A-20744 Bezpieczeństwo Windows Server 2016

Czas trwania: 5 dni

Dla kogo:
Szkolenie skierowane jest do administratorów i inżynierów IT chcących zdobyć wiedzę z zakresu podniesienia bezpieczeństwa infrastruktury opartej o środowisko Windows za pomocą najnowszych narzędzi zawartych w Windows Server 2016.

Wymagania wstępne:
- co najmniej dwa lata doświadczenia w IT
- praktyczna znajomość podstaw sieciowych, w tym TCP/IP, UDP i DNS
- praktyczna znajomość podstaw Active Directory Domain Services (AD DS)
- praktyczna znajomość podstaw wirtualizacji Microsoft Hyper-V
- podstawy bezpieczeństwa Windows Server

Zakres tematyczny:
1. Wykrywanie włamań przy użyciu narzędzi Sysinternals
    - przegląd wykrywania włamań
    - korzystanie z narzędzi Sysinternals do wykrywania włamania
2. Ochrona poświadczeń i dostępu uprzywilejowanego
    - zrozumienie praw użytkownika
    - konta komputerowe i usług
    - ochrona poświadczeń
    - zrozumienie uprzywilejowanego dostępu do stacji roboczych i serwerów skoku (jump)
    - wdrożenie rozwiązań hasła administratora lokalnego
3. Ograniczenie praw administratora przy pomocy JEA (Just Enough Administration)
    - zrozumienie JEA
    - konfigurowanie i wdrożenie JEA
4. Zarządzanie dostępem uprzywilejowanym i administracja lasami
    - zrozumienie lasów ESAE
    - przegląd MIM
    - wdrożenie JIT i zarządzanie dostępem uprzywilejowanym za pomocą MIM
5. Radzenie sobie ze złośliwym oprogramowaniem oraz z zagrożeniami
    - konfiguracja i zarządzanie Windows Defender
    - korzystanie z polityk ograniczenia oprogrmowania (Software Restriction Policy) oraz AppLocker
    - konfigurowanie i używanie strażnika urządzeń
    - używanie i wdrożenie Enhanced Mitigation Experience Toolkit
6. Analiza aktywności przy użyciu analityki zaawansowanego audytu oraz logów
    - przegląd audytu
    - zrozumienie zaawansowanego audytu
    - konfigurowanie audytu oraz logów Windows PowerShell
7. Analizowanie aktywności z funkcją Microsoft Advanced Threat Analytics oraz pakietem zarządzania operacyjnego
    - przegląd zaawansowanej analityki zagrożeń
    - zrozumienie OMS (Operations Management Suite)
8. Zabezpieczanie infrastruktury wirtualizacji
    - przegląd Guarded Fabric maszyn wirtualnych
    - zrozumienie ekranowanych i szyfrowanych maszyn wirtualnych
9. Zapewnienie infrastruktury serwerowej dla rozwoju aplikacji oraz obciążenia
    - korzystanie z Security Compliance Manager
    - wprowadzenie do nano serwera

- zrozumienie kontenerów

10. Ochrona danych za pomocą szyfrowania
    - planowanie i wdrożenie szyfrowania
    - planowanie i wdrożenie funkcji BitLocker
11. Ograniczanie dostępu do plików i folderów
    - wprowadzenie do FSRM
    - wdrożenie zarządzania klasyfikacją i zadania zarządzania plikami
    - zrozumienie dynamicznej kontroli dostępu (DAC)
12. Używanie zapory celem kontroli ruchu sieciowego
    - zrozumienie zapory systemu Windows
    - rozproszone, programowe zapory