Training: Microsoft

SC-500T00: Implement end-to-end security controls for cloud and AI workloads

Microsoft Partner

TRAINING GOALS:

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.

Audience Profile:
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.

CONSPECT:

- Secure access to resources by using Microsoft Entra
  - Module 1: Manage and implement authentication methods in Microsoft Entra ID
  - Module 2: Implement and configure Privileged Identity Management (PIM)
  - Module 3: Secure declarative agents and AI applications with Microsoft Entra
- Secure Azure Key Vault with defense in depth for the cloud and AI workloads
  - 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: Detect threats against Azure Key Vault using Microsoft Defender for Cloud
- Enforce security governance and regulatory compliance
  - Module 1: Enforce governance with Azure Policy and resource locks

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Module 2: Configure security controls and remediate recommendations in Defender for Cloud
- Module 3: Evaluate regulatory compliance using Microsoft Defender for Cloud
- Module 4: Govern Azure role-based access control assignments
- Module 5: Protect Azure data with Azure Backup
- Module 6: Embed security in Bicep pipelines for DevOps

- Implement security for Azure Storage for the cloud and AI security engineer
  - 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
- Implement security for Azure SQL databases
  - Module 1: Configure platform-level security for Azure SQL
  - Module 2: Configure auditing for Azure SQL Database and SQL Managed Instance
  - Module 3: Implement Microsoft Defender for Databases
- Implement network security controls in Azure
  - Module 1: Segment and isolate Azure workloads using network security controls
  - Module 2: Centralize and enforce traffic inspection using Azure Firewall
  - Module 3: Harden remote connectivity and deploy Microsoft Entra Private Access
  - Module 4: Eliminate public endpoint exposure using Private Link
- 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 protection for Copilot Studio agents using Microsoft Defender for Cloud Apps
  - Module 4: Secure AI model traffic using AI Gateway
  - Module 5: Configure and manage guardrails in Microsoft Foundry
  - Module 6: Protect AI workloads using Microsoft Defender for Cloud
  - Module 7: Govern Agent 365 agents using Microsoft Agent 365
  - Module 8: Discover and assess AI data risks with DSPM for AI
  - Module 9: Manage AI data compliance and retention
- 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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Module 6: Implement just-in-time virtual machine access
- Module 7: Configure Azure Machine Configuration for OS security baselines

- Secure Azure application platform services for the cloud and AI security engineer
  - Module 1: Detect container risks using Microsoft Defender for Containers
  - Module 2: Implement security controls for Azure Kubernetes Service
  - Module 3: Implement security for Azure Container Registry
  - Module 4: Secure Azure Functions and Logic Apps
  - Module 5: Secure Azure App Services and Web Application Firewall
  - Module 6: Secure Azure API Management
- Manage security posture by using Microsoft 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 and manage external attack surfaces with Microsoft Defender EASM
  - Module 4: Evaluate regulatory compliance using Microsoft Defender for Cloud
  - Module 5: Enable and configure workload protection plans in Microsoft Defender for Cloud
  - Module 6: Implement Microsoft Defender Vulnerability Management
- Implement activity and event collection 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: Collect Windows security events with data collection rules
  - Module 5: Collect Linux and syslog data with data collection rules
  - Module 6: Implement automated threat response with playbooks
  - Module 7: Manage data retention and archiving in Microsoft Sentinel
  - Module 8: Secure audit log access in Microsoft Sentinel
- Deploy and operate Microsoft Security Copilot
  - Module 1: Describe Microsoft Security Copilot
  - Module 2: Configure workspaces for Microsoft Security Copilot
  - Module 3: Manage Security Copilot agents and plugins

REQUIREMENTS:

- Practical experience in administration of Microsoft Azure and hybrid environments, including compute, network, and storage
- Strong familiarity with Microsoft Entra ID
- Familiarity with Microsoft 365 administration

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Working knowledge of Azure Key Vault, Azure Policy, Azure RBAC
- Familiarity with Microsoft Defender for Cloud at a foundational level
- Understanding of Azure networking concepts including virtual networks, subnets, and private endpoints
- Experience with Kusto Query Language (KQL) and Log Analytics workspaces

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Microsoft (course completion).

This course will help prepare you for the **Microsoft Certified: Cloud and AI Security Engineer Associate (beta)** certification, which is available through the Pearson VUE test centers.

TRAINER:

Microsoft Certified Trainer (MCT)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007