

kod szkolenia: Security Windows 10 / PL DL 2d

Bezpieczeństwo systemu Windows 10

Autorskie szkolenie Altkom Akademia Bezpieczeństwo systemu Windows 10 **Security Windows 10** kurs w formie Distance Learning. Docelowa grupa odbiorców:

- administrator
- specjalista IT
- architekt
- konsultant



Przeznaczenie szkolenia

Szkolenie skierowane do:

- specjalistów zarządzających bezpieczeństwem
- architektów sieciowych
- administratorów IT
- specjalistów IT
- konsultantów planujących wdrożenie systemu Windows 10 na komputerach klienckich w środowisku domenowym jak i poza domenowym.



Korzyści wynikające z ukończenia szkolenia

Wiedza i umiejętności z zakresu rekomendacji, które pomogą wzmocnić poziom zabezpieczenia komputerów stacjonarnych i komputerów przenośnych pracujących pod kontrolą systemu Windows 10 w domenie Active Directory Domain Services (AD DS) i poza domeną.



Oczekiwane przygotowanie słuchaczy

Dobra znajomość podstaw sieci, znajomość i doświadczenie w konfiguracji zabezpieczeń i administracji oraz doświadczenie z zakresu wspierania lub konfiguracji klientów Windows.

Umiejętność korzystania z anglojęzycznych materiałów.

Dla zwiększenia komfortu pracy oraz efektywności szkolenia zalecamy skorzystanie z dodatkowego ekranu. Brak dodatkowego ekranu nie jest przeciwwskazaniem do udziału w szkoleniu, ale w znaczący sposób wpływa na komfort pracy podczas zajęć

Informacje oraz wymagania dotyczące uczestniczenia w szkoleniach w formule zdalnej dostępne na:

<https://www.altkomakademia.pl/distance-learning/#FAQ>



Język szkolenia

- **Szkolenie:** polski
- **Materiały:** angielski



Szkolenie obejmuje

- * materiały w formie elektronicznej dostępne na platformie: <https://www.altkomakademia.pl/>
- * dostęp do portalu słuchacza Altkom Akademii



Czas trwania

2 dni / 14 godzin

Agenda szkolenia

1. Uwierzytelnianie i autoryzacja w Windows 10
 - proces uwierzytelniania i autoryzacji

- uwierzytelnianie biometryczne
 - wirtualne karty inteligentnej w procesie uwierzytelniania
 - **model kontroli dostępu** do systemu Windows
 - ochrona publicznych certyfikatów i kluczy
 - Tryb **Restricted Admin** dla połączeń pulpitu zdalnego
 - schowek dla poświadczeń – **Credential Locker**.
2. Ochrona wrażliwych danych
- szyfrowanie i ochrona dysków z zastosowaniem funkcji **BitLocker**
 - tryby pracy BitLocker oraz zarządzanie układem **TPM**
 - **zastosowanie ustawień GPO** do wdrożenia BitLocker
 - Ochrona danych na wymiennych dyskach z zastosowaniem funkcji BitLocker To Go
 - System szyfrowania plików EFS
 - Instalacja i zarządzanie urządzeniami w systemie Windows 10
 - Windows To Go.
3. Sposoby ochrony przed złośliwym oprogramowaniem
- funkcje zabezpieczeń stosowane w systemie Windows 10
 - konsola Centrum Akcji
 - bezpieczny rozruch (**Secure Boot**)
 - mechanizm User Account Control
 - oprogramowanie Windows Defender
 - zaporę systemu Windows 10
 - ograniczanie dostępu do aplikacji – AppLocker
 - odświeżanie i przywracanie komputera do stanu pierwotnego.
4. Klient Hyper-V
- zabezpieczanie systemów operacyjnych zarządzania
 - zabezpieczenia maszyn wirtualnych.
5. Wdrażanie rekomendowanych zasad bezpieczeństwa w kontekście bazowych ustawień systemu Windows 10
- wprowadzenie
 - projektowanie struktur jednostek organizacyjnych (OU) i zasad grupowych
 - ustawienia zasad domenowych
 - konfigurowanie ustawień haseł oraz zasad blokady konta
 - przypisywanie praw użytkownika
 - konfigurowanie opcji zabezpieczeń
 - konfiguracja zapory systemu Windows Firewall with Advanced Security
 - usługa Windows Update.
6. Narzędzia SCM, SCT i ASA
- wprowadzenie

- praca z programem SCM (Security Compliance Manager)
 - praca z programem SCT (Security Compliance Toolkit)
 - praca z programem ASA (Attack Surface Analyzer)
7. Przykładowe ustawienia bezpiecznego Windows 10