

kod szkolenia: SC-500 / PL AA 4d

Implement end to end security controls for cloud and AI workloads

Kurs w formie stacjonarnej.

Szkolenie SC-500 zastąpiło wygaszone szkolenie AZ-500.

Ten kurs przygotowuje Cię do projektowania, wdrażania i zarządzania kompleksową kontrolą bezpieczeństwa w środowiskach Microsoft Azure i Microsoft 365 - w tym w rozwijającym się krajobrazie obciążeń AI i autonomicznych agentów. Dzięki połączeniu sesji prowadzonych przez instruktorów i praktycznych laboratoriów rozwijasz praktyczne umiejętności w zakresie bezpieczeństwa tożsamości, ochrony infrastruktury chmurowej, wykrywania zagrożeń oraz zarządzania postawą. Kurs ten jest przeznaczony dla inżynierów bezpieczeństwa odpowiedzialnych za planowanie i wdrażanie kontroli bezpieczeństwa w środowiskach chmurowych, hybrydowych i wielochmurowych, wykorzystujących technologie bezpieczeństwa Microsoft.



Odbiorcy szkolenia

Szkolenie przeznaczone jest dla:

- Inżynierowie Bezpieczeństwa



Korzyści

Kończąc ten kurs, studenci poznają następujące zagadnienia:

- Zabezpieczenie dostępu do zasobów za pomocą Microsoft Entra ID i Azure Key Vault
- Egzekwowanie bezpieczeństwa i zgodności regulacyjnej
- Zabezpieczenie pamięci masowej, baz danych i sieci
- Zabezpieczanie zasobów obliczeniowych
- Zabezpieczanie rozwiązań AI
- Zarządzanie i monitorowanie bezpieczeństwa



Program szkolenia

1. Bezpieczny dostęp do zasobów dzięki wykorzystaniu Microsoft Entra
 - Zarządzanie i implementacja metod uwierzytelniania w Microsoft Entra ID
 - Implementacja i konfiguracja Zarządzania Uprzywilejowaną Tożsamością (PIM)
 - Uwierzytelnij wtyczkę API dla agentów deklaracyjnych z zabezpieczonymi API
2. Zabezpiecz Azure Key Vault z dogłębną obroną dla chmury i obciążeń AI
 - Konfiguruj i zabezpiecz Azure Key Vault
 - Zarządzanie kluczami i sekretami w Azure Key Vault
 - Zarządzanie certyfikatami i monitorowanie Azure Key Vault
 - Ochrona Azure Key Vault z użyciem Microsoft Defender for Cloud
3. Egzekwowanie zarządzania bezpieczeństwem i zgodności regulacyjnej
 - Wymuszanie zarządzania za pomocą Azure Policy i blokad zasobów
 - Konfiguruj kontrolę bezpieczeństwa i rekomendacje dotyczące remediacji w Defender for Cloud
 - Oceń zgodność regulacyjną w Defender for Cloud
 - Zarządzanie i przydzielanie ról RBAC o odpowiednich dla najmniejszych przywilejów
 - Chroń dane kopii zapasowej za pomocą funkcji zabezpieczeń Azure Backup
 - Implementacja kontroli bezpieczeństwa w infrastrukturze jako kod
4. Implementacja zabezpieczeń Azure Storage dla chmury oraz inżyniera bezpieczeństwa AI
 - Opis Azure storage services
 - Implementuj zabezpieczenia i zarządzaj dostępem dla Azure Storage
 - Konfiguracja zabezpieczeń sieciowych dla Azure Storage
 - Implementacja Microsoft Defender for Storage
5. Bezpieczeństwo Azure SQL Database
 - Konfiguracja bezpieczeństwa usługi Azure SQL
 - Konfiguruj audyt dla Azure SQL Database i SQL Managed Instance
 - Implementacja Microsoft Defender for Databases



Oczekiwane przygotowanie uczestnika

- Praktyczne doświadczenie w administracji Microsoft Azure oraz środowisk hybrydowych, w tym w zakresie wirtualnych maszyn, sieciowym i zasobów dyskowych
- Dobra znajomość Microsoft Entra ID
- Znajomość administracji Microsoft 365.

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

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



Czas trwania

4 dni / 28 godzin

Język

- Szkolenie: polski
- Materiały: angielski