Załącznik nr 3 do SWZ
Załącznik nr 1 do umowy

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA
USŁUGA SPOŁECZNA

Zadanie nr 3

1) Opis przedmiotu zamówienia

Przeprowadzenie szkolenia EC-Council - CEH - CertifiedEthical Hacker w wersji najbardziej aktualnej na dzień rozpoczęcia szkoleniawraz wydaniem vouchera na egzamin certyfikacyjny dla 9 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).

2) Szczegóły szkolenia

Przeprowadzenie szkolenia przygotowującego do egzaminu CEH(tm) – CertifiedEthicalHacker w wersji najbardziej aktualnej na dzień rozpoczęcia szkoleniawraz z voucherem na egzamin certyfikacyjny EC-Council - CEH ważnym min. 3 miesiące po zakończeniu szkolenia;

3) Odbiorcy szkolenia

Szkolenie przeznaczone jest dla 9 specjalistów i praktyków z zakresu informatyki śledczej oraz Cyberbezpieczeństwa z Wydziałów terenowych Centralnego Biura Zwalczania Cyberprzestepczości. Uczestnikami szkolenia będzie łącznie 9 osób w ramach jednej grupy szkoleniowej.

4) Wymagania ogólne dotyczące realizacji szkolenia

a) Szkolenie musi zostać przeprowadzone w oparciu o akredytowane materiały szkoleniowe EC-Council
b) Szkolenie musi być akredytowane przez organizację EC-Council, prowadzone przez trenera z użyciem materiałów i środowiska szkoleniowego dostarczanego przez EC-Council.
c) 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.
d) Wykonawca przeprowadzi szkolenie w języku polskim.
e) Wykonawca w uzgodnieniu z Zamawiającym wyznaczy termin realizacji szkolenia.
f) Szkolenie musi obejmować 5 kolejnych dni roboczych od poniedziałku do piątku.
g) Każdy dzień szkoleniowy to 7 godzin zegarowych. Dokładny harmonogram dzienny dla poszczególnych modułów zostanie uzgodniony z Wykonawcą w ramach kontaktów roboczych.
h) Wykonawca zapewni akredytowane materiały szkoleniowe EC-Councilodpowiednie dla tematyki szkolenia, dla każdego z uczestników szkolenia. Materiały szkoleniowe muszą być przygotowane w języku polskim lub angielskim. 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.

i) Uczestnicy otrzymają imienne certyfikaty ukończenia szkolenia, sygnowane przez firmę EC-Council.
j) Certyfikaty, o których mowa powyżej, muszą zawierać informację o ukończeniu akredytowanego szkolenia EC-Council oraz oznaczenia wskazujące na finansowanie ze środków FBW w ramach Projektu (Zamawiający przekaże Wykonawcy niezbędne pliki graficzne).
k) Po zakończeniu szkolenia Wykonawca zobowiązuje się do przekazania uczestnikom szkolenia imiennych voucherów na egzaminy certyfikacyjneEC-Council– CEHw wersji najbardziej aktualnej na dzień rozpoczęcia szkolenia.

5) Zakres merytoryczny szkolenia

Zakres merytoryczny szkolenia musi obejmować wszystkie tematy wyszczególnione w dokumentach dedykowanych dla szkolenia EC-Council - CEH - CertifiedEthical Hacker dostępnych na oficjalnej stronie EC-Council, to jest:

- Information security controls, laws, and standards.
- Various types of footprinting, footprinting tools, and countermeasures.
- Network scanning techniques and scanning countermeasures
- Enumeration techniques and enumeration countermeasures
- Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.
- Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.
- Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend against sniffing.
- Social engineering techniques and how to identify theft attacks to audit human-level vulnerabilities and social engineering countermeasures.
- DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.
- Session hijacking techniques to discover network-level session management, authentication/authorization, and cryptographic weaknesses and countermeasures.
- Webserver attacks and a comprehensive attack methodology to audit vulnerabilities in webserver infrastructure, and countermeasures.
- Web application attacks, comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.
- SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.
- Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.

- Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.
- Cloud computing concepts (Container technology, serverless computing), the working of various threats and attacks, and security techniques and tools.
- Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Threats to IoT and OT platforms and defending IoT and OT devices.
- Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.