kod szkolenia: SC-100 / PL DL 4d

Microsoft Cybersecurity Architect

Autoryzowane szkolenie w formule Distance Learning. Docelowa grupa odbiorów:

- **Administrator**
- **Specjalista IT**
- **Specjalista ds. bezpieczeństwa IT**

Zobacz film: https://youtu.be/ATEMHyzCssQ

Przeznaczenie szkolenia

Szkolenie dla osób pragnących zapoznać się z zasadami projektowania i oceny strategii cyberbezpieczeństwa w następujących obszarach: Zero Trust, Governance Risk Compliance (GRC), operacje bezpieczeństwa (SecOps) oraz dane i aplikacje. Uczestnicy również zapoznają się, jak zaprojektować rozwiązania z wykorzystaniem zasad zerowego zaufania oraz określać wymagania bezpieczeństwa dla infrastruktury chmurowej w różnych modelach usług (SaaS, PaaS, IaaS). Szkolenie w szczególności jest skierowane do specjalistów IT z zaawansowanym doświadczeniem i wiedzą w szerokim zakresie obszarów inżynierii bezpieczeństwa, w tym tożsamości i dostępu, ochrony platformy, operacji bezpieczeństwa, zabezpieczania danych i zabezpieczania aplikacji, wskazane jest również doświadczenie w zakresie wdrożeń hybrydowych i chmurowych. Kurs obejmuje takie zagadnienia jak:

- Projektowanie strategii i architektury Zero Trust,
- Ocena strategii technicznych i strategii operacji bezpieczeństwa w zakresie zarządzania ryzykiem (GRC),
- Projektowanie bezpieczeństwo dla infrastruktury,

Projektowanie strategii dla danych i aplikacji

Korzyści wynikające z ukończenia szkolenia

Uzyskanie wiedzy i praktycznych umiejętności w zakresie zarządzania bezpieczeństwem na platformie Microsoft. W tym zapoznanie się z:

- Procesem projektowania strategii i architektury Zero Trust.
- Oceną strategii technicznych i strategii operacji bezpieczeństwa w zakresie zarządzania ryzykiem (GRC).
- Procesem projektowania bezpieczeństwa dla infrastruktury.
- Procesem projektowania strategii dla danych i aplikacji.

Metoda egzaminowania

Egzamin w formie **on-line**. Zapis na stronie https://home.pearsonvue.com/Clients/Microsoft.aspx

Opis egzaminu

Po kursie SC-100 można przystąpić do certyfikowanego egzaminu: w autoryzowanym centrum egzaminacyjnym, online będąc monitorowanym przez zewnętrznego egzaminatora. Szczegóły na https://docs.microsoft.com/en-us/certifications/exams/sc-100

Oczekiwane przygotowanie słuchaczy

Co najmniej 2-letnie doświadczenie z zakresie zarządzania infrastrukturą Active Directory, 2-letnie doświadczenie w zakresie zarządzania środowiskiem chmurowym, posiadanie wiedzy i doświadczenia w szerokim zakresie obszarów inżynierii bezpieczeństwa, w tym tożsamości i dostępu, ochrony platformy, operacji bezpieczeństwa, zabezpieczania danych i zabezpieczania aplikacji, wskazane jest również doświadczenie w zakresie wdrożeń hybrydowych i chmurowych.
Umiejętność korzystania z anglojęzycznych materiałów

Język szkolenia

- **Szkolenie**: polski
- **Materiały**: angielski

Szkolenie obejmuje

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

Metoda szkolenia:

- wykład
- warsztaty

Czas trwania

4 dni / 28 godzin

Agenda szkolenia

Ścieżka szkoleniowa 01: Projektowanie rozwiązań zgodnych z najlepszymi praktykami i priorytetami w zakresie bezpieczeństwa

Wprowadzenie do Zero Trust i najlepszych praktyk

- Wprowadzenie do najlepszych praktyk
- Wprowadzenie do Zero Trust
- Inicjatywy Zero Trust RaMP
- Filary technologii Zero Trust

Projektuj rozwiązania zgodne z Cloud Adoption Framework (CAF) i Well-Architected Framework (WAF)

- Zdefiniuj strategię bezpieczeństwa
- Wprowadzenie do Cloud Adoption Framework
- Cloud Adoption Framework — bezpieczna metodologia
- Wprowadzenie do Azure Landing Zones
- Projektuj zabezpieczenia dzięki Azure Landing Zones
- Wprowadzenie do Well Architected Framework
- Well Architected Framework — filar bezpieczeństwa
- Rozwiązania z CAF i WAF

Projektuj rozwiązania, które są zgodne z Microsoft Cybersecurity Reference Architecture (MCRA) i Microsoft Cloud Security Benchmark (MCSB)

Wprowadzenie do MCRA i MCSB

Projektuj rozwiązania z najlepszymi praktykami dotyczącymi możliwości i kontroli

Projektuj rozwiązania z najlepszymi praktykami ochrony przed atakami

Opracuj strategię odporności na typowe cyberzagrożenia, takie jak ransomware

- Typowe cyberzagrożenia i wzorce ataków
- Wspieraj odporność biznesową
- Ochrona przed oprogramowaniem ransomware
- Konfiguracje bezpiecznego tworzenia kopii zapasowych i przywracania
- Aktualizacje zabezpieczeń

Ścieżka szkoleniowa 02: Projektowanie zabezpieczeń, tożsamości i zgodności

Projektuj rozwiązania pod kątem zgodności z przepisami

- Wprowadzenie do zgodności z przepisami
- Przekształć wymagania dotyczące zgodności w rozwiązanie zabezpieczające
- Spełnij wymagania dotyczące zgodności z Purview
- Spełnij wymagania dotyczące prywatności z Priva
- Użyj Azure Policy, aby spełnić wymagania dotyczące bezpieczeństwa i zgodności
- Oceń zgodność infrastruktury za pomocą usługi Microsoft Defender for Cloud

Projektowanie rozwiązań do zarządzania tożsamością i dostępem

- Zaprojektuj rozwiązanie do zarządzania sekretami, kluczami i certyfikatami
- Wprowadzenie do zarządzania tożsamością i dostępem
- Projektuj strategie dostępu do chmury, hybrydy i wielu chmur (w tym Azure AD)
- Zaprojektuj rozwiązanie dla tożsamości zewnętrznych
- Projektuj nowoczesne strategie uwierzytelniania i autoryzacji
- Dostosuj dostęp warunkowy i Zero Trust

Projektowanie rozwiązań zapewniających dostęp uprzywilejowany

- Wprowadzenie do dostępu uprzywilejowanego
- Model dostępu korporacyjnego
- Projektuj rozwiązania do zarządzania tożsamością
- Zaprojektuj rozwiązanie do zabezpieczenia administrowania tenantami
- Projektowanie do zarządzania uprawnieniami do infrastruktury chmury (CIEM)
- Zaprojektuj rozwiązanie dla stacji roboczych z dostępem uprzywilejowanym i usługi bastion

Projektowanie rozwiązań dla operacji bezpieczeństwa

- Wprowadzenie do operacji bezpieczeństwa (SecOps)
- Projektuj możliwości operacji bezpieczeństwa w środowiskach hybrydowych i wielochmurowych
- Zaprojektuj scentralizowane rejestrowanie i inspekcję
- Projektowanie rozwiązań SIEM
- Zaprojektuj rozwiązania do wykrywania i reagowania
- Zaprojektuj rozwiązanie dla SOAR
- Projektowanie przepływów pracy związanych z bezpieczeństwem
- Zaprojektuj zasięg wykrywania zagrożeń

Ścieżka szkoleniowa 03: Projektowanie rozwiązań zabezpieczających aplikacje i dane

Projektuj rozwiązania do zabezpieczania platformy Microsoft 365

- Zabezpieczenia dla Exchange, Sharepoint, OneDrive i Teams (M365)

- Oceń stan zabezpieczeń dla obciążeń związanych ze współpracą i produktywnością
- Zaprojektuj rozwiązanie Microsoft Defender 365
- Projektowanie konfiguracji i praktyki operacyjne dla M365

Projektowanie rozwiązań do zabezpieczania aplikacji

- Wprowadzenie do bezpieczeństwa aplikacji
- Projektuj i wdrażaj standardy w celu bezpiecznego rozwoju aplikacji
- Oceń stan zabezpieczeń istniejących aplikacji
- Zaprojektuj strategię cyklu życia bezpieczeństwa dla aplikacji
- Bezpieczny dostęp do tożsamości
- Zaprojektuj rozwiązanie do zarządzania API
- Zaprojektuj rozwiązanie zapewniające bezpieczny dostęp do aplikacji

Projektuj rozwiązania do zabezpieczania danych organizacji

- Wprowadzenie do bezpieczeństwa danych
- Zaprojektuj rozwiązanie do wykrywania i klasyfikowania danych za pomocą Microsoft Purview
- Zaprojektuj rozwiązanie do ochrony danych w spoczynku, danych w ruchu i danych w użyciu
- Bezpieczeństwo danych w obciążeniach platformy Azure
- Zabezpieczenia usługi Azure Storage
- Defender dla SQL i Defender dla pamięci masowej

Ścieżka szkoleniowa 04: Projektowanie rozwiązań bezpieczeństwa dla infrastruktury

Określ wymagania dotyczące zabezpieczania usług SaaS, PaaS i IaaS

- Zabezpieczanie SaaS, PaaS i Iaas (model współdzielonej odpowiedzialności)
- Punkty bazowe bezpieczeństwa dla usług w chmurze
- Określ wymagania bezpieczeństwa dla obciążeń internetowych
- Określ wymagania bezpieczeństwa dla kontenerów i orkiestracji kontenerów

Projektuj rozwiązania do zarządzania stanem bezpieczeństwa w środowiskach hybrydowych i wielochmurowych

- Wprowadzenie do środowisk hybrydowych i wielochmurowych
- Ocena postawy za pomocą MCSB
- Zaprojektuj zarządzanie postawą i ochronę obciążeń w środowiskach hybrydowych i wielochmurowych
- Omówienie oceny postawy za pomocą Defender for Cloud
- Ocena postawy za pomocą bezpiecznego wyniku usługi Microsoft Defender for Cloud
- Projektuj rozwiązania do ochrony obciążeń w chmurze, które korzystają z usługi Microsoft Defender for Cloud
- Zaprojektuj rozwiązanie do integracji środowisk hybrydowych i wielochmurowych przy użyciu usługi Azure Arc
- Zarządzanie zewnętrzną powierzchnią ataku

Projektowanie rozwiązań do zabezpieczania punktów końcowych serwerów i klientów

- Wprowadzenie do bezpieczeństwa punktów końcowych
- Określ wymagania bezpieczeństwa serwera i linie bazowe
- Określ wymagania dotyczące urządzeń mobilnych i klientów
- Określ wymagania dotyczące bezpieczeństwa IoT i urządzeń wbudowanych
- Microsoft Defender dla IoT
- Określ linie bazowe zabezpieczeń dla punktów końcowych serwera i klienta
- Zaprojektuj rozwiązanie dla bezpiecznego zdalnego dostępu

Projektowanie rozwiązań dla bezpieczeństwa sieci

- Projektowanie rozwiązań segmentacji sieci
- Projektuj rozwiązania do filtrowania ruchu z sieciowymi grupami zabezpieczeń
- Projektowanie rozwiązań do zarządzania stanem sieci
- Projektowanie rozwiązań do monitorowania sieci

Ścieżka szkoleniowa 05: Projektowanie rozwiązań zgodnych z najlepszymi praktykami i priorytetami w zakresie bezpieczeństwa

- Studium przypadku

Ścieżka szkoleniowa 06: Projektowanie operacji zabezpieczeń, tożsamości i możliwości zgodności

- Studium przypadku

Ścieżka szkoleniowa 07: Projektowanie rozwiązań zabezpieczających aplikacje i dane

- Studium przypadku

Ścieżka szkoleniowa 08: Projektowanie rozwiązań bezpieczeństwa dla infrastruktury

- Studium przypadku