

Bezpieczeństwo systemów w domenie Active Directory Windows Server 2016 w połączeniu z Windows 10

Autorskie szkolenie Altkom Akademia Bezpieczeństwo systemów w domenie Active Directory Windows Server 2016 w połączeniu z Windows 10 **Security MS** kurs w formie Distance Learning. Docelowa grupa odbiorców:

- **administrator**
- **specjalista IT**



Przeznaczenie szkolenia

Szkolenie skierowane do:

- administratorów
- specjalistów IT odpowiedzialnych za implementowanie polityki bezpieczeństwa w środowisku opartym o Microsoft Windows Server 2016 chcących poszerzyć swoją wiedzę w zakresie zabezpieczenia serwerów i stacji roboczych.



Korzyści wynikające z ukończenia szkolenia

Nabycie przez uczestnika umiejętności z zakresu zabezpieczania dostępu do danych i usług w środowisku opartym o system Windows Server 2016.

Po ukończeniu szkolenia Uczestnik:

- posiada wiedzę i umiejętności z zakresu zabezpieczania dostępu do danych i usług w środowisku opartym o system Windows Server 2016,
- wie na czym polega zabezpieczanie ról serwerowych,
- rozumie zasady konfiguracji PKI i bezpiecznego dostępu do środowiska,
- wie jak i potrafi właściwie zabezpieczyć dane,

- zna metody dystrybucji i zarządzania certyfikatami,
- potrafi korzystać z narzędzi do kontroli poufności w Windows 10.
- potrafi prawidłowo dokonywać oceny jakości dostarczanych przez siebie produktów i usług w aspekcie merytorycznym.
- zdobył kompetencje, dzięki którym jest gotów do samodzielnego poszukiwania rozwiązań podnoszących jakość realizowanych przez siebie zadań oraz zwiększających ich efektywność.



Oczekiwane przygotowanie słuchaczy

Wiedza z zakresu administrowania usługami serwera MS Windows Server 2012/2016, usługami Active Directory, stacjami roboczymi, podstawy wiedzy związanej z bezpieczeństwem systemów lub ukończone szkolenie:

- MS 20410 – Installing and Configuring Windows Server 2012
- MS 20740 – Instalacja, przestrzeń dyskowa i przetwarzanie danych w Windows Server 2016

Umiejętność korzystania z anglojęzycznych materiałów.

Szkolenia poprzedzające: **MS 20410** oraz **MS 20740**

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

5 dni / 35 godzin

Agenda szkolenia

1. Wprowadzenie do bezpieczeństwa systemów Microsoft
 - Definicje zagrożeń
 - Definicje ataków
2. Planowanie i konfigurowanie strategii autoryzacji i uwierzytelniania
 - Komponenty modelu uwierzytelniania
 - Planowanie i wdrażanie strategii uwierzytelniania
 - Konta użytkowników, komputerów i grup
3. Zabezpieczanie serwerów Windows Server 2016 i klientów Windows 10
 - Kontrolery domen
 - RODC
 - PowerShell for JIT Administration
 - Szablony zabezpieczeń, GPO
 - Microsoft Security Compliance Toolkit
 - Audyt zdarzeń
 - Archiwizacja i odzyskiwanie
 - Serwery DNS
 - Serwery DHCP
 - EFS
 - BitLocker
 - Serwery plików i wydruku
4. Konfigurowanie bezpiecznego dostępu do plików (DAC)
 - Wprowadzenie do dynamicznej kontroli dostępu
 - Konfiguracja DAC
5. Instalacja, konfigurowanie i zarządzanie urzędem certyfikacji (Certification Authority)
 - Przegląd PKI
 - Wprowadzenie do urzędów certyfikatów

- Instalacja CA
 - Zarządzanie urzędem certyfikatów
6. Konfiguracja, dostarczanie i zarządzanie certyfikatami
- Przegląd certyfikatów
 - Zatwierdzanie certyfikatów
 - Szablony certyfikatów
 - Wdrażanie archiwizacji kluczy
7. Bezpieczna transmisja danych
- Zabezpieczenie transmisji w usłudze IIS przy wykorzystaniu SSL
 - Wprowadzenie do IPSec
 - Planowanie i wdrażanie bezpiecznej transmisji danych z użyciem IPSec
8. Zabezpieczanie zdalnego dostępu
- Połączenia VPN
 - Konfiguracja NPS (RADIUS)
 - Połączenia Direct Access
 - Web Application Proxy
 - Bezpieczne połączenia RDP – konfiguracja TS Gateway
9. Wdrażanie WSUS
- Instalacja Windows Server Update Services
 - Zarządzanie infrastrukturą WSUS
10. Bezpieczeństwo stacji roboczej Windows 10
- Konfiguracja środowiska przy wykorzystaniu polityk grupowych
 - Windows Defender Security Center
 - Kontrola uruchamianych aplikacji AppLocker