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

Overview

Course Duration: 4 Days

About This Course

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

Course Outline

Module 1: Secure access to resources by using Microsoft Entra

Controlling who can access what, and under what conditions, is one of the most consequential responsibilities in cloud security. A misconfigured authentication policy, an overprivileged account left unreviewed, or a poorly secured AI agent can each become the foothold an attacker needs to move laterally through your environment.

In this learning path, you build the skills to close those gaps. You start by designing and deploying secure authentication in Microsoft Entra ID, including configuring multifactor authentication. Next, you configure Conditional Access policies, passwordless options, and self-service password reset for hybrid environments. You then move into privileged access, where you implement Just-in-Time access for Microsoft Entra roles

and Azure resources using Privileged Identity Management (PIM). Just-in-Time access eliminates standing permissions that create unnecessary risk. Finally, you apply these identity and access principles to a modern challenge: securing AI-powered applications and declarative agents that use API plugins to act on behalf of users.

By the end of this learning path, you have a practical, defense-in-depth approach to access security, spanning credential hardening, privileged access governance, and identity-aware AI application design.

- 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

Module 2: Secure Azure Key Vault with defense in depth for the cloud and AI workloads

Implement a defense-in-depth security strategy for Azure Key Vault. In this learning path, you apply security-hardened vault configuration, enforce least-privilege access with just-in-time activation, manage the full lifecycle of keys, secrets, and certificates, and use Microsoft Defender for Cloud to detect exposed credentials and malicious access patterns targeting your vaults.

- 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

Module 3: Enforce security governance and regulatory compliance

Enforce security governance and regulatory compliance across Azure environments. Configure Azure Policy and resource locks to block noncompliant deployments. Then manage security standards and remediate recommendations in Defender for Cloud, evaluate regulatory compliance posture, govern RBAC role assignments at scale, protect backup data against ransomware and deletion, and embed security controls into Bicep pipelines before resources reach production.

- 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

Module 4: Implement security for Azure Storage for the cloud and AI security engineer

Implement a defense-in-depth security strategy for Azure Storage. In this learning path, you harden storage accounts against common attack vectors, and govern access with Microsoft Entra ID managed identities and stored access policies. Next you configure network perimeter controls using firewall rules and private endpoints, and enable Microsoft Defender for Storage to detect threats including malicious file uploads and compromised AI agent credentials.

- Describe Azure storage services
- Implement security and manage access for Azure Storage
- Configure network security for Azure Storage
- Implement Microsoft Defender for Storage

Module 5: Implement security for Azure SQL databases

Implement end-to-end security for Azure SQL Database and SQL Managed Instance. Configure Entra ID authentication with managed identity access, deploy private endpoints, and apply encryption and access controls to protect sensitive financial data. Establish compliant audit trails and enable Microsoft Defender for Databases to detect SQL injection, anomalous access, and vulnerability exposures.

- Configure platform-level security for Azure SQL
- Configure auditing for Azure SQL Database and SQL Managed Instance
- Implement Microsoft Defender for Databases

Module 6: Implement network security controls in Azure

Implement defense-in-depth network security controls in Azure. Segment workloads and enforce least-privilege access using NSGs, ASGs, and Azure Virtual Network Manager. Inspect and control traffic centrally with Azure Firewall. Harden remote and hybrid connectivity and replace broad VPN access with Zero Trust application-level access using Microsoft Entra Private Access. Eliminate public exposure of PaaS and AI services using private endpoints and Azure Private Link.

- 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

Module 7: Implement security for AI

AI workloads introduce new attack surfaces across identity, data, and runtime layers that traditional security controls don’t fully address. In this learning path, you implement layered AI security controls across the Microsoft security platform.

You start by discovering and assessing AI data risks using Microsoft Purview Data Security Posture Management (DSPM). Next you secure agent identities using Microsoft Entra Agent ID and Conditional Access, and analyze AI identity blast radius and attack paths in Microsoft Defender XDR. From there, you configure real-time runtime protection for Copilot Studio agents using Microsoft Defender for Cloud Apps, and secure AI model traffic using AI Gateway in Microsoft Foundry. Finally, you configure guardrails in Microsoft Foundry, protect AI workloads using Microsoft Defender for Cloud, and govern deployed agents using Microsoft Agent 365.

- 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

Module 8: Implement security for servers and virtual machines

Implement layered security controls across Azure virtual machines and Arc-enabled hybrid servers. Configure disk encryption options including encryption at host with customer-managed keys and confidential disk encryption. Enable Trusted Launch security features—Secure Boot, vTPM, and integrity monitoring—to protect against boot-level threats. Eliminate public RDP and SSH exposure with Azure

Bastion. Extend Azure security governance to on-premises and multicloud servers using Azure Arc. Deploy Microsoft Defender for Servers for vulnerability scanning, endpoint detection, agentless machine scanning, and File Integrity Monitoring. Enforce just-in-time VM access to eliminate permanently open management ports. Apply Azure Machine Configuration to audit and enforce OS security baselines across your entire server estate.

- 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

Module 9: Secure Azure application platform services for the cloud and AI security engineer

Implement security controls across Azure application platform services—from container workloads to the API layer. Configure Microsoft Defender for Containers to detect risks in AKS and ACR, enforce AKS security baselines, harden container registries and runtime environments. Then apply authentication, network access, and policy controls across Azure Function apps, Logic apps, App Services, Web Application Firewall, and Azure API Management.

- 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

Module 10: Manage security posture by using Microsoft Defender for Cloud

Learn to build and maintain a strong security posture across your hybrid and multicloud estate using Microsoft Defender for Cloud. You start by connecting on-premises, AWS, and GCP environments to establish unified visibility. You then identify and prioritize security risks using Cloud Security Posture Management (CSPM)—including Secure Score, attack path analysis, and Cloud Security Explorer. You extend that posture view outside-in with Microsoft Defender External Attack Surface Management (EASM) to discover unknown internet-facing assets and surface exploitable exposure. You assess your organization's compliance posture against regulatory frameworks and generate audit-ready reports. Finally, you enable Cloud Workload Protection Platform (CWPP) plans to defend servers, storage, databases, and AI workloads against active threats. Then configure Microsoft Defender Vulnerability Management to scan and remediate vulnerabilities on Azure VMs.

- 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

Module 11: Implement activity and event collection in Microsoft Sentinel

Build a complete event collection and response architecture in Microsoft Sentinel. In this learning path, you set up and secure a Microsoft Sentinel workspace, deploy Content Hub solutions, and connect Azure resource data. Then you collect Linux and Windows security events with data collection rules, and implement automated response workflows with Logic Apps playbooks. The final stage is to manage data retention and audit log access to meet compliance requirements.

- 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

Module 12: Deploy and operate Microsoft Security Copilot

In this learning path, you build a working foundation with Microsoft Security Copilot and advance to enterprise-grade deployment and day-to-day operations. You start by exploring core concepts, how Security Copilot processes natural language prompts, the elements of an effective prompt, and the steps to enable the solution for your organization. You then plan and configure workspaces with the right Security Compute Units, data residency settings, and role assignments to support enterprise segmentation requirements. Finally, you govern plugin access and manage the full lifecycle of both Microsoft-built and partner-built agents to keep your deployment running smoothly and securely.

- Describe Microsoft Security Copilot
- Configure workspaces for Microsoft Security Copilot
- Manage plugins and agents in Microsoft Security Copilot

Prerequisites

- Familiarity with Microsoft Entra ID concepts, including users, groups, and directory roles
- Understanding of Azure role-based access control (RBAC), including role assignments and the Azure scope hierarchy (management group, subscription, resource group, resource) and managed identities
- Basic experience navigating the Azure portal and the Microsoft Entra admin center
- Familiarity with Zero Trust security principles, including least privilege and assume breach
- Awareness of Microsoft Entra ID P2 or Microsoft Entra ID Governance licensing requirements
- Working knowledge of Azure Key Vault, including deploying and using a vault
- Familiarity with Microsoft Defender for Cloud at a foundational level
- Working knowledge of Azure administration at the AZ-104 level, including resource management, role assignments, and virtual network concepts
- Familiarity with Microsoft Defender for Cloud at a foundational level
- Familiarity with Azure Storage accounts including Blob Storage and Azure Files
- Understanding of Azure networking concepts including virtual networks, subnets, and private endpoints
- Familiarity with Azure Key Vault at a conceptual level
- Understanding of Microsoft Defender for Cloud at a conceptual level
- Familiarity with Azure virtual networks, subnets, and basic networking concepts
- Experience deploying and configuring Azure resources in the Azure portal (AZ-104 level)

- Basic understanding of network security concepts such as firewalls, encryption, and access control
- Working knowledge of Microsoft Entra ID and Azure identity concepts
- Familiarity with Microsoft Defender portal and Microsoft Purview portal navigation
- Experience managing cloud security configurations in Azure
- Awareness of AI agent concepts and Microsoft Copilot technologies
- Working knowledge of Azure Virtual Machines, including deploying and managing VMs
- Familiarity with Azure Arc server connectivity
- Completion of (or equivalent knowledge to) Connect hybrid and multicloud environments to Microsoft Defender for Cloud
- Completion of (or equivalent knowledge to) Enable and configure workload protection plans in Microsoft Defender for Cloud
- Familiarity with Azure networking concepts including virtual networks, subnets, and private endpoints
- Basic understanding of container concepts and Azure Kubernetes Service
- Familiarity with Microsoft Defender for Cloud and the Microsoft Defender portal
- Understanding of Azure resource types and Azure role-based access control (RBAC)
- Knowledge of cloud security concepts including misconfigurations, vulnerabilities, and exposure
- Familiarity with cloud identity and access management concepts across Azure, AWS, and GCP
- Working knowledge of Azure resource deployment and Azure role-based access control (RBAC)
- Familiarity with Log Analytics workspaces and basic Kusto Query Language (KQL) queries
- Understanding of Windows Server administration and Windows event logs
- Familiarity with networking fundamentals including TCP/UDP and the syslog protocol
- Foundational understanding of security operations concepts including Security Information and Event Management (SIEM), incidents, and alerting
- Working knowledge of security operations and incident response
- Familiarity with Microsoft security products and services
- Basic knowledge of Azure subscription management and Microsoft Entra roles