SC-100T00: Microsoft Cybersecurity Architect

Course Content

Course Description:

In this course, students will be prepared 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).

Course Objectives:

Upon successful completion of this course, students will be able to:

- Understand the Well-Architected Framework and how it can be used to design solutions in the cloud that adhere to sound design principles including security
- Understand how to support business resiliency
- Specify requirements to secure Active Directory Domain Services
- Design Security Event Management (SIEM) solutions
- Evaluate threats to business-critical applications by using threat modeling
- Specify security requirements for containers and container orchestration
- Design a solution for securing operational technology (OT) and industrial control systems (ICS) by using Microsoft Defender for IoT
- Design cohesive solutions that incorporate all of the required functions
- And so much more!

Prerequisites:

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.

Target 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.

SC-100T00: Microsoft Cybersecurity Architect

Topics:

Lesson 1: Introduction to Zero Trust and best practice frameworks
- Introduction to best practices
- Introduction to Zero Trust
- Zero Trust initiatives
- Zero Trust technology pillars part 1
- Zero Trust technology pillars part 2
- Knowledge check - Introduction to Zero Trust and best practice frameworks
- Summary - Introduction to Zero Trust and best practice frameworks

Lesson 2: Design solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)
- Define a security strategy
- Introduction to the Cloud Adoption Framework
- Cloud Adoption Framework secure methodology
- Introduction to Azure Landing Zones
- Design security with Azure Landing Zones
- Introduction to the Well-Architected Framework
- The Well-Architected Framework security pillar
- Knowledge check - Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)
- Summary - Design solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)

Lesson 3: Design solutions that align with the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB)
- Introduction to Microsoft Cybersecurity Reference Architecture and cloud security benchmark
- Design solutions with best practices for capabilities and controls
- Design solutions with best practices for attack protection
- Knowledge check - Design solution with Microsoft Cybersecurity Reference Architecture and Microsoft cloud security benchmark
- Summary - Design solution with Microsoft Cybersecurity Reference Architecture and Microsoft cloud security benchmark

Lesson 4: Design a resiliency strategy for common cyberthreats like ransomware
- Common cyberthreats and attack patterns
- Support business resiliency
- Ransomware protection
- Configurations for secure backup and restore
- Security updates
- Knowledge check - Design a resiliency strategy for common cyberthreats
- Summary - Design a resiliency strategy for common cyberthreats like ransomware

Lesson 5: Case study: Design solutions that align with security best practices and priorities
- Introduction
- Case study description
- Case study answers
- Conceptual walkthrough
- Technical walkthrough
- Knowledge check
- Summary

Lesson 6: Design solutions for regulatory compliance

- Introduction to regulatory compliance
- Translate compliance requirements into a security solution
- Address compliance requirements with Microsoft Purview
- Address privacy requirements with Microsoft Priva
- Address security and compliance requirements with Azure policy
- Evaluate infrastructure compliance with Defender for Cloud
- Knowledge check
- Summary - Design solutions for regulatory requirements

Lesson 7: Design solutions for identity and access management

- Introduction to Identity and Access Management
- Design cloud, hybrid and multicloud access strategies (including Microsoft Entra ID)
- Design a solution for external identities
- Design modern authentication and authorization strategies
- Align conditional access and Zero Trust
- Specify requirements to secure Active Directory Domain Services (AD DS)
- Design a solution to manage secrets, keys, and certificates
- Knowledge check - Design solutions for identity and access management
- Summary - Design solutions for identity and access management

Lesson 8: Design solutions for securing privileged access

- Introduction to privileged access
- The enterprise access model
- Design identity governance solutions
- Design a solution to secure tenant administration
- Design a solution for cloud infrastructure entitlement management (CIEM)
- Design a solution for privileged access workstations and bastion services
- Knowledge check - Design solutions for securing privileged access management
- Summary - Design solutions for securing privileged access

Lesson 9: Design solutions for security operations

- Introduction to Security operations (SecOps)
- Design security operations capabilities in hybrid and multicloud environments
- Design centralized logging and auditing
- Design security information and event management (SIEM) solutions
- Design solutions for detection and response
- Design a solution for security orchestration, automation, and response (SOAR)
- Design security workflows
- Design threat detection coverage
- Knowledge check - Design solutions for security operations
- Summary - Design solutions for security operations

Lesson 10: Case study: Design security operations, identity and compliance capabilities

- Introduction
- Case study description
- Case study answers
- Conceptual walkthrough
- Technical walkthrough
- Knowledge check
- Summary

Lesson 11: Design solutions for securing Microsoft 365

- Introduction to security for Exchange, Sharepoint, OneDrive and Teams
- Evaluate security posture for collaboration and productivity workloads
- Design a Microsoft Defender XDR solution
- Design configurations and operational practices for Microsoft 365
- Knowledge check - Design solutions for securing Microsoft 365
- Summary - Design solutions for securing Microsoft 365

Lesson 12: Design solutions for securing applications

- Introduction to application security
- Design and implement standards to secure application development
- Evaluate security posture of existing application portfolios
- Evaluate application threats with threat modeling
- Design security lifecycle strategy for applications
- Secure access for workload identities
- Design a solution for API management and security
- Design a solution for secure access to applications
- Knowledge check - Design solutions for securing applications
- Summary - Design solutions for securing applications

Lesson 13: Design solutions for securing an organization's data

- Introduction to data security
- Design a solution for data discovery and classification using Microsoft Purview
- Design a solution for data protection
- Design data security for Azure workloads
- Design security for Azure Storage
- Design a security solution with Microsoft Defender for SQL and Microsoft Defender for Storage
- Knowledge check - Design solutions for securing an organization's data
- Summary - Design solutions for securing an organization's data

Lesson 14: Case study: Design security solutions for applications and data

- Introduction
- Case study description
- Case study answers
- Conceptual walkthrough
- Technical walkthrough
- Knowledge check
- Summary

Lesson 15: Specify requirements for securing SaaS, PaaS, and IaaS services

- Introduction to security for SaaS, PaaS, and IaaS
- Specify security baselines for SaaS, PaaS, and IaaS services
- Specify security requirements for web workloads
- Specify security requirements for containers and container orchestration
- Knowledge check - Specify requirements for securing SaaS, PaaS and IaaS services
- Summary - Specify requirements for securing SaaS, PaaS, and IaaS services

SC-100T00: Microsoft Cybersecurity Architect

Lesson 16: Design solutions for security posture management in hybrid and multicloud environments

- Introduction to hybrid and multicloud posture management
- Evaluate security posture by using Microsoft Cloud Security Benchmark
- Design integrated posture management and workload protection
- Evaluate security posture by using Microsoft Defender for Cloud
- Posture evaluation with Microsoft Defender for Cloud secure score
- Design cloud workload protection with Microsoft Defender for Cloud
- Integrate hybrid and multicloud environments with Azure Arc
- Design a solution for external attack surface management
- Knowledge check - Design solutions for security posture management in hybrid and multicloud environments
- Summary - Design solutions for security posture management in hybrid and multicloud environments

Lesson 17: Design solutions for securing server and client endpoints

- Introduction to endpoint security
- Specify server security requirements
- Specify requirements for mobile devices and clients
- Specify internet of things (IoT) and embedded device security requirements
- Secure operational technology (OT) and industrial control systems (ICS) with Microsoft Defender for IoT
- Specify security baselines for server and client endpoints

- Design a solution for secure remote access
- Knowledge check - Design solutions for securing server and client endpoints
- Summary - Design solutions for securing server and client endpoints

Lesson 18: Design solutions for network security

- Introduction
- Design solutions for network segmentation
- Design solutions for traffic filtering with network security groups
- Design solutions for network posture management
- Design solutions for network monitoring
- Knowledge check - Design solutions for network security
- Summary - Design solutions for network security

Lesson 19: Case study: Design security solutions for infrastructure

- Introduction
- Case study description
- Case study answers
- Conceptual walkthrough
- Technical walkthrough
- Knowledge check
- Summary

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535