GTech Learn

"Our focus is your Success"

Microsoft Learning Partner

Course Contents

SC-500: Implement end-to-end security controls for cloud and AI workloads

Duration: **4 Days**	**Level**: **Intermediate**	**Role**: **Security Engineer**
Certification: **Available**	**Public Schedules**: View Dates	**Private Delivery:** Reach Us

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

Microsoft Solutions Partner
Security
Training Services

Email: info@gtechlearn.com

Overview

This course prepares you to design, implement, and manage end-to-end security controls across Microsoft Azure and Microsoft 365 environments — including the emerging landscape of AI workloads and autonomous agents. Through a combination of instructor-led sessions and hands-on labs, you build practical skills in identity security, cloud infrastructure protection, threat detection, and posture management. This course is intended for security engineers who are responsible for planning and implementing security controls across cloud, hybrid, and multi-cloud environments using Microsoft security technologies.

Audience Profile

As a candidate for this course, you're a security engineer who protects organizational systems and data across cloud and hybrid environments by implementing comprehensive security controls that prevent unauthorized access and mitigate risks proactively. This role spans multiple security domains including identity, network, application, data, and compute. This role also ensures that platforms, data, identities, and infrastructure used by AI workloads are securely implemented and monitored. You work closely with architects, administrators, engineers, analysts, and developers responsible for Azure, Microsoft 365, identity and access, information protection, security operations, devops, application development, database platforms, and networks. You should have practical experience in administration of Microsoft Azure and hybrid environments, including compute, network, and storage. You should have strong familiarity with Microsoft Entra ID and familiarity with Microsoft 365 administration. Your responsibilities for this role include:

- Securing access to resources by using Microsoft Entra ID and Azure Key Vault
- Enforcing security and regulatory compliance
- Securing storage, databases, and networking
- Securing compute
- Securing AI solutions
- Managing and monitoring security posture

Contents

Learning path 1: Identity Governance and Access Control

- The Standing Access Problem
- Privileged Identity Management (PIM)
- Entra Agent IDs and Managed Identity
- Conditional Access — Beyond Security Defaults
- Entra ID Protection and Sign-In Risk
- Risk-Based CA Policy Structure
- App Registration Model

Learning Path 2: Securing Azure Key Vault

- The AI secrets problem and risk model
- Key Vault object types: secrets, keys, certificates
- RBAC versus access policies
- Managed identity secret access flow

- Network controls, soft delete, and purge protection
- Defender for Key Vault and mention-only exam topics

Learning Path 3: Security Governance and Role Management

- Compliance audit scenario and governance goals
- Azure Policy model and policy effects
- Compliance dashboard and policy deployment via Bicep
- RBAC scope hierarchy and role assignment model
- Built-in versus custom roles
- Overprivileged access detection and resource locks

Learning Path 4: Security for Azure Storage Accounts

- Storage Accounts – default configuration
- Storage Firewall
- Data plane versus Management plane
- SAS tokens
- Stored access policies
- Storage service encryption
- Defender for Storage

Learning Path 5: Security for Azure Databases

- Common Database security faults
- SQL Authentication versus Microsoft Entra ID Authentication
- Migration to Entra Authentication
- Azure SQL Firewall
- Azure Private Link
- Azure SQL auditing
- Microsoft Sentinel Events logging
- Defender for Databases

Learning Path 6: Security for Azure Networking

- Common issue – Subnet sitting on the Internet
- Network Security Groups (NSG)
- NSG – Defaults and Rule Sets
- Application Security Groups (ASG)
- Azure Firewall
- Hub and Spoke Topology
- Service Endpoints versus Private Endpoints
- Microsoft Entra Private Access versus VPN
- Network Watcher

Learning Path 7: Security for Servers and Virtual Machines

- Common security scenario with Servers and VMs
- Just-in-Time (JIT)
- Azure Arc
- Defender for Servers
- Agent based versus Agentless scanning

- Finding vulnerabilities
- Server disk encryption
- Other exam related topics

Learning path 8: AI data risk and exposure with Microsoft Purview DSPM

- Data exposure challenge
- Potential AI risk with data exposure
- Purview DSPM
- Find potential risks
- SharePoint oversharing
- Reviewing Purview DSPM findings
- Remediation
- Other topics

Learning Path 9: AI agent identity and access security in Microsoft Entra

- Common security scenario with AI Agents
- Defining Microsoft Entra Agent ID
- Agent ID versus Workload ID
- What happens if an Agent ID is compromised?
- Defender XDR
- Specific Agent Identity concepts
- MFA and Agent ID?
- What Conditional Access covers
- Entra Agent ID governance and Microsoft 365

Learning Path 10: Microsoft Foundry and AI Gateway Security

- Common security issues with Microsoft Foundry
- API risks to AI Endpoints
- Prompt injection attacks
- API Gateway
- Two layer defense model
- Gateway controls and Foundry guardrails
- Defender for AI Services
- Supplemental exam topics

Learning Path 11: AI Security Monitoring with Defender for Cloud

- Defender for Cloud – Security Dashboard
- Risks and Recommendations
- Interpret Severity
- Monitoring Posture
- AI Focused dashboard versus Unified Defender for Cloud dashboard

Learning Path 12: Security for Application Platform Services

- Common security scenario with container – monitoring
- Container threat model
- Defender for Containers
- Container registry security

- Container network security
- AKS process flow for security implementation
- Common security scenario – API exposure
- Web Application Firewall (WAF)
- Shared security controls for Apps and APIs
- Gateway policies for Apps and APIs
- Other exam related topics discussion

Learning Path 13: Defender for Cloud Security Posture Management

- Security dashboard
- Secure Score
- Alerts versus Recommendations
- Regulatory Dashboard and Standards
- Key Vault security value
- CSPM Secret Scanning
- Remediation
- Secure Score for AWS and GCP
- CSPM depth plans versus security defaults
- Other exam related topics

Learning Path 14: Microsoft Sentinel Data Collection and Configuration

- Microsoft Sentinel architecture
- What is a connector
- Connect health and status
- Defender XDR connector
- Automation rules
- Sentinel Playbooks and Azure Logic Apps
- Sentinel configuration process
- Other exam related topics

Learning Path 15: Microsoft Security Copilot Configuration

- Security Copilot – Standalone versus Embedded Experience
- What is a Security Compute Unit (SCU)
- Least Privileged – Security Copilot Roles
- Data and Privacy settings
- Security PlugIns
- Automate Security Copilot tasks
- Other exam related topics

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