MS 500T00 Microsoft 365 Security Administration

Czas trwania: 4 dni

Dla kogo:
Szkolenie skierowane do administratorów, inżynierów systemowych odpowiedzialnych za zarządzanie zabezpieczeniem tożsamości i dostępu, ochronę przed zagrożeniami w środowisku Microsoft 365, ochronę informacji oraz za wewnętrzne zasady i zewnętrzne wymagania dotyczące przechowywania danych i prowadzenia dochodzeń.

Wymagania wstępne:
- rozumienie koncepcji platformy Microsoft Azure
- doświadczenie z urządzeniami z systemem Windows 10
- doświadczenie z Office 365
- podstawowe rozumienie autoryzacji i uwierzytelniania
- podstawowe rozumienie sieci komputerowych
- doświadczenie w zarządzaniu urządzeniami mobilnymi

Szkolenie przygotowuje do egzaminu:
MS-500: Microsoft 365 Security Administration

Zakres tematyczny:

1. Użytkownicy i grupy zabezpieczeń
    - pojęcia związane z zarządzaniem tożsamością i dostępem
    - model Zero Trust
    - planowanie rozwiązań dotyczących tożsamości i uwierzytelniania
    - konta i role użytkowników
    - zarządzanie hasłami
2. Synchronizacja tożsamości I ochrona
    - planowanie synchronizacji
    - konfigurowanie i zarządzanie synchronizowanymi tożsamościami
    - Azure AD Identity Protection
3. Zarządzanie tożsamością i dostępem
    - zarządzanie aplikacją
    - zarządzanie dostępem urządzeń
    - kontrola dostępu oparta na rolach (RBAC)
    - rozwiązania dla dostępu zewnętrznego
    - zarządzanie tożsamością uprzywilejowaną
4. Bezpieczeństwo w Microsoft 365
    - wektory zagrożeń i naruszenia bezpieczeństwa danych
    - strategia i zasady bezpieczeństwa
    - rozwiązania bezpieczeństwa dla Microsoft 365
    - Microsoft Secure Score
5. Ochrona przed zagrożeniami
    - ochrona online Exchange
    - Microsoft Defender for Office 365
    - Office 365 Advanced Threat Protection
    - zarządzanie bezpiecznymi załącznikami
    - zarządzanie bezpiecznymi linkami
    - Microsoft Defender for Identity
    - Microsoft Defender for Endpoint
6. Zarządzanie zagrożeniami

- Pulpit bezpieczeństwa
- Badanie zagrożeń i reagowanie
- Azure Sentinel
- Zaawansowana analiza zagrożeń

7. Bezpieczeństwo aplikacji w chmurze
   - wdrażanie zabezpieczenia aplikacji w chmurze
   - wykorzystanie informacji o zabezpieczeniach aplikacji w chmurze
8. Mobilność
   - planowanie zarządzania aplikacjami mobilnymi
   - planowanie zarządzania urządzeniami mobilnymi
   - wdrażanie zarządzania urządzeniami mobilnymi
   - rejestracja urządzeń
9. Ochrona informacji i zarządzanie
   - koncepcje ochrony informacji
   - zarządzanie i zarządzanie dokumentacją
   - etykiety wrażliwości
   - archiwizacja na platformie Microsoft 365
   - przechowywanie na platformie Microsoft 365
   - zasady przechowywania w Centrum zgodności platformy Microsoft 365
   - archiwizacja i przechowywanie w Exchange
   - zarządzanie in-place w SharePoint
10. Zarządzanie prawami i szyfrowanie
    - Information Rights Management (IRM)
    - Secure Multipurpose Internet Mail Extension (S-MIME)
    - szyfrowanie wiadomości w Office 365
11. Ochrona przed utratą danych
    - objaśnienie zapobiegania utracie danych
    - zasady zapobiegania utracie danych
    - niestandardowe zasady DLP
    - tworzenie zasady DLP do ochrony dokumentów
    - wskazówki dotyczące zasad
12. Zarządzanie zgodnością
    - centrum zarządzania godnością
13. Zarządzanie ryzykiem wewnętrznym
    - ryzyko wewnętrzne
    - dostęp uprzywilejowany
    - bariery informacyjne
    - budowanie murów etycznych w Exchange Online
14. Wykrywanie i odpowiadanie
    - wyszukiwanie zawartości
    - Audit Log Investigations
    - zaawansowane eDiscovery

Polecane szkolenia uzupełniające:

- MS 100 Microsoft 365 Identity and Services
- MS 101 Microsoft 365 Mobility and Security
- MS 300 Deploying Microsoft 365 Teamwork
- MS 301 Deploying SharePoint Server Hybrid
- MS 10961 Automating Administration with Windows PowerShell