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

Course Duration: 4 days

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

Course Syllabus

LP1: Secure access to resources by using Microsoft Entra

- 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

LP2: Secure Azure Key Vault with defense in depth for the cloud and AI workloads

- 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

LP3: Enforce security governance and regulatory compliance

- 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

LP4: Implement security for Azure Storage for the cloud and AI security engineer

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

LP5: Implement security for Azure SQL databases

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

LP6: Implement Network Security Controls in Azure

- 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

LP7: Implement Security for AI

- 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

LP8: Implement Security for Servers and Virtual Machines

- 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

LP9: Secure Azure Application Platform Services for the Cloud and AI Security Engineer

- Secure Azure App Service web apps
- Secure Azure Functions
- Secure Azure Container Apps
- Secure Azure Kubernetes Service (AKS)
- Secure Azure API Management
- Secure Azure Logic Apps
- Secure Azure Event Grid
- Secure Azure Service Bus
- Secure Azure Storage queues and Azure Storage tables

LP10: Manage Security Posture by Using Microsoft Defender for Cloud

- Describe Microsoft Defender for Cloud capabilities
- Manage security posture with Microsoft Defender for Cloud
- Enable enhanced security features in Microsoft Defender for Cloud
- Remediate security recommendations in Microsoft Defender for Cloud
- Implement regulatory compliance controls with Microsoft Defender for Cloud

LP11: Implement Activity and Event Collection in Microsoft Sentinel

- Collect security events from Windows devices using the Microsoft Sentinel agent
- Collect security events from Linux devices using the Microsoft Sentinel agent
- Collect security events from Azure resources using the Azure Monitor agent
- Collect security events from Microsoft 365 services using the Microsoft Sentinel data connector
- Collect security events from Microsoft Defender for Endpoint using the Microsoft Sentinel data connector
- Collect security events from Microsoft Defender for Identity using the Microsoft Sentinel data connector
- Collect security events from Microsoft Defender for Office 365 using the Microsoft Sentinel data connector
- Collect security events from third-party solutions using the Common Event Format connector

LP12: Deploy and Operate Microsoft Security Copilot

- Deploy Microsoft Security Copilot
- Operate Microsoft Security Copilot
- Extend Microsoft Security Copilot
- Integrate Microsoft Security Copilot with Microsoft Sentinel
- Integrate Microsoft Security Copilot with Microsoft Defender XDR
- Integrate Microsoft Security Copilot with Microsoft Intune
- Integrate Microsoft Security Copilot with Microsoft Purview