Załącznik nr 1.5 do SWZ

Nr wew. postępowania 67/22

**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**

Zadanie nr 5

USŁUGA SPOŁECZNA

1. **Opis przedmiotu zamówienia**

Przeprowadzenie szkolenia CompTIA CASP+\* wraz z 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).

1. **Szczegóły szkolenia**

 Przeprowadzenie szkolenia przygotowującego do egzaminu CompTIA Advanced Security Practitioner (CASP+)\* wraz z voucherem na egzamin certyfikacyjny CompTIA CASP+\* ważnym min. 3 miesiące po zakończeniu szkolenia;

1. **Odbiorcy szkolenia**

Szkolenie przeznaczone jest dla9 specjalistów i praktyków z zakresu informatyki śledczej oraz z cyberbezpieczeństwa. Uczestnikami szkolenia będzie łącznie 9 osób w ramach jednej grupy szkoleniowej.

1. **Wymagania ogólne dotyczące realizacji szkolenia**
2. Wykonawca musi posiadać status autoryzowanego partnera CompTIA.
3. 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.
4. Wykonawca przeprowadzi szkolenie w języku polskim.
5. Wykonawca w uzgodnieniu z Zamawiającym wyznaczy termin realizacji szkolenia.
6. Szkolenie musi obejmować 5 kolejnych dni roboczych od poniedziałku do piątku.
7. Każdy dzień szkoleniowy to 7 godzin zegarowych. Dokładny harmonogram dzienny
dla poszczególnych modułów zostanie uzgodniony z Wykonawcą w ramach kontaktów roboczych.
8. Wykonawca zapewni akredytowane materiały szkoleniowe CompTIA odpowiednie 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.
9. Wykonawca zapewni dla każdego z uczestników szkolenia konsultacje on-line
w zakresie tematyki określonej w szkoleniu do 14 dni kalendarzowych po zakończeniu szkolenia.
10. Uczestnicy otrzymają imienne certyfikaty ukończenia szkolenia, sygnowane przez firmę CompTIA. Certyfikaty muszą zawierać informację o ukończeniu szkolenia Comptia oraz oznaczenia wskazujące na finansowanie ze środków FBW w ramach Projektu (Zamawiający przekaże Wykonawcy niezbędne pliki graficzne).
11. Po zakończeniu każdego z modułów Wykonawca zobowiązuje się do przekazania uczestnikom szkolenia imiennych voucherów na egzaminy certyfikacyjne CompTIA CASP+\*
12. **Zakres merytoryczny szkolenia**

Zakres merytoryczny szkolenia musi obejmować wszystkie tematy wyszczególnione w dokumentach „CompTIA Certification Exam Objectives” dla szkolenia CompTIA Advanced Security Practitioner (CASP+), dostępnych na oficjalnej stronie CompTIA, to jest:

* Given a scenario, analyze the security requirements and objectives to ensure
an appropriate, secure network architecture for a new or existing network.
* Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.
* Given a scenario, integrate software applications securely into an enterprise architecture
* Given a scenario, implement data security techniques for securing enterprise architecture.
* Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.
* Given a set of requirements, implement secure cloud and virtualization solutions.
* Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.
* Explain the impact of emerging technologies on enterprise security and privacy
* Given a scenario, perform threat management activities.
* Given a scenario, analyze indicators of compromise and formulate an appropriate response.
* Given a scenario, perform vulnerability management activities.
* Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.
* Given a scenario, analyze vulnerabilities and recommend risk mitigations.
* Given a scenario, use processes to reduce risk.
* Given an incident, implement the appropriate response.
* Explain the importance of forensic concepts.
* Given a scenario, use forensic analysis tools.
* Given a scenario, apply secure configurations to enterprise mobility.
* Given a scenario, configure and implement endpoint security controls.
* Explain security considerations impacting specific sectors and operational technologies.
* Explain how cloud technology adoption impacts organizational security.
* Given a business requirement, implement the appropriate PKI solution.
* Given a business requirement, implement the appropriate cryptographic protocols and algorithms.
* Given a scenario, troubleshoot issues with cryptographic implementations.
* Given a set of requirements, apply the appropriate risk strategies.
* Explain the importance of managing and mitigating vendor risk.
* Explain compliance frameworks and legal considerations, and their organizational impact.
* Explain the importance of business continuity and disaster recovery concepts.

\*w wersji kodowej (examcode) najbardziej aktualnej na dzień podpisania umowy