

Szkolenie: Microsoft
MS-20744 - Securing Windows Server 2016



Cel szkolenia:

Szkolenie **MS-20744 - Securing Windows Server 2016** przeznaczone jest dla **profesjonalistów IT** chcących zdobyć wiedzę odnośnie podniesienia **bezpieczeństwa infrastruktury**, którą zarządzają. Kurs uczy jak chronić poświadczenia i prawa administracyjne, aby zapewnić stan, w którym administratorzy mogą wykonać tylko te zadania, które mogą i tylko w określonym czasie. Ponadto kurs wskazuje jak łagodzić zagrożenia związane z działaniem złośliwego oprogramowania, przedstawia w jak sposób diagnozować problemy z **bezpieczeństwem** przy użyciu zasad inspekcji oraz rozwiązania **Advanced Threat Analysis** dostępnego w **Windows Server 2016**.

Szkolenie obejmuje zakresem również zabezpieczanie platformy wirtualizacji, korzystanie z nowych opcji wdrażania oprogramowania - serwer Nano czy kontenery mające na celu zwiększenie bezpieczeństwa.

Kurs objaśnia także jak chronić dostęp do plików i folderów za pomocą szyfrowania i funkcji dynamicznej kontroli dostępu, a także jak zwiększyć **bezpieczeństwo sieciowe**.

Plan szkolenia:

- Wykrywanie zagrożeń przy użyciu narzędzi Sysinternals
 - Przegląd zagadnień związanych z wykrywaniem zagrożeń
 - Narzędzia pakietu Sysinternals wykorzystywane do wykrywania zagrożeń
- Ochrona poświadczeń i dostępu uprzywilejowanego
 - Prawa użytkownika
 - Konta komputerów i usług
 - Ochrona poświadczeń
 - Stacje robocze uprzywilejowanego dostępu i serwery dostępu pośredniego
 - Konfiguracja i wdrożenie Local Administrator Password Solution (LAPS)
- Ograniczanie uprawnień administratora przy użyciu Just Enough Administration (JEA)
 - Idea rozwiązania JEA
 - Konfiguracja i wdrożenie (JEA)
- Ograniczanie praw administratora i lasy administracyjne
 - Lasy Enhanced Security Administrative Environment (ESAE)
 - Przegląd rozwiązania Microsoft Identity Manager (MIM)

- Wdrażanie Just In Time (JIT) and Privileged Access Management (PAM) z wykorzystaniem MIM
- Minimalizowanie zagrożeń związanych z działaniem złośliwego oprogramowania i innych zagrożeń
 - Konfiguracja Windows Defender
 - Wdrożenie AppLocker
 - Konfigurowanie i korzystanie z Device Guard
 - Wdrożenie i korzystanie z Enhanced Mitigation Experience Toolkit (EMET)
- Analiza aktywności z wykorzystaniem zaawansowanych zasad inspekcji oraz analiza zdarzeń
 - Przegląd zasad inspekcji
 - Idea zaawansowanego audytu
 - Konfigurowanie inspekcji i zbierania informacji przy użyciu Windows PowerShell
- Analiza aktywności z wykorzystaniem Microsoft Advanced Threat Analytics (ATA) i Operations Management Suite (OMS)
 - Przegląd funkcjonalności ATA
 - Idea rozwiązania OMS
- Zabezpieczanie infrastruktury wirtualizacji
 - Przegląd zabezpieczania maszyn wirtualnych z użyciem infrastruktury Guarded Fabric
 - Osłanianie i szyfrowane maszyny wirtualne
- Zabezpieczanie wdrażania oprogramowania i infrastruktury serwerowej
 - Korzystanie z Security Compliance Manager (SCM)
 - Wstęp do serwera w wersji Nano
 - Kontenery
- Szyfrowanie danych
 - Planowanie i wdrożenie Encrypting File System (EFS)
 - Planowanie i wdrożenie BitLocker
- Kontrola dostępu do plików i folderów
 - Wstęp do File Server Resource Manager (FSRM)
 - Implementacja zarządzania klasyfikacją i zadania związane z klasyfikacją plików
 - Dynamic Access Control (DAC)
- Wykorzystanie firewalla do kontroli ruchu sieciowego
 - Windows Firewall
 - Rozproszone programowe rozwiązania typu firewall
- Ochrona ruchu sieciowego
 - Zagrożenia wynikające z pracy w sieci i reguły bezpieczeństwa sieciowego
 - Konfiguracja zaawansowanych ustawień DNS
 - Analiza ruchu sieciowego z wykorzystaniem Microsoft Message Analyzer

- Zabezpieczanie i analiza połączeń związanych z protokołem SMB
- Aktualizowanie Windows Server
 - Przegląd usługi WSUS
 - Wdrażanie poprawek systemowych za pomocą WSUS

Wymagania:

- Bardzo dobra znajomość zagadnień związanych z podstawami sieci, w tym TCP/IP, UDP, DNS
- Bardzo dobra znajomość zagadnień związanych z Active Directory Domain Services (AD DS)
- Bardzo dobra znajomość zagadnień związanych z podstawami wirtualizacji w oparciu o Microsoft Hyper-V
- Rozumienie zasad związanych z bezpieczeństwem Windows

Poziom trudności



Certyfikaty:

Uczestnicy po zakończeniu szkolenia **MS-20744 - Securing Windows Server 2016** otrzymują **certyfikat** ukończenia **autoryzowanego kursu Microsoft**.

Prowadzący:

Microsoft Certified Trainer.

Informacje dodatkowe:

Zajęcia prowadzone są w języku polskim, materiały oraz oprogramowanie są w języku angielskim.