Introduction:
The **Microsoft Securing Windows Server 2016** course provides comprehensive training to equip IT professionals with the skills necessary to secure and protect Windows Server 2016 environments. The course emphasizes proactive security measures to safeguard infrastructure against current threats. Participants will learn to configure administrative credentials, mitigate malware, implement auditing and threat analysis, and apply encryption and Dynamic Access Control (DAC) to restrict data access. This course also covers how to enhance network security, optimize file services, and ensure secure network traffic.

The course is designed for IT professionals working in environments with managed Internet access and cloud services, making it an ideal choice for those responsible for securing Windows Server 2016 networks.

Targeted Groups:
This training is tailored for IT professionals tasked with managing and securing Windows Server 2016 networks, particularly those working with domain-based environments, cloud services, and network infrastructure.

Course Objectives:
After completing this course, participants will be able to:

- Implement Windows Server 2016 security best practices.
- Restrict administrator rights using Just Enough Administration (JEA).
- Manage privileged access securely to reduce security risks.
- Effectively mitigate malware and other security threats.
- Utilize advanced auditing and log analytics for activity analysis.
- Deploy and configure Advanced Threat Analytics (ATA) and Microsoft Operations Management Suite (OMS).
- Implement Guarded Fabric VMs for added security.
- Use the Security Compliance Toolkit (SCT) and containers to enhance security.
- Plan and implement strategies for data protection and encryption.
- Optimize and secure file services and secure network traffic using firewalls and encryption.

- Implement DNSSEC and analyze network traffic with Message Analyzer.

Targeted Competencies:
The course will develop competencies in:

- Implementing user rights, security options, and Group Managed Service Accounts.
- Limiting administrator privileges using Just Enough Administration (JEA).
- Securing applications with Windows Defender and AppLocker.
- Configuring and managing advanced auditing tools.
- Protecting data with encryption and BitLocker.
- Implementing DAC for secure and granular data access.
- Securing DNS and mitigating potential threats.

Course Content:

Unit 1: Attacks, Breach Detection, and Sysinternals Tools

- Understanding cyber-attacks and common breach detection techniques.
- Utilizing Sysinternals tools to examine system activity and identify threats.

Unit 2: Protecting Credentials and Privileged Access

- Examining user rights and managing service accounts.
- Deploying Privileged Access Workstations and jump servers for enhanced security.
- Integrating Local Administrator Password Solutions (LAPS) to secure privileged accounts.

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

- Introduction to JEA and its benefits in securing administrative access.
- Verifying and deploying JEA to restrict excessive administrative rights.

Unit 4: Privileged Access Management and Administrative Forest

- Overview of Enhanced Security Administrative Environment (ESAE) forests.
- Using Microsoft Identity Manager (MIM) and Just In Time (JIT) administration.
- Managing Privileged Access Management (PAM) for secure access.

Unit 5: Mitigating Malware and Threats

- Configuring and managing Windows Defender to protect against malware.
- Utilizing software restrictions and Device Guard for enhanced system security.

Unit 6: Analyzing Activity with Advanced Auditing and Log Analytics

- Introduction to advanced auditing techniques.
- Using Windows PowerShell for auditing and logging activities.
- Leveraging log analytics to identify and respond to security incidents.

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

- Deploying and configuring ATA to detect advanced security threats.
- Integrating OMS for continuous monitoring and security management.
- Setting up Azure Security Center to enhance threat detection.

Unit 8: Securing Virtualization Infrastructure

- Understanding Guarded Fabric and its role in securing virtualized environments.
- Provisioning shielded and encryption-supported virtual machines (VMs) to protect against attacks.

Unit 9: Securing Application Development and Server-Workload Infrastructure

- Using the Security Compliance Manager (SCM) to enforce security baselines.

- The role of containers in application security, including best practices for container security.

Unit 10: Planning and Protecting Data

- Formulating data protection strategies using encryption tools.
- Implementing BitLocker for disk encryption and secure data storage.
- Utilizing Azure Information Protection to safeguard sensitive data.

Unit 11: Optimizing and Securing File Services

- Introduction to File Server Resource Manager (FSRM) for managing file services.
- Implementing classification and file management tasks to secure sensitive information.
- Using DAC to control access to data based on classification.

Unit 12: Securing Network Traffic with Firewalls and Encryption

- Understanding network-related security threats and their mitigation.
- Configuring and managing Windows Firewall with Advanced Security.
- Implementing IPsec to encrypt network traffic and secure communication.
- Utilizing Datacenter Firewall to protect network traffic from external and internal threats.

Unit 13: Securing Network Traffic

- Advanced configuration of DNS settings to enhance security.
- Analyzing network traffic using Microsoft Message Analyzer.
- Ensuring server security by analyzing and securing SMB traffic.

Conclusion:
The **Microsoft Securing Windows Server 2016** course equips IT professionals with the critical skills to protect Windows Server environments from advanced threats. By mastering security best practices, credential protection, malware mitigation, and data encryption techniques, participants will ensure their

organizations are better protected against breaches and cyber-attacks. This course is essential for those responsible for securing and managing Windows Server 2016 in enterprise environments.