Document Generated: 11/15/2026

Learning Style: Virtual Classroom

Technology: Microsoft

Difficulty: Intermediate

Course Duration: 4 Days

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

About This Course:

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 Objectives:

- 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

Audience:

- 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.

Prerequisites:

This course is designed for IT professionals with a working background in Microsoft cloud technologies. Before enrolling, learners should have:

- Hands-on experience administering Microsoft Azure and hybrid environments, including compute, networking, and storage
- Strong familiarity with Microsoft Entra ID (formerly Azure Active Directory)
- Working knowledge of Microsoft 365 administration

Course Outline:

1 - 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

Module assessment

2 - 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

3 - Authenticate your API plugin for declarative agents with secured APIs

Integrate an API plugin with an API secured with a key

Integrate an API plugin with an API secured with OAuth

Module assessment

4 - 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

5 - Manage keys and secrets in Azure Key Vault

Manage cryptographic keys in Azure Key Vault

Manage secrets in Azure Key Vault

6 - Manage certificates and monitor Azure Key Vault

Manage certificates in Azure Key Vault

Enable Key Vault audit logging

7 - 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

8 - Enforce governance with Azure Policy and resource locks

Assign built-in Azure Policy definitions

Create and deploy custom policy definitions

Implement resource locks

9 - Configure security controls and remediate recommendations in Defender for Cloud

Configure Defender for Cloud and manage security standards

Deploy remediation controls at scale

10 - 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

11 - 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

12 - Protect backup data with Azure Backup security features

Enable soft delete and immutable vaults

Configure Multi-User Authorization and RBAC for backup

13 - Implement security controls in infrastructure as code

Scan IaC templates using Microsoft Defender for DevOps

Enforce policy compliance in IaC deployments

14 - 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

15 - 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

16 - 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

17 - 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

18 - 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

19 - 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

20 - 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

21 - 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

22 - 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

23 - 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

24 - 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

25 - 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

26 - Analyze AI identity risks using Microsoft Defender XDR

Discover AI agents in the Microsoft Defender portal

Assess blast radius and attack paths

27 - Enable real-time protection for Copilot Studio agents

Explore Copilot Studio AI agent protection

Enable protection in Microsoft Defender

Review AI agent protection outputs

28 - Configure AI Gateway security in Microsoft Foundry

Examine AI Gateway architecture

Create and configure AI Gateway

Secure and monitor AI Gateway access

29 - 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

30 - 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

31 - 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

32 - Manage agents using Microsoft Agent 365

Enable and navigate Microsoft Agent 365

Register agents and apply access controls

Monitor agent activity and enforce governance

33 - 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

34 - 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

35 - 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

36 - Plan and implement Azure Bastion

Plan Azure Bastion deployment

Deploy and configure Azure Bastion

Connect to VMs through Azure Bastion

37 - 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

38 - 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

39 - 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

40 - 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

41 - 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

42 - 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

43 - 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

44 - 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

45 - 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

46 - 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

47 - 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

48 - 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

49 - 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

50 - 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

51 - 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

52 - 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

53 - 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

54 - Manage content in Microsoft Sentinel

Use solutions from the content hub

Use repositories for deployment

Module assessment

55 - 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

56 - 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

57 - 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

58 - 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

59 - 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

60 - 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

61 - 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

62 - 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

63 - 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