



# GTech Learn

*"Our focus is your Success"*



## Course Contents

# SC-100: Microsoft Cyber Security Architect

<b>Duration:</b> 4 Days	<b>Level:</b> Advance	<b>Role:</b> Solution Architect
<b>Certification:</b> Available	<b>Public Schedules:</b> <a href="#">View Dates</a>	<b>Private Delivery:</b> <a href="#">Reach Us</a>

### What's included?

- ✓ Learn from Microsoft Certified Trainer (MCT's)
- ✓ 24x7 Lab Access
- ✓ Official Courseware
- ✓ Exam Preps / Practice Tests
- ✓ Badges & Completion Certificate
- ✓ Discounted Exam Vouchers



Email: [info@gtechlearn.com](mailto:info@gtechlearn.com)

## Overview

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.

## Contents

### Learning path 1: Introduction to Zero Trust and best practice frameworks

- Introduction to best practices
- Introduction to Zero Trust
- Zero Trust RaMP initiatives
- Zero Trust technology pillars

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

- Define a security strategy
- Introduction to Cloud Adoption Framework
- Cloud Adoption Framework—secure methodology
- Introduction to Azure landing zones
- Design security with Azure landing zones
- Introduction to Well-Architected Framework
- Well-Architected Framework—security pillar
- Solutions with CAF and WAF
- Case study

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

- Introduction to MCRA and MCSB
- Design solutions with best practices for capabilities and controls
- Design solutions with best practices for attack protection
- Case study

## **Learning Path 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
- Case study

## **Learning Path 5: 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
- Use Azure Policy to address security and compliance requirements
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
- Case study

## **Learning Path 6: Design solutions for identity and access management**

- Introduction to identity and access management
- Design cloud, hybrid and multicloud access strategies (including Azure AD)
- Design a solution for external identities
- Design modern authentication and authorization strategies
- Align Conditional Access and Zero Trust
- Design a solution to manage secrets, keys and certificates
- Case study

## Learning Path 7: Design solutions for securing privileged access

- Introduction to privileged access
- Enterprise access model
- Design identity governance solutions
- Design a solution for securing administration of cloud tenants
- Design for cloud infrastructure entitlement management (CIEM)
- Design a solution for privileged access workstations and bastion services
- Case study

## Learning Path 8: 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 SIEM solutions
- Design solutions for detection and response
- Design a solution for SOAR
- Design security workflows
- Design threat detection coverage
- Case study

## Learning Path 9: Design solutions for securing Microsoft 365

- Security for Exchange, Sharepoint, OneDrive and Teams (M365)
- Evaluate security posture for collaboration and productivity workloads
- Design a Microsoft Defender 365 solution
- Design configurations and operational practices for M365
- Case study

## Learning Path 10: Design solutions for securing applications

- Intro to App Security
- Design and implement standards to secure application development
- Evaluate security posture of existing application portfolios
- Design security life cycle strategy for applications
- Design a solution for API management and security
- Design a solution for secure access to applications
- Securing containerized applications
- Case study

**Learning Path 11: Design solutions for securing an organization's data**

- Intro to data security
- Design a solution for data discovery and classification using Microsoft Purview
- Design a solution for protection of data at rest, data in motion, and data in use
- Data security in Azure workloads
- Security for Azure Storage
- Defender for SQL and Defender for Storage
- Case study

**Learning Path 12: Specify requirements for securing SaaS, PaaS, and IaaS services**

- Securing SaaS, PaaS and IaaS (shared responsibility model)
- Security baselines for cloud services
- Specify security requirements for web workloads
- Specify security requirements for containers and container orchestration
- Case study

**Learning Path 13: Design solutions for security posture management in hybrid and multicloud environments**

- Introduction to hybrid and multicloud environments
- Posture evaluation with MCSB
- Overview of posture evaluation with Defender for Cloud
- Posture evaluation with Microsoft Defender for Cloud secure score
- Design posture management and workload protection in hybrid and multicloud environments
- Design cloud workload protection solutions that use Microsoft Defender for Cloud
- Design a solution for integrating hybrid and multicloud environments by using Azure Arc
- External attack surface management
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
- Microsoft Defender for IoT
- Case study

**Learning Path 14: Design solutions for securing server and client endpoints**

- Introduction to endpoint security
- Specify server security requirements and baselines
- Specify requirements for mobile devices and clients
- Specify IoT and embedded device security requirements
- Specify security baselines for server and client endpoints
- Design a solution for secure remote access

- Case study

## **Learning Path 15: Design solutions for network security**

- 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
- Case study

## **Learning Path 16: Case Study**

## **Learning Path 17: Case Study**

## **Learning Path 18: Case Study**

## **Learning Path 19: Case Study**

## About GTech Learn

Established in 2011 in the USA, GTech Learn is one of the leading IT training organizations in North America & South East Asia. Driven by its unique USPs, GTech Learn is spurring competition, meeting the unmet needs of customers, assisting in skills upgrade, and supplementing talent pools with its presence in the USA, Canada, Singapore and India. This is consistent with our vision to help our Learners with skills upgrade for enhanced career opportunities.

As a Microsoft Learning Partner, we offer a broad range of learning solutions across the full Microsoft technology stack that can be customized.

Since 2011, GTech Learn has been developing custom-fit learning solutions that involve creating and delivering maximum results.

We have successfully helped all types of businesses, government entities, and individuals. For this reason, GTech has chosen by Microsoft to deliver comprehensive learning programs around the globe.

With flexible learning options, state-of-the-art delivery methods, numerous language preferences, experienced instructors, and complete dedication to our students, GTech Learn has the capabilities to help students develop their Microsoft skill sets and achieve increasingly high standards of productivity while organizations of all sizes realize the full potential of their technology investments.

## Our Accreditations with Microsoft



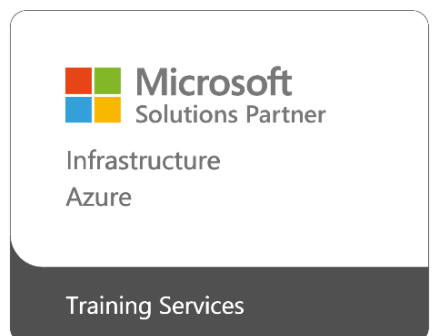
Microsoft Solutions Partner  
Security  
Training Services



Microsoft Solutions Partner  
Modern Work  
Training Services



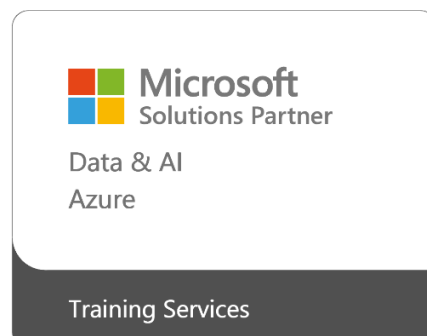
Microsoft Solutions Partner  
Business Applications  
Training Services



Microsoft Solutions Partner  
Infrastructure  
Azure  
Training Services



Microsoft Solutions Partner  
Digital & App Innovation  
Azure  
Training Services



Microsoft Solutions Partner  
Data & AI  
Azure  
Training Services