Szkolenie autoryzowane

MS 102T00 Microsoft 365 Administrator

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

Szkolenie obejmuje takie kluczowe elementy, jak: administracja Microsoft 365: Zarządzanie dzierżawą Microsoft 365, Synchronizacja tożsamości Microsoft 365 oraz Bezpieczeństwo i zgodność Microsoft 365.

W ramach zarządzania dzierżawą Microsoft 365 dowiesz się, jak skonfigurować dzierżawę Microsoft 365, w tym profil organizacyjny, opcje subskrypcji dzierżawy, usługi składowe, konta użytkowników i licencje, grupy zabezpieczeń oraz role administracyjne. Następnie przejdziesz do konfigurowania platformy Microsoft 365, koncentrując się głównie na konfigurowaniu łączności klienta pakietu Office. Na koniec zbadasz, jak zarządzać instalacjami klienckimi Microsoft 365 Apps opartymi na użytkownikach dla wdrożeń korporacyjnych.

Następnie kurs przechodzi do dogłębnej analizy synchronizacji tożsamości Microsoft 365, ze szczególnym uwzględnieniem Azure Active Directory Connect i Connect Cloud Sync. Dowiesz się, jak zaplanować i wdrożyć każdą z tych opcji synchronizacji katalogów, jak zarządzać zsynchronizowanymi tożsamościami oraz jak wdrożyć zarządzanie hasłami w Microsoft 365 przy użyciu uwierzytelniania wieloskładnikowego i samoobsługowego zarządzania hasłami.

W ramach zarządzania bezpieczeństwem platformy Microsoft 365 rozpoczniesz analizę typowych rodzajów wektorów zagrożeń i naruszeń danych, z którymi borykają się obecnie organizacje. Następnie dowiesz się, w jaki sposób rozwiązania bezpieczeństwa platformy

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Microsoft 365 radzą sobie z każdym z tych zagrożeń. Zostaniesz wprowadzony do Microsoft Secure Score, a także do Azure Active Directory Identity Protection. Następnie dowiesz się, jak zarządzać usługami bezpieczeństwa Microsoft 365, w tym Exchange Online Protection, Safe Attachments i Safe Links. Na koniec zapoznasz się z różnymi raportami, które monitorują stan bezpieczeństwa organizacji. Następnie przejdziesz od usług bezpieczeństwa do analizy zagrożeń; w szczególności przy użyciu Microsoft 365 Defender, Microsoft Defender for Cloud Apps i Microsoft Defender for Endpoint.

Po zapoznaniu się z pakietem zabezpieczeń platformy Microsoft 365 należy następnie przeanalizować kluczowe składniki zarządzania zgodnością platformy Microsoft 365. Rozpoczyna się to od przeglądu wszystkich kluczowych aspektów zarządzania danymi, w tym archiwizacji i przechowywania danych, szyfrowania wiadomości Microsoft Purview i zapobiegania utracie danych (DLP). Następnie zagłębiamy się w archiwizację i przechowywanie danych, zwracając szczególną uwagę na zarządzanie ryzykiem wewnętrznym Microsoft Purview, bariery informacyjne i zasady DLP. Następnie zbadano, jak wdrożyć te funkcje zgodności przy użyciu klasyfikacji danych i etykiet wrażliwości.

Szkolenie przeznaczone jest dla osób aspirujących do roli administratora Microsoft 365, które ukończyły co najmniej jedną ze ścieżek certyfikacji administratorów opartych na rolach Microsoft 365.

Szkolenie prowadzone jest w języku polskim, materiały są w języku angielskim.

Korzyści

Po ukończeniu szkolenia uczestnik będzie wiedział jak:

- w sposób praktyczny zarządzać platformą Microsoft 365
- projektować, konfigurować i zarządzać dzierżawą platformy Microsoft 365
- funkcjonuje produkt Microsoft 365
- konfigurować Microsoft 365
- zarządzać aplikacjami Microsoft 365 do wdrożeń w przedsiębiorstwach
- planować i wdrażać synchronizację tożsamości
- zarządzać archiwizacją i retencją danych
- etykietować dane
- zarządzać ryzykiem i mechanizmami zapobiegania wypływu informacji
- zarządzać mechanizmami zabezpieczeń

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Wymagania

Przed przystąpieniem do tego szkolenia, uczestnicy muszą posiadać:

- podstawowe doświadczenie w pracy z usługami Microsoft 365
- biegłą znajomość DNS
- biegłą znajomość PowerShell

Harmonogram szkolenia

Moduł 1: Konfiguracja środowiska Microsoft 365

- Konfiguracja profilu organizacji firmy
- Zarządzanie subskrypcjami dzierżawców na platformie Microsoft 365
- Integracja platformy Microsoft 365 z aplikacjami angażującymi klientów

Moduł 2: Zarządzanie użytkownikami, kontaktami i licencjami na platformie Microsoft 365

- Określanie modelu tożsamości użytkownika
- Tworzenie kont użytkowników w Microsoft 365
- Zarządzanie kontami użytkowników i licencjami na platformie Microsoft 365
- Odzyskiwanie usuniętych kont użytkowników w Microsoft 365
- Wykonywanie zbiorczej konserwacji użytkowników w Azure Active Directory
- Tworzenie użytkowników-gości i zarządzanie nimi
- Tworzenie kontaktów pocztowych i zarządzanie nimi

Moduł 3: Tworzenie i zarządzanie grupami na platformie Microsoft 365

- Typy grup dostępnych na platformie Microsoft 365
- Tworzenie grup i zarządzanie za pomocą centrum administracyjnego Microsoft 365 i PowerShell
- Tworzenie grup i zarządzanie nimi w Exchange Online i SharePoint Online

Moduł 4: Dodawanie domeny niestandardowej Microsoft 365

- Weryfikacja czynników, które należy brać pod uwagę przy dodawaniu domeny
- Planowanie stref DNS używanych w domenie niestandardowej
- Planowanie wymagań dotyczących rekordów DNS dla domeny niestandardowej
- Dodawanie domeny niestandardowej do wdrożenia platformy Microsoft 365

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Moduł 5: Konfiguracja łączności klienta z Microsoft 365

- Używanie automatycznego wykrywania do łączenia klienta programu MS Outlook z usługą Exchange Online
- Identyfikacja rekordów DNS potrzebnych programowi Outlook i innym klientom związanym z pakietem Office do automatycznego lokalizowania usług na platformie Microsoft 365 przy użyciu procesu automatycznego wykrywania.
- Protokoły łączności, które pozwalają programowi Outlook na łączenie się usługą Microsoft 365
- Identyfikacja narzędzi, które mogą pomóc w rozwiązaniu problemów z łącznością we wdrożeniach platformy Microsoft 365

Moduł 6: Konfiguracja roli administratora w Microsoft 365

- Model uprawnień platformy Microsoft 365
- Role administratora platformy Microsoft 365
- Przypisywanie ról administratora do użytkowników w Microsoft 365
- Delegowanie ról administracyjnych partnerom
- Zarządzanie uprawnieniami przy użyciu jednostek administracyjnych w usłudze Azure Active Directory
- Zwiększanie uprawnień przy wykorzystaniu z usługi Azure AD Privileged Identity Management
- Najlepsze praktyki podczas konfigurowania ról administracyjnych

Moduł 7: Zarządzanie kondycją i usługami dzierżawców na platformie Microsoft 365

- Monitorowanie kondycji usług w Microsoft 365
- Monitorowanie stanu dzierżawców za pomocą Microsoft 365 Adoption Score
- Monitorowanie stanu dzierżawców za pomocą Microsoft 365 Usage Analytics
- Opracowywanie planu reagowania na incydenty
- Zapytania o asystę Microsoft

Moduł 8:

- Wdrażanie Microsoft 365 Apps dla przedsiębiorstwa
- Funkcje Microsoft 365 Apps dla przedsiębiorstw
- Sprawdzanie zgodności aplikacji przy wykorzystaniu Readiness Toolkit
- Samoobsługowa instalacja Microsoft 365 Apps dla przedsiębiorstw
- Wdrażanie Microsoft 365 Apps za pomocą Microsoft Configuration Manager
- Wdrażanie Microsoft 365 Apps z chmury
- Wdrażanie Microsoft 365 Apps z lokalnego źródła
- Zarządzaj aktualizacjami Microsoft 365 Apps
- Zarządzanie aplikacjami w chmurze za pomocą centrum administracyjnego Microsoft 365 Apps

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Moduł 9: Analiza środowiska pracy Microsoft 365 za pomocą Microsoft Viva Insights

- Funkcje analityczne Microsoft Viva Insights
- Statystyki zespołu i organizacji

Moduł 10: Synchronizacja tożsamości

- Modele tożsamości dla platformy Microsoft 365
- Opcje uwierzytelniania dla hybrydowego modelu tożsamości
- Przeglądanie synchronizacji katalogów

Moduł 11: Przygotowanie do synchronizacji tożsamości z Microsoft 365

- Planowanie wdrożenia usługi Azure Active Directory
- Przygotowanie się do synchronizacji katalogów
- Wybór narzędzi do synchronizacji katalogów
- Planowanie synchronizacji katalogów przy użyciu Azure AD Connect
- Planowanie synchronizacji katalogów przy użyciu usługi Azure AD Connect Cloud Sync

Moduł 12: Implementacja narzędzi do synchronizacji katalogów

- Konfiguracja wstępnych wymagań Azure AD Connect
- Monitorowanie usługi synchronizacji przy użyciu usługi Azure AD Connect Health
- Konfigurowanie wstępnych wymagań usługi Azure AD Connect Cloud Sync
- Konfiguracja synchronizacji w chmurze Azure AD Connect
-

Moduł 13: Zarządzanie zsynchronizowanymi tożsamościami

- Zarządzanie użytkownikami i grupami za pomocą synchronizacji katalogów
- Korzystanie z Azure AD Connect Sync Security Groups w celu utrzymania synchronizacji katalogów
- Konfiguracja filtrów obiektów do synchronizacji katalogów
- Microsoft Identity Manager
- Rozwiązywanie problemów z synchronizacją katalogów

Moduł 14: Zarządzanie bezpiecznym dostępem użytkowników w Microsoft 365

- Zarządzanie hasłami użytkowników
- Uwierzytelnianie z przekazywaniem i uwierzytelnianie wieloskładnikowe
- Logowania bez hasła za pomocą Microsoft Authenticator
- Samoobsługowe zarządzanie hasłami

- Windows Hello dla firm
- Wdrożenie Azure AD Smart Lockout
- Wdrożenie zasady dostępu warunkowego
- Poznaj ustawienia domyślne zabezpieczeń w usłudze Azure AD
- Badanie problemów z uwierzytelnianiem przy użyciu dzienników logowania

Moduł 15: Analizowanie wektorów zagrożeń i naruszeń bezpieczeństwa danych

- Omówienie metody Phishingu
- Porównanie spamu i złośliwego oprogramowania
- Sprawdzanie naruszeń konta
- Rodzaje ataków i ich analiza

Moduł 16: Model bezpieczeństwa Zero Trust

- Zasady i elementy modelu Zero Trust
- Planowanie modelu bezpieczeństwa Zero Trust w organizacji
- Strategia firmy Microsoft dotycząca Zero Trust

Moduł 17: Zabezpieczenia w usłudze Microsoft 365 Defender

- Zwiększanie bezpieczeństwa poczty e-mail przy wykorzystaniu usługi Exchange Online Protection i usługi Microsoft Defender dla usługi Office 365
- Ochrona tożsamości organizacji za pomocą usługi Microsoft Defender for Identity
- Ochrona sieci firmowej przed zaawansowanymi zagrożeniami, przy wykorzystaniu Microsoft Defender for Endpoint
- Ochrona przed cyberatakami - usługa Microsoft 365 Threat Intelligence
- Korzystanie z Microsoft Cloud App Security
- Analiza raportów zabezpieczeń w usłudze Microsoft 365 Defender

Moduł 18: Microsoft Secure Score

- Omówienie narzędzia Microsoft Secure Score

Moduł 19: Uprzywilejowane zarządzanie tożsamościami

- Wstęp do Privileged Identity Management w usłudze Azure AD
- Konfigurowanie Privileged Identity Management
- Audyt Privileged Identity Management
- Kontrola zadań administratora za pomocą Privileged Identity Management dostępem
-

Moduł 20: Omówenie usługi Azure Identity Protection

- Omówienie usługi Azure Identity Protection
- Zapoznanie się z lukami w zabezpieczeniach i zdarzeniami ryzyka wykrytymi przez usługę Azure Identity Protection

Moduł 21: Ochrona Exchange Online

- Sprawdzanie potoku ochrony przed złośliwym oprogramowaniem
- Wykrywanie wiadomości ze spamem lub złośliwym oprogramowaniem za pomocą funkcji automatycznego przeczyszczanie o zerowej godzinie (ZAP)
- Ochrona za pomocą usługi Exchange Online Protection
- Inne zabezpieczenia anti-spoofing
- Filtrowanie spamu wychodzącego

Moduł 22: Omówienie usługi Microsoft Defender for Office 365

- Korzystanie z Safe Attachments oraz Safe Links
- Konfigurowanie zasad filtrowania spamu wychodzącego

Moduł 23: Zarządzanie Safe Attachments i Safe Links w Microsoft 365

Moduł 24: Analiza zagrożeń w usłudze Microsoft 365 Defender

- Microsoft Intelligent Security Graph
- Zasady alertów na platformie Microsoft 365
- Wykrywanie zagrożeń za pomocą usługi Microsoft Threat Protection
- Zaawansowane wykrywanie zagrożeń w usłudze Microsoft 365 Defender
- Identyfikacja zagrożeń za pomocą raportów usługi Microsoft Defender

Moduł 25: Omówienie ochrony aplikacji za pomocą usługi Microsoft Defender Cloud Apps

- Wstęp do usługi Microsoft Defender Cloud Apps
- Wdrażanie usługi Microsoft Defender Cloud Apps
- Konfiguracja zasad dotyczących plików w Microsoft Defender Cloud Apps
- Zarządzanie alertami w Microsoft Defender Cloud Apps
- Konfigurowanie i rozwiązywanie problemów z Cloud Discovery w Microsoft Defender Cloud Apps

Moduł 26: Omówienie ochrony punktów końcowych za pomocą usługi Microsoft Defender for Endpoint

- Wstęp do usługi Microsoft Defender for Endpoint
- Konfigurowanie Microsoft Defender for Endpoint w usłudze Microsoft Intune
- Zarządzanie lukami w zabezpieczeniach punktów końcowych za pomocą usługi Microsoft

Defender Vulnerability Management

Moduł 27: Wdrożenie ochrony przed zagrożeniami za pomocą usługi Microsoft Defender for Office 365

- Wykrywanie ataków za pomocą narzędzia Threat Explorer
- Identyfikacja problemów z cyberbezpieczeństwem za pomocą Threat Trackers
- Symulacja ataku

Moduł 28: Zarządzania danymi w Microsoft Purview

- Zarządzanie danymi i zgodność w Microsoft Purview
- Ochrona poufnych danych za pomocą rozwiązania Microsoft Purview Information Protection
- Zarządzanie danymi organizacji za pomocą rozwiązania Microsoft Purview Data Lifecycle Management
- Minimalizacja ryzyka wewnętrznego dzięki Microsoft Purview Insider Risk Management
- Microsoft Purview eDiscovery

Moduł 29: Archiwizacja i zarządzanie rekordami na platformie Microsoft 365

- Dostęp do archiwalnych skrzynek pocztowych na platformie Microsoft 365
- Zarządzanie rekordami Microsoft Purview
- Przywracanie usuniętych danych w Exchange Online oraz w SharePoint Online

Moduł 30: Przechowywanie na platformie Microsoft 365

- Zasady i etykiety przechowywania
- Definiowanie zakresu zasad przechowywania
- Ograniczanie zmian przechowywania za pomocą Preservation Lock
- Szyfrowanie wiadomości Microsoft Purview

Moduł 31: Konfiguracja szyfrowania wiadomości Microsoft Purview

- Definiowanie reguł przepływu poczty, aby zaszyfrować wiadomości e-mail
- Zaawansowane szyfrowanie wiadomości Microsoft Purview

Moduł 32: Badanie zgodności na platformie Microsoft 365

- Planowanie zabezpieczenia i zgodności na platformie Microsoft 365
- Zarządzaj wymaganiami dotyczącymi zgodności z Compliance Manager
- Pulpit nawigacyjny Compliance Manager

Moduł 33: Wdrożenie Microsoft Purview Insider Risk Management

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

- Zarządzanie ryzykiem wewnętrznym
- Działania i alerty związane z zarządzaniem ryzykiem wewnętrznym
- Przypadki zarządzania ryzykiem wewnętrznym

Moduł 34: Wdrażanie barier informacyjnych Microsoft Purview

- Omówienie barier informacyjnych Microsoft Purview
- Konfiguracja barier informacyjne w Microsoft Purview
- Omówienie barier informacyjnych w Microsoft Teams, w usłudze OneDrive oraz w SharePoint
- Microsoft Purview Data Loss Prevention

Moduł 35: Zapobieganie utracie danych punktu końcowego

- Zasady DLP
- Analiza raportów DLP

Moduł 36: Wdrożanie Microsoft Purview Data Loss Prevention

- Planowanie wdrożenia Microsoft Purview Data Loss Prevention
- Implementacja domyślnych zasad DLP Microsoft Purview
- Projektowanie niestandardowej polityki DLP
- Tworzenie niestandardowych zasad DLP z szablonu
- Konfigurowanie powiadomienia e-mail dotyczące zasad DLP

Moduł 37: Wdrożenie klasyfikacji danych o informacjach wrażliwych

- Wdrożenie klasyfikacji danych w Microsoft 365
- Tworzenie i testowanie klasyfikatora
- Przeglądanie poufnych danych za pomocą Eksploratora treści i Eksploratora aktywności
- Wykrywanie dokumentów zawierających poufne informacje za pomocą Document Fingerprinting
- Przeglądanie i wdrażanie etykiet wrażliwości

Moduł 38: Zarządzanie ochroną danych za pomocą etykiet wrażliwości

- Określanie zakresu etykiet wrażliwości
- Automatycznie stosowanie etykiet wrażliwości
- Zasady etykiet wrażliwości

Moduł 39: Planowanie strategii wdrażania etykiet wrażliwości

- Tworzenie i publikowanie etykiet wrażliwości
- Usuwanie etykiet wrażliwości

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Tagi:

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.