

kod szkolenia: Security Windows 11 / PL AA 2d

Bezpieczeństwo systemu Windows 11

Szkolenie w formule stacjonarnej

Autorskie szkolenie Altkom Akademia Bezpieczeństwo systemu Windows 11 Security Windows 11.

Dobierz formułę

szkolenia: <https://www.altkomakademia.pl/dobierz-formule-szkolenia-do-celu-poziomu-i-efektu-ktory-chcesz-osiagnac/>

Docelowa grupa odbiorców:

- administrator
- specjalista IT
- HelpDesk

Dyrektywa NIS2

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi.

[Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2](#)



Odbiorcy szkolenia

Szkolenie skierowane do osób odpowiedzialnych za zabezpieczenie infrastruktury stacji roboczych

opartej o Windows 11 i pragnących nabyć umiejętności potrzebne do lepszego zarządzania i ochrony dostępu do danych i informacji, uproszczenia wdrażania i zarządzania infrastrukturą tożsamości oraz zapewnienia bardziej bezpiecznego dostępu do danych



Korzyści

Wiedza i umiejętności z zakresu rekomendacji, które pomogą wzmocnić poziom zabezpieczenia komputerów stacjonarnych i komputerów przenośnych pracujących pod kontrolą systemu Windows 11 w domenie Active Directory Domain Services (AD DS) i poza domeną.

Kurs zapewnia uczestnikom wiedzę i umiejętności zabezpieczenia systemów Windows 11.



Program szkolenia

1. Uwierzytelnianie i autoryzacja w Windows 11

- proces uwierzytelniania i autoryzacji
- uwierzytelnianie biometryczne
- wirtualne karty inteligentnej w procesie uwierzytelniania
- model kontroli dostępu do systemu Windows
- ochrona publicznych certyfikatów i kluczy

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 11
- Windows To Go.

3. Sposoby ochrony przed złośliwym oprogramowaniem

- funkcje zabezpieczeń stosowane w systemie Windows 11
- bezpieczny rozruch (Secure Boot)
- mechanizm User Account Control
- oprogramowanie Windows Defender
- zaporę systemu Windows 11
- ograniczanie dostępu do aplikacji – AppLocker
- odświeżanie i przywracanie komputera do stanu pierwotnego.

4. Wdrażanie rekomendowanych zasad bezpieczeństwa w kontekście bazowych ustawień systemu Windows 11

- 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.

5. Narzędzia SCM i SCT

- wprowadzenie
- praca z programem SCM (Security Compliance Manager)
- praca z programem SCT (Security Compliance Toolkit)

6. Przykładowe ustawienia bezpiecznego Windows 11



Oczekiwane przygotowanie uczestnika

- Dobra znajomość podstaw sieci, znajomość i doświadczenie w konfiguracji zabezpieczeń i administracji oraz doświadczenie z zakresu wspierania lub konfiguracji klientów Windows.
- Mile widziane doświadczenie w administracji środowiskiem opartym na Windows Server.
- 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>



Szkolenie obejmuje

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

Metoda szkolenia:

- teoria

- dema
- wspólne projekty
- labolatoria indywidualne
- 50% teoria
- 50% praktyka



Czas trwania

2 dni / 14 godzin

Język

- Szkolenie: polski
- Materiały: angielski