

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.

***This course will be available on 2/7/2026 and is the successor of AZ-500T00.*

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
- Secure Azure Key Vault with defense in depth for the cloud and AI workloads
- Enforce security governance and regulatory compliance
- Implement security for Azure Storage for the cloud and AI security engineer
- Implement security for Azure SQL databases
- Implement network security controls in Azure
- Implement security for AI
- Implement security for servers and virtual machines
- Secure Azure application platform services for the cloud and AI security engineer
- Manage security posture by using Microsoft Defender for Cloud
- Implement activity and event collection in Microsoft Sentinel
- Deploy and operate Microsoft Security Copilot