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

AWS Security Essentials

Sztuczna inteligencja w chmurze – wyzwania i innowacje według AWS

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

Szkolenie **AWS Security Essentials** jest przeznaczone dla osób, które chcą poznać podstawowe zasady bezpieczeństwa w środowisku Amazon Web Services. Program obejmuje kluczowe zagadnienia związane z ochroną danych, zarządzaniem tożsamością i dostępem, bezpieczeństwem sieci oraz monitorowaniem środowiska AWS zgodnie z modelem współodpowiedzialności i najlepszymi praktykami Amazon Web Services. Praktyczne laboratoria umożliwiają zdobycie podstawowych umiejętności w zakresie zabezpieczania zasobów chmurowych.

Odbiorcy szkolenia

Ten kurs jest przeznaczony dla:

- Profesjonalistów IT na poziomie biznesowym, zainteresowanych praktykami bezpieczeństwa w chmurze
- Profesjonalistów ds. bezpieczeństwa z minimalną wiedzą praktyczną na temat AWS.

Korzyści

W tym kursie nauczysz się:

- Identyfikować korzyści i obowiązki związane z bezpieczeństwem podczas korzystania z chmury AWS
- Opisywać funkcje zarządzania dostępem i kontroli w AWS
- Zrozumieć różne metody szyfrowania danych w celu zabezpieczenia wrażliwych informacji
- Opisywać, jak zabezpieczyć dostęp do zasobów AWS w sieci

- Określić, które usługi AWS można wykorzystać do rejestrowania i monitorowania bezpieczeństwa.

Program szkolenia

Moduł 1: Bezpieczeństwo w AWS
Zasady projektowania bezpieczeństwa w chmurze AWS
Model współodpowiedzialności AWS
Moduł 2: Bezpieczeństwo CHMURY
Infrastruktura globalna AWS
Bezpieczeństwo centrów danych
Zgodność i zarządzanie
Moduł 3: Bezpieczeństwo W CHMURZE – Część 1
Zarządzanie tożsamościami i dostępem
Ochrona danych
Laboratorium 01 – Wprowadzenie do polityk bezpieczeństwa
Moduł 4: Bezpieczeństwo W CHMURZE – Część 2
Zabezpieczanie infrastruktury
Kontrola monitorowania i detekcji
Laboratorium 02 – Zabezpieczanie zasobów VPC za pomocą grup bezpieczeństwa
Moduł 5: Bezpieczeństwo W CHMURZE – Część 3
Ochrona przed atakami DDoS
Podstawy reagowania na incydenty
Laboratorium 03 – Automatyzowanie reakcji na incydenty z użyciem AWS Config i AWS Lambda
Moduł 6: Podsumowanie kursu
Przegląd narzędzia AWS Well-Architected

Oczekiwane przygotowanie uczestnika

Zalecamy, aby uczestnicy tego kursu posiadali:

- Znajomość praktyk bezpieczeństwa IT oraz pojęć związanych z infrastrukturą, a także znajomość podstawowych zagadnień związanych z chmurą obliczeniową.

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.