Microsoft Cybersecurity Architect

Duration: 4 Days

Course 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).

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.

Course Outline:

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

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

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

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

Case study: Design solutions that align with security best practices and priorities

- Introduction
- Case study description10 min
- Case study answers20 min
- Conceptual walkthrough25 min
- Technical walkthrough

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

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

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

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

Case study: Design security operations, identity and compliance capabilities

- 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

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

Case study: Design security solutions for applications and data

- Introduction
- Case study description
- Case study answers
- Conceptual walkthrough
- Technical walkthrough

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

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

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

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