

Certified Cloud Security Engineer

EC-Council Certified Cloud Security Engineer (CC|CSE) to szkolenie przygotowane przez specjalistów ds. bezpieczeństwa rozwiązań chmurowych oraz ekspertów branżowych. Stanowi ono przekrojowy przegląd rozwiązań generycznych (vendor-neutral) oraz konkretnych rozwiązań dostawców usług chmurowych (vendor-specific). Szczególny nacisk położony jest na dobre praktyki bezpieczeństwa chmurowego, technologie, standardy i frameworki oraz na praktyczne umiejętności posługiwania się rozwiązaniami oferowanymi przez Amazon Web Services (AWS), Azure i Google Cloud Platform (GCP). Program szkolenia bazuje na rzeczywistych rolach i odpowiedzialnościach specjalistów ds. bezpieczeństwa chmurowego i idealnie odpowiada na potrzeby zarówno początkujących jak i doświadczonych ekspertów związanych z cyberbezpieczeństwem.

- Szczególny nacisk na szkoleniu skierowany jest na praktyczne umiejętności korzystania z rozwiązań AWS, Azure i GCP (ponad 50 ćwiczeń laboratoryjnych)
- Szkolenie omawiane są zarówno techniczne, jak i operacyjne zagadnienia związane z bezpieczeństwem chmury, jak również testy penetracyjne, analiza powłamaniowa, reakcja na incydenty bezpieczeństwa, Business Continuity i Disaster Recovery

LAB-INTENSIVE CLOUD SECURITY PROGRAM - About 3rd Part Subscription

This program will require you to sign up for third party services that may incur fees. Be sure to follow proper guidelines for removing billable services from your account before you leave your lab. Deviating from our specific instructions may result in unwanted fees for

services from third-party service providers. If you sign-up and provide credit card, you will be responsible for any fees related to services you activate. We strongly advise you not to deviate from our explicit instructions while connected to the platforms unless you are fully aware of what the services are and what the respective third-party charges for their use.



Przeznaczenie szkolenia

Szkolenie skierowane jest do:

- Administratorów systemów,
- Administratorów sieci i osób odpowiedzialnych za cyberbezpieczeństwo infrastruktury i sieci tradycyjnych rozwiązań
- Inżynierów pracujących z chmurą, którzy szczególnie zainteresowani są bezpieczeństwem tworzonych rozwiązań



Korzyści wynikające z ukończenia szkolenia

- Szkolenie C|CSE dostarcza praktycznej wiedzy na temat tworzenia i zabezpieczania infrastruktury chmurowej oraz aplikacji.
- Szkolenie jest unikatowym połączeniem tematów ogólnych oraz konkretnych rozwiązań dostawców usług chmurowych (AWS, Azure, GCP).
- Szkolenie uczy dobrych praktyk zabezpieczania infrastruktury chmurowej poprzez analizę rozwiązań do przechowywania danych i związanych z nimi zagrożeń, jak również konfigurację usług, projektowanie i wdrażanie planu reakcji na incydenty oraz audyt rozwiązań chmurowych.
- Szkolenie uczy dobrych praktyk w zakresie tworzenia i zarządzania narzędziami SIEM i SOAR oraz zespołem ekspertów SOC reagujących na incydenty bezpieczeństwa.
- Szkolenie uczy praktycznego zastosowania i wdrożenia najważniejszych standardów, norm oraz regulacji prawnych związanych z chmurą (ISO/IEC 27017, HIPAA, PCI DSS).
- Szkolenie uczy praktycznych metod analizy powłamaniamiowej w chmurze oraz metod jej automatyzacji.
- Szkolenie kompleksowo przygotowuje do roli eksperta ds. bezpieczeństwa rozwiązań chmurowych.



Metoda egzaminowania

Możliwość zdawania egzaminu w akredytowanych centrach egzaminacyjnych EC Council (ECC).

Informacje o egzaminie:

Nazwa egzaminu: Certified Cloud Security Engineer

Kod egzaminu: 312-40

Liczba pytań: 125

Czas trwania: 4 hours

Format egzaminu: Pytania wielokrotnego wyboru



Oczekiwane przygotowanie słuchaczy

- Podstawowa wiedza na temat systemów operacyjnych Windows i Linux.
- Podstawowa znajomość pojęć związanych z sieciami (protokół TCP/IP, usługi DNS/DHCP, adresacja IP).
- Zalecane są co najmniej 2 lata doświadczenia w branży informatycznej.



Język szkolenia

- Szkolenie: polski
- Materiały: angielski



Czas trwania

5 dni / 40 godzin

Agenda szkolenia

1. Wprowadzenie do bezpieczeństwa rozwiązań chmurowych
2. Bezpieczeństwo platform i infrastruktury w chmurze
3. Bezpieczeństwo aplikacji w chmurze
4. Bezpieczeństwo danych w chmurze

5. Bezpieczeństwo operacyjne w chmurze
6. Testy penetracyjne w chmurze
7. Reagowanie na incydenty w chmurze
8. Analiza powłamaniowa w chmurze
9. Ciągłość działania i odtwarzanie awaryjne w chmurze
10. Strategia zarządzania, zarządzanie ryzykiem, normy i standardy w chmurze