kod szkolenia: MS-500 / PL DL 4d

Microsoft 365 Security Administrator

Szkolenie zostaje wycofane przez firmę Microsoft z dniem 30.06.2023 Autoryzowane szkolenie Microsoft 365 Security Administrator **MS-500** kurs w formule **Distance Learning.** Docelowa grupa odbiorców:

- **Administrator**
- **Administrator IT**
- **Specjalista Bezpieczeństwa IT**

Zobacz film: https://youtu.be/3XFvR5s_BbY

Przeznaczenie szkolenia

Szkolenie skierowane do osób zajmujących następujące stanowiska w organizacji:

- Administrator
- Administrator IT
- Specjalista Bezpieczeństwa IT

Cel kursu:

- Zapoznanie się z podstawami bezpieczeństwa platformy Microsoft 365.

Szkolenie skierowane do:
osób posiadających już pewne doświadczenie w zakresie zarządzania usługą **Microsoft 365**, którzy odpowiadają za zabezpieczanie środowiska korporacyjnego Microsoft. W szczególności szkolenie jest dedykowane dla **administratorów bezpieczeństwa Microsoft 365** odpowiedzialnych za aktywnie zabezpieczanie środowiska korporacyjnego Microsoft 365 i którzy współpracują z **administratorem Microsoft 365 Enterprise**, interesariuszami biznesowymi i innymi administratorami obciążeń, aby

planować i wdrażać strategie zabezpieczeń oraz zapewnić zgodność rozwiązań z zasadami i przepisami organizacji. Obowiązki obejmują reagowanie na zagrożenia, wdrażanie, zarządzanie i monitorowanie rozwiązań w zakresie bezpieczeństwa i zgodności dla środowiska Microsoft 365, reagowanie na incydenty, dochodzenia i egzekwowanie zarządzania danymi. **Administrator Microsoft 365 Security** zna się na obciążeniach Microsoft 365 i środowiskach hybrydowych. Ta rola ma duże umiejętności i doświadczenie w zakresie ochrony tożsamości, ochrony informacji, ochrony przed zagrożeniami, zarządzania bezpieczeństwem i zarządzania danymi.

Korzyści wynikające z ukończenia szkolenia

Uzyskanie wiedzy i praktycznych umiejętności w zakresie zarządzania bezpieczeństwem na platformie Microsoft 365. W tym zapoznanie się z:

- Administracją dostępem użytkowników i grup na platformie **Microsoft 365**.
- Zarządzaniem usługą **Azure Identity Protection**.
- Planowaniem i implementacją **Azure AD Connect**.
- Wykorzystaniem dostępu warunkowego.
- Wektorami zagrożeń związanymi z **atakami cybernetycznymi**.
- Rozwiązaniami zabezpieczającymi dla platformy Microsoft 365.
- Wykorzystaniem **Microsoft Secure Score** do oceny i poprawy stanu bezpieczeństwa.
- Konfiguracją różnych zaawansowanych usług ochrony przed zagrożeniami dla platformy Microsoft 365.
- Planowaniem i wdrażaniem bezpiecznych urządzeń mobilnych.
- Wdrażaniem zarządzania prawami do informacji.
- Bezpieczeństwem wiadomości w Office 365.
- Konfigurowaniem zasady zapobiegania utracie danych.
- Wdrażaniem i zarządzaniem **Cloud App Security**.
- Implementacją ochrony informacji systemu **Windows** dla urządzeń.
- Planowaniem i wdrażaniem **systemu archiwizacji i przechowywania danych.**
- Tworzeniem i zarządzaniem dochodzeniami dotyczącymi zbierania **elektronicznych materiałów dowodowych**.
- Zarządzaniem żądaniami podmiotów danych **RODO**.
- Wykorzystaniem etykiet wrażliwości.

Metoda egzaminowania

Egzamin w formie **on-line**. Zapis na stronie https://home.pearsonvue.com/Clients/Microsoft.aspx

Opis egzaminu

Po kursie **MS-500** można przystąpić do certyfikowanego egzaminu **Microsoft**.Szczegóły na:
https://docs.microsoft.com/en-us/learn/certifications/exams/ms-500
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4PsHt

Oczekiwane przygotowanie słuchaczy

Przed przystąpieniem do tego kursu studenci muszą posiadać wiedzę w zakresie:

- Podstawowe zrozumienie pojęciowe platformy Microsoft Azure.
- Doświadczenie z urządzeniami z systemem Windows 10.
- Doświadczenie z Office 365.
- Podstawowe rozumienie autoryzacji i uwierzytelniania.
- Podstawowa znajomość sieci komputerowych.
- Praktyczna wiedza z zakresu zarządzania urządzeniami mobilnymi
- 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

* **podręcznik** w formie elektronicznej dostępny na platformie: https://learn.microsoft.com/pl-pl/training/
* dostęp do portalu słuchacza Altkom Akademii

Metoda szkolenia:

- Wykład
- Demonstracja
- Laboratoria

Ilość teorii do praktyki:

- 50% teoria
- 50% praktyka

Czas trwania

4 dni / 28 godzin

Agenda szkolenia

1. Zarządzanie użytkownikami i grupami.
   - Koncepcje zarządzania tożsamością i dostępem
   - **Model Zero Trust**
   - Planowanie rozwiązań dotyczących tożsamości i uwierzytelniania
   - Konta użytkowników i role
   - Zarządzanie hasłami.
2. Synchronizacja i ochrona tożsamości.
   - Planowanie synchronizacji katalogów
   - Konfiguracja i zarządzanie zsynchronizowanymi tożsamościami
   - Ochrona tożsamości w usłudze **Azure AD**.
3. Zarządzanie tożsamością i dostępem.
   - Zarządzanie aplikacją
   - Zarządzanie tożsamością
   - Zarządzanie dostępem do urządzenia
   - Kontrola dostępu oparta na rolach (**RBAC**)

- Rozwiązania dla dostępu z zewnątrz
- Uprzywilejowane zarządzanie tożsamością.

4. Bezpieczeństwo w Microsoft 365.
   - Wektory zagrożeń i naruszenia bezpieczeństwa danych
   - Strategia i zasady bezpieczeństwa
   - Rozwiązania zabezpieczające firmy Microsoft
   - Bezpieczny wynik.
   - Ochrona przed zagrożeniami.
5. Ochrona online programu **Exchange** (EOP)
   - **Microsoft Defender** dla Office 365
   - Zarządzanie bezpiecznymi załącznikami
   - Zarządzanie bezpiecznymi linkami
   - Microsoft Defender dla tożsamości
   - Microsoft Defender dla punktów końcowych.
6. Zarządzanie zagrożeniami.
   - Pulpit bezpieczeństwa
   - Badanie zagrożeń i reakcja
   - **Azure Sentinel**
   - Zaawansowana analiza zagrożeń.
7. Bezpieczeństwo aplikacji w chmurze firmy Microsoft.
   - Wdrażanie zabezpieczeń aplikacji w chmurze
   - Wykorzystanie informacji o bezpieczeństwie aplikacji w chmurze.
8. Mobilność
   - Zarządzanie aplikacjami mobilnymi (**MAM**)
   - Zarządzanie urządzeniami mobilnymi (**MDM**)
   - Wdrażanie usługi urządzeń mobilnych
   - Rejestracja urządzenia w zarządzaniu urządzeniami mobilnymi.
9. Ochrona i zarządzanie informacjami.
   - Koncepcje ochrony informacji
   - Zarządzanie i zarządzanie dokumentacją
   - **Etykiety wrażliwości**
   - **Archiwizacja** w Microsoft 365
   - **Retencja** w Microsoft 365
   - Zasady przechowywania w Centrum zgodności Microsoft 365
   - Archiwizacja i przechowywanie w **Exchange**
   - Zarządzanie rekordami w miejscu w **SharePoint.**
10. Zarządzanie prawami i szyfrowanie.
    - Zarządzanie prawami do informacji (IRM)
    - Bezpieczne uniwersalne rozszerzenie poczty internetowej (S-MIME)
    - Szyfrowanie wiadomości Office 365.

11. Zapobieganie utracie danych.
    - Podstawy zapobiegania utracie danych
    - Tworzenie zasady **DLP**
    - Dostosowanie zasady DLP
    - Tworzenie zasady DLP do ochrony dokumentów
    - Wskazówki dotyczące polityki.
12. Zarządzanie zgodnością.
    - Centrum zgodności.
13. Zarządzanie ryzykiem wewnętrznym.
    - Ryzyko wewnętrzne
    - Uprzywilejowany dostęp
    - Bariery informacyjne
    - Budowanie murów etycznych w **Exchange Online**.
14. Prowadzenie poszukiwań i dochodzeń.
    - Wyszukiwanie treści
    - Dziennik audytu dochodzenia
    - Zaawansowane **eDiscovery.**