

kod szkolenia: SC-100 / PL DL 4d

Microsoft Cybersecurity Architect

Autoryzowane szkolenie w formule Distance Learning. Szkolenie dla osób pragnących zapoznać się z zasadami projektowania i oceny strategii cyberbezpieczeństwa w obszarach: Zero Trust, Governance Risk Compliance (GRC), operacji bezpieczeństwa (SecOps) oraz danych i aplikacji. Uczestnicy uczą się, jak zaprojektować rozwiązania z wykorzystaniem zasad zerowego zaufania oraz określać wymagania bezpieczeństwa dla infrastruktury chmurowej w różnych modelach usług (SaaS, PaaS, IaaS).

Docelowa grupa odbiorców:

- Administrator
- Specjalista IT
- Specjalista ds. bezpieczeństwa IT

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

Wywiad: 15 minut z ekspertem z tematyki Microsoft Azure:

Zobacz film: <https://youtu.be/sXfpx7KEqQ8>

Wywiad: 15 minut z ekspertem z tematyki bezpieczeństwa usług chmurowych Microsoft 365:

Zobacz film: <https://youtu.be/8p5ioOu4WX8>



Odbiorcy szkolenia

Szkolenie w szczególności skierowane jest do:

- Administratorów bezpieczeństwa i specjalistów IT z zaawansowanym doświadczeniem w inżynierii bezpieczeństwa.
- Osób posiadających wiedzę w obszarach takich jak: tożsamość i dostęp, ochrona platformy, operacje bezpieczeństwa, zabezpieczanie danych oraz zabezpieczanie aplikacji.
- Profesjonalistów z doświadczeniem we wdrożeniach hybrydowych i chmurowych.



Korzyści

Uzyskanie wiedzy i praktycznych umiejętności w zakresie projektowania bezpieczeństwa na platformie Microsoft.

W tym zapoznanie się z:

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

Szkolenie pomaga uczestnikom przygotować się do egzaminu SC-100.

Become Microsoft Certified: https://arch-center.azureedge.net/Credentials/Certification-Poster_en-us.pdf



Program szkolenia

1. Projektowanie rozwiązań zgodnych z najlepszymi praktykami i priorytetami w zakresie bezpieczeństwa
 - Wprowadzenie do Zero Trust i najlepszych praktyk

- Inicjatywy Zero Trust RaMP
- Filary technologii Zero Trust
- Projektowanie rozwiązań zgodne z Cloud Adoption Framework (CAF) i Well-Architected Framework (WAF)
- Definiowanie strategii bezpieczeństwa
- Wprowadzenie do Cloud Adoption Framework
 - Cloud Adoption Framework — bezpieczna metodologia
 - Wprowadzenie do Azure Landing Zones
 - Projektowanie zabezpieczeń dzięki Azure Landing Zones
 - Wprowadzenie do Well Architected Framework
 - Well Architected Framework — filar bezpieczeństwa
 - Rozwiązania z CAF i WAF
- Projektowanie rozwiązań zgodnych z Microsoft Cybersecurity Reference Architecture (MCRA) i Microsoft Cloud Security Benchmark (MCSB)
 - Wprowadzenie do MCRA i MCSB
 - Projektowanie rozwiązań z najlepszymi praktykami dotyczącymi możliwości i kontroli
 - Projektowanie rozwiązań z najlepszymi praktykami ochrony przed atakami
 - Strategia odporności na typowe cyberzagrożenia, takie jak ransomware
 - Typowe cyberzagrożenia i wzorce ataków
 - Wspieranie odporności biznesowej
 - Ochrona przed oprogramowaniem ransomware
 - Konfiguracje bezpiecznego tworzenia kopii zapasowych i przywracania
 - Aktualizacje zabezpieczeń
- 2. Projektowanie zabezpieczeń, tożsamości i zgodności
 - Projektowanie rozwiązania pod kątem zgodności z przepisami
 - Wprowadzenie do zgodności z przepisami
 - Przekształcanie wymagań dotyczących zgodności w rozwiązanie zabezpieczające
 - Spełnianie wymagań dotyczących zgodności z Purview
 - Spełnianie wymagań dotyczących prywatności z Priva
 - Użycie Azure Policy, aby spełnić wymagania dotyczące bezpieczeństwa i zgodności
 - Ocena zgodności infrastruktury za pomocą usługi Microsoft Defender for Cloud
 - Projektowanie rozwiązań do zarządzania tożsamością i dostępem
 - Projektowanie rozwiązania do zarządzania sekretami, kluczami i certyfikatami
 - Wprowadzenie do zarządzania tożsamością i dostępem
 - Projektowanie strategii dostępu do chmury, hybrydy i wielu chmur (w tym Azure AD)
 - Projektowanie rozwiązania dla tożsamości zewnętrznych
 - Projektowanie nowoczesnych strategii uwierzytelniania i autoryzacji
 - Dostosowywanie dostępu warunkowego i Zero Trust
 - Projektowanie rozwiązań zapewniających dostęp uprzywilejowany
 - Wprowadzenie do dostępu uprzywilejowanego
 - Model dostępu korporacyjnego

- Projektowanie rozwiązania do zarządzania tożsamością
- Projektowanie rozwiązania do zabezpieczenia administrowania tenantami
- Projektowanie do zarządzania uprawnieniami do infrastruktury chmury (CIEM)
- Projektowanie rozwiązania dla stacji roboczych z dostępem uprzywilejowanym i usługi bastion
- Projektowanie rozwiązań dla operacji bezpieczeństwa
 - Wprowadzenie do operacji bezpieczeństwa (SecOps)
 - Projektowanie możliwości operacji bezpieczeństwa w środowiskach hybrydowych i wielochmurowych
 - Projektowanie scentralizowanego rejestrowania i inspekcji
 - Projektowanie rozwiązań SIEM
 - Projektowanie rozwiązania do wykrywania i reagowania
 - Projektowanie rozwiązania dla SOAR
 - Projektowanie przepływów pracy związanych z bezpieczeństwem
 - Projektowanie zasięgu wykrywania zagrożeń
- 3. Projektowanie rozwiązań zabezpieczających aplikacje i dane
 - Projektowanie rozwiązania do zabezpieczania platformy Microsoft 365
 - Zabezpieczenia dla Exchange, Sharepoint, OneDrive i Teams (M365)
 - Ocena stanu zabezpieczeń dla obciążeń związanych ze współpracą i produktywnością
 - Projektowanie rozwiązań Microsoft Defender 365
 - Projektowanie konfiguracji oraz praktyki operacyjne dla M365
 - Projektowanie rozwiązań do zabezpieczania aplikacji
 - Wprowadzenie do bezpieczeństwa aplikacji
 - Projektowanie i wdrażanie standardu w celu bezpiecznego rozwoju aplikacji
 - Ocena stanu zabezpieczeń istniejących aplikacji
 - Projektowanie strategii cyklu życia bezpieczeństwa dla aplikacji
 - Bezpieczny dostęp do tożsamości
 - Projektowanie rozwiązania do zarządzania API
 - Projektowanie rozwiązania zapewniającego bezpieczny dostęp do aplikacji
 - Projektowanie rozwiązania do zabezpieczania danych organizacji
 - Wprowadzenie do bezpieczeństwa danych
 - Projektowanie rozwiązania do wykrywania i klasyfikowania danych za pomocą Microsoft Purview
 - Projektowanie rozwiązania 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
- 4. Projektowanie rozwiązań bezpieczeństwa dla infrastruktury
 - Określanie wymagań dotyczących zabezpieczania usług SaaS, PaaS i IaaS
 - Zabezpieczanie SaaS, PaaS i IaaS (model współdzielonej odpowiedzialności)
 - Punkty bazowe bezpieczeństwa dla usług w chmurze
 - Określanie wymagań bezpieczeństwa dla obciążeń internetowych
 - Określanie wymagań bezpieczeństwa dla kontenerów i orkiestracji kontenerów

- Projektowanie rozwiązania do zarządzania stanem bezpieczeństwa w środowiskach hybrydowych i wielochmurowych
 - Wprowadzenie do środowisk hybrydowych i wielochmurowych
 - Ocena postawy za pomocą MCSB
 - Projektowanie zarządzania postawą i ochroną 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
 - Projektowanie rozwiązania do ochrony obciążeń w chmurze, które korzystają z usługi Microsoft Defender for Cloud
 - Projektowanie rozwiązania 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
 - Określanie wymagań bezpieczeństwa serwera i linii bazowych
 - Określanie wymagań dotyczących urządzeń mobilnych i klientów
 - Określanie wymagań dotyczących bezpieczeństwa IoT i urządzeń wbudowanych
 - Microsoft Defender dla IoT
 - Określanie linii bazowych zabezpieczeń dla punktów końcowych serwera i klienta
 - Projektowanie rozwiązania dla bezpiecznego zdalnego dostępu
- Projektowanie rozwiązań dla bezpieczeństwa sieci
 - Projektowanie rozwiązań segmentacji sieci
 - Projektowanie rozwiązania do filtrowania ruchu z sieciowymi grupami zabezpieczeń
 - Projektowanie rozwiązań do zarządzania stanem sieci
 - Projektowanie rozwiązań do monitorowania sieci
- 5. Projektowanie rozwiązań zgodnych z najlepszymi praktykami i priorytetami w zakresie bezpieczeństwa
 - Studium przypadku
- 6. Projektowanie operacji zabezpieczeń, tożsamości i możliwości zgodności
 - Studium przypadku
- 7. Projektowanie rozwiązań zabezpieczających aplikacje i dane
 - Studium przypadku
- 8. Projektowanie rozwiązań bezpieczeństwa dla infrastruktury
 - Studium przypadku



Oczekiwane przygotowanie uczestnika

- 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.
 - Znajomość technologii zabezpieczeń i zgodności firmy Microsoft.
 - Znajomość pojęć związanych z ochroną informacji.
 - Średniozaawansowana znajomość systemu Windows 10/11
 - Umiejętność korzystania z anglojęzycznych materiałów
 - Szkolenia poprzedzające: AZ-900, SC-900, SC-300, SC-401, SC-200
- Umiejętność korzystania z anglojęzycznych materiałów



Szkolenie obejmuje

Szkolenie obejmuje:

* podręcznik w formie elektronicznej dostępny na platformie:

<https://learn.microsoft.com/pl-pl/training/>

* dostęp do portalu słuchacza Altkom Akademii

- szkolenie prowadzone w formie prezentacji
- demonstracje trenera
- ćwiczenia praktyczne w formie case studies

Metoda szkolenia:

formuła Distance Learning



Język

- Szkolenie: polski
- Materiały: angielski

Metoda egzaminacyjna

Become Microsoft Certified: https://arch-center.azureedge.net/Credentials/Certification-Poster_en-us.pdf

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

Czas trwania

4 dni / 28 godzin

Opis egzaminu

Microsoft Certified: Cybersecurity Architect Expert

Exam URL: <https://docs.microsoft.com/en-us/learn/certifications/exams/SC-100>

Become Microsoft Certified: https://arch-center.azureedge.net/Credentials/Certification-Poster_en-us.pdf