cloud migration.
- Learn the Well-Architected Framework (WAF) principles for designing secure cloud solutions.

Module 3: Design Solutions Aligned with MCRA and MCSB

- Utilize Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft Cloud Security Benchmark (MCSB) for designing secure solutions.

Module 4: Design a Resiliency Strategy for Cyberthreats

- Address common threats like ransomware.
- Design secure backup and restore solutions.
- Manage security updates for business resiliency.

Module 5: Case Study: Security Best Practices and Priorities

- Analyze business requirements and technical capabilities.
- Design cohesive solutions incorporating required functions.

Module 6: Design Solutions for Regulatory Compliance

- Translate compliance requirements into security solutions using Microsoft Purview and Priva.
- Use Azure Policy and Microsoft Defender for Cloud for compliance and security.

Module 7: Design Solutions for Identity and Access Management

- Design cloud, hybrid, and multicloud access strategies.
- Develop solutions for Azure Active Directory, external identities, and authentication/authorization strategies.
- Manage secrets, keys, and certificates.

Module 8: Design Solutions for Securing Privileged Access

- Understand privileged access and the Enterprise Access Model.
- Design identity governance and secure administration solutions.
- Address cloud infrastructure entitlement management.

Module 9: Design Solutions for Security Operations

- Develop security operations capabilities across hybrid and multicloud environments.

- Implement centralized logging, SIEM solutions, and security workflows.
- Use MITRE ATT&CK for threat detection.

Module 10: Case Study: Security Operations, Identity, and Compliance

- Analyze requirements and technical capabilities.
- Design integrated solutions for security operations, identity, and compliance.

Module 11: Design Solutions for Securing Microsoft 365

- Evaluate and design security solutions for Microsoft 365, including Microsoft 365 Defender.

Module 12: Design Solutions for Securing Applications

- Assess security posture and threats to applications.
- Implement lifecycle strategies for application security and API management.
- Secure application development processes.

Module 13: Design Solutions for Securing Data

- Use Microsoft Purview for data discovery and classification.
- Design solutions for data protection in Azure Storage and SQL.

Module 14: Case Study: Security Solutions for Applications and Data

- Analyze business and technical requirements.
- Design comprehensive security solutions for applications and data.

Module 15: Specify Requirements for SaaS, PaaS, and IaaS Services

- Define security baselines for various cloud service models.
- Address IoT, web workloads, and container security.

Module 16: Design Solutions for Security Posture Management

- Use Microsoft Cloud Security Benchmark and Defender for Cloud to evaluate and manage security posture.

Module 17: Design Solutions for Securing Endpoints

- Specify security requirements for servers, mobile devices, and IoT.
- Design solutions for OT and ICS security using Microsoft Defender for IoT.

Module 18: Design Solutions for Network Security

- Implement network segmentation, traffic filtering, and network posture measurement.

Module 19: Case Study: Security Solutions for Infrastructure

- Analyze requirements and design integrated security solutions for infrastructure.