MServer-SEC

Securing Windows Server 2016/2019

Description:

This five-day course teaches IT professionals how they can enhance the security of the IT infrastructure that they administer. This course explains how you can use auditing and the Advanced Threat Analysis feature in Windows Server 2016 to identify security issues. You will also learn how to mitigate malware threats, secure your virtualization platform, and use deployment options such as Nano server and containers to enhance security. The course also explains how you can help protect access to files by using encryption and dynamic access control, and how you can enhance your network's security.

Students will be able to:

- Secure Windows Server.
- Protect credentials and implement privileged access workstations.
- Limit administrator rights with Just Enough Administration.
- Manage privileged access.
- Mitigate malware and threats.
- Analyze activity with advanced auditing and log analytics.
- Deploy and configure Advanced Threat Analytics and Microsoft Operations Management Suite.
- Configure Guarded Fabric virtual machines (VMs).
- Use the Security Compliance Toolkit (SCT) and containers to improve security.
- Plan and protect data.
- Optimize and secure file services.
- Secure network traffic with firewalls and encryption.
- Secure network traffic by using DNSSEC and Message Analyzer.

Course requirements:

This course is intended for:

IT professionals

Literature:

All participants will receive OKsystem study materials.

Hardware:

Classrooms are equipped with high-performance computers with Internet access and the possibility of wireless connection.

Syllabus:

Module 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

Module 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
- Lab: Configuring and deploying LAPs

Module 3: Limiting administrator rights with Just Enough Administration

- Understanding JEA
- Verifying and deploying JEA
- Lab: Limiting administrator privileges with JEA

Module 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

Module 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

Module 6: Analyzing activity with advanced auditing and log analytics

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

Module 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

Module 8: Secure Virtualization Infrastructure

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

Module 9: Securing application development and server-workload infrastructure

- Using SCT
- Understanding containers
- Lab: Using SCT
- Lab: Deploying and configuring containers

Module 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

Module 11: Optimizing and securing file services

- File Server Resource Manager
- Implementing classification and file management tasks
- Dynamic Access Control
- Lab: Quotas and file screening
- Lab: Implementing Dynamic Access Control

Module 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

Module 13: Securing network traffic

- Configuring advanced DNS settings
- Examining network traffic with Message Analyzer
- Securing and analyzing SMB traffic
- Lab: Securing DNS
- Lab: Microsoft Message Analyzer and SMB encryption

Contact us
OKsystem a.s., Na Pankráci 1690/125, 140 00 Prague 4
(+420) 236 072 111 skoleni@oksystem.cz www.okskoleni.cz