Microsoft - Implement end-to-end security controls for cloud and AI workloads

Course Number: SC-500T00

Duration: 4 days

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.

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 Details

Outline

- Manage and implement authentication methods in Microsoft Entra ID
  - Explore Microsoft Entra ID authentication methods
  - Configure multifactor authentication in Microsoft Entra ID
  - Implement passwordless authentication in Microsoft Entra ID
  - Configure self-service password reset in Microsoft Entra ID
  - Exercise - Configure authentication methods in Microsoft Entra ID
  - Module assessment
- Implement and configure Privileged Identity Management (PIM)
  - Why Privileged Identity Management and just-in-time access matter
  - Core capabilities of Privileged Identity Management (PIM)
  - Implement just-in-time access for Microsoft Entra roles
  - Implement just-in-time access for Azure roles and resources
  - Scaling with PIM for Groups
  - Applying JIT access to AI workloads, agents, and applications
  - JIT design patterns and best practices
  - Module assessment
- Authenticate your API plugin for declarative agents with secured APIs
  - Integrate an API plugin with an API secured with a key
  - Exercise - Integrate an API plugin with an API secured with a key
  - Integrate an API plugin with an API secured with OAuth
  - Exercise - Integrate an API plugin with an API secured with OAuth
  - Module assessment
- Configure and secure Azure Key Vault

    - Deploy Azure Key Vault with security controls
    - Configure access to Azure Key Vault
    - Configure Key Vault firewall and network settings
    - Knowledge check
- Manage keys and secrets in Azure Key Vault
    - Manage cryptographic keys in Azure Key Vault
    - Manage secrets in Azure Key Vault
    - Knowledge check
- Manage certificates and monitor Azure Key Vault
    - Manage certificates in Azure Key Vault
    - Enable Key Vault audit logging
    - Knowledge check
- Protect Azure Key Vault with Microsoft Defender for Cloud
    - Scan for exposed secrets using Defender Cloud Security Posture Management (CSPM)
    - Enable Microsoft Defender for Key Vault
    - Investigate and respond to Defender for Key Vault alerts
    - Knowledge check
- Enforce governance with Azure Policy and resource locks
    - Assign built-in Azure Policy definitions
    - Create and deploy custom policy definitions
    - Implement resource locks
    - Knowledge check
- Configure security controls and remediate recommendations in Defender for Cloud
    - Configure Defender for Cloud and manage security standards
    - Deploy remediation controls at scale
    - Knowledge check
- Evaluate regulatory compliance in Defender for Cloud
    - Understand compliance standards and controls in Defender for Cloud
    - Navigate the regulatory compliance dashboard and investigate control gaps
    - Assign standards and communicate compliance posture

    - Knowledge check
- Manage and right-size RBAC role assignments for least privilege
    - Assign and manage Azure built-in roles
    - Create custom Azure roles and Microsoft Entra roles
    - Evaluate and remediate overprivileged access
    - Knowledge check
- Protect backup data with Azure Backup security features
    - Enable soft delete and immutable vaults
    - Configure Multi-User Authorization and RBAC for backup
    - Knowledge check
- Implement security controls in infrastructure as code
    - Scan IaC templates using Microsoft Defender for DevOps
    - Enforce policy compliance in IaC deployments
    - Knowledge check
- Describe Azure storage services
    - Describe Azure storage accounts
    - Describe Azure storage redundancy
    - Describe Azure storage services
    - Identify Azure data migration options
    - Identify Azure file movement options
    - Module assessment
- Implement security and manage access for Azure Storage
    - Configure storage account security settings
    - Select an authorization model for Azure Storage
    - Manage access with stored access policies
    - Disable Shared Key authorization and enforce with Azure Policy
    - Knowledge check
- Configure network security for Azure Storage
    - Describe Azure Storage network security controls
    - Configure virtual network and IP rules
    - Configure resource instance rules and trusted services

    - Implement private endpoints for storage accounts
    - Knowledge check
- Implement Microsoft Defender for Storage
    - Explore Microsoft Defender for Storage capabilities
    - Enable and deploy Defender for Storage
    - Configure malware scanning and sensitive data detection
    - Configure alert routing and validate Defender coverage
    - Knowledge check
- Configure platform-level security for Azure SQL
    - Configure authentication and managed identity access
    - Implement network isolation
    - Encrypt and protect data in transit and at rest
    - Apply data masking and row-level security
    - Knowledge check
- Configure auditing for Azure SQL Database and SQL Managed Instance
    - Describe Azure SQL auditing capabilities
    - Configure audit destinations for Azure SQL Database
    - Configure auditing for SQL Managed Instance
    - Design a compliant audit strategy
    - Knowledge check
- Implement Microsoft Defender for Databases
    - Explore Microsoft Defender for Databases capabilities
    - Enable Defender for Azure SQL Databases at subscription scope
    - Enable Defender for open-source relational databases
    - Configure vulnerability assessment
    - Configure alert routing and validate coverage
    - Knowledge check
- Segment and isolate Azure workloads using network security controls
    - Assess network segmentation gaps
    - Control traffic with network security groups (NSGs)
    - Simplify rule management with application security groups
    - Enforce consistent policy with Azure Virtual Network Manager

    - Verify effective network security rules with Network Watcher
    - Knowledge check
- Centralize and enforce traffic inspection using Azure Firewall
    - Determine when centralized traffic inspection is required
    - Configure Azure Firewall rules and policies
    - Secure a Virtual WAN hub with Azure Firewall
    - Knowledge check
- Secure remote and hybrid connectivity using VPN gateways and Microsoft Entra Private Access
    - Assess security risks in hybrid connectivity
    - Harden VPN gateway security
    - Replace broad VPN access with Microsoft Entra Private Access
    - Knowledge check
- Eliminate public network exposure of Azure PaaS services
    - Assess the risk of public PaaS endpoint exposure
    - Configure private endpoints to eliminate public PaaS exposure
    - Expose internal services securely using Azure Private Link service
    - Enforce and audit private endpoint adoption
    - Knowledge check
- Secure access for Microsoft Entra Agent Identity
    - Map authentication flows and Conditional Access scope
    - Configure Conditional Access policies for agents
    - Control agent access and lifecycle
    - Knowledge check
- Analyze AI identity risks using Microsoft Defender XDR
    - Discover AI agents in the Microsoft Defender portal
    - Assess blast radius and attack paths
    - Knowledge check
- Enable real-time protection for Copilot Studio agents
    - Explore Copilot Studio AI agent protection
    - Enable protection in Microsoft Defender
    - Review AI agent protection outputs

    - Knowledge check
- Configure AI Gateway security in Microsoft Foundry
    - Examine AI Gateway architecture
    - Create and configure AI Gateway
    - Secure and monitor AI Gateway access
    - Knowledge check
- Configure and manage guardrails in Microsoft Foundry
    - Understand guardrails and Microsoft Content Safety
    - Understand safety controls in Microsoft Foundry
    - Try out built-in guardrails
    - Create and manage blocklists in Microsoft Foundry
    - Configure and apply guardrails in Microsoft Foundry
    - Choose and refine the right guardrails for your AI workloads
    - Module assessment
- Protect AI workloads with Microsoft Defender for Cloud
    - Enable the AI workloads plan
    - Review insights in the Data & AI security dashboard
    - Assess and improve AI security posture with Cloud Security Posture Management (CSPM)
    - Detect AI threats at runtime with Cloud Workload Protection (CWP)
    - Investigate AI security alerts with prompt evidence in Microsoft Defender XDR
    - Module assessment
- Enable Defender for AI Services workload protection in Microsoft Defender for Cloud
    - Enable and configure the Defender for AI Services plan
    - Monitor AI security with the Data and AI dashboard
    - Knowledge check
- Manage agents using Microsoft Agent 365
    - Enable and navigate Microsoft Agent 365
    - Register agents and apply access controls
    - Monitor agent activity and enforce governance
    - Knowledge check
- Identify AI data risks using Microsoft Purview Data Security Posture Management

    - Configure Data Security Posture Management (DSPM) for AI
    - Assess SharePoint overexposure
    - Identify risks in Copilot and AI app interactions
    - Knowledge check
- Implement disk encryption for Azure virtual machines
    - Choose the right disk encryption option for Azure VMs
    - Configure encryption at host with customer-managed keys
    - Apply confidential disk encryption to confidential virtual machines
    - Knowledge check
- Configure trusted launch security features for Azure virtual machines
    - Identify Trusted Launch components and VM security types
    - Enable Trusted Launch on new and existing Gen2 VMs
    - Migrate Gen1 VMs and configure Trusted Launch components
    - Enforce Trusted Launch adoption with Azure Policy
    - Knowledge check
- Plan and implement Azure Bastion
    - Plan Azure Bastion deployment
    - Deploy and configure Azure Bastion
    - Connect to VMs through Azure Bastion
    - Knowledge check
- Manage security for Arc-enabled hybrid servers
    - Control access and extension security for Arc-enabled servers
    - Apply Azure Policy to Arc-enabled servers
    - Monitor Arc server security posture in Defender for Cloud
    - Knowledge check
- Implement Microsoft Defender for Servers
    - Onboard servers to Defender for Servers
    - Configure vulnerability scanning with Defender Vulnerability Management
    - Configure Defender for Endpoint integration, agentless scanning, and File Integrity Monitoring
    - Knowledge check

- Enable and enforce just-in-time VM access
  - Examine just-in-time VM access requirements and VM eligibility
  - Enable and configure JIT access policies
  - Request Just-in-time (JIT) access and audit access activity
  - Knowledge check
- Enforce VM security configuration with Azure Machine Configuration
  - Explore Azure Machine Configuration extension capabilities and modes
  - Apply built-in security baseline policies
  - Author and assign custom machine configurations
  - Knowledge check
- Detect container risks using Microsoft Defender for Containers
  - Explore Microsoft Defender for Containers
  - Enable and configure Defender for Containers
  - Assess container image vulnerabilities
  - Detect container runtime threats and misconfigurations
  - Knowledge check
- Implement security controls for Azure Kubernetes Service
  - Control AKS cluster access with Microsoft Entra ID and RBAC
  - Secure AKS network access
  - Implement workload identity and secrets management for AKS
  - Enforce pod and container security
  - Knowledge check
- Implement security controls for Azure Container Registry, Container Instances, and Container Apps
  - Secure Azure Container Registry
  - Implement security controls for Azure Container Instances
  - Implement security controls for Azure Container Apps
  - Knowledge check
- Implement security controls for Azure Function apps and Logic apps
  - Configure authentication and authorization for Function apps
  - Secure network access for Function apps
  - Implement security controls for Logic apps

- Knowledge check

- Implement security controls for Azure App Services and Web Application Firewall
  - Implement security controls for Azure App Service
  - Configure Web Application Firewall policies
  - Protect App Service with Web Application Firewall
  - Knowledge check

- Implement API backend security using Azure API Management
  - Configure API authentication and authorization policies
  - Implement API network security and threat protection
  - Secure API Management backend connections
  - Configure AI Gateway in API Management for Azure AI Foundry
  - Knowledge check

- Connect hybrid and multicloud environments to Microsoft Defender for Cloud
  - Explore the Defender for Cloud multicloud connectivity model
  - Plan a connector strategy for hybrid and multicloud environments
  - Connect on-premises machines using Azure Arc
  - Connect AWS accounts to Defender for Cloud
  - Connect GCP projects to Defender for Cloud
  - Verify multicloud coverage and validate protection
  - Knowledge check

- Identify security risks by using Cloud Security Posture Management
  - Explore CSPM plans and posture visibility
  - Analyze security recommendations with risk prioritization
  - Identify attack paths and choke points
  - Hunt for risks with cloud security explorer
  - Knowledge check

- Discover unprotected assets and vulnerabilities by using Microsoft Defender External Attack Surface Management
  - Explore EASM features and capabilities
  - Discover assets using recursive discovery
  - Analyze your attack surface with dashboards
  - Integrate EASM insights with Defender for Cloud

    - Knowledge check
- Evaluate regulatory compliance in Defender for Cloud
    - Understand compliance standards and controls in Defender for Cloud
    - Navigate the regulatory compliance dashboard and investigate control gaps
    - Assign standards and communicate compliance posture
    - Knowledge check
- Enable and configure workload protection plans in Microsoft Defender for Cloud
    - Understand the Defender for Cloud CWPP plan catalog
    - Enable workload protection plans in Environment Settings
    - Configure Defender for Storage and Defender for Databases
    - Deploy plans at scale and verify coverage
    - Knowledge check
- Configure Microsoft Defender Vulnerability Management settings for Azure VMs
    - Explore Microsoft Defender Vulnerability Management (MDVM) integration with Defender for Servers
    - Configure vulnerability scanning for Azure VMs
    - Review and manage vulnerability findings
    - Apply Plan 2 premium MDVM capabilities
    - Knowledge check
- Create and manage Microsoft Sentinel workspaces
    - Plan for the Microsoft Sentinel workspace
    - Create a Microsoft Sentinel workspace
    - Manage workspaces across tenants using Azure Lighthouse
    - Understand Microsoft Sentinel permissions and roles
    - Manage Microsoft Sentinel settings
    - Configure logs
    - Module assessment
    - Summary and resources
- Manage content in Microsoft Sentinel
    - Use solutions from the content hub
    - Use repositories for deployment
    - Module assessment

    - Summary and resources
- Connect Microsoft services to Microsoft Sentinel
    - Plan for Microsoft services connectors
    - Connect the Microsoft 365 connector
    - Connect the Microsoft Entra connector
    - Connect the Microsoft Entra ID Protection connector
    - Connect the Azure Activity connector
    - Module assessment
    - Summary and resources
- Connect syslog data sources to Microsoft Sentinel
    - Plan for syslog data collection
    - Collect data from Linux-based sources using syslog
    - Configure the Data Collection Rule for Syslog Data Sources
    - Parse syslog data with KQL
    - Module assessment
    - Summary and resources
- Connect Common Event Format logs to Microsoft Sentinel
    - Plan for Common Event Format connector
    - Connect your external solution using the Common Event Format connector
    - Module assessment
    - Summary and resources
- Connect Windows hosts to Microsoft Sentinel
    - Plan for Windows hosts security events connector
    - Connect using the Windows Security Events via AMA Connector
    - Connect using the Security Events via Legacy Agent Connector
    - Collect Sysmon event logs
    - Module assessment
    - Summary and resources
- Implement automation rules and playbooks in Microsoft Sentinel
    - Understand Microsoft Sentinel automation options
    - Create automation rules in Microsoft Sentinel
    - Configure and activate a Content Hub playbook

    - Author a custom playbook with Azure Logic Apps
    - Knowledge check
- Manage data storage and query audit logs in Microsoft Sentinel
    - Create custom log tables in Microsoft Sentinel
    - Implement data retention in Microsoft Sentinel
    - Connect Microsoft Purview Audit to Microsoft Sentinel
    - Query Purview Audit logs in Microsoft Defender XDR
    - Knowledge check
- Describe Microsoft Security Copilot
    - Get acquainted with Microsoft Security Copilot
    - Describe Microsoft Security Copilot terminology
    - Describe how Microsoft Security Copilot processes prompt requests
    - Describe the elements of an effective prompt
    - Describe how to enable Microsoft Security Copilot
    - Module assessment
    - Summary and resources
- Configure workspaces for Microsoft Security Copilot
    - Plan a workspace deployment
    - Create a Security Copilot workspace
    - Configure workspace access and settings
    - Assign workspaces for integrated agents
    - Monitor and manage workspace capacity
    - Knowledge check
- Manage plugins and agents in Microsoft Security Copilot
    - Configure plugin settings in Security Copilot
    - Discover and set up Microsoft-built agents
    - Acquire and configure partner agents from Security Store
    - Manage Security Copilot agents
    - Knowledge check