Pipeline

Pipeline is a Leading Learning Partners Association Member

MOC SC-500T00 - IMPLEMENT ENDTOEND SECURITY CONTROLS FOR CLOUD AND AI WORKLOADS

CORSO CON DOCENTE

Durata	Prezzo	Orari	Calendario
4 giorni	~~1.690,00€~~ 1.436,50€ + IVA	9:00 – 13:00 | 14:00 – 17:00	21/09/2026 Aula Virtuale 16/11/2026 Aula Virtuale 25/01/2027 Aula Virtuale 22/03/2027 Aula Virtuale 24/05/2027 Aula Virtuale

Questo corso SC-500 – Implement end-to-end security controls for cloud and AI workloads prepara a progettare, implementare e gestire controlli di sicurezza completi negli ambienti Microsoft Azure e Microsoft 365. Attraverso sessioni con docente e laboratori pratici, i partecipanti sviluppano competenze nella protezione delle identità e delle infrastrutture cloud, nel rilevamento delle minacce e nella gestione della postura di sicurezza, affrontando anche la protezione dei workload di intelligenza artificiale e degli agenti autonomi in ambienti cloud, ibridi e multi-cloud.

Contenuti del corso

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

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

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

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

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

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

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

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

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 and Logic apps
- Implement security controls for Azure App Services and Web Application Firewall
- Implement API backend security using Azure API Management

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

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

Deploy and operate Microsoft Security Copilot

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

Partecipanti

Questo corso SC-500 – Implement end-to-end security controls for cloud and AI workloads è rivolto ai Security Engineer che si occupano di proteggere sistemi, dati e infrastrutture aziendali negli ambienti cloud, ibridi e multi-cloud attraverso l'implementazione di controlli di sicurezza completi.

È ideale per professionisti con esperienza pratica nell'amministrazione di Microsoft Azure e degli ambienti ibridi, comprese risorse di calcolo, reti e archiviazione, e con una buona conoscenza di Microsoft Entra ID e Microsoft 365. I partecipanti acquisiscono competenze nella protezione degli accessi, nell'applicazione dei requisiti di sicurezza e conformità, nella messa in sicurezza di reti, database, infrastrutture e soluzioni di intelligenza artificiale, oltre che nella gestione e nel monitoraggio della postura di sicurezza.

Prerequisiti

Per partecipare al corso SC-500 – Implement end-to-end security controls for cloud and AI workloads è consigliabile possedere esperienza pratica nell'amministrazione di Microsoft Azure e degli ambienti ibridi, comprese le risorse di calcolo, rete e archiviazione.

È inoltre raccomandata una buona conoscenza di Microsoft Entra ID e una familiarità di base con l'amministrazione di Microsoft 365.

Obiettivi

Al termine del corso SC-500 – Implement end-to-end security controls for cloud and AI workloads gli allievi avranno compreso come progettare, implementare e gestire controlli di sicurezza completi negli ambienti Microsoft Azure, Microsoft 365, ibridi e multi-cloud. I partecipanti acquisiranno inoltre competenze pratiche per proteggere identità, accessi, reti, risorse di calcolo, sistemi di archiviazione e database, applicare i requisiti di sicurezza e conformità, rilevare e mitigare le minacce e monitorare la postura di sicurezza, garantendo anche la protezione dei workload di intelligenza artificiale e degli agenti autonomi.

Lingua

Lingua utilizzata nel corso/dal docente: Italiano
Il materiale didattico e l'ambiente di laboratorio sono in lingua Inglese

Materiali e Bonus

Il corso SC-500 – Implement end-to-end security controls for cloud and AI workloads include:

- documentazione didattica ufficiale Microsoft Learning accessibile via web, di durata illimitata;
- **un ambiente di laboratorio** con macchine virtuali accessibili online;
- un **attestato di frequenza** inviato via e-mail una settimana dopo il termine del corso.