Zadanie nr 3

Załącznik nr 3.1 do SWZ

Załącznik nr 1

II MODUŁ: IDENTYFIKACJA I ANALIZA DANYCH TELEINFORMATYCZNYCH W SYTUACJI KRYZYSOWEJ

PKT. 1 Szkolenie specjalistyczne doskonalące umiejętność analizy śledczej urządzeń stacjonarnych i mobilnych

Moduł tematyczny: Szkolenie z analizy śledczej urządzeń stacjonarnych (ComputerForensics)

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ A. INFORMACJE O PRZEDMIOCIE ZAMÓWIENIA

1. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest świadczenie specjalistycznych usług szkoleniowych podnoszących umiejętności pozyskiwania, badania i dokonywania analizy śledczej informacji z cyfrowych nośników danych pochodzących z urządzeń stacjonarnych (Computer/Digital Forensics). Szkolenia organizowane będą w ramach projektu „Skuteczni w działaniu – współpraca służb w sytuacjach zagrożenia infrastruktury krytycznej" współfinansowanego z Funduszu Bezpieczeństwa Wewnętrznego, realizowanego przez Komendę Wojewódzką Policji z siedzibą w Radomiu w formie wykładów, ćwiczeń praktycznych oraz laboratoryjnych przewidzianych dla 50 osób – specjalistów i praktyków z zakresu informatyki śledczej.

2. Cel szkolenia

Celem realizowanych szkoleń jestpodniesienie kompetencji specjalistów do walki z Cyberprzestępczością oraz praktyków informatyki śledczej w obszarzebadania i analizy urządzeń komputerowych. Wykorzystanie w praktyce umiejętności nabytych na szkoleniach powinno zwiększyć efektywność pozyskiwania danych z nośników, zmaksymalizować skuteczność ich analizy, a także umożliwić skrócenie czasu niezbędnego na wykorzystanie tych danych w procesie wykrywczym. Wynikiem przeprowadzonych szkoleń powinno być nabycie przez ich uczestnikówpraktycznej wiedzy i specjalistycznych umiejętności z zakresu informatyki śledczej w obszarze ujawniania, gromadzenia zabezpieczania i prezentacji dowodów cyfrowych. Pozyskane w wyniku szkoleń nowe zdolności oraz podniesione w ten sposób kompetencje powinny pozytywnie wpłynąć na prowadzone czynności w ramach procesu wykrywczego i tym samym zwiększyć skuteczność ochrony obiektów infrastruktury krytycznej, zarówno na etapie prewencji, jak też działań reaktywnych w sytuacji rzeczywistego zagrożenia.

3. Odbiorcy szkolenia

Odbiorcami – uczestnikami szkoleń będących przedmiotem zamówienia będą specjaliści oraz praktycy wykonujący badania i analizy cyfrowego materiału dowodowego z Wydziału dw. z Cyberprzestępczością i Laboratorium Kryminalistycznego z Komend Wojewódzkich Policji. Uczestnikami szkolenia będzie łącznie pięćdziesiąt osób podzielonych na pięć dziesięcioosobowych grup szkoleniowych.

4. Termin realizacji szkolenia

Z uwagi na podział odbiorców docelowych na 5 grup szkoleniowych,realizacja usługi szkolenia powinna zostać przeprowadzona w 5 terminach uwzględniających 5 dni roboczych trwania zajęć szkoleniowych w systemie od poniedziałku do piątku.Każdy dzień szkoleniowy powinien się składać
z 8 godzin szkoleniowych (z wliczeniem czasu przerw kawowych i obiadowych), co odpowiada łącznie 40 godzinom szkoleniowym, z czego min. 16 godzin musza stanowić zajęcia praktyczne.Wykonawca zobowiązuje się do wykonania szkolenia w przeciągu sześciu miesięcyod daty podpisania umowy.Szkolenie odbędzie się w pięciu terminach, osobno dla każdej grupy.Dokładne terminy przeprowadzenia szkoleń dla poszczególnych grup szkoleniowych będą uzgodnione w trybie ustaleń roboczych z wyłonionym Wykonawcą.

5. Miejsce realizacji szkolenia

Usługa szkoleniowa powinna być przeprowadzona w formie stacjonarnej, na poziomie eksperckim w postaci zajęć teoretycznych – wykładów oraz praktycznych ćwiczeń laboratoryjnych w siedzibie zapewnionej przez Wykonawcę na terenie Polski. Zamawiający wymaga, aby szkolenie zostało przeprowadzone w sali wyposażonej w klimatyzację, bezprzewodowy oraz przewodowy Internet, a także indywidualne stanowisko komputerowe dla każdego uczestnikaumożliwiające przeprowadzenie zajęć praktycznych z wykorzystaniem oprogramowania informatyki śledczej.

CZĘŚĆ B. WYMAGANIA

1. Zakres merytoryczny szkolenia

Wykonawca zobowiązany jest zapewnić realizację zajęć teoretycznych z niżej wymienionych zagadnień:

- Aspekty prawne informatyki śledczej
- Dobre praktyki informatyki śledczej
- Zadania zespołu badawczego, role poszczególnych członków zespołu
- Ocena ryzyka i zarządzanie ryzykiem w informatyce śledczej
- Postępowanie na miejscu zdarzenia
    - Metodyka prowadzenia oględzin
    - Identyfikacja śladów/przedmiotów/nośników dowodowych
    - Zabezpieczanie dowodów cyfrowych
        - Procedury, mechanizmy i pojęcia dotyczące akwizycji danych
        - Narzędzia „Triage”
        - Zabezpieczanie danych ulotnych (RAM)
        - Zabezpieczanie danych „live”

        - Zabezpieczanie danych z zasobów sieciowych (serwery danych, chmury, serwisy społecznosciowe, dane komunikatorów)
        - Klonowanie nośników
        - Wykonywanie kopii binarnych
        - Wyliczanie i weryfikacja sum kontrolnych
    - Dokumentacja prowadzonych czynności
    - Zarządzanie i postępowanie z dowodami
- Stanowisko badawcze w Informatyce śledczej
    - Sprzęt informatyczny i narzędzia fizyczne
        - Blockery sprzętowe
        - Stacje dokujące
        - Klonery dysków
    - Interfejsy komunikacyjne i transmisyjne
    - Przegląd, omówienie funkcjonalności, zasady działania programów i aplikacji do analizy dowodów cyfrowych (Forensic Tools)
    - Oprogramowanie Open Source
    - Oprogramowanie komercyjne
- Analiza dowodów cyfrowych
    - Teoria, zasady i metodyka procesu informatyki śledczej
    - Rozpoznawanie dowodów elektronicznych (eDiscovery)
    - Pojęcie dowodu cyfrowego
        - Koncepcje dowodów cyfrowych
        - Kategorie dowodów cyfrowych
    - Standardy jakości w Informatyce śledczej
    - Metodyka prowadzenia badań
    - Dokumentowanie czynności śledczych
    - Pojęcie łańcucha dowodowego
    - Badanie dysków twardych oraz hybrydowych (HDD, MHDD, HHD, SHDD)
        - Budowa, systemy plików, sposoby adresacji, interfejsy, kategorie
    - Badanie nośników zewnętrznych (USB)
        - Budowa, systemy plików, sposoby adresacji, interfejsy, kategorie
    - Badanie macierzy dyskowych i serwerów NAS
        - Budowa, systemy plików, sposoby adresacji, interfejsy, kategorie
    - Wykrywanie, identyfikacja, badanie i analiza maszyn wirtualnych
    - Analiza danych szyfrowanych
        - Pojęcie kryptologii i kryptografii
        - Rodzaje szyfrowania
        - Przestrzenie, pliki, kontenery szyfrowane
        - Metody, sposoby, narzędzia, deszyfracji
    - Wykrywanie, identyfikacja, badanie i analiza maszyn wirtualnych
    - Prezentacja dowodów cyfrowych i wyników badań
        - Raportowanie
        - Ekstrakcja, Kompilacja, konwersja danych
        - Prezentacja podsumowań, wniosków i zestawień

- Analiza danych systemów operacyjnych (Windows, Linux, MacOs)
  - Artefakty systemowe
  - Artefakty użytkownika
  - Rejestry systemowe
  - Alternatywne strumienie i kontenery danych
  - Elementy usunięte
  - Pliki skrótów LNK, pliki PREFTECH, pagesys, pliki wymiany, miniatury
  - Folder RECENT.
  - Metadane
- Analiza danych przeglądarek internetowych, klientów poczty elektronicznej, komunikatorów internetowych
- Podstawy odzyskiwania danych utraconych
  - Narzędzia, metody, procedury odzyskiwania danych
  - Analiza przestrzeni nieprzydzielonej
  - Analiza „slackspace"
  - Analiza Volume ShadowCopies

- Postępowanie z incydentami informatycznymi
  - Rodzaje, podział, definicje, teoria incydentów informatycznych
  - Analiza zagrożeń i podatności
  - Plan reagowania na incydenty
  - Zarządzania reagowaniem na incydenty
  - Identyfikacja incydentu
  - Podstawowe kroki reagowania na incydenty
  - Raport z działań następczych

Wykonawca zobowiązany jest zapewnić realizację zajęć praktycznych (w formie ćwiczeń bądź laboratoriów) z niżej wymienionych zagadnień:

- Konfiguracja i przygotowanie stanowiska badawczego
- Postępowanie na miejscu zdarzenia/ujawnianie śladów/ przedmiotów/ nośników
- Konstrukcja łańcucha dowodowego, zarządzanie dowodami
- Ujawnianie, identyfikacja i akwizycja danych
- Analiza pozyskanych dowodów za pomocą narzędzi IŚ
- Raportowanie i dokumentowanie czynności śledczych

2. Zamawiający wymaga, aby Wykonawca zapewnił w ramach usługi:

a) Zakwaterowanie uczestników szkolenia o poniższych wymaganiach:
- Wykonawca zakwateruje uczestników szkolenia w hotelu posiadającym kategorię min. 3 gwiazdkową znajdującym sięw obrębie miasta, w którym będzie realizowane szkolenie.
- Zakwaterowanie w pokojach 1, 2 – osobowych. Pokoje dwuosobowe muszą być wyposażone w oddzielne łóżka. Wykonawca zobowiązany jest do udostępnienia pokoi dla uczestników szkolenia minimum 1 godzinę przed rozpoczęciem szkolenia.

- w każdym pokoju musi być węzeł sanitarny (umywalka i prysznic/wanna z ciepłą i zimną wodą, toaleta), ręcznik oraz ręcznik kąpielowy, mydło, papier toaletowy;
- Wykonawca zapewnia bezpłatny dostęp do sieci wi-fi na terenie obiektu;
- na terenie obiektu zostaną bezpłatnie udostępnione miejsca parkingowe na 10 samochodów osobowych.

b) Wyżywienie uczestników szkolenia o poniższych wymaganiach:
   - Pełne wyżywienie uczestników szkolenia. Wyklucza się catering. Wyżywienie musi obejmować obiad i kolację (dzień 1), śniadanie, obiad i kolację (dzień 2-4), śniadanie i obiad (dzień 5).

c) Salę wykładowądo przeprowadzenie zajęć teoretycznych i praktycznych. 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, ciastka kruche lub ciasta. Serwis kawowy musi być zorganizowany w tym samym budynku, co szkolenia (najlepiej w tej samej sali lub jej sąsiedztwie).

d) Imienne certyfikaty w wersji papierowej,zgodnie z obowiązującymi przepisami dotyczącymi danych osobowych, na podstawie uzyskanych bezpośrednio od uczestników szkolenia danych osobowych, poświadczające uczestnictwo w szkoleniu, zawierające m.in. następujące dane: temat szkolenia, czas realizacji szkolenia, miejsce szkolenia, podpisane przez organizatora szkolenia i prowadzącego zajęcia, rozdane 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)

e) Sprzęt, oprogramowanie i narzędzia, a także materiały dydaktyczne niezbędne do realizacji programu szkolenia (m.in. stanowisko komputerowe - badawcze dla każdego uczestnika szkolenia, środki piśmiennicze, nagłośnienie, rzutnik multimedialny).

f) Udostępnienie i przekazanie uczestnikom szkolenia materiałów dydaktycznych, w formie cyfrowej, zawierających w szczególności opis oraz informacje na temat wybranych zagadnień przekazywanych i omawianych na szkoleniu (np. skrypt, opisy ćwiczeń).

3. Warunki udziału w postępowaniu

W celu zapewnienia odpowiedniego poziomu merytorycznego oraz efektywności przeprowadzonych zajęć, Zamawiający wymaga, by:

a) Trener bądź trenerzy przeprowadzający szkolenie z ramienia Wykonawcy posiadali udokumentowane doświadczenie w przeprowadzaniu szkoleń z obszaru Informatyki śledczej (Cyber/Digital/ ComputerForensics) na poziomie eksperckim bądź podobnych merytorycznie minimum 5 szkoleń w ostatnich 3latach potwierdzone certyfikatami, listami referencyjnymi, dyplomami bądź innymi równoważnymi dokumentami.(wymóg obligatoryjny uprawniający do składania oferty).

4. Zatrudnienie na podstawie stosunku pracy

Wykonawca lub Podwykonawca zobowiązuje się do nawiązania stosunku pracy, w rozumieniu art. 22 § 1 ustawy z dnia 26.06.1974 r. – Kodeks pracy, przy wykonywaniu czynności

polegających na sporządzaniu dokumentacji dot. niniejszego szkolenia (listy obecności, ankiety ewaluacyjne, zaświadczenia, certyfikaty itp.).

CZĘŚĆ C. WARUNKI WYBORU OFERTY/WYKONAWCY

Kryteria oceny ofert z podaniem ich procentowego znaczenia:

a. wartość oferty brutto - 60 %
b. doświadczenie trenera- 40 %.

Przy dokonywaniu oceny Komisja Przetargowa posłuży się następującymi wzorami

a) dla kryterium cena:

$$C = \frac{C_N}{C_O} \times 60 \text{ pkt}$$

gdzie:

C - przyznane punkty w kryterium cena,

CN - najniższa wartość ofertowa (brutto) spośród wszystkich ofert podlegających ocenie,

CO - wartość oferty ocenianej (brutto).

b) dla kryterium doświadczenie trenerów w przeprowadzaniu szkoleń w Informatyki śledczej (Cyber/Digital/ ComputerForensics) na poziomie eksperckim

Wykonawca zobowiązany jest wpisać do oferty wszystkich trenerów przeznaczonych do realizacji szkolenia.

Proponowane kryteria wyboru ofert:

- doświadczenie trenera do 3 lat - 0 punktów,
- doświadczenie trenera 4 - 5 lat - 10 punktów
- doświadczenie trenera 6 - 7 lat - 20 punktów,
- doświadczenie trenera 8 -9 lat – 30 punktów,
- doświadczenie trenera 10 i więcej lat - 40 punktów

W przypadku wskazania więcej niż jednego trenera, do wyliczenia punktów za kryterium doświadczenie trenerów prowadzących szkolenie, Zamawiający przyjmie średnią arytmetyczną

będącą ilorazem sumy lat doświadczenia trenerów i ilości trenerów. Z powyższych wyliczeń, do oceny Zamawiający przyjmie wartość całkowitą (pełne lata).

Doświadczenie należy podać w pełnych latach. W przypadku podania niepełnych lat Zamawiający przyjmie jedynie pełne lata.

łączna ilość punktów ocenianej oferty (łączna punktacja):

W=C+D

gdzie:

W – łączna punktacja,
C – punkty za wartość oferty brutto,
D – punkty za doświadczenie trenera/trenerów.

Za ofertę najkorzystniejszą uznana zostanie oferta, która uzyska największą liczbę punktów w ocenie końcowej i przedstawia najkorzystniejszy stosunek ceny i doświadczenia trenerów.

Zamawiający zastosuje zaokrąglenie wyników do dwóch miejsc po przecinku

CZĘŚĆ D. POSTANOWIENIA KOŃCOWE

1. Z uwagi na obowiązujący na terenie RP stan epidemii, mając na uwadze ewentualność wprowadzenia obostrzeń w zakresie gromadzenia osób, Zamawiający zastrzega sobie możliwość zmiany terminu usługi w uzgodnieniu z wykonawcą.