Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

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

CODE:	LENGTH:	PRICE:
MCS_SC-500T00	32 Hours (4 days)	kr33,000.00

Description

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

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

Prerequisites

• Familiarity with Microsoft Entra ID concepts, including users, groups, and directory roles
• Understanding of Azure role-based access control (RBAC), including role assignments and the Azure scope hierarchy (management group, subscription, resource group, resource)
• Basic experience navigating the Azure portal and the Microsoft Entra admin center
• Familiarity with Zero Trust security principles, including least privilege and assume breach
• Awareness of Microsoft Entra ID P2 or Microsoft Entra ID Governance licensing requirements
• Working knowledge of Azure Key Vault, including deploying and using a vault
• Understanding of Azure role-based access control (RBAC) and managed identities
• Familiarity with Microsoft Defender for Cloud at a foundational level
• Working knowledge of Azure administration at the AZ-104 level, including resource management, role assignments, and virtual network concepts
• Understanding of Azure role-based access control (RBAC) including role assignments and scope hierarchy
• Basic experience navigating the Azure portal and Microsoft Entra admin center
• Familiarity with Azure Storage accounts including Blob Storage and Azure Files
• Familiarity with Microsoft Entra ID and Azure role-based access control (RBAC)
• Understanding of Azure networking concepts including virtual networks, subnets, and private endpoints
• Familiarity with Azure Key Vault at a conceptual level
• Understanding of Microsoft Defender for Cloud at a conceptual level

Programme

Manage and implement authentication methods in Microsoft Entra ID

- Introduction
- 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
- Exercise - Configure authentication methods in Microsoft Entra ID
- Module assessment
- Summary

Implement and configure Privileged Identity Management (PIM)

- Introduction
- 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
- Summary

Authenticate your API plugin for declarative agents with secured APIs

- Introduction
- Integrate an API plugin with an API secured with a key
- Exercise - Integrate an API plugin with an API secured with a key
- Integrate an API plugin with an API secured with OAuth
- Exercise - Integrate an API plugin with an API secured with OAuth
- Module assessment
- Summary

Configure and secure Azure Key Vault

- Introduction
- Deploy Azure Key Vault with security controls
- Configure access to Azure Key Vault
- Configure Key Vault firewall and network settings
- Knowledge check
- Summary

Manage keys and secrets in Azure Key Vault

- Introduction
- Manage cryptographic keys in Azure Key Vault
- Manage secrets in Azure Key Vault
- Knowledge check
- Summary

Manage certificates and monitor Azure Key Vault

- Introduction
- Manage certificates in Azure Key Vault
- Enable Key Vault audit logging
- Knowledge check
- Summary

Protect Azure Key Vault with Microsoft Defender for Cloud

- Introduction
- 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
- Knowledge check
- Summary

Enforce governance with Azure Policy and resource locks

- Introduction
- Assign built-in Azure Policy definitions
- Create and deploy custom policy definitions
- Implement resource locks
- Knowledge check
- Summary

Configure security controls and remediate recommendations in Defender for Cloud

- Introduction
- Configure Defender for Cloud and manage security standards
- Deploy remediation controls at scale
- Knowledge check
- Summary

Evaluate regulatory compliance in Defender for Cloud

- Introduction
- Understand compliance standards and controls in Defender for Cloud
- Navigate the regulatory compliance dashboard and investigate control gaps
- Assign standards and communicate compliance posture
- Knowledge check
- Summary

Manage and right-size RBAC role assignments for least privilege

- Introduction
- Assign and manage Azure built-in roles
- Create custom Azure roles and Microsoft Entra roles
- Evaluate and remediate overprivileged access
- Knowledge check
- Summary

Protect backup data with Azure Backup security features

- Introduction
- Enable soft delete and immutable vaults
- Configure Multi-User Authorization and RBAC for backup
- Knowledge check
- Summary

Implement security controls in infrastructure as code

- Introduction
- Scan IaC templates using Microsoft Defender for DevOps
- Enforce policy compliance in IaC deployments
- Knowledge check
- Summary

Describe Azure storage services

- Introduction
- Describe Azure storage accounts
- Describe Azure storage redundancy
- Describe Azure storage services
- Identify Azure data migration options
- Identify Azure file movement options
- Module assessment
- Summary

Implement security and manage access for Azure Storage

- Introduction
- 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
- Knowledge check
- Summary

Configure network security for Azure Storage

- Introduction
- 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
- Knowledge check
- Summary

Implement Microsoft Defender for Storage

- Introduction
- 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
- Knowledge check
- Summary

Configure platform-level security for Azure SQL

- Introduction
- 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
- Knowledge check
- Summary

Configure auditing for Azure SQL Database and SQL Managed Instance

- Introduction
- Describe Azure SQL auditing capabilities
- Configure audit destinations for Azure SQL Database
- Configure auditing for SQL Managed Instance
- Design a compliant audit strategy
- Knowledge check
- Summary

Implement Microsoft Defender for Databases

- Introduction
- 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
- Knowledge check
- Summary

Session Dates

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.