SVILUPPIAMO COMPETENZE
TRASFERIAMO E DIVULGHIAMO CONOSCENZE PER OTTENERE PRESTAZIONI MIGLIORI PER LA TUA AZIENDA

Securing Windows Server 2016 (MOC 20744)

DESCRIZIONE

Questo corso è destinato ai professionisti IT con lo scopo di far loro acquisire competenze per migliorare la sicurezza delle infrastrutture IT che amministrano.
Questo corso descrive come è possibile mitigare le minacce di malware, individuare problemi di sicurezza utilizzando il controllo e la funzione Advanced Analysis minacce in Windows Server 2016, garantire la sua piattaforma di virtualizzazione e utilizzare le nuove opzioni di distribuzione, come ad esempio server e contenitori Nano per migliorare la sicurezza. Il corso spiega anche come proteggere l'accesso ai file utilizzando la crittografia, il controllo di accesso dinamico e come si può migliorare la sicurezza della rete.

A CHI SI RIVOLGE

Professionisti IT che hanno bisogno di gestire in modo sicuro le reti utilizzando Windows Server 2016.

PRE-REQUISITES

- Almeno due anni di esperienza nel settore IT;
- Frequenza dei corsi Microsoft 20740, 20741 e 20742 o conoscenza equivalente;
- Consolidata conoscenza pratica dei fondamenti di networking, tra cui il protocollo TCP/IP, User Datagram Domain Name System (DNS) Protocol (UDP);
- Consolidata conoscenza pratica dei Servizi di dominio Active Directory (AD DS);
- Consolidata conoscenza pratica dei fondamenti di virtualizzazione Microsoft Hyper-V.
- Comprensione dei principi di sicurezza di Windows Server.

OBIETTIVI

- Proteggere Windows Server;
- Gestire linee di base di sicurezza;
- Configurare e amministrare quel tanto che basta e just-in-time (JIT);
- Gestire la sicurezza dei dati;
- Configurare Windows Firewall e un firewall di protezione del traffico di rete;
- Garantire la protezione della infrastruttura di virtualizzazione;
- Gestire malware e minacce;
- Configurare il controllo avanzato;
- Gestire gli aggiornamenti del software;
- Gestire le minacce utilizzando Analytics avanzata delle minacce (ATA) e Microsoft Operations Management Suite (OMS).

MODULI

Module 1: Breach detection and using the Sysinternals tools

- Overview of breach detection
- Using the Sysinternals tools to detect breaches

Module 2: Protecting credentials and privileged access

- Understanding user rights
- Computer and service accounts
- Protecting credentials
- Understanding privileged-access workstations and jump servers
- Deploying a local administrator-password solution

Module 3: Limiting administrator rights with Just Enough Administration

- Understanding JEA
- Configuring and deploying JEA

Module 4: Privileged Access Management and administrative forests

- Understanding ESAE forests
- Overview of MIM
- Implementing JIT and Privileged Access Management by using MIM

Module 5: Mitigating malware and threats

- Configuring and managing Windows Defender
- Using software restricting policies (SRPs) and AppLocker
- Configuring and using Device Guard
- Using and deploying the Enhanced Mitigation Experience Toolkit

Module 6: Analysing activity by using advanced auditing and log analytics

- Overview of auditing

- Understanding advanced auditing
- Configuring Windows PowerShell auditing and logging

Module 7: Analysing activity with Microsoft Advanced Threat Analytics feature and Operations Management Suite

- Overview of Advanced Threat Analytics
- Understanding OMS

Module 8: Securing your virtualization an infrastructure

- Overview of Guarded Fabric VMs
- Understanding shielded and encryption-supported VMs

Module 9: Securing application development and server-workload infrastructure

- Using Security Compliance Manager
- Introduction to Nano Server
- Understanding containers

Module 10: Protecting data with encryption

- Planning and implementing encryption
- Planning and implementing BitLocker

Module 11: Limiting access to file and folders

- Introduction to FSRM
- Implementing classification management and file-management tasks
- Understanding Dynamic Access Control (DAC)

Module 12: Using firewalls to control network traffic flow

- Understanding Windows Firewall
- Software-defined distributed firewalls

Module 13: Securing network traffic

- Network-related security threats and connection-security rules
- Configuring advanced DNS settings
- Examining network traffic with Microsoft Message Analyzer
- Securing SMB traffic, and analysing SMB traffic

Module 14: Updating Windows Server

- Overview of WSUS
- Deploying updates by using WSUS