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

CODICE	SC-500T00
DURATA	4 gg
PREZZO	1.590,00 €
EXAM	

DESCRIZIONE

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.

** Questo corso sostituisce il corso AZ-500T00 - Secure cloud resources with Microsoft security technologies

TARGET

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

CONTENUTI

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