Możliwość dofinansowania

Testy penetracyjne i zabezpieczanie aplikacji w środowisku chmury AWS

Numer usługi 2025/07/04/10671/2857975

3 813,00 PLN brutto
3 100,00 PLN netto
158,88 PLN brutto/h
129,17 PLN netto/h

Sages Spółka z ograniczoną odpowiedzialnością

4,4 / 5
288 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
24 h
06.10.2025 do 08.10.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie adresowane jest do inżynierów i pasjonatów bezpieczeństwa zainteresowanych prowadzeniem testów penetracyjnych w środowisku AWS
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	29-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Przedstawienie mechanizmów bezpieczeństwa AWS

Przedstawienie narzędzi i technik przydatnych do przeprowadzenia testów penetracyjnych w środowisku AWS

Przedstawienie usług AWS, które można wykorzystać w celu zabezpieczenia aplikacji

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Przedstawienie mechanizmów bezpieczeństwa AWS Przedstawienie narzędzi i technik przydatnych do przeprowadzenia testów penetracyjnych w środowisku AWS	Wykorzystuje usługi AWS w celu zabezpieczenia aplikacji	Obserwacja w warunkach rzeczywistych
		Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie będzie prowadzone zdalnie, w czasie rzeczywistym, na żywo, z trenerem, możliwością zadawania pytań.

Każdego dnia zajęcia w godz. 9:00-17:00, z przerwą na lunch około godz. 13:00

Mechanizmy bezpieczeństwa AWS

Zdobywanie dostępu

Wykorzystanie podatności

Utrzymywanie dostępu i zacieranie śladów

Omijanie mechanizmów wykrywających włamania

Konfiguracja usług zabezpieczających i wykrywających ataki

Narzędzia do prowadzenia audytu konfiguracji usług AWS

Walidacja

Harmonogram

Liczba przedmiotów/zajęć: 3

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 3 Mechanizmy bezpieczeństwa AWS. Zdobywanie dostępu	Sebastian Chmielewski	06-10-2025	09:00	17:00	08:00
2 z 3 Wykorzystanie podatności. Utrzymywanie dostępu i zacieranie śladów. Omijanie mechanizmów wykrywających włamania	Sebastian Chmielewski	07-10-2025	09:00	17:00	08:00
3 z 3 Konfiguracja usług zabezpieczających i wykrywających ataki. Narzędzia do prowadzenia audytu konfiguracji usług AWS	Sebastian Chmielewski	08-10-2025	09:00	17:00	08:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 813,00 PLN
Koszt przypadający na 1 uczestnika netto	3 100,00 PLN
Koszt osobogodziny brutto	158,88 PLN
Koszt osobogodziny netto	129,17 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Sebastian Chmielewski

Ekspert QA z ponad 12-letnim doświadczeniem, specjalizujący się w zapewnianiu bezpieczeństwa produktów oraz szeroko pojętym zapewnieniu jakości oprogramowania. Moje kompetencje obejmują automatyzację testów funkcjonalnych i wydajnościowych, testy penetracyjne, a także przeglądy kodu, co pozwala na identyfikację i eliminację potencjalnych zagrożeń już na najwcześniejszych etapach cyklu życia aplikacji. W trakcie mojej kariery osiągnąłem znaczące sukcesy w dziedzinie bug bounty – zgłosiłem 48 podatności w serwisie BugCrowd, co plasuje mnie na pozycji 650 w światowym rankingu na tej platformie. Zdobyłem certyfikaty OSWE (Offsec Web Expert) i OSED (Offsec Exploit Developer).

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

część teoretyczna szkolenia, slajdy - zostanie przekazana uczestnikom na szkoleniu w formie pdf.

uczestnik otrzyma certyfikat uczestnictwa z opisem nabytych umiejętności

Warunki uczestnictwa

Umiejętność posługiwania się systemem Linux i narzędziami AWS z linii komend

Mile widziana podstawowa znajomość podatności z listy OWASP Top Ten i umiejętność prowadzenia testów penetracyjnych aplikacji web z użyciem narzędzia typu Proxy (Burp Suite, OWASP ZAP, Caido)

Informacje dodatkowe

Szkolenie będzie prowadzone zdalnie, w czasie rzeczywistym, na żywo, z trenerem, możliwością zadawania pytań.

Warunki techniczne

szkolenie na platformie zoom, wymagane:

stabilne połączenie internetowe (zalecane min. 10Mbit/s download i 1Mbit/s upload)

przeglądarka internetowa Chrome

zainstalowana aplikacja Zoom App

dobrej jakości słuchawki oraz mikrofon (opcjonalnie) kamera internetowa

link do szkolenia zostanie przesłany uczestnikom przed szkoleniem i będzie aktywny do końca szkolenia.

Kontakt

Agata Tuliszka-Kamińska

E-mail a.kaminska@sages.com.pl
Telefon (+48) 530 612 226