MS20744C: Securing Windows Server 2016

40 HORAS

INTRODUCTION

This five-day, instructor-led course teaches IT professionals how they can enhance the security of the IT infrastructure that they administer. This course begins by emphasizing the importance of assuming that network breaches have occurred already, and then teaches you how to protect administrative credentials and rights to help ensure that administrators can perform only the tasks that they need to, when they need to.

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.

AT COURSE COMPLETION

After completing this course, 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.

PREREQUISITES

Students should have at least two years of experience in the IT field and should have:

- Completed courses 740, 741, and 742, or the equivalent.
- A solid, practical understanding of networking fundamentals, including TCP/IP, User Datagram Protocol (UDP), and Domain Name System (DNS).
- A solid, practical understanding of Active Directory Domain Services (AD DS) principles.
- A solid, practical understanding of Microsoft Hyper-V virtualization fundamentals.
- An understanding of Windows Server security principles.

COURSE OUTLINE

Module 1: Attacks, breach detection, and Sysinternals tools

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

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

Module 3: Limiting administrator rights with Just Enough Administration

- Understanding JEA
- Verifying and deploying JEA

Module 4: Privileged access management and administrative forests

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

Module 5: Mitigating malware and threats

- Configuring and managing Windows Defender
- Restricting software
- Configuring and using the Device Guard feature

Module 6: Analyzing activity with advanced auditing and log analytics

- Overview of auditing
- Advanced auditing
- Windows PowerShell auditing and logging

Teatinos 550, Santiago Centro – Mesa Central +56 22 6576300
www.sondatraining.com - contacto@sondatraining.com

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

Module 8: Secure Virtualization Infrastructure

- Guarded Fabric
- Shielded and encryption-supported virtual machines

Module 9: Securing application development and server-workload infrastructure

- Using SCT
- Understanding containers

Module 10: Planning and protecting data

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

Module 11: Optimizing and securing file services

- File Server Resource Manager
- Implementing classification management and file-management tasks
- 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

Module 13: Securing network traffic

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