

kod szkolenia: AA_20744 / PL DL 5d

Securing Windows Server 2016

Szkolenie autorskie. **Odpowiednik autoryzowanego kursu MS 20744**

Szkolenia o podobnej tematyce:

*MS 20744: Securing Windows Server 2016

*Security MS: Bezpieczeństwo systemów w domenie Active Directory Windows Server 2016 w połączeniu z Windows 10

*AZ-800: Administering Windows Server Hybrid Core Infrastructure

*AZ-801: Configuring Windows Server Hybrid Advanced Services



Przeznaczenie szkolenia

Szkolenie skierowane do osób odpowiedzialnych za zarządzanie bezpieczeństwem infrastruktury IT.

Kurs obejmuje takie zagadnienia jak:

- ochrona poświadczeń administracyjnych i praw, by administratorzy mogli wykonywać tylko te zadania, które są im potrzebne, kiedy zajdzie taka potrzeba
- korzystanie z inspekcji i funkcji zaawansowanej analizy zagrożeń w systemie Windows Server 2016 w celu identyfikowania problemów związanych z bezpieczeństwem
- ograniczanie zagrożenia złośliwym oprogramowaniem
- zabezpieczanie platformy wirtualizacji i wykorzystanie opcji wdrażania, takich jak serwer Nano i kontenery, aby zwiększyć bezpieczeństwo
- ochrona dostępu do plików za pomocą szyfrowania i dynamicznej kontroli dostępu
- sposoby zwiększania bezpieczeństwa sieci.



Korzyści wynikające z ukończenia szkolenia

Uzyskanie wiedzy i praktycznych umiejętności w zakresie zabezpieczeń systemu Windows Server 2016.

W tym zapoznanie się z:

- Zabezpieczeniem systemu Windows Server
- Ochroną poświadczenia i wdrażaniem stacji roboczych z dostępem uprzywilejowanym
- Ograniczeniem uprawnień administracyjnych z wykorzystaniem Just Enough Administration
- Zarządzaniem dostępem uprzywilejowanym
- Ograniczeniem złośliwego oprogramowania i zagrożeń

- Analizą aktywności za pomocą zaawansowanego audytu i analizy dzienników
- Wdrażaniem i konfiguracją Advanced Threat Analytics i Microsoft Operations Management Suite
- Konfiguracją maszyn wirtualnych w wykorzystaniu Guarded Fabric (VM)
- Wykorzystaniem Security Compliance Toolkit (SCT) i kontenerów do poprawy bezpieczeństwa
- Planowaniem i ochroną danych
- Optymalizacją i zabezpieczaniem usługi plików
- Zabezpieczaniem ruchu sieciowego za pomocą zapór ogniowych i szyfrowania
- Zabezpieczaniem ruchu sieciowego za pomocą DNSSEC i Message Analyzer



Oczekiwane przygotowanie słuchaczy

Uczestnicy powinni mieć co najmniej dwa lata doświadczenia w dziedzinie IT oraz wskazane jest uczestnictwo w kursach 20740, 20741 i 20742 lub równoważna wiedza. Solidne, praktyczne zrozumienie podstaw sieci, w tym TCP / IP, User Datagram Protocol (UDP) i Domain Name System (DNS), solidne, praktyczne zrozumienie zasad usług domenowych w usłudze Active Directory (AD DS), solidne, praktyczne zrozumienie podstaw wirtualizacji Microsoft Hyper-V, zrozumienie zasad bezpieczeństwa systemu 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:

<http://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. Ataki, wykrywanie naruszeń i narzędzia Sysinternals:
 - Zrozumienie ataków
 - Wykrywanie naruszeń bezpieczeństwa
 - Badanie aktywności za pomocą narzędzi Sysinternals.
2. Ochrona poświadczeń i uprzywilejowanego dostępu:
 - Zrozumienie praw użytkownika
 - Konta komputerowe i serwisowe
 - Ochrona poświadczeń
 - Stacje robocze z dostępem uprzywilejowanym i serwery przesiadkowe
 - Rozwiązania dla hasła administratora lokalnego.
3. Ograniczanie uprawnień administratora za pomocą Just Enough Administration:
 - Zrozumienie JEA
 - Weryfikowanie i wdrażanie JEA.
4. Uprzywilejowane zarządzanie dostępem i lasy administracyjne:
 - Lasy ESAE
 - Omówienie programu Microsoft Identity Manager
 - Przegląd administracji JIT i PAM.
5. Łagodzenie złośliwego oprogramowania i zagrożeń:
 - Konfigurowanie i zarządzanie Windows Defender
 - Oprogramowanie ograniczające
 - Konfigurowanie i korzystanie z funkcji Device Guard.
6. Analiza aktywności za pomocą zaawansowanego audytu i analizy dziennika:
 - Przegląd audytu
 - Zaawansowany audyt
 - Kontrola i rejestrowanie Windows PowerShell.
7. Wdrażanie i konfigurowanie Advanced Threat Analytics i Microsoft Operations Management Suite:
 - Wdrażanie i konfigurowanie usługi ATA
 - Wdrażanie i konfigurowanie pakietu Microsoft Operations Management Suite

- Wdrażanie i konfigurowanie Azure Security Center.
8. Bezpieczna infrastruktura wirtualizacji:
- Guarded fabric
 - Maszyny wirtualne ekranowane i obsługiwane przez szyfrowanie.
9. Zabezpieczanie rozwoju aplikacji i infrastruktury obciążenia serwera:
- Korzystanie z SCT
 - Zrozumienie kontenerów.
10. Planowanie i ochrona danych
- Planowanie i wdrażanie szyfrowania
 - Planowanie i wdrażanie funkcji BitLocker
 - Ochrona danych za pomocą usługi Azure Information Protection.
11. Optymalizacja i zabezpieczenie usług plików:
- Menedżer zasobów serwera plików
 - Realizacja zadań związanych z klasyfikacją i zarządzaniem plikami
 - Dynamiczna kontrola dostępu.
12. Zabezpieczanie ruchu sieciowego za pomocą zapór ogniowych i szyfrowania:
- Zrozumienie zagrożeń bezpieczeństwa związanych z siecią
 - Zrozumienie Zapory systemu Windows z zaawansowanymi zabezpieczeniami
 - Konfigurowanie IPsec
 - Zapora centrum danych.
13. Zabezpieczanie ruchu sieciowego:
- Konfigurowanie zaawansowanych ustawień DNS
 - Badanie ruchu sieciowego za pomocą Analizatora wiadomości
 - Zabezpieczanie i analiza ruchu SMB.