kod szkolenia: SC-5008 / PL DL 1d

Configure and govern entitlement with Microsoft Entra ID

Szkolenie z zakresu wdrażania oraz nadzorowania mechanizmów zarządzania tożsamością i dostępem w obszarze Microsoft Entra ID, ze szczególnym naciskiem na Identity Governance. Uczestnicy poznają, jak planować i wdrażać Entitlement Management (katalogi zasobów, pakiety dostępu, organizacje powiązane oraz cykl życia użytkowników zewnętrznych), jak przeprowadzać Access Reviews w celu utrzymania zasady najmniejszych uprawnień (least privilege), jak projektować dostęp uprzywilejowany z użyciem Privileged Identity Management (PIM) oraz Privileged Access Groups, a także jak monitorować i analizować zdarzenia dostępu poprzez dzienniki logowań, dzienniki inspekcji oraz integrację z narzędziami SIEM (np. Microsoft Sentinel). Celem jest zbudowanie spójnego podejścia do kontroli uprawnień zgodnego z zasadami Zero Trust oraz wymaganiami audytowymi i regulacyjnymi.

Odbiorcy szkolenia

Szkolenie przeznaczone dla:

- Administratorów tożsamości i dostępu (Identity & Access Administrators) pracujących z Microsoft Entra ID oraz Azure.
- Specjalistów ds. bezpieczeństwa i zgodności, którzy chcą wdrożyć kontrolę uprawnień oraz procesy recertyfikacji dostępu (Access Reviews).
- Administratorów aplikacji i właścicieli zasobów (aplikacje, grupy, subskrypcje Azure), odpowiedzialnych za przyznawanie i przeglądy dostępu.
- Osób projektujących procesy onboarding/offboarding i współpracę z użytkownikami zewnętrznymi (B2B), które chcą zautomatyzować przyznawanie dostępu przez pakiety dostępu.

Korzyści

1. Planowanie i wdrożenie Entitlement Management – tworzenie katalogów, pakietów dostępu oraz reguł przydziału i zatwierdzania.
2. Zarządzanie dostępem użytkowników zewnętrznych (B2B) – organizacje powiązane, polityki współpracy oraz kontrola cyklu życia dostępu.
3. Projektowanie i uruchamianie Access Reviews – konfiguracja przeglądów dla grup i aplikacji, harmonogramy cykliczne, automatyzacja i egzekwowanie wyników.
4. Monitorowanie i utrzymanie Microsoft Entra ID – analiza dzienników logowań i audytu, raportowanie (workbooks), Identity Secure Score oraz integracja z rozwiązaniami SIEM.
5. Wdrożenie dostępu uprzywilejowanego – strategia privileged access, konfiguracja PIM (role Entra i zasoby Azure), Privileged Access Groups oraz konta awaryjne (break-glass).

Program szkolenia

Moduł 1: Planowanie i wdrożenie Entitlement Management w Microsoft Entra ID

- Definiowanie katalogów zasobów (resource catalogs) i pakietów dostępu (access packages).
- Konfiguracja zarządzania uprawnieniami: przepływy zatwierdzeń, zasady przypisania, warunki dostępu.
- Organizacje powiązane (connected organizations) oraz scenariusze współpracy B2B.
- Przegląd uprawnień per użytkownik (per-user entitlements) i audyt przydziałów.

Moduł 2: Planowanie, wdrożenie i zarządzanie Access Reviews

- Planowanie przeglądów dostępu: co i kogo recertyfikować (grupy, aplikacje, role).
- Tworzenie przeglądów dla grup i aplikacji oraz programów przeglądów (access review programs).
- Monitorowanie wyników przeglądów i egzekwowanie decyzji.
- Automatyzacja zadań oraz konfiguracja cyklicznych (recurring) Access Reviews.

Moduł 3: Monitorowanie i utrzymanie Microsoft Entra ID

- Analiza i diagnostyka zdarzeń logowania (sign-in logs) w kontekście problemów z dostępem.
- Przegląd i monitorowanie dzienników inspekcji (audit logs).
- Eksport logów do narzędzi SIEM oraz wykorzystanie workbooków i raportowania.
- Monitorowanie postawy bezpieczeństwa (Identity Secure Score) i podstawowe wskaźniki governance.

Moduł 4: Planowanie i wdrożenie dostępu uprzywilejowanego

- Strategia privileged access dla użytkowników administracyjnych (role, zakresy, JIT).
- Konfiguracja Privileged Identity Management (PIM) dla ról Microsoft Entra oraz ról zasobów Azure.
- Planowanie i konfiguracja Privileged Access Groups.

- Analiza historii audytu i raportów PIM oraz konta awaryjne (emergency access / break-glass).

Moduł 5: Przegląd możliwości Microsoft Entra Permissions Management

- Omówienie zastosowań i korzyści: widoczność uprawnień w środowiskach chmurowych, analiza ryzyk.
- Dashboard i raporty: identyfikacja nadmiarowych uprawnień oraz priorytetyzacja działań.
- Ciągłe monitorowanie i remediacja – podejście operacyjne do utrzymania najmniejszych uprawnień.

Oczekiwane przygotowanie uczestnika

- Podstawowa wiedza z zakresu administracji Azure oraz pracy z Microsoft Entra ID (np. użytkownicy, grupy, role, rejestracje aplikacji – na poziomie ogólnym).
- Zrozumienie podstaw zarządzania dostępem (RBAC, least privilege) oraz koncepcji Zero Trust.
- Podstawowa orientacja w logach i monitorowaniu (sign-in logs / audit logs) będzie pomocna.
- Mile widziane: ogólna znajomość procesów onboarding/offboarding oraz współpracy z użytkownikami zewnętrznymi (B2B).

Szkolenie obejmuje

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

Produkt zawiera:

- Wykład (60%)
- Warsztaty (10%)
- Ćwiczenia (30%)

Główne narzędzia dydaktyczne obejmują prezentacje PowerPoint, praktyczne środowiska laboratoryjne i zasoby usługi Microsoft Learn https://learn.microsoft.com/pl-pl/training/

Czas trwania

1 dni / 7 godzin

Język

- Wykład: polski
- Materiały: angielski