Załącznik nr 1.2 do SWZ

Nr wew. postępowania 74/22

**Szczegółowy opis przedmiotu zamówienia**

**Szkolenia realizowane w ramach Projektu pt.: „Skuteczni w działaniu – współpraca służb w sytuacjach zagrożenia infrastruktury krytycznej” o nr PL/2020/PR/0080 dofinansowanego z Funduszy Bezpieczeństwa Wewnętrznego na podstawie Porozumienia finansowego nr 80/PL/2020/FBW**

1. **Opis przedmiotu zamówienia**

Przeprowadzenie szkolenia w formule Online z zakresu OSINT (Open Source Intelligence) na poziomie średnio-zaawansowanym dla 6 osób w ramach projektu pt. „Skuteczni w działaniu – współpraca służb w sytuacjach zagrożenia infrastruktury krytycznej” współfinansowanego z Funduszu Bezpieczeństwa Wewnętrznego
(nr 80/PL/2020/FBW).

1. **Odbiorcy szkolenia**

Szkolenie przeznaczone jest dla 6 (sześciu) pracowników i funkcjonariuszy – specjalistów z zakresu zwalczania cyberprzestępczości. Uczestnikami szkolenia będzie łącznie 6 osób w ramach jednej grupy szkoleniowej.

1. **Wymagania ogólne dotyczące realizacji szkolenia**
2. Wykonawca szkolenia zapewni dla każdego uczestnika dostęp do platformy szkoleniowej do komunikacji audio/video dającej możliwość przeprowadzenia na żywo, przy użyciu sieci Internet, zajęć teoretycznych i praktycznych z możliwością udostępniania obrazu z pulpitu zarówno przez prowadzących, jak i uczestników. Indywidualne stanowiska robocze (komputery kursantów) zostaną zapewnione przez Zamawiającego.
3. Wykonawca przeprowadzi szkolenie w języku polskim.
4. Szkolenie odbędzie się w ramach jednej grupy szkoleniowej.
5. Wykonawca w uzgodnieniu z Zamawiającym wyznaczy termin realizacji szkolenia.
6. Szkolenie musi obejmować 2 kolejne dni robocze, łącznie 14 godzin szkoleniowych.
7. Każdy dzień szkoleniowy to min. 7 godzin zegarowych. Dokładny harmonogram dzienny szkolenia zostanie uzgodniony z Wykonawcą w ramach kontaktów roboczych.
8. Wykonawca zapewnia materiały szkoleniowe odpowiednie dla tematyki szkolenia
dla każdego z uczestników szkolenia. Materiały szkoleniowe muszą być przygotowane w języku polskim. Materiały szkoleniowe mogą być w formie papierowej lub w formie elektronicznej. Koszty opracowania, powielenia i transportu materiałów szkoleniowych ponosi Wykonawca. Wykonawca ponosi pełną odpowiedzialność za zgodność merytoryczną oraz aktualność przekazywanych danych/informacji w materiałach szkoleniowych.
9. Uczestnicy otrzymają imienne certyfikaty ukończenia szkolenia.
10. **Zakres merytoryczny szkolenia**

Zakres merytoryczny szkolenia musi obejmować następujące elementy:

* Podstawy prawne białego wywiadu
* Genealogia białego wywiadu
* Różnice w wywiadzie : białym, szarym i czarnym
* Anatomia internetowej sieci społecznościowej
* Inżynieria społeczna i phishing
* Kradzież tożsamości
* Cyberstalking
* Hackowanie kont
* Cykl życia białego wywiadu (OSINT)
	+ Planowanie i kierunek
	+ Kolekcja danych
	+ Przetwarzanie danych
	+ Analiza danych
	+ Udostępnienie wyników
	+ Informacja zwrotna
* Anonimizacja i ukrywanie aktywności
* Wyszukiwarki internetowe na usługach OSINT-u
* Wyszukiwanie i analiza informacji technicznych
* Środowisko pracy OSINT
	+ Internetowe analizy dowodów
	+ Znacznik adresu domeny i adresu IP
	+ Osoby i kontakty Narzędzia do wyszukiwania
	+ Image / Video / Maps Wyszukiwanie narzędzi
	+ Narzędzia Online/offline
	+ Narzędzia do wizualizacji
	+ Pamięć analityczna
	+ Śledzenie odwiedzin w sieciach społecznościowych
	+ Narzędzia analityczne
	+ Wyszukiwarki firm i osób
	+ Narzędzia wywiadu gospodarczego
	+ Narzędzia do wyodrębniania metadanych
	+ Geolokalizacja rozpracowywanego celu
	+ Mapowanie sieci społecznościowych
	+ Systemy analizy zabezpieczeń w Social Media
* Budowa profilu internetowego
	+ Jak się ukryć w Internecie
	+ Anonimowa rejestracja usług
	+ Płatności za usługi w OSINT
	+ Bezpieczeństwo - zasady ogólne
	+ Budowa operacyjnych kont tożsamości
	+ Zdjęcia do profili i nowe dane
	+ Wtyczki i rozszerzenia do przeglądarek
* Metody i techniki gromadzenia informacji
* Wyszukiwarki Internetowe i mechanika witryny WWW
* Deep Web i Darknet
* Budowa adresów URL oraz nazwy domen
* Metadane - Informacje podstawowe
* SOCMINT - badanie sieci społecznościowych
* Wyszukiwanie archiwalnych i usuniętych stron
* Wyszukiwanie na podstawie zdjęcia
* Praca z Wyszukiwarkami
* Google Hacking
* Analiza wiadomości -email
* Wyciąganie informacji z obrazu i filmu
* Analiza plików tekstowych
* Geolokalizacja
* Tryby prywatne
* Wywiad gospodarczy i badanie firm
* Automatyzacja pracy w OSINT
* Metody zabezpieczania materiału dowodowego z sieci
* Tworzenie raportów ze śledztw OSINT