SC-100T00 Microsoft Cybersecurity Architect

Czas trwania: 4 dni

Dla kogo:
Szkolenie skierowane do administratorów, inżynierów systemowych oraz architektów pragnących zapoznać się z zasadami projektowania i oceny strategii cyberbezpieczeństwa w następujących obszarach: Zero Trust, Governance Risk Compliance (GRC), operacje bezpieczeństwa (SecOps) oraz danych i aplikacji.

Wymagania wstępne:

- 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

Szkolenie przygotowuje do egzaminu:
SC-100 Microsoft Cybersecurity Architect

Zakres tematyczny:

1. Budowa ogólnej strategii i architektury bezpieczeństwa
    - przegląd Zero Trust
    - Opracowanie punktów integracji w architekturze
    - Opracowanie wymagań bezpieczeństwa w oparciu o cele biznesowe
    - Przetransponowanie wymagań bezpieczeństwa na możliwości techniczne
    - Zaprojektowanie zabezpieczeń dla strategii odporności
    - Opracowanie strategii bezpieczeństwa dla środowisk hybrydowych i wielodostępnych
    - Projektowanie strategii technicznych i zarządzania dla filtrowania i segmentacji ruchu
    - Zapoznanie się z zabezpieczeniami protokołów
2. Zaprojektowanie strategii operacji bezpieczeństwa
    - Zrozumienie struktury, procesów i procedur dotyczących bezpieczeństwa
    - Zaprojektowanie strategii bezpieczeństwa logowania i audytu
    - Opracowanie operacji bezpieczeństwa dla środowisk hybrydowych i wielochmurowych
    - Opracowanie strategii zarządzania informacjami o zabezpieczeniach i zdarzeniami (SIEM) oraz orkiestracji bezpieczeństwa,
    - Ocena przepływów pracy związanych z bezpieczeństwem
    - Przegląd strategii bezpieczeństwa dotyczących zarządzania incydentami
    - Ocena strategii operacji bezpieczeństwa pod kątem udostępniania informacji o zagrożeniach technicznych
    - Monitorowanie źródeł, aby uzyskać wgląd w zagrożenia i środki łagodzące
3. Zaprojektowanie strategii bezpieczeństwa tożsamości
    - Bezpieczny dostęp do zasobów w chmurze
    - Rekomendacje bezpieczeństwa dla magazynu tożsamości
    - Rekomendacje bezpieczeństwa dla strategii bezpiecznego uwierzytelniania i autoryzacji
    - Bezpieczny dostęp warunkowy
    - Zaprojektowanie strategii przypisywania ról i delegowania

- Zdefiniowanie zarządzania tożsamością dla przeglądów dostępu i zarządzania uprawnieniami
- Zaprojektowanie strategii bezpieczeństwa dla roli uprzywilejowanego dostępu do infrastruktury
- Zaprojektowanie strategii bezpieczeństwa dla działań uprzywilejowanych
- Poznanie zabezpieczenia protokołów

4. Ocena strategii zgodności z przepisami
   - Interpretacja wymagań zgodności i ich możliwościami technicznymi
   - Ocena zgodności infrastruktury za pomocą programu Microsoft Defender for Cloud
   - Interpretacja oceny zgodności i rekomendowane działania w celu rozwiązania problemów lub poprawy bezpieczeństwa
   - Zaprojektowanie i zweryfikowanie wdrożenia Azure Policy
   - Zaprojektowanie wymagań pod kątem rezydencji danych
   - Przetransponowanie wymagań dotyczących prywatności na wymagania dotyczące rozwiązań bezpieczeństwa
5. Ocena stanu bezpieczeństwa i rekomendowane strategie techniczne zarządzania ryzykiem:
   - Ocena postawy bezpieczeństwa za pomocą testów porównawczych
   - Ocena stanu bezpieczeństwa za pomocą programu Microsoft Defender for Cloud
   - Ocena postawy bezpieczeństwa za pomocą bezpiecznych wyników
   - Ocena higieny bezpieczeństwa Cloud Workloads
   - Zaprojektowanie zabezpieczeń dla strefy Azure Landing Zone
   - Interpretacja analizy zagrożeń technicznych i rekomendowane środki ograniczające ryzyko
   - Rekomendowane funkcje bezpieczeństwa lub środki kontroli w celu złagodzenia zidentyfikowanych zagrożeń
6. Poznanie najlepszych praktyk dotyczących architektury i ich zmiany w chmurze
   - Planowanie i implementacja strategii bezpieczeństwa w zespołach
   - Ustalenie strategii i procesu proaktywnej i ciągłej ewolucji strategii bezpieczeństwa
   - Poznanie protokołów sieciowych i najlepszych praktyk dotyczących segmentacji sieci i filtrowania ruchu
7. Zaprojektowanie strategii zabezpieczania punktów końcowych serwera i klienta
   - Określenie podstawy bezpieczeństwa dla punktów końcowych serwera i klienta
   - Określenie wymagań bezpieczeństwa dla serwerów
   - Określenie wymagań bezpieczeństwa dla urządzeń mobilnych i klientów
   - Określenie wymagań dotyczących zabezpieczania usług domenowych w usłudze Active Directory
   - Zaprojektowanie strategii zarządzania tajemnicami, kluczami i certyfikatami
   - Opracowanie strategii bezpiecznego zdalnego dostępu
   - Zrozumienie struktury, procesów i procedur dotyczących bezpieczeństwa
   - Zrozumienie procedur głębokiej kryminalistyki według typu zasobów
8. Zaprojektowanie strategii zabezpieczania usług PaaS, IaaS i SaaS
   - Określenie podstawy bezpieczeństwa dla usług PaaS
   - Określenie podstawy bezpieczeństwa dla usług IaaS
   - Określenie podstawy bezpieczeństwa dla usług SaaS
   - Określenie wymagań dotyczących zabezpieczeń dla obciążeń IoT
   - Określenie wymagań bezpieczeństwa dla obciążeń danych
   - Określenie wymagań bezpieczeństwa dla obciążeń internetowych
   - Określenie wymagań bezpieczeństwa dla obciążeń pamięci masowej
   - Określenie wymagań bezpieczeństwa dla kontenerów
   - Określenie wymagań bezpieczeństwa dla orkiestracji kontenerów
9. Określenie wymagań bezpieczeństwa dla aplikacji:
   - Zrozumienie modelowania zagrożeń aplikacji
   - Określenie priorytetów łagodzenia zagrożeń dla aplikacji
   - Określenie standardów bezpieczeństwa podczas wdrażania nowej aplikacji

- Określenie strategii bezpieczeństwa dla aplikacji i interfejsów API

10. Opracowanie strategii zabezpieczania danych
    - Nadanie priorytetu łagodzenia zagrożeń dla danych
    - Opracowanie strategii identyfikacji i ochrony danych wrażliwych
    - Określenie standardu szyfrowania danych w spoczynku i w ruchu