kod szkolenia: Security MS_2022 / PL AA 5d

Implementacja cyberodporności w infrastrukturze Active Directory w kontekście dyrektywy NIS 2

Szkolenie w formule stacjonarnej.

Link do Twojej ścieżki rozwoju:
https://www.altkomakademia.pl/windows-server/

Szkolenie autorskie

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

Przeznaczenie szkolenia

Szkolenie skierowane do specjalistów IT odpowiedzialnych za implementowanie i utrzymywanie polityk bezpieczeństwa w środowisku Active Directory opartym o Windows Server 2022 i stacje klienckie Windows 11. Szkolenie jest również dedykowane dla organizacji, które są prawnie zobligowane do wdrożenia Dyrektywy Unii Europejskiej NIS2 i potrzebują zapewnić zespołom IT odpowiednie szkolenia z bezpieczeństwa. Szkolenie jest też dedykowane do administratorów i specjalistów IT 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 2022. Po ukończeniu szkolenia Uczestnik: posiada wiedzę i umiejętności z zakresu zabezpieczania dostępu do danych i usług w środowisku opartym o system Windows Server 2022, 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 11. Uczestnik potrafi prawidłowo dokonywać oceny jakości dostarczanych przez siebie produktów i usług w aspekcie merytorycznym. Uczestnik 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:

- Windows Server 2012/2016/2019/2022
- Usługami Active Directory
- Stacjami roboczymi Windows 10/11
- Podstawy wiedzy związanej z bezpieczeństwem systemów
- Umiejętność wykonywania zadań za pomocą komend PowerShell

Wskazane ukończone szkolenia, co najmniej jedno z Windows Server i co najmniej jedno z PowerShell:

- Wprowadzenie do zarządzania Windows Server 2019
- Zarządzanie Windows Server 2022
- Managing Windows 2022 Environments with Group Policy
- Identity with Windows Server 2019/2022
- Windows Server Administration 2019/2022
- PowerShell Fundamentals
- Automating Administration with Windows PowerShell

Umiejętność korzystania z anglojęzycznych materiałów

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

Metoda szkolenia:

- Wykład + warsztaty.

Czas trwania

5 dni / 35 godzin

Agenda szkolenia

1. Dyrektywa NIS2
   - Co to jest NIS2
   - Obszary objęte dyrektywą
   - Szkolenia informatyczne w kontekście NIS2
2. Wprowadzenie do bezpieczeństwa systemów
   - Definicje zagrożeń
   - Model obrony w głąb
   - Naruszenia zasad polityki bezpieczeństwa
   - Bezpieczeństwo osobowe
   - Ocena i analiza ryzyka
3. Planowanie i konfigurowanie strategii autoryzacji i uwierzytelniania
   - Komponenty modelu uwierzytelniania
   - Planowanie i wdrażanie strategii uwierzytelniania
   - Konta użytkowników, komputerów i grup
4. Bezpieczna administracja zdalna
   - Stacje robocze z dostępem uprzywilejowanym (PAW)

- Koncepcja administracji o najmniejszych uprawnieniach
- Delegowanie uprawnień
- Server Manager
- RSAT
- PowerShell Remoting
- Windows Admin Center

5. Zabezpieczanie serwerów Windows Server 2022

- Zarządzanie infrastrukturą Active Directory
- Kontrolery domeny – Windows Server Core i RODC
- PowerShell for JIT and JEA Administration
- Zabezpieczanie połączenia pomiędzy lasami Active Directory – relacje zaufania
- Zcentralizowane zarządzanie za pomocą obiektów zasad grupy
- Hardening środowiska Windows
- Zawansowane opcje inspekcji
- Subskrypcja podglądu zdarzeń
- Zabezpieczanie i odzyskiwanie po awarii usługi AD
- Zabezpieczanie servera DNS
- Zabezpieczanie servera DHCP
- Szyfrowanie plików EFS
- Szyfrowanie woluminów dyskowych Bitlocker
- Zabezpieczanie serwera plikowego

6. Instalacja, konfigurowanie i zarządzanie urzędem certyfikacji (Certification Authority)

- Wprowadzenie do PKI
- Wprowadzenie do urzędów certyfikatów
- Typy instalacji CA
- Zarządzanie urzędem certyfikatów
- Konfiguracja, dostarczanie i zarządzanie certyfikatami

7. Bezpieczna transmisja danych

- Zabezpieczenie transmisji w usłudze IIS przy wykorzystaniu SSL
- Zaawansowany Firewall
- Wprowadzenie do IPSec

8. Zabezpieczanie zdalnego dostępu

- Połączenia VPN
- Konfiguracja NPS (RADIUS)
- Połączenia Direct Access
- Web Application Proxy
- Bezpieczne połączenia RDP – konfiguracja TS Gateway

9. Zarządzanie aktualizacjami za pomocą serwera WSUS

- Instalacja Windows Server Update Services
- Zarządzanie infrastrukturą WSUS

10. Bezpieczeństwo stacji roboczej Windows 11
    - Konfiguracja środowiska przy wykorzystaniu polityk grupowych
    - Windows Defender Security Center
    - Kontrola uruchamianych aplikacji AppLocker
    - Windows LAPS