# Usługa - Szkolenie z Cyberbezpieczeństwa: Szkolenie dla programistów: Programowanie Defensywne

0/5

## Szkolenie z Cyberbezpieczeństwa: Szkolenie dla programistów: Programowanie Defensywne

Numer usługi: 2023/01/24/148153/1669748

Dostawca usług: Niebezpiecznik.pl Piotr Konieczny

Dostępność: Usługa otwarta

Forma świadczenia: zdalna w czasie rzeczywistym

Status usługi: opublikowana

Identyfikator projektu: Sektor IT

PLN

1 199,00 zł netto za osobę
1 474,77 zł brutto za osobę
149,88 zł netto za osobogodzinę
184,35 zł brutto za osobogodzinę

| Rodzaj | Kategoria / Podkategoria | Dofinansowanie | |
|---|---|---|---|
| Usługa szkoleniowa | Informatyka i telekomunikacja / Bezpieczeństwo IT | Tak | 05.07.2023 |

### Informacje o usłudze

| | |
|---|---|
| Sposób dofinansowania: | wsparcie dla osób indywidualnych<br>wsparcie dla przedsiębiorców i ich pracowników |
| Grupa docelowa usługi: | Szkolenie kierujemy przede wszystkim do programistów, raczej tych na początku kariery, zwłaszcza tych co jeszcze nie mieli zbyt wielu okazji programować defensywnie.<br>• programistów Java, JavaScript, Python (w tych językach mamy przykłady), chociaż programiści innych języków odkryją, że zasada jest ta sama.<br>• testerów automatycznych, AQAów, SDETów<br>• audytorów i pentesterów,<br>...ale tak naprawdę, z otwartymi rękami powitamy każdą osobę która chce podnosić swoje kwalifikacje i wiedzę w temacie defensywnego programowania bo co człowiek robi a jakie ma stanowisko to nie zawsze się pokrywa. :-) |
| Minimalna liczba uczestników: | 6 |
| Maksymalna liczba uczestników: | 20 |
| Data zakończenia rekrutacji: | 27-06-2023 |
| Liczba godzin usługi: | 8 |
| Podstawa uzyskania wpisu do świadczenia usługi: | Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0 |

### Ramowy program usługi

**Wstęp do programowania defensywnego**

- co to jest programowanie defensywne i czemu powinniśmy je praktykować
- defensywa w kodzie, w zależnościach, w infrastrukturze – cały łańcuch

- gdzie znajdziesz więcej informacji

Defensywne programowanie

- asercje, wyjątki, logowanie
- kontrakty i ochrona API
- czego w języku unikać i jak to można naprawić
- testy i scenariusze testowe
- jak i co zautomatyzować, narzędzia
- ochrona wbudowana w API i kodowanie

Defensywne budowanie oprogramowania i pomocne narzędzia

- narzędzia do budowy, CI, CD – gdzie co wpinamy
- stare zależności, dziurawe zależności
- domyślne konfiguracje
- jak i co zautomatyzować, narzędzia
- REST i jego ochrona
- obrazy Dockera i ich zabezpieczanie
- bezpiecznika recenzja kodu
- wyciek sekretów po fakcie

---

Harmonogram usługi

| Przedmiot / temat zajęć | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|
| Wstęp do programowania defensywnego | 05-07-2023 | 10:00 | 12:00 | 02:00 |
| Defensywne programowanie | 05-07-2023 | 12:00 | 15:00 | 03:00 |
| Defensywne budowanie oprogramowania i pomocne narzędzia | 05-07-2023 | 15:00 | 18:00 | 03:00 |

---

Główny cel usługi

Cel edukacyjny

Głównym celem szkolenia jest dostarczenie oraz poprawienie kompetencji uczestnika z zakresu Programowania Defensywnego. Po zakończonym szkoleniu uczestnik podniesie poziom bezpieczeństwa w swojej firmie oraz rozwiąże najczęściej pojawiające się problemy, samodzielnie realizując metody rozwiązania na poziomie zaawansowanym, z maksymalnym wykorzystaniem swoich nowo nabytych umiejętności.

Efekty uczenia się

Dzięki temu szkoleniu…

poznasz podstawy SAST,
zabezpieczysz kod, przerobisz zbyt ufnie napisane programy,
napiszesz kod, który zostanie zrecenzowany,
prześwietlisz projekt, dowiesz się, czy jest bezpieczny lub nie,
nauczysz się recenzować kod (obronność),
nauczysz się korzystać z narzędzi do czystego kodu, automatyzacji sprawdzeń oraz analizy statycznej,
poznasz zautomatyzację defensywną programowania i wbudowanie w cykl tworzenia programów
sam uszczelnisz aplikację: w kodzie, w konfiguracji...

Nasze szkolenie posiada unikatową formułę: **minimum teorii, maksimum praktyki**. Każde z omawianych zagadnień poprzedzamy teoretycznym wstępem oraz demonstracją ataku w wykonaniu trenera, ale główny nacisk kładziemy na **ćwiczenia praktyczne** wykonywane przez uczestników.

Ćwiczeniom praktycznym poświecamy najwięcej czasu, ponieważ pozwalają każdemu uczestnikowi szkolenia **własnoręcznie przeprowadzić omawiany atak**. Podczas szkolenia do dyspozycji uczestników oddajemy sieć laboratoryjną, w której znajdują się specjalnie przygotowane webaplikacje, wykorzystujące spotykane w rzeczywistym świecie oprogramowanie (wraz z występującymi w nim dziurami).

Dlaczego stawiamy na praktykę? Bo sama teoria w bezpieczeństwie nie wystarcza.

> powiedz mi, a zapomnę, pokaż — a zapamiętam, pozwól mi działać, a zrozumiem!

Po naszym szkoleniu będziesz naprawdę zmęczony, ale uwierz nam, że zamiast o odejściu od komputera będziesz myślał wyłącznie o tym, jak dalej pogłębiać swoją wiedze.

Sposób weryfikacji osiągnięcia efektów uczenia się

Test wiedzy przesyłany do Uczestników przed i po szkoleniu.

| | |
|---|---|
| Czy usługa prowadzi do nabycia kompetencji? | Tak |

## Kwalifikacje

Brak wyników.

## Cena

| | |
|---|---|
| Koszt przypadający na 1 uczestnika netto | 1 199,00 zł |
| Koszt przypadający na 1 uczestnika brutto | 1 474,77 zł |
| Koszt osobogodziny netto | 149,88 zł |
| Koszt osobogodziny brutto | 184,35 zł |

## Zajęcia poprowadzą

Tomasz Borek

W ramach firmy Niebezpiecznik.pl szkolę z zakresu Programowania Defensywnego (mój własny autorski program, z którym przyszedłem do Niebezpiecznika), Ataków i Ochrony Aplikacji Sieciowych oraz Bezpieczeństwa w Testach dla QA.

## Kontakt

Magda Kowalska
email: szkolenia@niebezpiecznik.pl
tel: (+48) 124 420 244

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

1. Materiały szkoleniowe (drukowany podręcznik z prezentacją).

2. Nielimitowany, wieczysty dostęp do serwera na którym znajdują się stale aktualizowane, przydatne informacje i narzędzia dotyczące tematyki szkolenia

Warunki uczestnictwa

**Każdy** uczestnik naszych szkoleń **musi** podpisać deklarację, że poznane ataki i narzędzia będzie wykorzystywał zgodnie z prawem.

Szkolenie odbywa się w formule BYOL (Bring Your Own Laptop). Wymagania: 2GB RAM, 5GB HDD.

Uczestnik tego szkolenia powinien:

1. Znać podstawy linii poleceń (zwłaszcza Linuksa, bo w ramach laboratoriów trzeba będzie modyfikować pliki konfiguracyjne, budować oprogramowanie, uruchamiać kontenery Dockera czy skrypty z parametrami lub zmieniać atrybuty plików)
2. Znać choć jeden język programowania z 3 użytych na szkoleniu: Java, Python, JavaScript, by móc przeczytać kod laboratoriów ze zrozumieniem, dodać lub zmienić potrzebne funkcje.
3. Znać podstawy Dockera: jak pobrać obraz, podstawy .Dockerfile, jak z obrazu zrobić kontener, start kontenera, podpięcie terminala do działającego kontenera.
4. Znać jedno z użytych narzędzi budowy: Maven, pip, npm w podstawowym zakresie: używać podstawowych komend i być w stanie czytać i modyfikować pliki konfiguracyjne wybranego narzędzia.

Informacje dodatkowe

https://niebezpiecznik.pl/szkolenia/programowanie-defensywne-szkolenie/?zai

---

Warunki techniczne

Warunki techniczne

Szkolenie prowadzone jest poprzez platformę ZOOM, Uczestnik dostaje zaproszenie do spotkania.