Możliwość dofinansowania

Szkolenie - OSINT w praktyce

Numer usługi 2026/02/17/165578/3341383

7 000,00 PLN brutto
7 000,00 PLN netto
250,00 PLN brutto/h
250,00 PLN netto/h
196,00 PLN cena rynkowa

LABA POLSKA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

zdalna w czasie rzeczywistym
Usługa szkoleniowa
28 h
09.04.2026 do 28.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Zachodniopomorskie Bony Szkoleniowe, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Kierunek - Rozwój

Grupa docelowa usługi	• **Przedsiębiorcy** – zainteresowani monitorowaniem wycieków danych i ograniczaniem zagrożeń cyberbezpieczeństwa w organizacji.
	• **Junior security managerowie** – chcący identyfikować słabe punkty organizacji, analizować ryzyko i wykorzystywać informacje pozyskane metodami OSINT do poprawy bezpieczeństwa.
	• **Dziennikarze, badacze i analitycy rynku** – pozyskujący i weryfikujący informacje śledcze, analizujący dane rynkowe oraz korzystający z legalnych źródeł publicznych.
	• **Prawnicy, komornicy i urzędnicy** – potrzebujący narzędzi do lokalizowania dłużników oraz potwierdzania wiarygodności osób, stron postępowań i świadków.
	
	Szkolenie kierowane jest też do uczestników projektów:
	
	• „**Zachodniopomorskie Bony Szkoleniowe**” realizowanego przez WUP w Szczecinie,
	  • „**MP**” oraz „**NSE**” realizowanych przez WUP w Krakowie,
	  • „**Kierunek – Rozwój**” realizowanego przez WUP Toruń.
	  • oraz innych projektów współfinansowanych ze środków publicznych.

Minimalna liczba uczestników	10
Maksymalna liczba uczestników	50
Data zakończenia rekrutacji	06-04-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

Liczba godzin usługi	28
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

Celem usługi jest przygotowanie uczestnika do planowania, realizowania i oceny procesu pozyskiwania oraz analizy informacji metodami OSINT, z uwzględnieniem zasad bezpieczeństwa operacyjnego, aspektów prawnych oraz opracowywania raportów analitycznych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje cykl wywiadowczy oraz etapy procesu OSINT.	Opisuje kolejne etapy procesu; wyjaśnia ich znaczenie; uzasadnia kolejność działań w analizowanym przypadku.	Test teoretyczny
Definiuje zasady bezpieczeństwa operacyjnego (OPSEC) w działaniach OSINT.	Wskazuje zagrożenia operacyjne; uzasadnia dobór środków zabezpieczających; opisuje konsekwencje braku zabezpieczeń.	Test teoretyczny
Planuje proces pozyskiwania informacji w oparciu o przedstawione studium przypadku.	Określa cel operacyjny; dobiera źródła informacji; uzasadnia wybór narzędzi.	Test teoretyczny
Analizuje dane pozyskane z otwartych źródeł i formułuje wnioski operacyjne.	Selekcjonuje informacje; ocenia ich wiarygodność; wyciąga logiczne wnioski.	Test teoretyczny
Projektuje strukturę raportu OSINT adekwatną do celu analizy.	Określa elementy raportu; uzasadnia sposób prezentacji danych; wskazuje sposób wizualizacji.	Test teoretyczny
Ocenia możliwości wykorzystania automatyzacji i AI w procesie OSINT.	Identyfikuje obszary automatyzacji; analizuje ryzyka; wskazuje ograniczenia technologiczne.	Test teoretyczny
Ocenia działania OSINT z uwzględnieniem aspektów prawnych i etycznych.	Wskazuje granice legalności; uzasadnia wybór działań zgodnych z prawem; analizuje ryzyko nadużyć.	Test teoretyczny
Przyjmuje odpowiedzialność za rzetelność i bezpieczeństwo pozyskiwanych informacji.	Formułuje rekomendacje minimalizujące ryzyko; wskazuje konsekwencje błędnych decyzji.	Test teoretyczny

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

W celu skutecznego uczestnictwa w szkoleniu wymagane jest zainteresowanie tematyką OSINT, analizy informacji oraz cyberbezpieczeństwa.

Za 1 godzinę usługi szkoleniowej uznaje się godzinę zegarową (60 minut). Szkolenie przeprowadzone będzie w formie zdalnej w czasie rzeczywistym w liczbie 28 godzin zegarowych. Zajęcia prowadzone są w krótkich modułach niewymagających stosowania przerw.

Każdy uczestnik musi posiadać dostęp do komputera z Internetem. Uczestnikom przed zajęciami zostanie przesłany link do wideokonferencji na platformie Zoom.

Program szkolenia dostosowany jest do potrzeb osób pracujących z informacją, bezpieczeństwem oraz analizą danych i koncentruje się na praktycznych zastosowaniach metod OSINT w pozyskiwaniu i weryfikacji informacji. Szkolenie obejmuje zarówno materiał teoretyczny, jak i praktyczne zadania warsztatowe.

Warunki organizacyjne: realizacja zadań będzie przeprowadzona w taki sposób, aby stopniowo narastał ich stopień trudności, ale ich realizacja była w zasięgu możliwości uczestników. Szkolenie, poprzez swój zakres tematyczny oraz część praktyczną realizowaną w trybie zadaniowym, wpłynie pozytywnie na poziom kompetencji uczestnika w obszarze OSINT.

Podczas części teoretycznej uczestnicy będą słuchać wykładu oraz analizować studia przypadków. Część praktyczna odbędzie się w formie zadań opracowywanych przez kursanta pod kierunkiem wykładowcy.

- Liczba godzin teoretycznych – 14
- Liczba godzin praktycznych – 13,5
- Walidacja – 0,5

Organizator zapewnia następujące materiały dydaktyczne: Templatki / wzory, Prezentacje

PLAN ZAJĘĆ

Zajęcia 1. Cykl wywiadowczy

- - Faza planowania i wymagań
  - Faza gromadzenia
  - Faza przetwarzania i oceny
  - Faza analizy i produkcji
  - Raportowanie

- Faza rozpowszechniania i konsumpcji
- Aspekty prawne działalności OSINT

Zajęcia 2. OPSEC – tworzenie bezpiecznego środowiska pracy Analityka OSINT

- Anonimizacja i ukrywanie aktywności w sieci
- Warsztaty

Zajęcia 3. Wywiad podmiotowy

- Cyfrowy ślad
- Metody zaawansowanego wyszukiwania informacji w wyszukiwarkach typu Google, Yandex, Baidu, Yahoo, Brave, DuckDuckGo
- Google hacking (operatory precyzyjnych wyszukiwań)
- Rozszerzenia do przeglądarek

Zajęcia 4. Wyszukiwanie i analiza informacji technicznych

- Adresy IP i domeny
- Analiza wiadomości e-mail
- Sieci bezprzewodowe
- Analiza plików i ich metadanych
- Wycieki danych
- Geolokalizacja – wyodrębnianie informacji z metadanych dokumentów i plików graficznych; weryfikacja faktów na podstawie nagrań wideo lub z kamer; możliwości identyfikacji miejsc na podstawie cech geomorfologicznych
- Warsztaty

Zajęcia 5. „Sock puppet" – fikcyjne konta w portalach

- Fikcyjne konta w portalach – tworzenie i analiza
- Warsztaty

Zajęcia 6. SOCMINT i narzędzia do analizy mediów społecznościowych

- Twitter
- Facebook
- LinkedIn
- Pozyskiwanie informacji z: Telegrama, VKontakte, Baidu
- Warsztaty

Zajęcia 7. Zaawansowane narzędzia do wyszukiwania i analizy adresów e-mail – warsztaty

- Prezentacja narzędzi
- Warsztaty

Zajęcia 8. Sieć TOR i Darknet

- Przeglądarka TOR – zasada działania
- Wyjaśnienie pojęcia deep web i dark web
- Zasady bezpiecznego poruszania się po sieci darknet

Zajęcia 9. Analiza powiązań podmiotów polskich z zagranicznymi

- Specyfika polskiego Internetu i źródeł z których można legalnie uzyskać informacje o osobach fizycznych i prawnych (rejestr CEiDG, rejestr KRS, SUDOP, Rejestr.io)

Zajęcia 10. Wyszukiwanie informacji gospodarczych w zagranicznych bazach danych

- Gdzie szukać zagranicznych informacji gospodarczych?
- Jak korzystać z zagranicznych rejestrów?
- Specyfika wyszukiwania w otwartych źródłach z uwzględnieniem rosyjskiego i chińskiego Internetu

Zajęcia 11. CSI Linux

- Zapoznanie z systemem CSI Linux
- Wyszukiwanie informacji za pomocą narzędzi systemowych CSI Linux
- Generowanie raportu
- Instalacja dodatkowych narzędzi OSINT w systemie CSI Linux

Zajęcia 12. Kali Linux i zaawansowane narzędzia OSINT

- Zapoznanie z systemem Kali Linux
- Podstawowe komendy w terminalu
- Instalacja narzędzi OSINT w Kali Linux

Zajęcia 13. Budowanie raportu oraz graficzne przedstawienie danych

- Budowanie raportu – plan i realizacja
- Prezentacja zebranych danych – raport i wersja graficzna
- Zadanie egzaminacyjne – projekt końcowy

Zajęcia 14. Automatyzacja OSINT i AI. Automatyzacja technik OSINT i prezentacja projektów

- Szukanie informacji w sposób zautomatyzowany
- Chat GPT na usługach OSINT
- Gotowe skrypty

Walidacja końcowa ma formę testu teoretycznego w postaci zadań otwartych. Obejmuje analizę studium przypadku z obszaru pozyskiwania i analizy informacji metodami OSINT oraz rozwiązanie zadań problemowych odnoszących się do przedstawionej sytuacji operacyjnej. Walidacja trwa 30 minut i realizowana jest w ramach czasu trwania usługi rozwojowej (ostatnie 30 minut ostatnich zajęć). Walidacja przeprowadzana jest w oparciu o wcześniej zdefiniowane kryteria weryfikacji efektów uczenia się i przeprowadzana przez osobę inną niż prowadząca szkolenie, co zapewnia rozdzielenie procesu kształcenia od procesu walidacji.

Zadania realizowane w trakcie zajęć mają charakter ćwiczeniowy i nie stanowią elementu walidacji efektów uczenia się. Po zakończeniu udziału w usłudze rozwojowej, uczestnik otrzymuje odpowiednie zaświadczenie o jej ukończeniu. Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej oraz zaliczenie walidacji efektów uczenia się.

Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Cykl wywiadowczy	Piotr Oleksiak	09-04-2026	18:30	20:30	02:00
2 z 15 OPSEC	Piotr Oleksiak	14-04-2026	18:30	20:30	02:00
3 z 15 Wywiad podmiotowy	Piotr Oleksiak	16-04-2026	18:30	20:30	02:00
4 z 15 Wyszukiwanie i analiza informacji technicznych	Piotr Oleksiak	21-04-2026	18:30	20:30	02:00
5 z 15 Sock puppet	Piotr Oleksiak	23-04-2026	18:30	20:30	02:00
6 z 15 SOCMINT	Piotr Oleksiak	28-04-2026	18:30	20:30	02:00
7 z 15 Analiza e-mail	Piotr Oleksiak	05-05-2026	18:30	20:30	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 15 TOR i Darknet	Piotr Oleksiak	07-05-2026	18:30	20:30	02:00
9 z 15 Analiza powiązań	Piotr Oleksiak	12-05-2026	18:30	20:30	02:00
10 z 15 Bazy zagraniczne	Piotr Oleksiak	14-05-2026	18:30	20:30	02:00
11 z 15 CSI Linux	Piotr Oleksiak	19-05-2026	18:30	20:30	02:00
12 z 15 Kali Linux	Piotr Oleksiak	21-05-2026	18:30	20:30	02:00
13 z 15 Budowanie raportu	Piotr Oleksiak	26-05-2026	18:30	20:30	02:00
14 z 15 Automatyzacja OSINT i AI	Piotr Oleksiak	28-05-2026	18:30	20:00	01:30
15 z 15 Walidacja	-	28-05-2026	20:00	20:30	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 000,00 PLN
Koszt przypadający na 1 uczestnika netto	7 000,00 PLN
Koszt osobogodziny brutto	250,00 PLN
Koszt osobogodziny netto	250,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Piotr Oleksiak

• Prezes agencji detektywistycznej HIIT Group oraz założyciel i prezes Fundacji CIIG – Cyber Intelligence and Investigation Group. Pomaga przedsiębiorcom w zabezpieczaniu biznesów i transakcji.
• Był operator HUMINT; pełnił funkcję przewodniczącego Sekcji Bezpieczeństwa w Przedsiębiorcy.pl. Jest laureatem Orłów Polskiej Przedsiębiorczości w dziedzinie usług detektywistycznych i wywiadowczych.
• Posiada kobaltową odznakę ATII za deanonimizację przestępców w Darknecie oraz jest certyfikowanym śledczym kryptowalut (CCI) i OSINT Coachem – Search Party CTF.
• Na kursie prezentuje praktyczne umiejętności wyszukiwania informacji z różnych źródeł publicznych, konfiguracji systemów pod kątem bezpieczeństwa oraz zastosowania narzędzi takich jak Google Dorks i techniki Google Hacking.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnikom zostaną przekazane materiały dydaktyczne w postaci:

- Templatki/ wzory
- prezentacje

Warunki uczestnictwa

Usługa nie przewiduje formalnych wymagań wstępnych; rekomendowana jest osobom zainteresowanym tematyką OSINT, analizą informacji oraz cyberbezpieczeństwem. Wymagana jest podstawowa znajomość obsługi komputera i Internetu.

Informacje dodatkowe

Uczestnik, dokonując zapisu na usługę, oświadcza, że usługa rozwojowa odbywa się poza godzinami pracy lub w dni wolne od pracy osoby biorącej udział w usłudze.

Organizator zapewnia dostępność osobom ze szczególnymi potrzebami podczas realizacji usług rozwojowych zgodnie z Ustawą z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz.U. 2022 poz. 2240) oraz „Standardami dostępności dla polityki spójności 2021-2027”. W przypadku potrzeby zapewnienia specjalnych udogodnień prosimy o kontakt pod numerem +48 739-270-704 lub mailem: olga.lackorzynska@l-a-b-a.pl przed zapisem na usługę.

Zawarto umowy z Wojewódzkimi Urzędami Pracy w:

- - Szczecinie w ramach projektu „**Zachodniopomorskie Bony Szkoleniowe**”.
  - Krakowie w ramach projektów „**Małopolski Pociąg do kariery**” i „**Nowy start w Małopolsce z EURESEM**”.
  - Toruniu w ramach projektu "**Kierunek – Rozwój".**

Warunki techniczne

Forma zdalna usługi w czasie rzeczywistym. Szkolenie prowadzone jest za pośrednictwem platformy Zoom. Dołączenie następuje poprzez kliknięcie w link wysłany uczestnikowi przed kursem oraz zalogowanie się i wpisanie imienia i nazwiska. Ważność linku - od rozpoczęcia szkolenia do jego zakończenia zgodnie z harmonogramem w karcie.

W celu prawidłowego i pełnego korzystania z usługi, uczestnik powinien dysponować:

Sprzęt i oprogramowanie: Komputer/laptop z systemem: Windows 10/11 64-bit **lub** macOS 10.14+ (Mojave) do 11+ (Big Sur)

Dodatkowe zalecenia: Stabilne połączenie internetowe. Urządzenie uczestnika powinno być wyposażone w **mikrofon oraz kamerę**, co zapewnia możliwość dwustronnej komunikacji i właściwego nadzoru nad przebiegiem usługi.

Kontakt

OLGA LACKORZYŃSKA

E-mail olga.lackorzynska@l-a-b-a.pl

Telefon (+48) 739 270 704