Training Program: SC-500: Implement End-to-End Security Controls for Cloud and AI Workloads

Published on 17/07/2026

DESCRIPTION OF THE TRAINING:

This course prepares you to design, implement, and manage end-to-end security controls in Microsoft Azure and Microsoft 365 environments, including the emerging landscape of AI workloads and autonomous agents. You'll leave with hands-on skills in identity security, cloud infrastructure protection, threat detection, and posture management.

EDUCATIONAL OBJECTIVES:

At the end of this training, participants will be able to:

- Secure access to resources using Microsoft Entra
- Secure Azure Key Vault with defense-in-depth for cloud and AI workloads
- Enforce security governance and regulatory compliance
- Implement security for Azure storage for cloud and AI security engineer
- Implement security for Azure SQL Databases
- Implement network security controls in Azure
- Implement security for AI
- Implement security for servers and virtual machines
- Secure Azure Application Platform Services for the Cloud and AI Security Engineer
- Manage security posture using Microsoft Defender for Cloud
- Implement activity and event collection in Microsoft Sentinel
- Deploy and operate Microsoft Security Copilot

TEACHING METHODS AND METHODS:

- This training will consist of theory and technical workshops that will allow you to be quickly operational.
- Material: A course material will be given to participants in electronic format.
- Evaluation: The achievements are evaluated throughout the training by the trainer (regular questions, practical work, MCQs or other methods).
- Satisfaction: at the end of the training, each participant answers an evaluation questionnaire which is then analysed with a view to maintaining and improving the quality of our training.
- Follow-up: one attendance sheet is signed per half-day by each of the participants.

TRAINING PROGRAM:

Manage and implement authentication methods in Microsoft Entra ID

- Describe Microsoft Entra ID authentication methods and authentication strength concepts.
- Configure multi-factor authentication by using Conditional Access policies and named locations.
- Implement passwordless authentication methods, including Windows Hello for Business, secret keys, and FIDO2 security keys.
- Configure self-service password reset for users in a hybrid environment.

Implémenter et configurer Privileged Identity Management (PIM)

- Explain why privileged identity management and just-in-time access are essential to a zero-trust security strategy.
- Describe the key features and assignment types in Privileged Identity Management (PIM)
- Implement just-in-time access for Microsoft Entra roles using PIM
- Implement just-in-time access for Azure resource roles using PIM
- Scale just-in-time access to groups using PIM for groups
- Apply just-in-time access models to AI workloads, agents, and applications
- Apply design principles and best practices for "just-in-time" privileged access.

Authenticate your API plugin for declarative agents with secure APIs

- Identify how secure an API is
- Design a secure way to integrate an API plugin for Microsoft 365 Copilot with an API
- Integrate an API plugin with a secure API with an API key
- Integrate an API plugin with a secure API with OAuth2
- Run the API plugin in Microsoft 365 Copilot to validate the results

Configure and secure Azure Key Vaults

- Deploy Azure Key Vault with security controls applied at creation time
- Configure role-based access control and just-in-time privilege for Key Vault operations
- Secure Key Vault network access using firewall rules, virtual network service endpoints, and private endpoints

Manage keys and secrets in Azure Key Vault

- Create and manage cryptographic keys, including HSM and BYOK-protected scenarios
- Configure automated key rotation policies to reduce the risk of exposure to ciphers
- Create a Secrets Rotation with No Downtime Using Dual IDs and Automated Rotation Schemes

Manage certificates and monitor Azure Key Vaults

- Manage certificate issuance, renewal, and lifecycle through built-in certificate authorities
- Configure Key Vault lifetime actions and contacts for the certificate for renewal and automatic notification
- Enable Key Vault diagnostic logging to support security investigations and meet compliance requirements.

Protect Azure Key Vault with Microsoft Defender for Cloud

- Use CSPM Defender's agentless scanning to uncover secrets exposed on VMs and cloud deployments.
- Enable Microsoft Defender for Key Vault and identify its threat detection capabilities
- Review and respond to Microsoft Defender for Key Vault security alerts

Enforce governance with Azure Policies and resource locks

- Assign built-in Azure Policy definitions and initiatives to enforce security configurations across the subscription and management group scope
- Create custom Azure Policy definitions with remediation tasks to apply controls that the built-in definitions don't cover
- Configure Azure resource locks to prevent critical resources from being deleted or modified

Configure security controls and remediate recommendations in Defender for Cloud

- Configure Defender for Cloud environment settings and security standards at the management group perimeter level
- Deploy security controls to remediate recommendations at scale using patches, governance rules, policy remediation tasks, and exemptions

Assess regulatory compliance in Defender for Cloud

- Explain how compliance standards, controls, and assessments work in Defender for Cloud, including the role of the Microsoft Cloud Security Benchmark
- Navigate the Regulatory Compliance Dashboard to identify and investigate failing compliance controls
- Assign regulatory compliance standards to Azure subscriptions and manage compliance scope in the Azure portal
- Generate compliance reports and communicate status by using audit downloads, compliance workbooks, and Microsoft Purview Compliance Manager.

Manage and adjust the size of RBAC role assignments for least privileges

- Assign built-in Azure roles to the appropriate scope using least-privilege principles
- Create custom Azure roles and Microsoft Entra roles for operations that the built-in roles don't cover at the appropriate permission level
- Identify overprivileged role assignments and remediate them using Defender for Cloud CSPM, Cloud Infrastructure Entitlement Management (CIEM), and Microsoft Entra access reviews

Protect backup data with Azure Backup security features

- Configure Vault Temporary Deletion and Immutability to Protect Backup Recovery Points from Deletion
- Implement multi-user authorization using Resource Guard to prevent unauthorized critical backup operations

Implement security controls in infrastructure as code

- Configure Microsoft Defender for DevOps to analyze Bicep and ARM patterns in GitHub Actions and Azure Pipelines
- Apply Azure Policy in a policy-as-code workflow to ensure security compliance when deploying IaC

Describe Azure Storage Services

- Compare Azure storage services
- Describe storage tiers
- Describe redundancy options
- Describe storage account options and storage types
- Identify file move options, including AzCopy, Azure Storage Explorer, and Azure File Sync
- Describe migration options, including Azure Migrate and Azure Data Box

Implement security and manage access for Azure Storage

- Configure storage account security settings, including secure transfer, Transport Layer Security (TLS), and anonymous access controls
- Select an appropriate authorization model for different access scenarios, including managed identity for AI agent workloads
- Create and manage stored access policies to control the lifecycle of SAP tokens
- Disable shared key permission and enforce compliance using Azure Policy

Configure network security for Azure storage

- Describe how Azure Storage firewall rules restrict access through the public endpoint
- Create virtual network rules and IP network rules for trusted sources
- Configure resource instance rules for Azure AI and PaaS services
- Add trusted service exceptions for Azure platform services
- Implement private endpoints for fully private storage connectivity

Implement Microsoft Defender for Storage

- Describe the three pillars of Microsoft Defender for Storage detection and how they differ from the classic plan.
- Enable Defender for Storage at the subscription and resource level using policy-driven deployment
- Configure malware scanning with monthly GB limits for cost control
- Configure sensitive data threat detection
- Set up alert notifications and verify that Defender outputs reach the appropriate security team

Configure platform-level security for Azure SQL

- Configure Microsoft Entra ID authentication and disable SQL authentication on Azure SQL
- Implement network isolation for Azure SQL using private endpoints and firewall rules
- Enable transparent data encryption and configure customer-managed keys for regulated workloads
- Enforce dynamic data masking and row-level security to restrict access to sensitive data

Configure auditing for Azure SQL Database and SQL Managed Instance

- Describe Azure SQL auditing capabilities and select the appropriate audit action groups
- Configure audit log destinations for Azure SQL Database
- Configure auditing for SQL Managed Instance
- Design a compliant audit strategy using multiple log destinations

Implement Microsoft Defender for Databases

- Describe Microsoft Defender for database plans and threat detection capabilities
- Enable Defender for Azure SQL Databases at the subscription scope
- Enable Defender for open source relational databases
- Configure vulnerability assessment to establish security baselines for Azure SQL
- Configure alert routing to provide Defender detections to the security operations team

Segment and isolate Azure workloads using network security controls

- Evaluate a virtual network topology to identify lateral movement risks and network segmentation gaps
- Configure NSG rules to enforce least-privilege access between Azure workloads

- Use ASGs to simplify and maintain NSG rule sets for aggregated workloads
- Configure Azure Virtual Network Manager security administrative rules to enforce organization-wide network security policies
- Verify effective network security rules using Network Watcher diagnostics

Centralize and enforce traffic inspection using Azure Firewall
- Determine when Azure Firewall is needed to address threats that Network Security Group (NSG) filtering can't mitigate
- Configure Azure Firewall Rule Collections and Firewall Policy to Control and Inspect Network Traffic
- Deploy Azure Firewall on a Virtual WAN hub to centralize inspection of hub-spoke and branch traffic

Secure remote and hybrid connectivity using VPN gateways and Microsoft Entra Private Access
- Identify security risks in VPN gateway configurations for site-to-site and point-to-site connections
- Configure VPN gateway settings to reduce the attack surface through stronger authentication and encryption
- Deploy Microsoft Entra Private Access to enforce Zero Trust app-level access for remote users

Eliminate public network exposure to Azure PaaS services
- Assess the attack surface created by public PaaS service endpoints in an Azure environment
- Set up private endpoints to route access to Azure PaaS and AI services over a private network
- Configure Azure Private Link service to expose internal services without creating a public endpoint
- Enforce private endpoint adoption at scale using Azure Policy and Defender for Cloud

Secure access for Microsoft Entra agent identity
- Map how AI agents authenticate and identify where Conditional Access applies
- Configure Conditional Access policies limited to agent identities
- Control access to agents and manage agent identity lifecycle events

Analyze AI identity risks using Microsoft Defender XDR
- Discover AI agents in Microsoft Defender XDR using AI agent inventory
- Assess the radius of agent identity explosion by looking at permissions, knowledge sources, and plan configuration
- Analyze attack paths that could lead to unauthorized access if an agent identity is compromised

Enable real-time protection for Copilot Studio agents
- Describe the AI agent protection capabilities available in Microsoft Defender for Cloud Apps
- Enable real-time protection for Copilot Studio agents in the Microsoft Defender portal
- Verify that agent protection results appear in Microsoft Defender XDR inventory, alerts, and Advanced Hunting.

Configure AI Gateway Security in Microsoft Foundry
- Review the AI Gateway architecture and explain how it secures AI model traffic
- Create and configure an AI gateway instance in Microsoft Foundry
- Apply access controls and monitoring to secure and audit AI Gateway usage

Configure and manage guardrails in Microsoft Foundry

- Explain how guardrails secure model interactions in Microsoft Foundry
- Describe security controls such as content filters, blacklists, and prompt shields
- Configure and validate custom guardrails for different types of workloads
- Evaluate guardrail effectiveness and refine configurations for continuous assurance

Protect AI workloads with Microsoft Defender for Cloud

- Enable and configure the AI workload plan in Microsoft Defender for Cloud
- Review AI asset overviews in the Data and AI Security Dashboard
- Assess and improve AI posture with Cloud Security Posture Management (CSPM)
- Detect and respond to runtime threats using workload protection
- Detect and respond to runtime threats using Cloud Workload Protection (CWP)

Enable Defender for AI workload protection in Microsoft Defender for Cloud

- Enable the Defender for AI plan and configure its components for an Azure subscription
- Review AI threat protection alerts in the Defender portal
- Monitor AI security posture using the data and AI security dashboard in Microsoft Defender for Cloud

Manage agents using Microsoft Agent 365

- Enable and access the Microsoft Agent 365 management interface in the Microsoft 365 admin center
- Enroll agents and apply access controls to enforce organizational policies
- Monitor agent activity and enforce governance controls by using Microsoft Agent 365

Identify AI data risks by using Microsoft Purview Data Security Posture Management

- Configure Microsoft Purview Data Security Posture Management (DSPM) for AI
- Assess the risks of overexposure of SharePoint data that affect AI foundational data.
- Identify sensitive data risks in Copilot and AI app interactions
- Interpret DSPM for AI dashboards and prioritize remediation actions

Implement disk encryption for Azure VMs

- Compare Azure managed disk encryption options and select the appropriate approach for new and existing VMs
- Configure encryption on the host with customer-managed keys using a disk encryption set and Azure Key Vault
- Apply confidential disk encryption to confidential virtual machines
- Enforce disk encryption compliance using Azure Policy

Configure approved launch security features for Azure VMs

- Identify how Trusted Launch protects against boot-level threats using Secure Boot, vTPM, and Health Monitoring
- Enable Trusted Launch and configure its security components on new and existing Azure VMs
- Upgrade existing Gen1 VMs to Gen2 with approved launch enabled
- Enforce Trusted Launch adoption using built-in Azure policies

Plan and implement Azure Bastion

- Select the appropriate Azure Bastion SKU based on scale, functionality, and cost requirements
- Deploy and configure Azure Bastion in an Azure virtual network
- Connect to Azure VMs through Azure Bastion using the portal and native client methods
- Configure advanced Bastion features, including native client support, shareable links, and session recording

Manage Arc-enabled hybrid server security

- Configure RBAC and allow/block lists to protect Arc-enabled servers from the installation of an unauthorized extension
- Assign and manage Azure Policies for Arc-enabled servers to enforce security baselines
- Monitor the security posture of Arc-enrolled servers in Microsoft Defender for Cloud
- Apply machine configuration policies to Arc-registered servers

Implement Microsoft Defender for Servers

- Select Defender for Plan 1 or Plan 2 servers based on required capabilities and integrate Azure VMs and Arc-connected servers
- Configure vulnerability scanning using agentless and agent-based Defender Vulnerability Management
- Manage Microsoft Defender for Endpoint integration and configure agentless scanning and file integrity monitoring

Enable and enforce just-in-time access to virtual machines

- Examine how just-in-time access to virtual machines reduces the attack surface on management ports
- Enable JIT and configure per-port access policies on Azure VMs
- Request and approve JIT access and check access activity
- Enforce JIT adoption in a VM estate using Azure Policy

Enforce VM security configuration with Azure Machine Configuration

- Learn how Azure Computer Configuration audits and enforces settings at the operating system level using Azure Policy
- Deploy the Azure Machine Configuration extension and configure the required prerequisites
- Assign built-in Windows and Linux security baseline policies in audit and enforcement modes
- Create and publish a custom computer configuration for organization-specific requirements

Detect container risks using Microsoft Defender for Containers

- Describe the architecture and protection pillars of Microsoft Defender for Containers.
- Enable and configure the Defender for Containers plan in Microsoft Defender for Cloud
- Evaluate the results of the vulnerability scan of container images from the scan performed by Azure Container Registry (ACR)
- Interpret run-time threat alerts and security posture recommendations for AKS clusters

Implement security controls for Azure Kubernetes Service

- Configure Microsoft Entra ID integration and RBAC for AKS API server authentication and authorization
- Implement network security controls, including private clusters, allowed IP address ranges, and network policies
- Apply workload identity and managed identities to eliminate credential management for AKS workloads
- Enforce pod security standards and container access restrictions

Implement security controls for Azure Container Registry, Container Instances, and Container Apps

- Implement access controls and network isolation for Azure Container Registry

- Configure security controls for Azure Container Instances workloads
- Apply ingress controls, managed identity, and secret management for Azure Container Apps

Implement security controls for Azure function apps and logic apps

- Configure authentication and authorization controls for Azure function apps
- Implement network access controls for function apps, including virtual network integration and private endpoints
- Enforce managed identity, connector security, and network isolation for Azure logic apps

Implement security controls for Azure App Services and Web Application Firewall

- Implement authentication, managed identity, and network controls for Azure App Service
- Configure web application firewall policies, including managed rule sets and custom rules
- Integrate Web Application Firewall with App Service for Edge Protection

Implement API backend security using Azure API Management

- Configure API authentication and authorization policies, including JWT and OAuth 2.0 validation with Microsoft Entra ID
- Implement network security controls, including IP filtering, rate limiting, and virtual network integration for API management
- Enforce back-end connection security using client certificate authentication and mutual TLS
- Configure AI Gateway in API Management to Secure and Govern AI Model Endpoints

Connect hybrid and multicloud environments to Microsoft Defender for Cloud

- Explain the multi-cloud connectivity model in Defender for Cloud, including how federated authentication works for AWS and GCP connectors
- Plan a connector policy for hybrid and multicloud environments, including scope, scan interval, and required permissions by environment type
- Connect on-premises machines to Defender for Cloud using Azure Arc-enabled servers
- Connect AWS accounts to Defender for Cloud using the cloud-native connector and CloudFormation template
- Connect GCP projects to Defender for Cloud using the cloud-native connector and GCloud deployment script
- Verify the health of multi-cloud connectivity and confirm CSPM and CWPP coverage surfaces in connected environments

Identify security risks using cloud security posture management

- Differentiate the foundational features of the CSPM and CSPM Defender plans, including AI-powered security posture management capabilities.
- Interpret the cloud security score and security recommendations using the risk-based prioritization model in the Microsoft Defender portal
- Identify externally exploitable attack paths, including those targeting AI workloads, using attack path analysis
- Run graph-based queries in Cloud Security Explorer to proactively detect security risks in Azure environments

Discover unprotected resources and vulnerabilities by using Microsoft Defender External Attack Surface Management

- Explore EASM features and functionality, including resource types, resource states, and how external monitoring differs from other Defender tools.
- Configure resource discovery using seeds to identify infrastructure and connections of unknown internet-facing resources

- Use EASM dashboards to prioritize vulnerabilities and security hygiene risks across your attack surface
- Integrate EASM findings with CSPM Defender to analyze attack paths from resources exposed on the internet

Assess regulatory compliance in Defender for Cloud

- Explain how compliance standards, controls, and assessments work in Defender for Cloud, including the role of the Microsoft Cloud Security Benchmark
- Navigate the Regulatory Compliance Dashboard to identify and investigate failing compliance controls
- Assign regulatory compliance standards to Azure subscriptions and manage compliance scope in the Azure portal
- Generate compliance reports and communicate status by using audit downloads, compliance workbooks, and Microsoft Purview Compliance Manager.

Enable and configure workload protection plans in Microsoft Defender for Cloud

- Identify the CWPP plans available in Defender for Cloud and explain which workloads protect each plan, including Defender for AI and Defender for APIs
- Enable subscription-level workload protection plans using environment settings in the Azure portal
- Configure Defender for Servers (Plan 1 and Plan 2) and Defender for Storage sub-settings for your protection needs
- Deploy protection plans at scale using management groups and Azure Policy, and verify plan coverage by using the Coverage workbook

Configure Microsoft Defender Vulnerability Management settings for Azure VMs

- Manage vulnerabilities Microsoft Defender integrates with Defender for Plan 1 and Plan 2 servers to provide agentless vulnerability scanning for Azure VMs
- Configure vulnerability scanning for Azure VMs at the subscription and machine scope level using Defender for Cloud settings.
- Review vulnerability findings, interpret CVE and severity data, and then create opt-out rules to manage accepted risks in the Defender portal
- Apply the premium capabilities of Defender for Servers Plan 2, including security baseline assessment and application blocking, to strengthen the security posture of VMs.

Create and manage Microsoft Sentinel workspaces

- Describe the architecture of the Microsoft Sentinel workspace
- Integrate a Microsoft Sentinel workspace with Microsoft Defender
- Manage a Microsoft Sentinel workspace in Microsoft Defender

Manage content in Microsoft Sentinel

- Install a content hub solution in Microsoft Sentinel
- Connect a GitHub repository to Microsoft Sentinel

Connect Microsoft services to Microsoft Sentinel

- Connect Microsoft Service Connectors
- Explain how connectors automatically declare incidents in Microsoft Sentinel

Connect Syslog data sources to Microsoft Sentinel

- Describe the Azure Monitor agent data collection rule for Syslog

- Install and configure the Azure Monitor Linux Agent extension with the Syslog data collection rule
- Run Azure Arc Linux deployment and sign-in scripts
- Verify that Syslog log data is available in Microsoft Sentinel
- Create an analyzer using KQL in Microsoft Sentinel

Connect Common Event Format logs to Microsoft Sentinel
- Explain the options for deploying the Common Event Format connector in Microsoft Sentinel
- Run the deployment script for the Common Event Format connector

Connect Windows hosts to Microsoft Sentinel
- Connect Windows Azure VMs to Microsoft Sentinel
- Connect non-Azure Windows hosts to Microsoft Sentinel
- Install and configure a data connector to collect Sysmon events

Implement automation rules and playbooks in Microsoft Sentinel
- Explain the difference between automation rules and playbooks in Microsoft Sentinel
- Create automation rules to automate incident management tasks
- Set up and activate a pre-built playbook from the Microsoft Sentinel Content Hub
- Create a custom Logic Apps playbook and connect it to an automation rule

Manage data storage and query audit logs in Microsoft Sentinel
- Create custom log tables in a Microsoft Sentinel workspace to store non-standard ingested data
- Configure data retention levels and archiving policies for Microsoft Sentinel tables
- Connect Microsoft Purview Audit as a data source in Microsoft Sentinel
- Query Purview audit logs in the Microsoft Defender XDR portal

Describe Microsoft Copilot Security
- Describe what Microsoft Security Copilot is.
- Describe Microsoft Security Copilot terminology.
- Describe how the Microsoft Security Copilot handles command requests.
- Describe the elements of an effective prompt
- Describe how to enable Microsoft Security Copilot.

Set up workspaces for Microsoft Security Copilot
- Plan a workspace deployment by evaluating capacity, data residency, and role requirements
- Create a Security Copilot workspace with the appropriate SCUs, geo-selection, and data sharing settings
- Assign and manage roles and permissions in a workspace
- Configure Workspace-Level Owner Settings and Plugins
- Assign workspaces for built-in Microsoft Security Copilot agents
- Monitor and adjust workspace capacity utilization

Manage plug-ins and agents in Microsoft Security Copilot
- Configure plug-in settings to govern who can add and manage custom plug-ins at the user and organization scope
- Restrict access to the pre-installed plugin to manage availability in embedded and standalone experiences
- Discover and configure Microsoft-developed agents using the Security Copilot agent library.

- Acquire and configure partner-developed agents using the Security Store, including the Global Admin approval workflow.
- Manage agents by monitoring runtime, modifying configuration, and conserving agent memory

PREREQUISITES:

To take this course, you should have hands-on experience administering Microsoft Azure and hybrid environments, including compute, networking, and storage. You should have a solid knowledge of Microsoft Entra ID and Microsoft 365 administration. Ideally, you should have completed the "AZ-900: Azure Fundamentals" training and the "AZ-104: Administration in Azure" training or have an equivalent level.

DURATION: 4 days (28 hours)

CONTACT PERSONS: Security Engineer

LEVEL: Advanced