Implement endtoend security controls for cloud and AI workloads (SC-500T00)

Duration: 4 Days
Audience: Professionnel TI

Who is this training for?

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.

Training objectives

After completing this course, students will be able to:

- Secure identity and access across users, applications, and agents.
- Protect secrets, keys, certificates, storage, and databases.
- Apply governance, policy, and least-privilege controls across Azure.
- Secure network access to Azure resources and services.
- Assess and protect AI workloads, agents, and data exposure paths.
- Secure compute, container, and application platforms.
- Manage cloud security posture across Azure, hybrid, and multicloud environments.

Summary

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.

Course outline

Learning

Path 1: Secure Access to resources using

Microsoft

Entra ID

- Module 1:

  Manage and Implement Authentication Methods in Microsoft Entra ID
- Module 2:

  Implement and Configure Privileged Identity

  Management

  (PIM)
-

  Module 3:

  Authenticate your API plugin for declarative agents

  with

  secured APIs

Learning

Path 2: Secure secrets and keys using Azure

Key Vault

-

Module 1:

Configure and Secure Azure Key Vault

- Module 2:

  Manage Keys and Secrets in Azure Key Vault

- Module 3:

  Manage Certificates and Monitor Azure Key Vault

- Module 4:

  Protect Azure Key Vault with Microsoft Defender

  for Cloud

Learning

Path 3: Implement governance to enforce

security

and regulatory compliance

- Module 1:

  Enforce Governance with Azure Policy and

  Resource

  Locks

- Module 2:

  Configure Security Controls and Remediate

  Recommendations

  in Defender for Cloud

-

Module 3:

Evaluate Regulatory Compliance in Defender for

Cloud

- Module 4:

  Manage and Right-Size RBAC Role Assignments for

  Least

  Privilege

- Module 5:

  Protect Backup Data with Azure Backup Security

  Features

- Module 6:

  Implement Security Controls in Infrastructure as

  Code

Learning

Path 4: Implement security for storage accounts

- Module 1:

  Describe Azure storage services

- Module 2:

  Implement Security and Manage Access for Azure

  Storage

-

Module 3:

Configure Network Security for Azure Storage

- Module 4:

  Implement Microsoft Defender for Storage

Learning

Path 5:

Implement

security for Azure

networking

- Module 1:

  Segment and Isolate Azure Workloads Using

  Network

  Security Controls

- Module 2:

  Centralize and Enforce Traffic Inspection Using

  Azure

  Firewall

- Module 3:

  Secure Remote and Hybrid Connectivity Using VPN

  Gateways

  and Microsoft Entra Private Access

- Module 4:

  Eliminate Public Network Exposure of Azure PaaS

  Services

Learning

Path 6:

Implement

security for AI

- Module 1:

  Secure Access for Microsoft Entra Agent Identity
- Module 2:

  Analyze AI Identity Risks Using Microsoft Defender

  XDR
- Module 3:

  Enable Real-Time Protection for Copilot Studio

  Agents
- Module 4:

  Configure AI Gateway Security in Microsoft

  Foundry
- Module 5:

  Configure and manage guardrails in Microsoft

  Foundry
- Module 6:

  Protect AI workloads with Microsoft Defender for

  Cloud
- Module 7:

  Enable Defender for AI Services Workload

  Protection

  in Microsoft Defender for Cloud
- Module 8:

  Manage Agents Using Microsoft Agent 365
-

Module 9:

Identify AI Data Risks Using Microsoft Purview Data

Security

Posture Management

Learning

Path 7: Implement security for servers and

virtual

machines

- Module 1:

  Implement Disk Encryption for Azure Virtual

  Machines
- Module 2:

  Configure Trusted Launch Security Features for

  Azure

  Virtual Machines
- Module 3:

  Plan and Implement Azure Bastion
- Module 4:

  Manage Security for Arc-Enabled Hybrid Servers
- Module 5:

  Implement Microsoft Defender for Servers
-

  Module 6:

  Enable and Enforce Just-in-Time VM Access -

  VM Access
- Module 7:

  Enforce VM Security Configuration with Azure

Machine

Configuration

Learning

Path 8: Implement security for application

platform

services

- Module 1:

  Detect Container Risks Using Microsoft Defender

  for

  Containers
- Module 2:

  Implement Security Controls for Azure Kubernetes

  Service
- Module 3:

  Implement Security Controls for Azure Container

  Registry,

  Container Instances, and Container Apps
- Module 4:

  Implement Security Controls for Azure Function

  Apps and

  Logic Apps
- Module 5:

  Implement Security Controls for Azure App Services

  and Web

  Application Firewall
- Module 6:

  Implement API Backend Security Using Azure API

  Management

Learning

Path 9: Manage security posture by using

Defender

for Cloud

- Module 1:

  Connect Hybrid and multicloud Environments to

  Microsoft

  Defender for Cloud

- Module 2:

  Identify Security Risks by Using Cloud Security

  Posture

  Management

- Module 3:

  Discover Unprotected Assets and Vulnerabilities by

  Using

  Microsoft Defender External Attack Surface

  Management

- Module 4:

  Evaluate Regulatory Compliance in Defender for

  Cloud

- Module 5:

  Enable and Configure Workload Protection Plans in

  Microsoft

  Defender for Cloud

- Module 6:

  Configure Microsoft Defender Vulnerability

  Management

  Settings for Azure VMs

Learning

Path 10: Implement activity and event

collections

in Microsoft Sentinel

- Module 1:

  Create and manage Microsoft Sentinel workspaces
- Module 2:

  Manage content in Microsoft Sentinel
- Module 3:

  Connect Microsoft services to Microsoft Sentinel
-

  Module 4:

  Connect syslog data sources to Microsoft Sentinel
- Module 5:

  Connect Common Event Format logs to Microsoft

  Sentinel
- Module 6:

  Connect Windows hosts to Microsoft Sentinel
-

  Module 7:

  Implement Automation Rules and Playbooks in

  Microsoft

  Sentinel
- Module 8:

  Manage Data Storage and Query Audit Logs in

  Microsoft

  Sentinel

Learning

Path 11:

Implement

Microsoft Security

Copilot

- Module 1:

  Describe Microsoft Security Copilot
- Module 2:

  Configure workspaces for Microsoft Security

  Copilot
- Module 3:

  Manage Plugins and Agents in Microsoft Security

  Copilot

Approach and methodology

Practical and structured approach combining focused theory with guided hands on labs. Participants progressively implement end to end security controls across Azure, Microsoft 365, and AI workloads through real world, scenario based exercises that promote immediate application of learning.

They learn how to secure identities, access, data, cloud infrastructure, secrets, applications, and AI solutions using tools such as Microsoft Entra ID, Azure Key Vault, Microsoft Defender, and Microsoft Security Copilot.

Led by a Microsoft certified trainer (MCT), the course emphasizes interactivity and the development of directly transferable technical skills to strengthen security posture in hybrid and multi cloud environments.

Prerequisites

A basic

knowledge is recommended before starting this course:

- Foundational

  Azure knowledge: subscriptions,

  resource groups, virtual networks, storage accounts, virtual machines, and

  Azure role-based access control.
- Basic

  identity and access knowledge: Microsoft Entra ID, users, groups, authentication, authorization,

  multifactor authentication, Conditional Access, and app or service identities.
- General

  security fundamentals: least privilege, defense in depth, Zero Trust, threat protection,

  encryption, auditing, and secure configuration.
- Basic

  cloud networking knowledge: VNets, subnets, private endpoints, firewalls, VPNs, and network

  security

  rules.

  Basic

  data and workload awareness: common Azure workload types such as storage, SQL databases,

  virtual

  machines, containers, App Services, and APIs.
- Familiarity

  with Microsoft security tools: Microsoft Defender for Cloud, Microsoft Sentinel, Microsoft Defender

  XDR, Microsoft Purview, or Security Copilot.

  Introductory

  AI awareness: basic

  concepts such as copilots, agents, prompts, models, and data grounding.
- Hands-on

  Azure portal experience: navigating the portal and making basic configuration changes in a lab

  environment.

Recommendations

Recommended Complementary Courses: AZ 104, SC 200, SC 300, SC 401

Certifications

Microsoft Certified: Cloud and AI Security Engineer Associate

Legal notices