MERCURY

Microsoft Securing Windows Server 2016 Course

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

MERCURY

Microsoft Securing Windows Server 2016 Course

Introduction:

The Microsoft Securing Windows Server 2016 course is a comprehensive Windows Server 2016 training program designed to provide in-depth knowledge and skills needed to protect and secure the IT infrastructure.

As part of the Microsoft Windows Server 2016 training, this course begins with the critical assumption that network breaches are already prevalent, emphasizing the need for robust security measures.

Participants will learn how to secure Windows Server 2016 by configuring administrative credentials, mitigating malware and security threats, utilizing auditing and advanced threat analysis features to pinpoint security issues, and applying encryption and Dynamic Access Control DAC to restrict data access.

The Microsoft Securing Windows Server 2016 course also guides on enhancing network security through secured file access using encryption and DAC dynamic access control and explains how to enhance the network's security.

Targeted Groups:

This Windows Server 2016 course is targeted at IT professionals who are tasked with administering Windows Server 2016 networks securely.

Microsoft Windows Server 2016 training is particularly suited for those working in domain-based environments with managed Internet access and cloud services.

Course Objectives:

After this securing Windows Server 2016 training, participants will be able to:

- Implement Windows Server 2016 security best practices to secure Windows Server.
- Restrict administrator rights with Just Enough Administration JEA.
- Manage privileged access securely.
- Effectively mitigate malware and security threats.
- Utilize advanced auditing and log analytics to analyze activity.
- Deploy and configure Advanced Threat Analytics ATA and Microsoft Operations Management Suite OMS.
- Configure Guarded Fabric VMs.
- Use the Security Compliance Toolkit SCT and containers to enhance security.
- Plan and implement strategies to protect data.
- Optimize and secure file services.
- Secure network traffic through the use of firewalls and encryption.
- Use DNSSEC and Message Analyzer to secure network traffic.

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

MERCURY

Targeted Competencies:

The MCSE securing Windows Server 2016 course is designed to develop competencies in:

- Implementing User Rights, Security Options, and Group-Managed Service Accounts.
- Limiting Administrator Privileges with JEA.
- Securing applications with Windows Defender and AppLocker.
- Configuring Advanced Auditing.
- Protecting Data with Encryption and BitLocker.
- Implementing DAC for secure data access.
- Securing DNS against potential threats.

Course Content:

Unit 1: Attacks, Breach Detection, and Sysinternals Tools:

- Understanding the nature of cyber-attacks.
- Identifying and detecting security breaches.
- Utilizing Sysinternals tools to examine system activity.

Unit 2: Protecting Credentials and Privileged Access:

- A thorough examination of User Rights.
- Insights into Computer and Service Accounts.
- Strategies for Protecting Credentials.
- Deploying Privileged Access Workstations and jump servers.
- Integrating Local Administrator Password Solutions LAPS.

Unit 3: Limiting Administrator Rights with Just Enough Administration JEA:

- Delving into the concept of JEA.
- Procedures for Verifying and Deploying JEA.

Unit 4: Privileged Access Management and Administrative Forest:

- An overview of Enhanced Security Administrative Environment ESAE forests.
- Exploring Microsoft Identity Manager MIM.
- Understanding Just In Time JIT administration and Privileged Access Management PAM.

Unit 5: Mitigating Malware and Threats:

- How to Configure and Manage Windows Defender.
- Techniques for Software Restriction.
- Making Use of Device Guard.

Unit 6: Analyzing Activity with Advanced Auditing and Log Analytics:

- Fundamentals of Auditing.
- Deep-diving into Advanced Auditing.
- Leveraging Windows PowerShell for Auditing and Logging.

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

MERCURY

Unit 7: Deploying and Configuring Advanced Threat Analytics ATA and Operations Management Suite OMS:

- Steps for Deploying and Configuring ATA.
- Integration of Microsoft Operations Management Suite.
- Setting up Azure Security Center for enhanced security.

Unit 8: Securing Virtualization Infrastructure:

- Understanding Guarded Fabric.
- Provisioning Shielded and Encryption-Supported VMs.

Unit 9: Securing Application Development and Server-Workload Infrastructure:

- Employing the Security Compliance Manager.
- The Role of Containers in Application Security.

Unit 10: Planning and Protecting Data:

- Formulating and Implementing Encryption Strategies.
- Incorporating BitLocker for Data Protection.
- Utilizing Azure Information Protection.

Unit 11: Optimizing and Securing File Services:

- An Introduction to File Server Resource Manager FSRM.
- Implementing Classification and File Management Tasks.
- Understanding Access Control in the context of DAC.

Unit 12: Securing Network Traffic with Firewalls and Encryption:

- Awareness of network-related security threats.
- Mastery of Windows Firewall with Advanced Security.
- Configuration of IPsec and its role in securing data.
- Advantages of Datacenter Firewall in protecting network traffic.

Unit 13: Securing Network Traffic:

- Advanced Configuration of DNS Settings for security.
- Analysis of Network Traffic with Microsoft Message Analyzer.
- Ensuring Server Security and Analyzing SMB Traffic.

Conclusion:

By incorporating the above-mentioned aspects into its curriculum, the Microsoft Securing Windows Server 2016 Course is essential for Windows Server 2016 security training that empowers IT professionals to effectively secure and mitigate threats within their Windows Server 2016 environments.