M20744

Správa bezpečnosti ve Windows Server 2016/2019

Popis:

Tento pětidenní kurz Vás naučí, jak zvýšit bezpečnost IT infrastruktury. Zjistíte, jak můžete pomocí auditu a funkce Advanced Threat Analysis v systému Windows Server 2016 identifikovat problémy se zabezpečením. Dozvíte se, jak zmírnit hrozby malware, jak zabezpečit virtualizační platformu, jak může nasazení Nano serverů a kontejnerů zvýšit bezpečnost. Kurz také vysvětluje, jak můžete chránit přístup k souborům pomocí šifrování a dynamického řízení přístupu i jak můžete zvýšit zabezpečení vaší sítě.

Absolvent kurzu bude umět:

- Zabezpečit Windows Server.
- Chránit přihlašovací údaje a implementovat pracovní stanice s privilegovaným přístupem.
- Omezit práva administrátora pomocí Just Enough Administration.
- Spravovat privilegované přístupy.
- Odstranit malware a hrozby.
- Analyzovat activity pomocí pokročilých auditovacích nástrojů a analytiky logů.
- Nasadit a konfigurovat Advanced Threat Analytics a Microsoft Operations Management Suite.
- Konfigurovat Guarded Fabric virtual machines (VMs).
- Zvýšit zabezpečení pomocí Security Compliance Toolkit (SCT) a kontejnerů.
- Plánovat a chránit data.
- Optimalizovat a zabezpečit souborové služby.
- Zabezpečit síťový provoz pomocí firewall a šifrování.
- Zabezpečit síťový provoz pomocí DNSSEC a Message Analyzer.

Požadavky pro absolvování kurzu:

Znalosti na úrovni kurzů M20740, M20741, and M20742.

Kurz určen pro:

IT Profesionály

Literatura:

Všichni účastníci školení obdrží originál studijních certifikovaných materiálů Microsoft.

Technické vybavení:

Prostorné učebny jsou vybaveny nadstandardními počítači s možností přístupu na Internet, včetně bezdrátového přístupu.

Osnova:

Module 1: Útoky, detekce narušení bezpečnosti a nástroje Sysinternals

- Formy útoků
- Sledování a detekce hrozeb a útoků
- Průzkym aktivity pomocí nástrojů Sysinternals
- Lab : Základní detekce hrozeb a útoků a strategie reakcí na incidenty

Module 2: Ochrana přihlašovacích údajů a řízení přístupu

- Uživatelská práva
- Počítačové a servisní účty
- Ochrana přihlašovacích údajů
- Stanice pro privilegované činnosti
- Řešení hesel pro lokální administrátory (LAPs)
- Lab: Implementace uživatelských práv, bezpečnostních voleb a group managed service accounts
- Lab: Konfigurace a nasazení LAPs

Module 3: Omezení administrátorských práv pomocí Just Enough Administration (JEA)

- Porozumění principům JEA
- Nasazení, správa a použití JEA
- Lab: Omezení administrátorských práv pomocí JEA

Module 4: Privileged access management (PAM) a administrativní AD lesy

- ESAE AD lesy
- Přehled možností Microsoft Identity Manager
- Metodika JIT a technologie PAM
- Lab: Omezení administrátorských práv pomocí PAM

Module 5: Mitigating malware and threats

- Konfigurace a správa Windows Defender
- Omezení software
- Konfigurace a použití technologie Device Guard
- Lab: Zabezpečení aplikací pomocí Windows Defender, AppLocker a Device Guard

Module 6: Analyzovat activity pomocí pokročilých auditovacích nástrojů a analytiky logů

- Přehled auditu
- Pokročilý audit
- Auditování a logování s Windows PowerShell
- Lab: Konfigurace pokročilého auditu

Module 7: Nasazení a konfigurace Advanced Threat Analytics (ATA) and Microsoft Operations Management Suite

- Nasazení a konfigurace ATA
- Nasazení a konfigurace Microsoft Operations Management Suite
- Nasazení a konfigurace Azure Security Center
- Lab: Nasazení a konfigurace ATA, Microsoft Operations Management Suite a Azure Security Center

Module 8: Zabezpečení virtualizační infrastruktury

- Virtualizační ochrana pomocí Guarded Fabric
- Shielded VMs a jejich šifrování
- Lab: Guarded fabric s Admin-trusted attestation a shielded VMs

Module 9: Bezpečný vývoj aplikací a ladění výkonu serverů

- Použití SCT
- Nano servery a kontejnery z pohledu bezpečnosti
- Lab: Použití SCT
- Lab: Nasazení a konfigurace kontejnerů

Module 10: Plánování a ochrana dat

- Možnosti a implementace šifrování
- Nasazení a správa BitLocker
- Ochrana dat pomocí Azure Information Protection
- Lab: Ochrana dat pomocí šifrování a technologie BitLocker

Module 11: Optimalizace a zabezpečení souborových služeb

- File Server Resource Manager
- Klasifikace souborů a správa souborů přes FSRM
- Dynamic Access Control
- Lab: Kvóty a file screening
- Lab: Implementace Dynamic Access Control

Module 12: Zabezpečení síťové komunikace pomocí firewallů a šifrování

- Síťové hrozby
- Využití Windows Firewall
- Konfigurace IPsec
- Nasazení Datacenter Firewall
- Lab: Konfigurace Windows Firewall

Module 13: Další zabezpečení síťové komunikace

- Zabezpečení DNS pomocí DNSSEC
- Průzkum a sledování síťové komunikace pomocí Message Analyzer
- Zabezpečení a analýza SMB komunikace
- Lab: Zabezpečení DNS
- Lab: Microsoft Message Analyzer a SMB šifrování