kod szkolenia: SC-5002 / PL DL 1d

Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls

Dyrektywa NIS2

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi.

Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2

Odbiorcy szkolenia

Kurs jest dedykowany dla osób, które planują wykorzystać usługi i obciążenia platformy Secure Azure w ramach oceny kontroli zgodności z przepisami Microsoft Defender for Cloud, lub specjalistów, którzy w swojej codziennej pracy wykonują zadania inżynierów bezpieczeństwa Azure. Kurs stanowi pomost pomiędzy umiejętnościami na poziomie podstawowym a umiejętnościami stowarzyszonymi na poziomie podstawowym. Kurs będzie również pomocny dla uczestników, którzy pragną zapoznać się rolami IT, w tym w infrastrukturalnymi, bezpieczeństwa i sieci.

Korzyści

Nabycie wiedzy i umiejętności w zakresie praktycznego zabezpieczania usług i obciążeń platformy Azure., w tym:

- Filtrowanie ruchu sieciowego za pomocą sieciowej grupy zabezpieczeń.
- Tworzenie obszaru roboczego Log Analytics dla usługi Microsoft Defender dla chmury.

- Konfigurowanie usługi Microsoft Defender dla chmury.
- Konfigurowanie dostępu do maszyny wirtualnej w trybie just-in-time (JIT).
- Konfigurowanie i integrowanie agenta Log Analytics oraz przestrzeni roboczej w usłudze Defender for Cloud.
- Konfigurowanie ustawień sieciowych Azure Key Vault oraz wykonanie przywracania magazynu kluczy z funkcją usuwania miękkiego i czyszczenia.

Program szkolenia

1. Filtrowanie ruchu sieciowego za pomocą sieciowej grupy zabezpieczeń przy użyciu Azure Portal.
   - Grupa zasobów platformy Azure.
   - Sieć wirtualna platformy Azure.
   - Jak sieciowe grupy zabezpieczeń filtrują ruch sieciowy.
   - Grupy zabezpieczeń aplikacji.
2. Utworzenie obszaru roboczego Log Analytics dla usługi Microsoft Defender for Cloud.
   - Defender dla komponentów monitorowanych w chmurze.
3. Konfiguracja usługi Microsoft Defender dla chmury.
   - Implementacja usługi Microsoft Defender dla chmury.
   - Postawa bezpieczeństwa.
   - Zabezpieczenia obciążenia.
   - Wdrażanie Microsoft Defender dla chmury.
   - Azure Arc .
   - Możliwości Azure Arc.
   - Test porównawczy bezpieczeństwa chmury Microsoft.
   - Poprawianie swojej zgodność z przepisami.
   - Konfigurowanie zasady Microsoft Defender dla chmury.
   - Przeglądanie i edycja zasad bezpieczeństwa.
   - Zarządzanie i wdrażanie rekomendacjami usługi Microsoft Defender dla chmury.
   - Zapoznanie się z bezpiecznym wynikiem.
   - MITRE Attack matrix.
   - Zdefiniowanie ataków typu brute-force.
   - Zapoznanie się z dostępem do maszyn wirtualnych w trybie just-in-time.
   - Wdrażanie dostępu do maszyn wirtualnych na czas.
4. Konfiguracja i integracja agenta Log Analytics i obszaru roboczego w usłudze Defender for Cloud.
   - Zbieranie danych z obciążeń za pomocą agenta Log Analytics.
   - Konfiguracja agenta i obszaru roboczego Log Analytics.
5. Konfiguracja ustawień sieciowych w Azure Key Vault.
   - Podstawowe pojęcia dotyczące usługi Azure Key Vault.
   - Najlepsze rozwiązania dotyczące Azure Key Vault.

- Zabezpieczenia Azure Key Vault.
- Konfiguracja zapory i sieci wirtualnej Azure Key Vault.
- Zapoznanie się z opcją usuwania nietrwałego usługi Azure Key Vault.
- Punkty końcowe usługi sieci wirtualnej dla Azure Key Vault.

6. Połączenie serwera Azure SQL przy użyciu prywatnego punktu końcowego platformy Azure.
   - Prywatny punkt końcowy platformy Azure.
   - Prywatne łącze platformy Azure.

Oczekiwane przygotowanie uczestnika

• Praktyczne doświadczenie w administrowaniu środowiskami Microsoft Azure i hybrydowymi.
• Dobra znajomość zagadnień obliczeniowych, sieci i zabezpieczeń na platformie Azure oraz znajomość Microsoft Entra ID.
• Znajomość technik zarządzania bezpieczeństwem i usuwania luk w zabezpieczeniach.
• Znajomość modelowania zagrożeń i wdrażania środków ochrony przed zagrożeniami.
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

1 dni / 7 godzin

Język

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