MICROSOFT OFFICIAL CURRICULUM

Implement end to end security controls for cloud and AI workloads

Microsoft

SC-500T00

Official Microsoft Learn-aligned instructor-led program for Implement end to end security controls for cloud and AI workloads.

Security | Intermediate | Security Copilot

DURATION	LEVEL	FORMAT	CERTIFICATION
4 days	Intermediate	Virtual, On-site, or Hybrid	SC-500T00

AUDIENCE PROFILE

Built for these roles

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

OVERVIEW

Executive 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.

PROGRAM OUTCOMES

Capabilities your teams will gain

- Strengthen capability in security scenarios
- Strengthen capability in security copilot scenarios
- Strengthen capability in role-based scenarios

ENTERPRISE CUSTOMIZATION

Enterprise customization

Tailor this program to your organization's priorities: Builds current Microsoft credential readiness for Implement end to end security controls for cloud and AI workloads using the official Microsoft Learn outline.

Customization options

- Align labs to your production environment and platform priorities
- Add readiness reviews and instructor-led practice sessions
- Extend into project-specific architecture or delivery coaching

CURRICULUM

Curriculum roadmap

1

MODULE 1

Secure access to resources by using Microsoft Entra

Learn to design and implement strong authentication controls, apply Just-in-Time privileged access strategies, and extend identity-based security to AI-powered applications 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

2

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. Configure hardened vault settings, control access through RBAC and just-in-time privilege, manage keys, secrets, and certificates, and detect threats using Microsoft Defender for Key Vault and Defender CSPM.

- 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

TRAINING PROVIDER
VNode ITeS
MICROSOFT CERTIFIED TRAINER
vnodeites.com
linkedin.com/company/vnodeites

TALK TO US
info@vnodeites.com
+91 9779 91 4792
WhatsApp · +91 9779 91 4792
+91 9419 11 4792

OFFICE
DLF Cyber City, Gurugram
Haryana — India
Azure · AI · Data · Power Platform

3

MODULE 3

Enforce security governance and regulatory compliance

Enforce security governance and regulatory compliance across Azure environments using Azure Policy, Microsoft Defender for Cloud, Azure RBAC. Then enable Azure Backup security features, and infrastructure as code scanning.

- 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

4

MODULE 4

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

Implement a defense-in-depth security strategy for Azure Storage. Harden storage accounts, govern access with Microsoft Entra ID and stored access policies, enforce network perimeter controls using firewall rules and private endpoints, and enable Microsoft Defender for Storage to detect threats from malicious 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

5

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

6

MODULE 6

Implement network security controls in Azure

Implement defense-in-depth network security controls in Azure. Segment workloads to control lateral movement, centralize traffic inspection with Azure Firewall, harden remote and hybrid connectivity, and eliminate public network exposure of PaaS and AI services using private endpoints.

- 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

7

MODULE 7

Implement security for AI

Implement a defense-in-depth security strategy for AI workloads across Microsoft's AI platform. Configure data security posture management in Microsoft Purview, secure agent identities in Microsoft Entra, and analyze AI identity risks in Microsoft Defender XDR. Then, enable real-time agent protection in Microsoft Defender, configure AI Gateway security in Microsoft Foundry, manage guardrails, protect AI workloads with Defender for Cloud, and govern agents with 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

8

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, Trusted Launch, Azure Bastion, Microsoft Defender for Servers, just-in-time VM access, and Azure Machine Configuration to close security gaps across your 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

9

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, secure Azure Kubernetes Service (AKS), Azure Container Registry (ACR), Container Instances, and Container Apps. 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

10

MODULE 10

Manage security posture by using Microsoft Defender for Cloud

Learn to manage cloud security posture using Microsoft Defender for Cloud. You connect hybrid and multicloud environments, identify risks, and assess compliance—then protect your workloads with threat detection and vulnerability 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

11

MODULE 11

Implement activity and event collection in Microsoft Sentinel

Build a complete event collection and response architecture in Microsoft Sentinel. Set up and secure a Microsoft Sentinel workspace, deploy Content Hub solutions, connect Azure resource data, collect Linux and Windows security events with data collection rules, implement automated response workflows with Logic Apps playbooks, and manage data retention for compliance.

- 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

12

MODULE 12

Deploy and operate Microsoft Security Copilot

Build hands-on expertise with Microsoft Security Copilot. Start with enabling the solution and writing effective prompts to configuring enterprise workspaces and managing plugins and agents at scale.

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

TRAINING PROVIDER
VNode ITeS
MICROSOFT CERTIFIED TRAINER
vnodeites.com
linkedin.com/company/vnodeites

TALK TO US
info@vnodeites.com
+91 9779 91 4792
WhatsApp · +91 9779 91 4792
+91 9419 11 4792

OFFICE
DLF Cyber City, Gurugram
Haryana — India
Azure · AI · Data · Power Platform