

Enhance endpoint security with Microsoft Intune and Microsoft Security Copilot

Bezpieczeństwo punktów końcowych wymaga dziś nie tylko właściwej konfiguracji urządzeń i aplikacji, ale także szybkiego dostępu do danych, podpowiedzi i analiz wspierających reakcję na zagrożenia. Szkolenie pokazuje, jak wykorzystać Microsoft Intune oraz Microsoft Security Copilot do wzmacniania ochrony urządzeń, zarządzania aplikacjami, pracy z danymi Intune oraz optymalizacji integracji między obiema usługami. Uczestnicy poznają podstawy Intune, możliwości Security Copilot, prompty, promptbooki, nowe funkcje oraz przykłady zastosowania Copilot w zadaniach związanych z bezpieczeństwem endpointów.



Odbiorcy szkolenia

Szkolenie jest przeznaczone dla osób odpowiedzialnych za bezpieczeństwo punktów końcowych, zarządzanie urządzeniami i aplikacjami oraz wykorzystanie Microsoft Intune i Microsoft Security Copilot w codziennej pracy administracyjnej lub bezpieczeństwa.

W szczególności kurs sprawdzi się dla:

- administratorów odpowiedzialnych za zarządzanie urządzeniami i aplikacjami w Microsoft Intune,
- administratorów, którzy chcą poznać możliwości wykorzystania Microsoft Security Copilot w pracy z danymi Intune,
- inżynierów bezpieczeństwa zajmujących się ochroną punktów końcowych,
- specjalistów odpowiedzialnych za integrację bezpieczeństwa i zgodności w środowisku urządzeń organizacji,
- osób pracujących z Microsoft Intune, które chcą lepiej przygotować środowisko do integracji z Microsoft Security Copilot,
- specjalistów IT chcących praktycznie korzystać z promptów, promptbooków i nowych funkcji Microsoft

Security Copilot.



Korzyści

- Podstawy Microsoft Intune – poznasz kluczowe funkcje Intune oraz możliwości zarządzania urządzeniami w środowisku organizacji.
- Zarządzanie aplikacjami – nauczysz się, jak skutecznie zabezpieczać aplikacje i zarządzać nimi z wykorzystaniem Microsoft Intune.
- Bezpieczeństwo i zgodność – dowiesz się, jak integrować mechanizmy bezpieczeństwa i zgodności w strategii zarządzania urządzeniami.
- Microsoft Security Copilot – poznasz, jak działa Security Copilot i jak może wspierać działania związane ze zwiększaniem bezpieczeństwa.
- Praca z promptami i promptbookami – nauczysz się wykorzystywać prompty oraz promptbooki w Microsoft Security Copilot.
- Integracja Intune z Security Copilot – dowiesz się, jak połączyć Microsoft Intune z Microsoft Security Copilot i wykorzystać dane Intune w pracy z Copilot.
- Optymalizacja środowiska Intune – poznasz, jak stosować konwencje nazewnictwa, zarządzać nazwami urządzeń oraz organizować użytkowników i urządzenia za pomocą grup.



Program szkolenia

1. Poznanie podstaw Microsoft Intune:

- Przegląd podstawowych funkcji Microsoft Intune.
- Omówienie możliwości zarządzania urządzeniami.
- Skuteczne zabezpieczanie aplikacji i zarządzanie nimi.
- Integracja bezpieczeństwa i zgodności.
- Optymalizacja strategii wdrożenia z wykorzystaniem Microsoft Intune.

2. Odkrywanie insightów z Microsoft Security Copilot:

- Przegląd Microsoft Security Copilot.
- Omówienie sposobu działania Microsoft Security Copilot.
- Poznanie doświadczeń Microsoft Security Copilot.
- Wdrożenie Microsoft Security Copilot w celu zwiększenia bezpieczeństwa.
- Wykorzystanie promptów w Microsoft Security Copilot.
- Włączanie promptbooków do Microsoft Security Copilot.
- Przegląd nowych funkcji Microsoft Security Copilot.

3. Optymalizacja Microsoft Intune pod kątem integracji z Microsoft Security Copilot:

- Omówienie zalet połączenia Microsoft Security Copilot i Microsoft Intune.

- Wprowadzanie silnych konwencji nazewnictwa.
- Zmiana nazwy urządzenia w Microsoft Intune.
- Dodawanie grup w Microsoft Intune w celu organizacji użytkowników i urządzeń.
- Omówienie uwierzytelniania w Microsoft Security Copilot.
- Integracja Microsoft Security Copilot z Microsoft Intune.
- Wykorzystanie funkcji promptingu w Microsoft Security Copilot.
- Przegląd przykładowych promptów dla Microsoft Intune.



Oczekiwane przygotowanie uczestnika

- Podstawowa wiedza o zasadach bezpieczeństwa IT.
- Znajomość Microsoft Intune.
- Doświadczenie w zarządzaniu urządzeniami w środowisku korporacyjnym.
- Znajomość Microsoft Entra ID.

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/jak-dzialamy/o-szkoleniach/?distance-learning>



Szkolenie obejmuje

- * materiały w formie elektronicznej dostępne na platformie: <https://learn.microsoft.com/pl-pl/training/>
- * dostęp do portalu słuchacza Altkom Akademii

Metoda szkolenia:

- Wykład i prezentacja produktu (50%)
- Ćwiczenia (50%)

Główne narzędzia dydaktyczne obejmują prezentacje PowerPoint, demonstracje na środowisku testowym, praktyczne środowiska laboratoryjne i zasoby Microsoft Learn



Czas trwania

1 dni / 7 godzin

Język

- Wykład: polski
- Materiały: angielski