INFOSECTRAIN
Educate. Excel. Empower.

Microsoft

SC-500

Cloud & AI Security

Certification & Training

Course Highlights

- 32-Hour LIVE Instructor-led Training
- Immersive Learning Schedule
- Highly Interactive and Dynamic Sessions
- Learn from Certified Experts
- Post Training Support
- Training Completion Certificate
- Access to Recorded Sessions
- Telegram Group for Exam Support
- Career Guidance & Mentorship

About Course

The Microsoft SC-500 Cloud & AI Security Certification Training Course from InfosecTrain is designed for security engineers responsible for protecting organizational systems, applications, and data across cloud and hybrid environments. Professionals in this role implement security controls to reduce risk, prevent unauthorized access, and strengthen overall security. Their responsibilities extend across multiple domains, including identity, networks, applications, data, and infrastructure. They also play a critical role in securing AI platforms, workloads, identities, and related infrastructure. Security engineers frequently collaborate with architects, administrators, developers, analysts, and other technology teams that manage Azure, Microsoft 365, DevOps, networking, databases, and information protection. Candidates are expected to have hands-on experience with Microsoft Azure administration, including compute, networking, and storage, along with a solid understanding of Microsoft Entra ID and Microsoft 365 administration. Key responsibilities include securing access through Microsoft Entra ID and Azure Key Vault, maintaining regulatory compliance, protecting storage and database environments, securing compute resources and AI solutions, and continuously monitoring and improving the organization's security posture.

Course Objectives

- Develop and deploy identity and access management controls within Microsoft Azure and Microsoft 365 environments.
- Apply Microsoft security solutions and industry-recommended practices to protect cloud, hybrid, and AI-driven workloads.
- Establish governance, compliance, and risk management frameworks for cloud and AI ecosystems.
- Strengthen the security of AI platforms, agents, and workloads by leveraging Microsoft Defender, Microsoft Entra, and other related security services.
- Identify, analyze, and respond to security threats across cloud-based and AI-enabled environments.
- Enhance the overall security posture through effective configuration management, posture assessment, and continuous security improvement.
- Implement identity protection mechanisms for AI environments, including Conditional Access policies and secure identity management controls.
- Design and oversee comprehensive security strategies for modern cloud, multi-cloud, and AI-centric infrastructures.

Target Audience

This course is particularly suitable for:

- Cloud Security Engineers
- AI Security Engineers
- Azure Security Engineers
- Microsoft 365 Security Professionals
- Identity and Access Management (IAM) Professionals
- Security Administrators
- Security Architects
- SOC Analysts
- DevSecOps Engineers
- Infrastructure and Network Security Professionals
- Cybersecurity Professionals working with cloud, hybrid, or multi-cloud environments

Pre-Requisites

- 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).
- 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.

Exam Information

Certification Name	SC-500
Exam Duration	120 minutes
Number of Questions	40-60
Exam Format	Multiple Choice Questions, labs and case-studies
Passing Score	700 out of 1000
Exam Language	English

Course Content

Module 1: 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

Module 2: 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

Module 3: 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

Module 4: 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

Module 5: 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

Module 6: 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

Module 7: 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

Module 8: 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

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

- 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 & 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

- 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

- 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 & operate Microsoft Security Copilot

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

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on