Szkolenie: Microsoft
MS-500T00 Microsoft 365 Security Administration

Gold Microsoft Partner

Cel szkolenia:

Podczas tego szkolenia, uczestnik nauczy się jak zabezpieczać dostęp użytkownika do zasobów firmowych. Szkolenie pokryje ochronę hasła użytkownika, wielo-czynnikowe uwierzytelnienie, jak włączyć Azure Identity Protection, jak ustawić i używać Azure AD Connect, oraz dostęp warunkowy w Microsoft 365. Uczestnik dowie się o technologiach bezpieczeństwa, które pomagają chronić środowisko Microsoft 365. W szczególności, uczestnik pozna wektory zagrożeń i rozwiązania bezpieczeństwa Microsoft 365 do zminimalizowania zagrożeń. Dowie się o Secure Score, ochronie Exchange Online , Azure Advanced Threat Protection, Microsoft Defender Advanced Threat Protection i zarządzaniu zagrożeniami. Szkolenie nauczy uczestnika na temat technologii ochrony informacji, które pomagają zabezpieczać środowisko Microsoft 365. Szkolenie omówi zarządzanie prawami do informacji, szyfrowanie wiadomości, jak i również etykiety, politykę i zasady wspierające zapobieganie utracie danych i ochronę informacji. Na koniec, uczestnik nauczy się o archiwizacji i utrzymywaniu danych w Microsoft 365, jak i zarządzaniu danymi i o tym jak przeprowadzać wyszukiwanie zawartości i dochodzenia. Szkolenie pokryje zasady utrzymywania danych i znaczniki, bezpośrednie zarządzanie zapisami w SharePoint, utrzymywaniem maili oraz jak przeprowadzać wyszukiwanie zawartości, które wspiera dochodzenia eDiscovery.

Grupa docelowa:

Administrator bezpieczeństwa Microsoft 365 współpracuje z Microsoft 365 Enterprise Administrator, udziałowcami i innymi administratorami pracy, w celu planowania i wdrażania strategii ochrony oraz do zapewnienia zgodności rozwiązań z poliyką firmy i przepisami prawnymi. Administratorzy bezpieczeństwa Microsoft 365 zabezpieczają środowiska firmowe Microsoft 365. Odpowiedzialności łączą w sobie: Odpowiadanie na zagrożenia, wdrażanie, zarządzanie i monitorowanie rozwiązań bezpieczeństwa i zgodności dla środowiska Microsoft 365. Administratorzy bezpieczeństwa Microsoft 365 odpowiadają na incidenty, dochodzenia i egzekwowanie zarządzania danymi. Są zaznajomieni z pracą w Microsoft 365 i środowiskami hybrydowymi. Ta rola wymaga doświadczenia i umiejętności związanych z ochroną tożsamości, ochroną informacji, ochroną przed zagrożeniami, zarządzaniem bezpieczeństwem i danymi.

Po ukończeniu szkolenia, uczestnik będzie potrafił:

- Administrować dostępem użytkownika i grup w Microsoft 365
- Opisać i zarządzać Azure Identity Protection
- Planować i wdrażać Azure AD Connect
- Zarządzać zsynchronizowanymi tożsamościami użytkowników
- Opisać i stosować dostęp warunkowy

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Opisać wektory zagrożeń cyberataków
- Opisać rozwiązania bezpieczeństwa w Microsoft 365.
- Używać Microsoft Secure Score do ewaluacji i doskonalenia stanu bezpieczeństwa
- Konfigurować różne usługi zaawansowanej ochrony przed zagrożeniami w Microsoft 365
- Planować i wdrażać bezpieczne urządzenia mobilne
- Zarządzać prawami do informacji
- Zabezpieczać wiadomości w Office 365
- Konfigurować zasady zapobiegania utracie danych
- Wdrażać i zarządzać Cloud App Security
- Stosować ochronę informacji Windows w urządzeniach
- Planować i wdrażać archiwizację danych i system utrzymywania danych
- Tworzyć i zarządzać dochodzeniami eDiscovery
- Zarządzać zapytaniami o dane według GDPR
- Opisać i używać etykiet wrażliwości

Plan szkolenia:

- Zarządzanie użytkownikami i grupami
  - Pojęcia zarządzania tożsamością i dostępem
  - Model zerowego zaufania
  - Planowanie tożsamości i rozwiązania uwierzytelnienia
  - Konta użytkownika i role
  - Zarządzanie tożsamością
- Synchronizacja i ochrona tożsamości
  - Planowanie synchronizacji
  - Konfiguracja i zarządzanie zsynchronizowanymi tożsamościami
  - Zarządzanie hasłem
  - Azure AD Identity Protection
- Zarządzanie dostępem
  - Dostęp warunkowy
  - Zarządzanie dostępem urządzeń
  - Kontrola dostępu oparta na rolach (RBAC)
  - Rozwiązania dostępu zewnętrznego
- Bezpieczeństwo w Microsoft 365
  - Wektory zagrożenia i naruszenia ochrony danych
  - Zasady i strategie bezpieczeństwa

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Rozwiązania bezpieczeństwa w Microsoft 365
- Secure Score

- Ochrona przed zagrożeniami
  - Exchange Online Protection (EOP)
  - Office 365 Advanced Threat Protection
  - Zarządzanie bezpiecznymi załącznikami
  - Zarządzanie bezpiecznymi linkami
  - Azure Advanced Threat Protection
  - Microsoft Defender Advanced Threat Protection
- Zarządzanie zagrożeniami
  - Panel bezpieczeństwa
  - Badanie zagrożeń i reagowanie
  - Azure Sentinel
  - Advanced Threat Analytics
- Usługa Cloud Application Security
  - Wdrażanie Cloud Application Security
  - Używanie informacji Cloud Application Security
- Mobilność
  - Zarządzanie aplikacjami mobilnymi (MAM)
  - Zarządzanie urządzeniami mobilnymi (MDM)
  - Wdrażanie usług urządzeń mobilnych
  - Zapisywanie urządzeń w Mobile Device Management
- Ochrona informacji
  - Pojęcia ochrony informacji
  - Etykiety wrażliwości
  - Azure Information Protection (AIP)
  - Windows Information Protection (WIP)
- Zarządzanie prawami i szyfrowanie
  - Zarządzanie prawami do informacji
  - Secure Multipurpose Internet Mail Extension (S/MIME)
  - Szyfrowanie wiadomości w Office 365
- Zapobieganie utracie danych
  - Podstawy zapobiegania utracie danych
  - Tworzenie polityki DLP
  - Dostosowywanie polityki DLP
  - Tworzenie polityki DLP do zabezpieczania dokumentów

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Wskazówki polityki
- Archiwizacja i utrzymywanie danych
  - Archiwizacja danych w Microsoft 365
  - Utrzymywanie danych w Microsoft 365
  - Zasady utrzymywania danych w cetrum zgodności Microsoft 365
  - Archiwizacja i utrzymywanie danych w Exchange
  - Bezpośrednie zarządzanie zapisami w SharePoint
- Wyszukiwanie zawartości i dochodzenia
  - Wyszukiwanie zawartości
  - Badanie zapisów audytowych
  - Zaawansowany eDiscovery
- Zgodność w Microsoft 365
  - Centrum zgodności
  - Rozwiązania centrum zgodności
  - Budowanie etycznych ścian w Exchange Online

Wymagania:

- Podstawową wiedzę na temat pojęć Microsoft Azure
- Doświadczenie z urządzeniami Windows 10
- Doświadczenie z Office 365.
- Podstawową wiedzę na temat uwierzytelnienia i upoważnienia
- Podstawową wiedzę na temat sieci komputerowych
- Wiedzę i doświadczenie na temat zarządzania urządzeniami mobilnymi

Poziom trudności

Certyfikaty:

Uczestnicy kursu **MS-500T00 Microsoft 365 Security Administration** otrzymują **certyfikat** ukończenia autoryzowanego szkolenia **Microsoft**.

Prowadzący:

Microsoft Certified Trainer.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Informacje dodatkowe:

Zajęcia prowadzone są w języku polskim, materiały źródłowe oraz oprogramowanie są w języku angielskim.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001