OD20744C: Securing Windows Server 2016 MOD

Course Details

Course Outline

1. **Attacks, breach detection, and Sysinternals tools**
    - Understanding attacks
    - Detecting security breaches
    - Examining activity with the Sysinternals tools
    - **Lab : Basic breach detection and incident response strategies**
    1. Identifying attack types
    2. Exploring 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
    - **Lab : Implementing user rights, security options, and group managed service accounts**
    1. Configuring user rights and account-security options
    2. Delegating privileges
    3. Creating group Managed Service Accounts
    4. Locating problematic accounts
    - **Lab : Configuring and deploying LAPs**
    5. Installing and configuring LAPs
    6. Deploying and testing LAPs
3. **Limiting administrator rights with Just Enough Administration**
    - Understanding JEA
    - Verifying and deploying JEA
    - **Lab : Limiting administrator privileges with JEA**
    1. Creating a role-capability file

2. Creating a session-configuration file
3. Creating a JEA endpoint
4. Connecting and testing a JEA endpoint
5. Deploying a JEA configuration to another computer

4. Privileged access management and administrative forests

- ESAE forests
- Overview of Microsoft Identity Manager
- Overview of JIT administration and PAM
- **Lab : Limiting administrator privileges with PAM**

1. Layered approach to security
2. Configuring trust relationships and shadow principals
3. Requesting privileged access
4. Managing PAM roles

5. Mitigating malware and threats

- Configuring and managing Windows Defender
- Restricting software
- Configuring and using the Device Guard feature
- **Lab : Securing applications with Windows Defender, AppLocker, and Device Guard Rules**

1. Configuring Windows Defender
2. Configuring AppLocker
3. Configuring Device Guard

6. Analyzing activity with advanced auditing and log analytics

- Overview of auditing
- Advanced auditing
- Windows PowerShell auditing and logging
- **Lab : Configuring advanced auditing**

1. Configuring the auditing of file system access
2. Auditing domain sign-ins
3. Managing advanced audit policy configuration
4. Windows PowerShell logging and auditing

7. Deploying and configuring Advanced Threat Analytics and Microsoft Operations Management Suite

- Deploying and configuring ATA
- Deploying and configuring Microsoft Operations Management Suite
- Deploying and configuring Azure Security Center
- **Lab : Deploying ATA, Microsoft Operations Management Suite, and Azure Security Center**

1. Preparing and deploying ATA
2. Preparing and deploying Microsoft Operations Management Suite
3. Deploying and configuring Azure Security Center

8. Secure Virtualization Infrastructure

- Guarded fabric
- Shielded and encryption-supported virtual machines
- **Lab : Guarded fabric with Admin-trusted attestation and shielded VMs**

1. Deploying a guarded fabric with admin-trusted attestation
2. Deploying a shielded VM

9. Securing application development and server-workload infrastructure

- Using SCT
- Understanding containers
- **Lab : Using SCT**

1. Configuring a security baseline for Windows Server 2016
2. Deploying the security baseline for Windows Server 2016
- **Lab : Deploying and configuring containers**

3. Deploying and managing a Windows container

10. Planning and protecting data

- Planning and implementing encryption
- Planning and implementing BitLocker
- Protecting data by using Azure Information Protection
- **Lab : Protecting data by using encryption and BitLocker**

1. Encrypting and recovering access to encrypted files
2. Using BitLocker to protect data

11. Optimizing and securing file services

- File Server Resource Manager
- Implementing classification and file management tasks
- Dynamic Access Control

- **Lab : Quotas and file screening**

1. Configuring File Server Resource Manager quotas
2. Configuring file screening and storage reports

- **Lab : Implementing Dynamic Access Control**

3. Preparing for implementing Dynamic Access Control
4. Implementing Dynamic Access Control
5. Validating and remediating Dynamic Access Control

12. Securing network traffic with firewalls and encryption

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

- **Lab : Configuring Windows Firewall with Advanced Security**

1. Creating and testing inbound rules
2. Creating and testing outbound rules
3. Creating and testing connection security rules

13. Securing network traffic

- Configuring advanced DNS settings
- Examining network traffic with Message Analyzer
- Securing and analyzing SMB traffic

- **Lab : Securing DNS**

1. Configuring and testing DNSSEC
2. Configuring DNS policies and RRL

- **Lab : Microsoft Message Analyzer and SMB encryption**

3. Installing and using the Message Analyzer
4. Configuring and verifying SMB encryption on SMB shares