Microsoft Cybersecurity Architect

Course SC-100T00: 4 days; Instructor-Led

Introduction

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).

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.

Job role: Solution Architect
Preparation for exam: SC-100

Prerequisites

Before attending this course, students must have:

- Highly recommended to have attended and passed one of the associate level certifications in the security, compliance and identity portfolio (such as AZ-500, SC-200 or SC-300)
- Advanced experience and knowledge in identity and access, platform protection, security operations, securing data and securing applications.
- Experience with hybrid and cloud implementations.

Course Outline

Module 1: Build an overall security strategy and architecture

Learn how to build an overall security strategy and architecture with zero trust in mind.

In this module, you will:

- Develop Integration points in an architecture
- Develop security requirements based on business goals
- Translate security requirements into technical capabilities
- Design security for a resiliency strategy
- Design security strategy for hybrid and multi-tenant environments
- Design technical and governance strategies for traffic filtering and segmentation

Lessons

- Introduction
- Zero Trust overview
- Develop Integration points in an architecture
- Develop security requirements based on business goals
- Translate security requirements into technical capabilities
- Design security for a resiliency strategy
- Design a security strategy for hybrid and multi-tenant environments
- Design technical and governance strategies for traffic filtering and segmentation

- Exercise: Build an overall security strategy and architecture

Module 2: Design a security operations strategy
Learn how to design a cybersecurity strategy for security operations (SecOps).

In this module, you will:
- Design a logging and auditing security strategy.
- Develop security operations for hybrid and multicloud environments.
- Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR).
- Evaluate security workflows.
- Review security strategies for incident management.
- Evaluate security operations for technical threat intelligence.
- Monitor sources for insights on threats and mitigations.

Lessons
- Introduction
- Understand security operations frameworks, processes, and procedures
- Design a logging and auditing security strategy
- Develop security operations for hybrid and multicloud environments
- Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR)
- Evaluate security workflows
- Review security strategies for incident management
- Evaluate security operations for technical threat intelligence
- Monitor sources for insights on threats and mitigations
- Exercise: Design a security operations strategy

Module 3: Design an identity security strategy
Learn how to design a cybersecurity strategy for identity management.

In this module, you will:
- Recommend an identity store for security.
- Recommend secure authentication and security authorization strategies.
- Secure conditional access.
- Design a strategy for role assignment and delegation.
- Define Identity governance for access reviews and entitlement management.
- Design a security strategy for privileged role access to infrastructure.
- Design a security strategy for privileged access.

Lessons
- Introduction
- Secure access to cloud resources
- Recommend an identity store for security
- Recommend secure authentication and security authorization strategies
- Secure conditional access
- Design a strategy for role assignment and delegation
- Define Identity governance for access reviews and entitlement management
- Design a security strategy for privileged role access to infrastructure
- Design a security strategy for privileged activities
- Exercise: Design an identity security strategy

Module 4: Evaluate a regulatory compliance strategy
Learn how to evaluate a cybersecurity strategy for regulatory compliance.

In this module, you will:

- Interpret compliance requirements and their technical capabilities.
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud.
- Interpret compliance scores and recommend actions to resolve issues or improve security.
- Design and validate implementation of Azure Policy.
- Design for data residency Requirements.
- Translate privacy requirements into requirements for security solutions.

Lessons

- Introduction
- Interpret compliance requirements and their technical capabilities
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
- Interpret compliance scores and recommend actions to resolve issues or improve security
- Design and validate implementation of Azure Policy
- Design for data residency requirements
- Translate privacy requirements into requirements for security solutions
- Exercise: Evaluate a regulatory compliance strategy

Module 5: Evaluate security posture and recommend technical strategies to manage risk

Learn how to evaluate an organization's security posture and recommend technical strategies to manage risk.

In this module, you will:

- Evaluate security postures by using benchmarks.
- Evaluate security postures by using Microsoft Defender for Cloud.
- Evaluate security postures by using Secure Scores.
- Evaluate security hygiene 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.

Lessons

- Introduction
- Evaluate security postures by using benchmarks
- Evaluate security postures by using Microsoft Defender for Cloud
- Evaluate security hygiene of cloud workloads
- Design security for an Azure Landing Zone
- Interpret technical threat intelligence and recommend risk mitigations
- Evaluate security postures by using secure scores
- Recommend security capabilities or controls to mitigate identified risks
- Exercise: Evaluate security posture and recommend technical strategies to manage risk

Module 6: Understand architecture best practices and how they are changing with the Cloud

Learn best practices for cybersecurity architecture and how they have been affected by cloud computing.

In this module, you will:

- Plan and implement a security strategy across teams.
- Establish a strategy and process for proactive and continuous evolution of a security strategy.

Lessons

- Introduction
- Plan and implement a security strategy across teams
- Establish a process for proactive and continuous evolution of a security strategy
- Exercise: Understand architecture best practices and how they are changing with the Cloud

Module 7: Design a strategy for securing server and client endpoints

Learn how to design a cybersecurity strategy to secure server and client endpoints.

In this module, you will:

- Design a logging and auditing security strategy.
- Develop security operations for hybrid and multicloud environments.
- Design a strategy for Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR).
- Evaluate security workflows.
- Review security strategies for incident management.
- Evaluate security operations for technical threat intelligence.
- Monitor sources for insights on threats and mitigations.

Lessons

- Introduction
- Specify security baselines for server and client endpoints
- Specify security requirements for servers
- Specify security requirements for mobile devices and clients
- Specify requirements for securing Active Directory Domain Services
- Design a strategy to manage secrets, keys, and certificates
- Design a strategy for secure remote access
- Plan for endpoint forensics
- Exercise: Design a strategy for securing server and client endpoints

Module 8: Design a strategy for securing PaaS, IaaS, and SaaS services

Learn how to design a cybersecurity strategy which will secure cloud services in the SaaS, PaaS and IaaS service models.

In this module, you will:

- Specify security baselines for SaaS, PaaS and IaaS services.
- Specify security requirements for web, storage, data and IoT workloads.
- Specify security requirements for containers and container orchestration.

Lessons

- Introduction
- Specify security baselines for PaaS services
- Specify security baselines for IaaS services
- Specify security baselines for SaaS services
- Specify security requirements for IoT workloads
- Specify security requirements for data workloads
- Specify security requirements for web workloads
- Specify security requirements for storage workloads
- Specify security requirements for containers
- Specify security requirements for container orchestration
- Exercise: Design a strategy for securing PaaS, IaaS, and SaaS services

Module 9: Specify security requirements for applications

Learn how to specify cybersecurity requirements for applications.

In this module, you will:

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

Lessons

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

- Exercise: Specify security requirements for applications

Module 10: Design a strategy for securing data
Learn how to design a cybersecurity strategy to secure data.

In this module, you will:
- 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.

Lessons
- Introduction
- Prioritize mitigating threats to data
- Design a strategy to identify and protect sensitive data
- Specify an encryption standard for data at rest and in motion
- Exercise: Design a strategy for securing data

Module 11: Recommend security best practices using Microsoft Cybersecurity Reference Architectures (MCRA) and Microsoft Cloud Security Benchmarks
You'll learn how to use guidance in Microsoft Cybersecurity Reference Architectures and Microsoft Cloud Security Benchmarks to help an organization apply Zero Trust principles and secure their infrastructure.

In this module, you will:
- Use the Microsoft Cybersecurity Reference Architecture (MCRA) to recommend security best practices
- Use Microsoft Cloud Security Benchmarks to recommend security best practices
- Use the Zero Trust Rapid Modernization Plan (RaMP) to recommend a strategy for updating organizational security

Lessons
- Introduction
- Recommend best practices for cybersecurity capabilities and controls
- Recommend best practices for protecting from insider and external attacks
- Recommend best practices for Zero Trust security
- Recommend best practices for Zero Trust Rapid Modernization Plan

Module 12: Recommend a secure methodology using the Cloud Adoption Framework (CAF)
You'll learn how to use the Cloud Adoption Framework to recommend security best practices that help an organization move to the cloud while improving overall security posture.

In this module, you will:
- Recommend a DevSecOps process
- Recommend a methodology for asset protection
- Recommend strategies for managing and minimizing risk

Lessons
- Introduction
- Recommend a DevSecOps process
- Recommend a methodology for asset protection
- Recommend strategies for managing and minimizing risk

Module 13: Recommend a ransomware strategy by using Microsoft Security Best Practices
You'll learn how to execute the three important phases of ransomware protection: create a recovery plan, limit the scope of damage, make it hard to get in.

In this module, you will:
- Recognize different types of ransomware

- Help an organization mitigate risk of a ransomware attack by creating a recovery plan
- Help an organization mitigate risk of a ransomware attack by limiting the scope of damage
- Help an organization mitigate risk of a ransomware attack by hardening key infrastructure elements

Lessons

- Introduction
- Plan for ransomware protection and extortion-based attacks
- Protect assets from ransomware attacks
- Recommend Microsoft ransomware best practices

