

Windows Server ist ein Server-Betriebssystem von Microsoft. Neben Basis-Funktionen wie Datei- und Druckdiensten stellt es die Infrastruktur für alle Microsoft Enterprise Server zur Verfügung.

Ihr Nutzen

Nach diesem Seminar sind Sie in der Lage Windows Server Umgebungen nach Security-Aspekten zu konfigurieren. Sie erkennen Angriffsvektoren und können Maßnahmen zum Schutz der Infrastruktur ableiten und konfigurieren.

Preis pro Teilnehmer

EUR 2550,- exklusive der gesetzlichen MwSt.

Seminardauer

4 Tag(e)/Day(s)

Seminarinhalte

1. Tag

* Einbrüche, Attacken und Vektoren erkennen

- Angriffstypen, Cybercrime und Vektoren
- Verwenden der Sysinternals Tools

* Benutzer-Rechte, Security Optionen und Service Accounts

- Verstehen von Benutzer-Rechten
- Computer und Service-Accounts
- Privileged Access Workstations und Jump Server
- Local Admin Password Solutions (Windows LAPS)
- Restricted Groups, GMSAs
- Credential Guard konfigurieren
- Protected Group
- Admin SD Holder nutzen

2. Tag

* Beschränkung von Administrations-Rechten

- Verstehen von Just-Enough-Administration (JEA)
- Konfiguration von JEA
- Role und Session Configuration Files
- JEA Endpoints erstellen
- Verteilen von JEA mit DSC

* Privileged Access Management und Admin-Forests

- Enhanced Security Administrative Environment (ESEA)
- Ausblick auf RAMP
- Privileged Identity Management mit AAD (Overview)
- Just In Time (JIT) Administration
- Layered Security Approach

* Schutz vor Malware und anderen Threats

- Windows Defender konfigurieren
- Software-Restriction Policies und AppLocker
- Device Guard verwenden

3. Tag

* Analyse von Aktivitäten

- Überblick über Windows Server Auditing
- PowerShell Auditing und Logging
- Advanced Audit Policies

* Virtuelle Umgebungen und Infrastrukturen schützen

- Guarded Fabric VMs mit Administrator-Trusted Attestation

Voraussetzungen

Gute Administrationskenntnisse inkl. Netzwerk und Active Directory in Windows Server

Hinweise

MOC20744,

Version: 2022

- Shielded und Encryption-Supported VMs

* Schützen von Developer und Server-Workloads

- Security Compliance Manager
- Container nutzen

* Datenschutz durch Verschlüsselung

- Deployment von EFS und BitLocker

* Schutz von Files und Foldern

- File Server Resource Manager (FSRM)
- DFS nutzen, File Screening
- Dynamic Access Control einsetzen

4. Tag

* Konfiguration der Windows Firewall

- Inbound/Outbound Rules konfigurieren
- SD Distributed Firewalls

* Netzwerk-Traffic absichern

- Connection Security Rules und IPSec
- Advanced DNS Settings
- Tracing von abgesichertem Traffic
- SMB traffic absichern
- DNSSEC konfigurieren

* Patching von Windows Server

- WSUS Konfiguration

