

kod szkolenia: AWS-SEC-BP / PL DL 1d

AWS Security Best Practices

Sztuczna inteligencja w chmurze – wyzwania i innowacje według AWS

Zobacz film: <https://youtu.be/2PddkjDfIQ4>



Odbiorcy szkolenia

Kurs jest przeznaczony dla:

- Architektów rozwiązań, inżynierów chmurowych, w tym inżynierów bezpieczeństwa, inżynierów ds. dostarczania i wdrożenia, specjalistów ds. usług profesjonalnych oraz Cloud Center of Excellence (CCOE).



Korzyści

W tym kursie nauczysz się:

- Projektować i wdrażać bezpieczną infrastrukturę sieciową
- Projektować i wdrażać bezpieczeństwo obliczeń
- Projektować i wdrażać rozwiązanie do logowania.



Program szkolenia

Moduł 1: Przegląd bezpieczeństwa AWS

- Model wspólnej odpowiedzialności
- Wyzwania dla klientów
- Ramy i standardy
- Ustanawianie najlepszych praktyk

- Zgodność w AWS

Moduł 2: Zabezpieczanie sieci

- Elastyczność i bezpieczeństwo
- Zabezpieczenia wewnątrz Amazon Virtual Private Cloud (Amazon VPC)
- Usługi zabezpieczeń
- Rozwiązania zabezpieczeń firm trzecich

Moduł 3: Bezpieczeństwo Amazon EC2

- Twardość obliczeniowa
- Szyfrowanie Amazon Elastic Block Store (EBS)
- Bezpieczne zarządzanie i konserwacja
- Wykrywanie podatności
- Korzystanie z AWS Marketplace

Moduł 4: Monitorowanie i powiadamianie

- Rejestrowanie ruchu sieciowego
- Rejestrowanie ruchu użytkownika i interfejsu API (Application Programming Interface)
- Widoczność z Amazon CloudWatch
- Udoskonalanie monitorowania i powiadamiania
- Weryfikowanie środowiska AWS.



Oczekiwane przygotowanie uczestnika

Przed uczestnictwem w tym kursie, uczestnicy powinni ukończyć następujące kursy:

- AWS Security Fundamentals
- AWS Security Essentials.



Szkolenie obejmuje

- 1 dzień pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty.



Czas trwania

1 dni / 7 godzin

Język

- Szkolenie: polski
- Materiały: angielski.