Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com
Phone: 0870 251 1000

AZ-500T00: Microsoft Azure Security Technologies

CODE:	LENGTH:	PRICE:
MCS_AZ-500T00	32 Hours (4 days)	€2,590.00

Description

This course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organization’s security posture, and identify and remediate security vulnerabilities. This course includes security for identity and access, platform protection, data and applications and security operations.

Audience

This course is for Azure Security Engineers who are planning to take the associated certification exam, or who are performing security tasks in their day-to-day job. This course would also be helpful to an engineer that wants to specialize in providing security for Azure-based digital platforms and play an integral role in protecting an organization's data.

Programme

1. AZ-500: Secure identity and access

Master identity and access management in Microsoft Entra ID, securing users, groups, and external identities, implementing authentication and authorization controls, and managing application access and security.

Modules in this learning path

- Manage security controls for identity and access

This module focuses on effectively managing security controls in Microsoft Entra ID by securing identities, authentication, and authorization to protect users, groups, and external identities against threats while ensuring secure and seamless access to resources.

- Manage Microsoft Entra application access

This module covers managing application access in Microsoft Entra ID, including controlling enterprise app access, managing app registrations and permissions, utilizing service principals, and configuring the Microsoft Entra Application Proxy for secure access.

2. AZ-500: Secure networking

Master the intricacies of securing Azure networks, encompassing virtual networks, encryption, firewall setup, private access, and DDoS protection, with this comprehensive training.
Prerequisites
It is beneficial to have a solid infrastructure background in networking and servers.

Modules in this learning path

- Plan and implement security for virtual networks

This module is designed to provide administrators with the knowledge and skills needed to plan and implement robust security measures for Azure virtual networks, ensuring the confidentiality, integrity, and availability of network resources.

- Plan and implement security for private access to Azure resources

This module focuses on equipping administrators with the knowledge and skills required to plan and implement robust security measures for private access to Azure resources, safeguarding sensitive data and enhancing network integrity.

- Plan and implement security for public access to Azure resources

This module empowers admins to plan and implement strong security for Azure resources, ensuring app/service confidentiality, integrity, and availability.

3. AZ-500: Secure compute, storage, and databases

Master the art of securing Azure compute resources, storage, and databases, including advanced security measures, encryption, access control, and database protection.

Modules in this learning path

- Plan and implement advanced security for compute

This module is designed to provide administrators with the knowledge and skills needed to plan and implement advanced security measures for Azure compute resources, safeguarding applications and data against evolving security threats.

- Plan and implement security for storage

This module is designed to provide administrators with the knowledge and skills required to plan and implement comprehensive security measures for Azure storage resources, safeguarding data integrity, confidentiality, and availability.

- Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

This module is designed to empower administrators with the knowledge and skills needed to plan and implement robust security measures for Azure SQL Database and Azure SQL Managed Instance, ensuring data protection and regulatory compliance.

4. AZ-500: Secure Azure using Microsoft Defender for Cloud and Microsoft Sentinel

Master the art of managing security operations in Azure, from governance and policy creation to infrastructure security, key management, security posture, threat protection, and advanced security monitoring and automation.

Modules in this learning path

- Implement and manage enforcement of cloud governance policies

This module focuses on enabling administrators to effectively plan, implement, and manage security governance in Azure, ensuring compliance with organizational policies and best practices.

- Manage security posture by using Microsoft Defender for Cloud

This module teaches administrators to manage and improve cloud security using Microsoft Defender for Cloud, focusing on proactive risk identification and remediation.

- Configure and manage threat protection by using Microsoft Defender for Cloud

This module focuses on the essential techniques for configuring and managing threat protection exclusively with Microsoft Defender for Cloud, empowering cybersecurity specialists to strengthen the security posture of their cloud environments.

- Configure and manage security monitoring and automation solutions

This module teaches how to set up and manage security tools with Azure Monitor and Microsoft Sentinel. It helps organizations quickly find and deal with security issues in their cloud setup.

Session Dates

Aikataulutamme kiinnostuksen mukaan. Ota yhteyttä

Additional Information

This training is also available as onsite training. Please contact us to find out more.