

Szkolenie: Microsoft

Zarządzanie bezpieczeństwem w środowisku MS Windows Server i Windows 10/11 (on-premises)



DOSTĘPNE TERMINY

2024-08-19 | 5 dni | Warszawa / Wirtualna sala
2024-09-02 | 5 dni | Warszawa / Wirtualna sala
2024-09-23 | 5 dni | Warszawa / Wirtualna sala (Termin gwarantowany)
2024-10-21 | 5 dni | Warszawa / Wirtualna sala
2024-12-16 | 5 dni | Kraków / Wirtualna sala

Cel szkolenia:

Działania każdej branży skupiają się wokół ciągłej dostępności do zgromadzonych i przetwarzanych danych z zachowaniem ich poufności. Zapewnienie odpowiedniego poziomu bezpieczeństwa zarówno na poziomie infrastruktury serwerowej, jak i stacji klienckich nierozdzielnie związane jest ze znajomością problematyki bezpieczeństwa. Oprócz umiejętności identyfikacji zagrożeń i ich potencjalnych skutków niezbędne jest posiadanie wiedzy i umiejętności w zakresie wykorzystania najnowszych narzędzi, które mają na celu zapewnienie wymaganego poziomu bezpieczeństwa.

Celem szkolenia popartego licznymi przykładami jest zwiększenie świadomości w zakresie zagrożeń i zarządzania bezpieczeństwem środowisk opartych o produkty serwerowe i klienckie systemy operacyjne firmy Microsoft.

Plan szkolenia:

- Identyfikacja zagrożeń występujących w środowisku Windows wg norm ISO/IEC
 - Klasyfikacja współczesnych zagrożeń
 - Zakres systemu zarządzania bezpieczeństwem
 - Szacowanie kosztów i szans osiągnięcia założonego poziomu zabezpieczeń
- Bezpieczne uwierzytelnianie i ochrona poświadczeń w systemie Windows (z wykorzystaniem narzędzia MimiKatz)
 - Przegląd metod uwierzytelniania
 - Analiza ryzyka procesu uwierzytelniania
 - Ataki typu Offline - eskalacja uprawnień
 - Ataki Pass-the-hash i Pass-the-Ticket
 - Legacy LAPS i Windows LAPS
 - Zarządzanie politykami haseł domenowych z uwzględnieniem PSO

- Zarządzalne konta serwisowe (gMSA)
- Credential Guard
- Tymczasowa przynależność do grup zabezpieczeń ADDS (Just in Time Administration)
- Autoryzacja dostępu do zasobów
 - Kontrola i inspekcja dostępu na podstawie ACL
 - Projektowanie zaawansowanych zasad inspekcji
 - Autoryzacja oparta na oświadczeniach
- Kontrola praw i uprawnień użytkowników
 - Przegląd i konfiguracja uprawnień użytkowników
 - Optymalizacja narzędzia UAC
 - Restrykcje dotyczące korzystania z nośników zewnętrznych
 - Reguły AppLocker dotyczące uruchamianego oprogramowania
 - Limitowane sesje PowerShell (Just Enough Administration)
- Infrastruktura Klucza Publicznego
 - Planowanie, wdrożenie i utrzymanie roli AD CS
 - Metody dystrybucji i zarządzanie certyfikatami
 - Zabezpieczanie komunikacji – protokoły TLS i IPsec oraz rola Windows Defender Firewall with Advanced Security
 - Podpisywanie cyfrowe dokumentów MS Office i plików PDF
 - Podpisywanie skryptów PowerShell
- Uwierzytelnianie dwuskładnikowe w oparciu o karty inteligentne
 - Przegląd infrastruktury kart inteligentnych i tokenów
 - Dwuskładnikowe uwierzytelnianie na stacjach roboczych
- Szyfrowanie danych w oparciu o dobre praktyki
 - Bitlocker i Bitlocker To Go
 - Encrypted File System
- Network Policy Server
 - Kontrola dostępu do sieci bezprzewodowych z wykorzystaniem serwera RADIUS
- Analiza ruchu sieciowego
 - Działania mające na celu zabezpieczenie protokołu SMB
 - Zabezpieczenie systemu rozwiązywania nazw DNS
- Konfiguracja uprawnień usług systemowych
- Analiza bezpieczeństwa i hardening systemów
 - Zaawansowane monitorowanie bezpieczeństwa systemów w oparciu o Sysmon
 - Security Compliance Toolkit (SCT)
 - Restricted Groups

- Tiering Active Directory
- Polityki uwierzytelniania
- Idea wykorzystania stacji uprzywilejowanego dostępu (PAW) oraz serwerów przesiadkowych (Jump servers)
- Zarządzanie poprawkami systemowymi i omówienie mechanizmu Windows Update for Business

Wymagania:

- Doświadczenie we wdrażaniu i zarządzaniu środowiskiem Active Directory w dowolnej wersji Windows Server.
- Doświadczenie w administrowaniu stacjami roboczymi.

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia **Zarządzanie bezpieczeństwem w środowisku MS Windows Server i Windows 10/11 (on-premises)** otrzymują certyfikat wystawiony imiennie oraz na firmę, sygnowany przez Compendium CE.

Prowadzący:

Microsoft Certified Trainer.

Informacje dodatkowe:

Oferowane szkolenie jest autorskim kursem Compendium CE.