
Securing Windows Server 2016

Topics:

1. Attacks, Breach Detection, and Sysinternals Tools

- Understanding attacks
- Detecting security breaches
- Examining activity with the Sysinternals tools

2. Protecting Credentials and Privileged Access

- Understanding User Rights
- Computer and Service Accounts
- Protecting Credentials
- Privileged Access Workstations and jump servers
- Local administrator password solution

3. Limiting Administrator Rights with Just Enough Administration (JEA)

- Understanding JEA
- Verifying and Deploying JEA

4. Privileged Access Management and Administrative Forest

- ESAE forests
- Overview of Microsoft Identity Manager (MIM)
- Overview of JIT administration and PAM

5. Mitigating Malware and Threats

- Configuring and Managing Windows Defender
- Restricting software
- Configuring and Using Device Guard

6. Analyzing Activity with Advanced Auditing and Log Analytics

- Overview of Auditing
- Advanced Auditing
- Windows PowerShell Auditing and Logging

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

- Deploying and configuring ATA
- Deploying and configuring Microsoft Operations Management Suite
- Deploying and configuring Azure Security Center

8. Secure Virtualization Infrastructure

- Guarded Fabric
- Shielded and Encryption-Supported VMs

9. Securing Application Development and Server-Workload Infrastructure

- Using Security Compliance Manager
- Understanding Containers

10. Planning and Protecting Data

- Planning and Implementing Encryption
- Planning and Implementing BitLocker

- Protecting data by using Azure Information Protection

11. Optimizing and Securing File Services

- Introduction to FSRM
- Implementing Classification and File-Management Tasks
- Access Control (DAC)

12. Securing Network Traffic with Firewalls and Encryption

- Understand network-related security threats
- Understanding Windows Firewall with Advanced Security
- Configuring IPsec
- Datacenter Firewall

13. Securing Network Traffic

- Configuring Advanced DNS Settings
- Examining Network Traffic with Microsoft Message Analyzer
- Securing Server Analyzing SMB Traffic