

SC-500T00: Implement end-to-end security controls for cloud and AI workloads

Course Description

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.

Course Duration

4 days

Prerequisites

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

Course Outline

- Manage and implement authentication methods in Microsoft Entra ID
- Implement and configure Privileged Identity Management (PIM)
- Authenticate your API plugin for declarative agents with secured APIs
- Configure and secure Azure Key Vault
- Manage keys and secrets in Azure Key Vault
- Manage certificates and monitor Azure Key Vault
- Protect Azure Key Vault with Microsoft Defender for Cloud
- Enforce governance with Azure Policy and resource locks
- Configure security controls and remediate recommendations in Defender for Cloud
- Evaluate regulatory compliance in Defender for Cloud
- Manage and right-size RBAC role assignments for least privilege
- Protect backup data with Azure Backup security features
- Implement security controls in infrastructure as code
- Describe Azure storage services
- Implement security and manage access for Azure Storage
- Configure network security for Azure Storage
- Implement Microsoft Defender for Storage
- Configure platform-level security for Azure SQL

- Configure auditing for Azure SQL Database and SQL Managed Instance
- Implement Microsoft Defender for Databases
- Segment and isolate Azure workloads using network security controls
- Centralize and enforce traffic inspection using Azure Firewall
- Secure remote and hybrid connectivity using VPN gateways and Microsoft Entra Private Access
- Eliminate public network exposure of Azure PaaS services
- Secure access for Microsoft Entra Agent Identity
- Analyze AI identity risks using Microsoft Defender XDR
- Enable real-time protection for Copilot Studio agents
- Configure AI Gateway security in Microsoft Foundry
- Configure and manage guardrails in Microsoft Foundry
- Protect AI workloads with Microsoft Defender for Cloud
- Enable Defender for AI Services workload protection in Microsoft Defender for Cloud
- Manage agents using Microsoft Agent 365
- Identify AI data risks using Microsoft Purview Data Security Posture Management
- Implement disk encryption for Azure virtual machines
- Configure trusted launch security features for Azure virtual machines
- Plan and implement Azure Bastion
- Manage security for Arc-enabled hybrid servers
- Implement Microsoft Defender for Servers
- Enable and enforce just-in-time VM access
- Enforce VM security configuration with Azure Machine Configuration
- Detect container risks using Microsoft Defender for Containers
- Implement security controls for Azure Kubernetes Service
- Implement security controls for Azure Container Registry, Container Instances, and Container Apps
- Implement security controls for Azure Function apps and Logic apps
- Implement security controls for Azure App Services and Web Application Firewall
- Implement API backend security using Azure API Management
- Connect hybrid and multicloud environments to Microsoft Defender for Cloud
- Identify security risks by using Cloud Security Posture Management
- Discover unprotected assets and vulnerabilities by using Microsoft Defender External Attack Surface Management
- Evaluate regulatory compliance in Defender for Cloud
- Enable and configure workload protection plans in Microsoft Defender for Cloud
- Configure Microsoft Defender Vulnerability Management settings for Azure VMs
- Create and manage Microsoft Sentinel workspaces
- Manage content in Microsoft Sentinel
- Connect Microsoft services to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Implement automation rules and playbooks in Microsoft Sentinel
- Manage data storage and query audit logs in Microsoft Sentinel
- Describe Microsoft Security Copilot
- Configure workspaces for Microsoft Security Copilot
- Manage plugins and agents in Microsoft Security Copilot

Who Should Attend

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.