Bezpieczeństwo sieci opartej na Windows Server 2019

Opis: Warsztaty prezentują metody i aspekty bezpieczeństwa w oparciu o platformę środowiska Windows Server 2019.

Czas: 24 godziny

Wymagania wstępne: Co najmniej dwuletnie praktyczne doświadczenie w zarządzaniu środowiskiem na poziomie serwerowych systemów operacyjnych lub adekwatna praktyczna wiedza z następujących dziedzin:

- podstaw zagadnień sieciowych, włączając protokoły TCP/IP i usługi DNS, DHCP;
- zarządzania infrastrukturą Active Directory Domain Services (AD DS);
- podstaw wirtualizacji na platformie Microsoft Hyper-V.

Dla kogo: Warsztaty przeznaczone dla profesjonalistów IT, chcących zdobyć wiedzę na temat zwiększenia bezpieczeństwa infrastruktury, którą zarządzają. Pokazują, jak łagodzić zagrożenia związane z działaniem złośliwego oprogramowania, w jaki sposób diagnozować problemy z bezpieczeństwem przy użyciu zasad inspekcji oraz rozwiązania Advanced Threat Analysis, dostępnego w Windows Server 2019.

Zakres tematyczny:

1) Ochrona poświadczeń i dostępu uprzywilejowanego

a. Prawa użytkownika
b. Prezentacja tożsamości kont komputerów i kont serwisowych
c. Ochrona poświadczeń
d. Stacje robocze uprzywilejowanego dostępu i serwery dostępu pośredniego
e. Konfiguracja i wdrożenie Local Administrator Password Solution (LAPS)

2) Ograniczanie uprawnień administratora przy użyciu Just Enough Administration (JEA)

a. Idea rozwiązania JEA
b. Konfiguracja i wdrożenie JEA

3) Wykrywanie zagrożeń przy użyciu narzędzi Sysinternals

a. Przegląd zagadnień związanych z wykrywaniem zagrożeń
b. Narzędzia pakietu Sysinternals wykorzystywane do wykrywania zagrożeń

4) Ochrona przed niepożądanym oprogramowaniem i zagrożeniami

a. Konfiguracja usługi Windows Defender
b. Wdrożenie AppLocker

c. Konfigurowanie i korzystanie z Device Guard
d. Wdrożenie i korzystanie z Enhanced Mitigation Experience Toolkit (EMET)

5) Analiza aktywności przy użyciu zaawansowanych metod audytowania i logów serwisowych

a. Przegląd zasad inspekcji
b. Idea zaawansowanego audytu
c. Konfigurowanie inspekcji i zbierania informacji przy użyciu Windows PowerShell

6) Analiza aktywności z wykorzystaniem Microsoft Advanced Threat Analytics (ATA) i Operations Management Suite (OMS)

a. Przegląd funkcjonalności ATA
b. Idea rozwiązania OMS

7) Zabezpieczanie infrastruktury wirtualizacji

a. Przegląd zabezpieczania maszyn wirtualnych z użyciem infrastruktury Guarded Fabric
b. Osłaniane i szyfrowane maszyny wirtualne

8) Zabezpieczanie wdrażania oprogramowania i infrastruktury serwerowej

a. Korzystanie z Security Compliance Manager (SCM)
b. Wstęp do serwera w wersji Nano
c. Kontenery - Szyfrowanie danych
d. Planowanie i wdrożenie Encrypting File System (EFS)
e. Planowanie i wdrożenie BitLocker
f. Kontrola dostępu do plików i folderów

9) Konfiguracja usługi Firewall i kontrola usług ruchu sieciowego

a. Windows Firewall
b. Rozwiązania programowe Firewall

10) Ochrona ruchu sieciowego

a. Zagrożenia wynikające z pracy w sieci i reguły bezpieczeństwa sieciowego
b. Konfiguracja zaawansowanych ustawień DNS
c. Analiza ruchu sieciowego z wykorzystaniem Microsoft Message Analyzer
d. Zabezpieczanie i analiza połączeń związanych z protokołem SMB

11) Zarządzanie aktualizacjami przez usługę Windows Server Update Services

a. Prezentacja usługi WSUS
b. Wdrażanie polityki aktualizacji przez usługę WSUS