Załącznik nr 1 do zapytania ofertowego nr 7/POWR/Z042/2022

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przygotowanie i przeprowadzenie szkolenia Certified Ethical Hacker dla studentów Akademii WSB w Dąbrowie Górniczej i Wydziału Zamiejscowego w Cieszynie

Założenia organizacyjne, cel, zakres programowy szkolenia	Efekty uczenia	Liczba uczestników szkolenia, liczba grup, godzin, lokalizacja	Minimalne wymagania dla wykładowcy / trenera
1. Certified Ethical Hacker adresowane jest do studentów/ek którzy/e są zainteresowani/e zdobyciem nowych umiejętności i wiedzy na temat cyberbezpieczeństwa. Szkolenie winno być autoryzowane przez EC-Counsil 2. Szkolenie winno być realizowane w postaci praktycznej. Poszczególne etapy szkolenia teoretycznego powinny być podsumowywane przekrojowymi ćwiczeniami. 3. Szkolenie winno przygotować uczestników do egzaminu CEH. 4. Szkolenie winno zakończyć się egzaminem wewnętrznym – Uczestnicy szkolenia, którzy pozytywnie zaliczą egzamin wewnętrzny otrzymują od Wykonawcy zaświadczenie o ukończeniu szkolenia oraz voucher umożliwiający przystąpienie do zewnętrznego egzaminu certyfikującego umożliwiającego uzyskanie certyfikatu CEH uznawanego i rozpoznawalnego na całym świecie.	**Po zakończeniu szkolenia** **Uczestnicy winni w szczególności umieć:** • definiować i charakteryzować najważniejsze techniki ataków hakerskich • przeprowadzać rekonesans dotyczący własnej firmy czy konkurencji • skanować, testować i przełamywać zabezpieczenia systemów • identyfikować i analizować podatności w organizacji • rozpoznawać i zapobiegać metodom eskalacji uprawnień w systemach • tworzyć lepsze polityki na urządzeniach IDS/IPS dotyczące wykrywania włamań • rozpoznawać socjotechniki wykorzystywane przez przestępców • tworzyć wirusy, hakować urządzenia mobilne, smartfony	**Liczba grup i uczestników:** 6 grup szkoleniowych - każda licząca ok. 12 osób, tj. łącznie ok. 72 osoby **Liczba godzin:** 40 h dydaktycznych x 6 grup = 240 h dydaktycznych (1 h dyd. = 45 minut) **Lokalizacja:** **- 4 grupy – ok. 48 osób** Akademia WSB ul. Cieplaka 1c 41-300 Dąbrowa Górnicza **- 2 grupy – ok. 24 osoby** Akademia WSB Wydział Zamiejscowy w Cieszynie ul. Frysztacka 44 43-400 Cieszyn	• min. wykształcenie wyższe lub certyfikat umożliwiający przeprowadzenie danego wsparcia, • min. 2 letnie doświadczenie zawodowe jako trener Ethical Hackingu, • realizacja minimum 3 szkoleń/kursów z zakresu Ethical Hackingu w ciągu ostatnich 2 lat **Uwaga !** W celu potwierdzenia spełnienia warunku należy do oferty dołączyć **min. 3** referencje, zaświadczenia lub inne dokumenty wystawione przez **min. 3 różne podmioty** zlecające przeprowadzenie szkolenia (w przypadku szkoleń zamkniętych, organizowanych na zlecenie danego podmiotu) lub wystawione przez uczestników szkolenia bądź podmioty, kierujące swoich pracowników na szkolenie

Zakres tematyczny szkolenia winien obejmować m.in: • Wprowadzenie do etycznego hakingu (Introduction to Ethical Hacking) • Zbieranie informacji o ataku (Footprinting and Reconnaissance) • Skanowanie sieci (Scanning Networks) • Enumeracja (Enumeration) • Analiza podatności (Vulnerability Analysis) • Hackowanie systemu (System Hacking) • Złośliwe oprogramowanie (Malware Threats) • Monitorowanie i przechwytywanie danych (Sniffing) • Inżynieria społeczna – socjotechniki (Social Engineering) • Ataki DDoS (Denial-of-Service) • Przejęcie/przechwytywanie sesji (Session Hijacking) • Omijanie IDS, zapór Firewall i Honeypots (Evading IDS, Firewalls, and Honeypots) • Hakowanie serwerów sieciowych (Hacking Web Servers) • Hakowanie aplikacji internetowych (Hacking Web Applications) • Ataki przez zapytania w SQL (Injection SQL) • Hakowanie sieci bezprzewodowych (Hacking Wireless Networks) • Hakowanie mobilnych platform (Hacking Mobile Platforms) • Hakowanie Internetu Rzeczy (IoT and OT Hacking) • Bezpieczeństwo chmury (Cloud Computing)	• analizować złośliwe oprogramowanie • identyfikować potencjał zagrożeń płynących z "Internetu Rzeczy" (IoT) i jak się przed nimi zabezpieczyć • określić wyzwania dla sieci przemysłowych i wpływ cyberbezpieczeństwa na koncepcje OT (Operational Technology) • charakteryzować najważniejsze elementy systemów kontenerowych (Docker, Kubernetes) • weryfikować bezpieczeństwo rozwiązań chmurowych takich jak AWS • rozpoznawać subtelne różnice między backdoor'ami, trojanami oraz innymi zagrożeniami Uczestnicy szkolenia winni być przygotowani do zdania egzaminu CEH.		(w przypadku szkoleń otwartych) **z zakresu Ethical Hackingu.** **Referencje muszą dotyczyć szkoleń wykazanych w załączniku nr 3.** **UWAGA: DOKUMENTY MUSZĄ BYĆ WYSTAWIONE PRZEZ RÓŻNE PODMIOTY ZLECAJĄCE PRZEPROWADZENIE SZKOLENIA ORAZ DOTYCZYĆ SZKOLEŃ ZREALIZOWANYCH W RÓŻNYCH TERMINACH**

• Kryptografia (Cryptography)			

Dodatkowe informacje:

Szkolenie winno zostać zrealizowane w terminie do 30.06.2022 r.

Wykonawca w ramach realizacji przedmiotu zamówienia zobowiązany jest do:

1. Realizacji usługi szkoleniowej obejmującej kompleksowe przygotowanie uczestników do certyfikowanego egzaminu, przeprowadzenie autoryzowanego szkolenia zgodnie z programem i harmonogramem oraz przeprowadzenie egzaminu wewnętrznego na zakończenie szkolenia.
2. Zapewnienia materiałów szkoleniowych w wersji papierowej lub elektronicznej, sprzętu komputerowego i oprogramowania niezbędnego do prawidłowej realizacji szkolenia oraz certyfikowanego egzaminu.
3. Prowadzenia odpowiedniej dokumentacji, dostarczonej przez zamawiającego tj.: programu szkoleniowego, harmonogramu zajęć, dzienników zajęć, list obecności, listy odbioru materiałów dydaktycznych, listy odbioru certyfikatów, pretestów i posttestów oraz ich analizy, ankiet ewaluacyjnych, raportu poszkoleniowego.
4. Przygotowania dla każdego uczestnika dokumentów do egzaminu końcowego oraz wydanie certyfikatów/zaświadczeń o ukończeniu szkolenia.