Możliwość dofinansowania

Cybersecurity – podstawy testów bezpieczeństwa aplikacji i systemów IT

Numer usługi 2026/06/08/196109/3612828

2 950,77 PLN brutto
2 399,00 PLN netto
196,72 PLN brutto/h
159,93 PLN netto/h
261,33 PLN cena rynkowa

QUALITY ISLAND SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
15:00 h
06.08.2026 do 07.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery
Grupa docelowa usługi	Szkolenie skierowane jest do osób chcących zdobyć lub rozwinąć kompetencje w zakresie podstaw cyberbezpieczeństwa oraz testowania bezpieczeństwa aplikacji i systemów informatycznych. Usługa dedykowana jest w szczególności testerom oprogramowania, specjalistom QA, analitykom, programistom, administratorom systemów oraz osobom planującym rozwój kariery w branży IT. Program jest odpowiedni dla osób początkujących, które chcą poznać zagadnienia związane z bezpieczeństwem aplikacji i usług cyfrowych. Szkolenie ma charakter praktyczny i przygotowuje uczestników do samodzielnej identyfikacji podstawowych zagrożeń bezpieczeństwa, wykonywania podstawowych testów bezpieczeństwa oraz wykorzystywania narzędzi wspierających analizę podatności systemów informatycznych. Usługa również adresowana dla Uczestników Projektu MP i/lub dla Uczestników Projektu NSE.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	31-07-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestników do samodzielnego identyfikowania podstawowych zagrożeń bezpieczeństwa oraz wykonywania podstawowych testów bezpieczeństwa aplikacji i systemów informatycznych. Uczestnik po zakończeniu usługi potrafi rozpoznawać najczęściej występujące podatności, analizować ryzyka bezpieczeństwa oraz wykorzystywać wybrane narzędzia wspierające ocenę bezpieczeństwa oprogramowania.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza Uczestnik: rozumie podstawowe pojęcia związane z cyberbezpieczeństwem, zna najczęściej występujące zagrożenia bezpieczeństwa aplikacji i systemów IT, rozumie znaczenie testów bezpieczeństwa w procesie zapewnienia jakości oprogramowania, zna podstawowe metody identyfikacji podatności i ryzyk bezpieczeństwa. Umiejętności Uczestnik: identyfikuje podstawowe zagrożenia bezpieczeństwa w aplikacjach i systemach, analizuje potencjalne ryzyka związane z bezpieczeństwem oprogramowania, wykorzystuje narzędzia wspierające podstawowe testy bezpieczeństwa, interpretuje wyniki analiz i testów bezpieczeństwa, dokumentuje wykryte problemy oraz rekomendacje działań naprawczych. Kompetencje społeczne Uczestnik: samodzielnie wykonuje podstawowe zadania związane z analizą bezpieczeństwa aplikacji, stosuje dobre praktyki bezpieczeństwa podczas pracy z oprogramowaniem, współpracuje z zespołem projektowym w zakresie identyfikacji zagrożeń i ryzyk, rozwija kompetencje niezbędne do dalszego rozwoju zawodowego w obszarze cyberbezpieczeństwa.	Weryfikacja efektów uczenia się odbywa się poprzez obserwację uczestnika podczas wykonywania zadań praktycznych związanych z identyfikacją zagrożeń bezpieczeństwa oraz analizą podatności aplikacji i systemów informatycznych. Ocenie podlega w szczególności: poprawność identyfikowania podstawowych zagrożeń bezpieczeństwa w aplikacjach i systemach IT, umiejętność rozpoznawania podatności oraz potencjalnych ryzyk bezpieczeństwa, wykorzystanie narzędzi wspierających analizę bezpieczeństwa oprogramowania, poprawność interpretacji wyników testów i analiz bezpieczeństwa, umiejętność dokumentowania wykrytych problemów oraz formułowania rekomendacji działań naprawczych, stosowanie podstawowych zasad cyberbezpieczeństwa podczas wykonywania zadań praktycznych, samodzielność podczas realizacji ćwiczeń związanych z oceną bezpieczeństwa aplikacji i systemów, aktywny udział w warsztatach i zadaniach praktycznych realizowanych podczas szkolenia.	Obserwacja w warunkach rzeczywistych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Dzień 1

Moduł 1. Wprowadzenie do cyberbezpieczeństwa i roli testera w zapewnianiu bezpieczeństwa

- podstawowe pojęcia związane z cyberbezpieczeństwem,
- znaczenie bezpieczeństwa w procesie wytwarzania oprogramowania,
- rola testera w identyfikowaniu zagrożeń i podatności,
- najczęstsze zagrożenia występujące w systemach informatycznych.

Moduł 2. Podstawy komunikacji sieciowej i mechanizmów uwierzytelniania

- podstawowe zasady działania protokołu HTTP,
- wymiana danych pomiędzy aplikacjami i systemami,
- mechanizmy logowania i uwierzytelniania użytkowników,
- podstawowe zagrożenia związane z komunikacją sieciową.

Moduł 3. Najczęściej występujące podatności w aplikacjach internetowych

- charakterystyka najczęściej spotykanych podatności,
- zagrożenia związane z nieprawidłową obsługą danych użytkownika,
- przykłady podatności występujących w aplikacjach webowych,
- konsekwencje występowania podatności dla organizacji i użytkowników.

Moduł 4. Standardy bezpieczeństwa i OWASP Top 10

- wprowadzenie do standardów bezpieczeństwa aplikacji,
- omówienie najważniejszych kategorii ryzyka według OWASP,
- identyfikacja najczęściej występujących zagrożeń,
- dobre praktyki związane z bezpieczeństwem oprogramowania.

Dzień 2

Moduł 5. Narzędzia wspierające testowanie bezpieczeństwa

- przegląd narzędzi wykorzystywanych do analizy bezpieczeństwa,
- konfiguracja podstawowego środowiska testowego,
- wykorzystanie narzędzi do identyfikacji podatności,
- analiza wyników generowanych przez narzędzia.

Moduł 6. Praktyczne ćwiczenia z identyfikacji podatności

- wykonywanie podstawowych testów bezpieczeństwa,
- identyfikowanie podatności w aplikacjach,
- analiza potencjalnych zagrożeń,
- ćwiczenia praktyczne na przygotowanych przykładach.

Moduł 7. Analiza wyników i raportowanie podatności

- interpretacja wyników testów bezpieczeństwa,
- ocena poziomu ryzyka wykrytych problemów,
- dokumentowanie podatności i rekomendowanie działań naprawczych,
- przygotowanie raportów z przeprowadzonych testów.

Moduł 8. Wprowadzenie do testów penetracyjnych i podsumowanie szkolenia

- podstawowe informacje o testach penetracyjnych,
- znaczenie testów bezpieczeństwa w organizacjach,
- możliwości dalszego rozwoju kompetencji w obszarze cyberbezpieczeństwa,
- podsumowanie najważniejszych zagadnień.

Moduł 9. Walidacja efektów uczenia się

- wykonanie zadania praktycznego polegającego na identyfikacji zagrożeń i podatności,
- obserwacja uczestnika podczas realizacji ćwiczeń,
- analiza poprawności interpretacji wyników testów bezpieczeństwa,
- ocena umiejętności dokumentowania wykrytych problemów oraz formułowania rekomendacji działań naprawczych.

Harmonogram

Liczba pozycji harmonogramu: 13

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 Wprowadzenie do cyberbezpieczeństwa i roli testera w zapewnianiu bezpieczeństwa	Zajęcia	TOMASZ STELMACH	06-08-2026	08:00	09:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 13 Podstawy komunikacji sieciowej i mechanizmów uwierzytelniania	Zajęcia	TOMASZ STELMACH	06-08-2026	09:00	10:15	01:15
3 z 13 -	Przerwa	-	06-08-2026	10:15	10:45	00:30
4 z 13 Najczęściej występujące podatności w aplikacjach internetowych	Zajęcia	TOMASZ STELMACH	06-08-2026	10:45	12:30	01:45
5 z 13 -	Przerwa	-	06-08-2026	12:30	13:00	00:30
6 z 13 Standardy bezpieczeństwa i OWASP Top 10	Zajęcia	TOMASZ STELMACH	06-08-2026	13:00	15:00	02:00
7 z 13 Narzędzia wspierające testowanie bezpieczeństwa	Zajęcia	TOMASZ STELMACH	07-08-2026	08:00	09:30	01:30
8 z 13 -	Przerwa	-	07-08-2026	09:30	10:00	00:30
9 z 13 Praktyczne ćwiczenia z identyfikacji podatności	Zajęcia	TOMASZ STELMACH	07-08-2026	10:00	12:00	02:00
10 z 13 -	Przerwa	-	07-08-2026	12:00	12:30	00:30
11 z 13 Analiza wyników i raportowanie podatności	Zajęcia	TOMASZ STELMACH	07-08-2026	12:30	13:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 13 Wprowadzenie do testów penetracyjnych i podsumowanie szkolenia	Zajęcia	TOMASZ STELMACH	07-08-2026	13:30	14:45	01:15
13 z 13 -	Walidacja	-	07-08-2026	14:45	16:00	01:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	15:00
w tym suma godzin zajęć	11:45
w tym suma godzin walidacji	01:15
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	17:15

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 950,77 PLN
Koszt przypadający na 1 uczestnika netto	2 399,00 PLN
Koszt osobogodziny brutto	196,72 PLN

Koszt osobogodziny netto	159,93 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	15:00

Prowadzący

Liczba prowadzących: 1

1 z 1

TOMASZ STELMACH

Tomasz Stelmach to ekspert z ponad 15-letnim doświadczeniem w obszarze testowania oprogramowania, zapewnienia jakości oraz bezpieczeństwa aplikacji i systemów informatycznych. Jest założycielem i liderem firmy Quality Island, specjalizującej się w usługach QA, testach bezpieczeństwa oraz rozwoju kompetencji specjalistów IT.

W trakcie swojej kariery uczestniczył w realizacji projektów informatycznych dla organizacji z różnych branż, ze szczególnym uwzględnieniem sektora bankowego i finansowego. Pełnił role Testera Oprogramowania, Testera Automatyzującego, QA Leada, Kierownika Testów, Architekta Testów oraz Managera Testów. W swojej pracy odpowiadał za zapewnienie jakości i bezpieczeństwa systemów informatycznych, analizę ryzyk, identyfikację podatności oraz wdrażanie dobrych praktyk związanych z cyberbezpieczeństwem i ochroną danych.

Od wielu lat prowadzi szkolenia, warsztaty, konsultacje i audyty jakości, przygotowując uczestników do samodzielnego wykonywania zadań związanych z testowaniem oprogramowania oraz podstawami bezpieczeństwa aplikacji. W pracy szkoleniowej szczególny nacisk kładzie na praktyczne aspekty identyfikowania zagrożeń, analizę podatności oraz rozwijanie świadomości bezpieczeństwa w projektach IT.

Jest organizatorem Testing Ground Conference oraz prelegentem konferencji technologicznych, gdzie dzieli się wiedzą z zakresu jakości oprogramowania, testowania, cyberbezpieczeństwa oraz rozwoju kompetencji zawodowych w branży IT.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy szkolenia otrzymają materiały szkoleniowe w formie elektronicznej, obejmujące:

- checklistę wspierającą analizę bezpieczeństwa aplikacji i identyfikację najczęściej występujących podatności,
- materiały dotyczące kodów odpowiedzi HTTP wykorzystywanych podczas testowania aplikacji webowych i usług sieciowych,
- materiał wprowadzający do narzędzia OWASP ZAP wraz z przykładami jego wykorzystania podczas testów bezpieczeństwa,
- przykładowy raport z testów bezpieczeństwa prezentujący sposób dokumentowania wyników oraz zgłaszania wykrytych podatności,
- materiały edukacyjne dotyczące rodzajów ataków oraz najczęściej występujących podatności bezpieczeństwa w aplikacjach i systemach informatycznych,

- zestaw ćwiczeń praktycznych realizowanych podczas szkolenia.

Uczestnicy otrzymają również dostęp do materiałów wykorzystywanych podczas warsztatów praktycznych oraz przykładowych scenariuszy związanych z analizą bezpieczeństwa aplikacji i systemów IT.

Informacje dodatkowe

Usługa dostępna dla uczestników projektu „Małopolski Pociąg do Kariery – sezon 1” oraz „Nowy Start w Małopolsce z EURESem”. Realizacja możliwa z wykorzystaniem bonów szkoleniowych zgodnie z zasadami projektu.

Warunki techniczne

Usługa realizowana będzie w formie zdalnej w czasie rzeczywistym z wykorzystaniem platformy szkoleniowej ClickMeeting.

Uczestnik powinien dysponować:

- komputerem lub laptopem wyposażonym w mikrofon oraz głośniki lub słuchawki,
- stabilnym dostępem do Internetu,
- aktualną przeglądarką internetową (Google Chrome, Microsoft Edge, Mozilla Firefox lub równoważną),
- aktywnym adresem e-mail umożliwiającym otrzymywanie materiałów szkoleniowych oraz informacji organizacyjnych.

Ze względu na praktyczny charakter szkolenia uczestnik powinien posiadać możliwość instalacji bezpłatnego oprogramowania wykorzystywanego podczas zajęć, w szczególności:

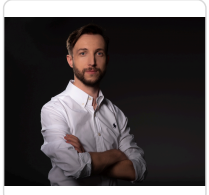
- narzędzia OWASP ZAP lub równoważnego oprogramowania wspierającego analizę bezpieczeństwa aplikacji,
- przeglądarki internetowej umożliwiającej wykonywanie ćwiczeń praktycznych,
- oprogramowania umożliwiającego korzystanie z materiałów szkoleniowych udostępnianych przez trenera.

Przed rozpoczęciem szkolenia uczestnicy otrzymają:

- link do platformy szkoleniowej ClickMeeting,
- instrukcję logowania i udziału w zajęciach,
- informacje organizacyjne dotyczące realizacji usługi,
- listę niezbędnego oprogramowania wykorzystywanego podczas warsztatów praktycznych,
- dostęp do materiałów szkoleniowych w formie elektronicznej.

Uczestnik powinien posiadać podstawowe umiejętności obsługi komputera oraz możliwość aktywnego udziału w ćwiczeniach praktycznych związanych z identyfikacją zagrożeń, analizą podatności oraz oceną bezpieczeństwa aplikacji i systemów informatycznych.

Kontakt



TOMASZ STELMACH

E-mail tomaszstelmach@qualityisland.pl
Telefon (+48) 532 417 054