

## MS-SC100T00: MICROSOFT CYBERSECURITY ARCHITECT



DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
4 Days	Advanced	Security	Instructor-led	NA

### 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 PROFILE

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.

### PREREQUISITES

Before attending this course, students must have:

- Advanced experience and knowledge in identity and access, platform protection, security operations, securing data and securing applications.
- Experience with hybrid and cloud implementations.

### COURSE OBJECTIVES

After completing this course, students will be able to:

- Design a Zero Trust strategy and architecture
- Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies
- Design security for infrastructure
- Design a strategy for data and applications

### COURSE CONTENT

#### Module 1: Introduction to Zero Trust and best practice frameworks

You learn what best practices are, how cybersecurity architects use them, and some key best practice frameworks for Microsoft cybersecurity capabilities. You also learn about the concept of Zero Trust, and how to get started with Zero Trust in an organization.

##### Lessons

- Introduction to best practices
- Introduction to Zero Trust
- Zero Trust initiatives
- Zero Trust technology pillars part 1
- Zero Trust technology pillars part 2
- Module assessment
- Summary - Introduction to Zero Trust and best practice frameworks

After completing this module, students will be able to:

- Understand how to use best practices as a cybersecurity architect.
- Understand the concept of Zero Trust and how it can be used to modernize an organizations cybersecurity.
- Understand when to use different best practice frameworks like MCRA, CAF, and WAF.

#### Module 2: Design security solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)

You'll learn about the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF) and how you can use them to design more secure solutions.

##### Lessons

- 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
- Module assessment
- Summary - Design solutions that align with the Cloud Adoption Framework (CAF) and Well-Architected Framework (WAF)

After completing this module, students will be able to:

- Understand the Cloud Adoption Framework and how it can be used to accelerate and secure an organizations move to the cloud.
- 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.

### Module 3: Design solutions that align with the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB)

You learn about the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB) and how you can use them to design more secure solutions.

Lessons

- 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 protecting against insider, external and supply chain attacks.
- Module assessment
- Summary - Design solution with Microsoft Cybersecurity Reference Architecture and Microsoft cloud security benchmark

After completing this module, students will be able to:

- Understand how to use Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB) to design more secure solutions.

### Module 4: Design a resiliency strategy for ransomware and other attacks based on Microsoft Security Best Practices

You learn about common cyberthreats like ransomware and what kinds of attack patterns an organization must be prepared for.

Lessons

- Common cyberthreats and attack patterns
- Support business resiliency
- Design solutions for mitigating ransomware attacks, including prioritization of BCDR and privileged access
- Design solutions for business continuity and disaster recovery (BCDR), including secure backup and restore
- Evaluate solutions for security updates
- Module assessment
- Summary - Design a resiliency strategy for common cyberthreats like ransomware

After completing this module, students will be able to:

- Understand common cyberthreats like ransomware.

- Understand how to support business resiliency.
- Design configurations for secure backup and restore.
- Design solutions for managing security updates.

### Module 5: Case study: Design solutions that align with security best practices and priorities

Apply your cybersecurity architect skills on a real business scenario in the area of security best practices. You analyze design requirements, answer conceptual and technical questions and design a solution to meet the business needs.

Lessons

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

After completing this module, students will learn:

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

### Module 6: Design solutions for regulatory compliance

You'll learn how to interpret and translate regulatory requirements into technical solutions. You'll also learn how to use capabilities found in Microsoft Purview, Microsoft Priva, and Defender for Cloud for compliance.

Lessons

- Introduction to regulatory compliance
- Translate compliance requirements into security controls
- Design a solution to address compliance requirements by using Microsoft Purview
- Address privacy requirements with Microsoft Priva
- Address security and compliance requirements with Azure policy
- Evaluate and validate alignment with regulatory standards and benchmarks by using Microsoft Defender for Cloud
- Module assessment
- Summary - Design solutions for regulatory requirements

After completing this module, students will be able to:

- Translate compliance requirements into a security solution

- Address compliance requirements with Microsoft Purview
- Design a solution to address privacy requirements with Microsoft Priva
- Design Azure Policy solutions to address security and compliance requirements
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud

### Module 7: Design solutions for identity and access management

You learn about various strategies for managing identities and access to resources, including hybrid and multicloud scenarios, external identities, and conditional access.

Lessons

- 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 harden Active Directory Domain Services (AD DS)
- Design a solution to manage secrets, keys, and certificates
- Module assessment
- Summary - Design solutions for identity and access management

After completing this module, students will be able to:

- Design cloud, hybrid and multicloud access strategies
- Design a solution for Azure Active Directory (Azure AD), part of Microsoft Entra
- Design a solution for external identities
- Design modern authentication and authorization strategies
- Specify requirements to secure Active Directory Domain Services
- Design a solution to manage secrets, keys, and certificates

### Module 8: Design solutions for securing privileged access

You learn advanced techniques for designing solutions that manage privileged access effectively.

Lessons

- Introduction to privileged access
- The enterprise access model
- Evaluate the security and governance of Microsoft Entra ID solutions
- Design a solution to secure tenant administration

- Design a solution for privileged access workstations and bastion services
- Evaluate an access review management solution
- Evaluate the security and governance of on-premises Active Directory Domain Services (AD DS), including resilience to common attacks
- Module assessment
- Summary - Design solutions for securing privileged access

After completing this module, students will be able to:

- Understand privileged access and the Enterprise Access Model
- Design identity governance solutions
- Design a solution for securing administration of cloud tenants

## Module 9: Design solutions for security operations

You learn techniques to design security operations capabilities including logging, auditing, Security Information and Event Management (SIEM), Security Orchestration and Automated Response (SOAR), and security workflows.

Lessons

- Introduction to Security operations (SecOps)
- Design monitoring to support hybrid and multicloud environments
- Design centralized logging and auditing, including Microsoft Purview Audit.
- Design security information and event management (SIEM) solutions
- Design solutions for detection and response that includes extended detection and response (XDR) and security information and event management (SIEM).
- Design a solution for security orchestration, automation, and response (SOAR)
- Design and evaluate security workflows, including incident response, threat hunting, and incident management
- Design and evaluate threat detection coverage by using MITRE ATT&CK matrices, including Cloud, Enterprise, Mobile, and ICS
- Module assessment
- Summary - Design solutions for security operations

After completing this module, students will be able to:

- Design security operations capabilities in hybrid and multicloud environments.
- Design centralized logging and auditing.

- Design Security Information and Event Management (SIEM) solutions.
- Design a solution for detection and response that includes Extended Detection and Response (XDR).
- Design a solution for security orchestration, automation, and response (SOAR).
- Design security workflows.
- Design and evaluate threat detection with the MITRE ATT&CK framework.

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

Apply your cybersecurity architect skills on a real business scenario in the area of security operations, identity, and compliance. You analyze design requirements, answer conceptual and technical questions and design a solution to meet the business needs.

Lessons

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

After completing this module, students will be able to:

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

## Module 11: Design solutions for securing Microsoft 365

You learn how to design security solutions for Exchange, Sharepoint, OneDrive, and Teams.

Lessons

- Introduction to security for Exchange, Sharepoint, OneDrive and Teams
- Evaluate security posture for productivity and collaboration workloads by using metrics
- Design a Microsoft Defender XDR solution
- Design configurations and operational practices for Microsoft 365
- Evaluate data security and compliance controls in Microsoft Copilot for Microsoft 365 services
- Evaluate solutions for securing data in Microsoft 365 using Microsoft Purview
- Module assessment
- Summary - Design solutions for securing Microsoft 365

By the end of this module, you're able to:

- Evaluate security posture for collaboration and productivity workloads
- Design a Microsoft Defender XDR solution
- Design configurations and operational practices for Microsoft 365

## Module 12: Design solutions for securing applications

You learn how to secure applications, APIs and the development process using techniques like posture management, threat modeling, and secure access for workload identities.

Lessons

- 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
- Module assessment
- Summary - Design solutions for securing applications

By the end of this module, you're able to:

- Evaluate security posture of existing application portfolios
- Evaluate threats to business-critical applications by using threat modeling
- Design and implement a full lifecycle strategy for application security
- Design and implement standards and practices for securing the application development process
- Design a solution for workload identity to authenticate and access Azure cloud resources
- Design a solution for API management and security
- Design a solution for secure access to applications

## Module 13: Design solutions for securing an organization's data

You learn about designing solutions that secure an organization's data using capabilities like Microsoft Purview, Defender for SQL, Defender for Storage.

Lessons

- Introduction to data security

- Evaluate solutions for data discovery and classification
- Evaluate solutions for encryption of data at rest and in transit, including Azure KeyVault and infrastructure encryption
- 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
- Module assessment
- Summary - Design solutions for securing an organization's data

By the end of this module, you are able to:

- Design a solution for data discovery and classification using Microsoft Purview
- Specify priorities for mitigating threats to data
- Design a solution for protection of data at rest, data in motion, and data in use
- Design a security solution for data in Azure workloads
- Design a security solution for data in Azure Storage
- Design a security solution that includes Microsoft Defender for SQL and Microsoft Defender for Storage

## Module 14: Case study: Design security solutions for applications and data

Apply your cybersecurity architect skills on a real business scenario in the area of securing applications and data. You analyze design requirements, answer conceptual and technical questions and design a solution to meet the business needs.

### Lessons

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

You learn:

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

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

You learn how to analyze security requirements for different cloud offerings (SaaS, PaaS, and IaaS),

IoT workloads, web workloads and containers.

### Lessons

- Introduction to security for SaaS, PaaS, and IaaS
- Specify security baselines for SaaS, PaaS, and IaaS services
- Specify security requirements for IoT workloads
- Specify security requirements for web workloads
- Specify security requirements for containers and container orchestration
- Evaluate AI Services security
- Module assessment
- Summary - Specify requirements for securing SaaS, PaaS, and IaaS services

By the end of this module, you are able to:

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

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

You learn how to design security posture management solutions that integrate into hybrid and multicloud scenarios using capabilities in Microsoft Defender for Cloud, Azure Arc and Microsoft Cloud Security Benchmark (MCSB).

### Lessons

- 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
- Posture management using Exposure management attack paths
- Module assessment

- Summary - Design solutions for security posture management in hybrid and multicloud environments

By the end of this module, you're able to:

- Evaluate security posture by using Microsoft Cloud Security Benchmark, Microsoft Defender for Cloud, and Secure Scores
- Design integrated security posture management and workload protection solutions in hybrid and multicloud environments
- Design cloud workload protection solutions that use Microsoft Defender for Cloud

## Module 17: Design solutions for securing server and client endpoints

You learn how to analyze the security requirements for different types of endpoints including servers, clients, IoT, OT, mobile, and embedded devices. These requirements take into account different platforms and operating systems and set standards for endpoint protection, hardening, and configuration.

### Lessons

- 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
- Evaluate Windows Local Admin Password Solution (LAPS) solutions
- Module assessment
- Summary - Design solutions for securing server and client endpoints

By the end of this module, you're able to:

- Specify security requirements for servers
- Specify security requirements for mobile devices and clients
- Specify security requirements for IoT devices and embedded systems
- Design a solution for securing operational technology (OT) and industrial control systems (ICS) by using Microsoft Defender for IoT

- Specify security baselines for server and client endpoints
- Design a solution for secure remote access

## Module 18: Design solutions for network security

You learn how to design secure network solutions using techniques like network segmentation, traffic filtering, network monitoring and posture management.

### Lessons

- 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

- Evaluate solutions that use Microsoft Entra Internet Access
- Evaluate solutions that use Microsoft Entra Private Access
- Module assessment
- Summary - Design solutions for network security

By the end of this module, you are able to:

- Design solutions for network segmentation
- Design solutions for filtering traffic with network security groups
- Design solutions for network posture measurement
- Design solutions for network monitoring

## Module 19: Case study: Design security solutions for infrastructure

Apply your cybersecurity architect skills on a real business scenario in the area of infrastructure security. You analyze design requirements, answer conceptual and technical questions and design a solution to meet the business needs.

### Lessons

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

### You learn:

- How to analyze business requirements
- How to match technical capabilities to meet those needs
- How to design cohesive solutions that incorporate all of the required functions

## ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to write the Microsoft SC-100: Microsoft Cybersecurity Architect exam.