Załącznik nr 1.4 do SWZ
Nr wew. postępowania 55/22

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 – część II

Zadanie nr 4
USŁUGA SPOŁECZNA

1.	**Cykl szkoleń dla administratorów policyjnych zasobów teleinformatycznych**
Temat szkolenia	Szkolenie Certified Ethical Hacker
Odbiorcy szkolenia	Szkolenie przeznaczone jest dla 10 uczestników - pracowników Wydziału Łączności i Informatyki KWP zs. w Radomiu.
Wymagania ogólne dotyczące realizacji szkolenia	• Szkolenie odbędzie się w formie stacjonarnej w wybranym przez Wykonawcę miejscu na terenie Polski. • Transport do i z miejsca szkolenia dla uczestników szkolenia zapewni Zamawiający. • Szkolenie musi być akredytowane przez organizację EC-Council, poprowadzone przez certyfikowanego trenera EC-Council z użyciem materiałów i środowiska szkoleniowego dostarczonego przez EC-Council. • Szkolenie musi być przeprowadzone w najnowszej wersji szkolenia Certified Ethical Hacker. • Wykonawca szkolenia zapewni odpowiednie zaplecze techniczne (urządzenia sieciowe) do celów szkolenia i indywidualne stanowiska robocze (komputery kursantów) dla każdego z uczestników szkolenia. • Wykonawca przeprowadzi szkolenie w języku polskim. • Szkolenie odbędzie się w ramach jednej zamkniętej grupy szkoleniowej. Termin szkolenia zostanie ustalony z Wykonawcą w ramach kontaktów roboczych. • Wykonawca zrealizuje szkolenie w terminie 2 miesięcy od daty podpisania umowy. • Szkolenie musi obejmować 5 kolejnych dni roboczych, łącznie min. 35 godzin zegarowych. Każdy dzień szkoleniowy to min. 7 godzin zegarowych.

	• Dokładny zakres podziału godzin zostanie zrealizowany na zasadach określonych przez EC-Council, uzgodniony z Wykonawcą w ramach kontaktów roboczych i przedstawiony w harmonogramie szkolenia. • Dokładne terminy i harmonogram szkolenia zostaną uzgodnione z Wykonawcą w ramach kontaktów roboczych i muszą być przedstawione Zamawiającemu w przeciągu maksymalnie 3 dni od podpisania umowy. • Wykonawca zapewni materiały szkoleniowe akredytowane przez EC-Council, dla każdego z uczestników szkolenia. • Materiały szkoleniowe muszą być przygotowane w języku polskim lub angielskim. Materiały szkoleniowe mogą być w formie papierowej lub elektronicznej w wersji obejmującej szkolenie. • Wykonawca ponosi koszty opracowania, powielania i transportu materiałów szkoleniowych. • Wykonawca zapewni konsultacje on-line w zakresie tematyki określonej w szkoleniu do 14 dni kalendarzowych po zakończeniu szkolenia dla każdego z uczestników szkolenia. • Uczestnicy szkolenia otrzymają imienne certyfikaty ukończenia akredytowanego szkolenia EC-Council, sygnowane przez firmę EC-Council oraz podpisane przez trenera. Imienne certyfikaty poświadczające uczestnictwo w szkoleniu w wersji papierowej, rozdane zostaną uczestnikom najpóźniej ostatniego dnia świadczenia usługi. Certyfikaty, o których mowa powyżej, muszą zawierać oznaczenia wskazujące na finansowanie ze środków FBW w ramach Projektu (Zamawiający przekaże Wykonawcy niezbędne pliki graficzne). • Po zakończeniu szkolenia Wykonawca, na zasadach określonych przez EC-Council, umożliwi każdemu uczestnikowi udział w egzaminie certyfikacyjnym. Wykonawca zapewni egzamin w formie stacjonarnej, w akredytowanym przez EC-Council centrum egzaminacyjnym, w terminie indywidualnie określonym dla każdego uczestnika szkolenia. • Wykonawca przeprowadzi ankietę ewaluacyjną po szkoleniu, której wzór stanowi załącznik do umowy. Na podstawie przeprowadzonych ankiet sporządzi analizę ankiet ewaluacyjnych. • Wymaga się, aby prowadzący szkolenie/trener przeprowadził minimum 3 szkolenia z zakresu Certified Ethical Hacker w okresie ostatniego roku poprzedzającego złożenie oferty.
Zakres merytoryczny szkolenia	• 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.
Zakwaterowanie i wyżywienie	• Wykonawca szkolenia zapewni uczestnikom nocleg (5 dób hotelowych) w standardzie minimum 3-gwiazdkowym, znajdującym się w obrębie miasta w którym będzie realizowane szkolenie • Wykonawca zobowiązany jest do udostępnienia pokoi dla uczestników szkolenia w dzień poprzedzający szkolenie do godziny

	18.00, zaś wykwaterowanie umożliwi w ostatnim dniu szkolenia do standardowej godziny wymeldowania oferowanej przez obiekt noclegowy z zastrzeżeniem możliwości pozostawienia na parkingu pojazdów przeznaczonych do transportu uczestników szkolenia. • Wymogi dotyczące zakwaterowania uczestników: ○ Wszyscy uczestnicy jednej grupy szkoleniowej muszą być zakwaterowani w jednym obiekcie; ○ Zakwaterowanie w pokojach 1- lub 2-osobowych (pokoje dwuosobowe muszą być wyposażone w oddzielne łóżka); ○ W każdym pokoju musi znajdować się węzeł sanitarny (umywalka i prysznic/wanna z ciepłą i zimną wodą, toaleta), ręcznik oraz ręcznik kąpielowy, mydło, papier toaletowy; ○ Wykonawca zapewni bezpłatny dostęp do sieci Wi-Fi na terenie obiektu; ○ Na terenie obiektu zostaną bezpłatnie udostępnione miejsca parkingowe w ilości równej ilości uczestników szkolenia; • Wykonawca szkolenia zapewni uczestnikom wyżywienie. Wyżywienie musi obejmować w dniu zakwaterowania kolację. W pierwszym, drugim, trzecim, czwartym dniu szkoleniowym śniadanie, obiad dwudaniowy i kolację. W ostatnim dniu szkolenia śniadanie i obiad dwudaniowy. • W każdym dniu szkolenia (podczas przerw) zostanie zorganizowany serwis kawowy, w trakcie których zostanie podana: kawa, herbata, woda mineralna (gazowana i niegazowana), soki, cukier, mleczko do kawy, ciasta kruche lub ciasta. Serwis kawowy musi być zorganizowany w tym samym budynku co szkolenie (najlepiej w tej samej Sali lub jej bezpośrednim sąsiedztwie).