

Załącznik nr 1 do zapytania ofertowego

Opis przedmiotu zamówienia

I. Zamówienie obejmuje Przeprowadzenie szkoleń dla informatyków z zakresu cyberbezpieczeństwa

II. Liczba jednostek objętych zamówieniem 1 jednostka (Urząd):

- Urząd Gminy Bodzechów z/s w Ostrowcu Św.

III. Liczba osób objętych szkoleniem:

- Urząd Gminy Bodzechów z/s w Ostrowcu Św. – łącznie 2 osoby

IV. Opis przedmiotu zamówienia:

1. Wykonawca jest zobowiązany do przeprowadzenia szkoleń dla informatyków z zakresu cyberbezpieczeństwa w terminie od podpisania umowy do **10.06.2026 r.** w podziale na **cztery części:**

Część I: Elementy systemu zabezpieczeń infrastruktury teleinformatycznej

Część II: Analiza logów i ruchu sieciowego

Część III: Veeam Backup & Replication: Konfigurowanie, zarządzanie i odzyskiwanie(VMCE).

Część IV: Cyberbezpieczeństwo systemów operacyjnych

2. Wykonawca musi wykazać, że:

- w okresie od **01.01.2024 r.** do **30.04.2026 r.** wykonał **należycie co najmniej 3** zamówienia obejmujące wykonanie szkoleń z zakresu cyberbezpieczeństwa w jednostkach sektora finansów publicznych z zastrzeżeniem minimum po jednym w **2026, 2025 i 2024** roku. (Wymagamy uzupełnienia **Załącznika nr 4 – Wykaz usług** a także dołączenia dokumentów potwierdzających wykonanie usługi np. **referencji**),

- trener który będzie realizował zamówienie przeprowadził w okresie od **01.01.2024 r.** do **30.04.2026 r.** wykonał **przynajmniej 3** szkolenia na temat bezpieczeństwa IT z zastrzeżeniem minimum po jednym w **2026, 2025 i 2024** roku. (Wymagamy uzupełnienia **Załącznika nr 5 – Wykaz osób** a także dołączenia dokumentu potwierdzającego posiadane kwalifikacje np. **certyfikat**),

- gwarantuje wysoką jakość usług szkoleniowych w związku z posiadaniem certyfikatu systemu zarządzania jakością zgodnego z normą PN-EN ISO 9001:2015-10.

3. Program szkolenia powinien obejmować minimum poniższy zakres tematyczny dla:

Część I: Elementy systemu zabezpieczeń infrastruktury teleinformatycznej

- 1) Zapoznanie z elementami podatnymi na niebezpieczeństwo oraz metodami ich wykorzystywania przez intruza.
- 2) Przewidywanie zagrożeń bezpieczeństwa na podstawie modelu STRIDE.
- 3) Wyznaczenie zagrożeń i analiza ryzyka dla kont w organizacji.
- 4) Typowe zagrożenia usług katalogowych i DNS oraz zastosowanie metod zabezpieczających te usługi
- 5) Wyznaczenie zagrożeń, projektowanie zabezpieczeń i analiza ryzyka dla danych.
- 6) Wyznaczenie zagrożeń, projektowanie zabezpieczeń i analiza ryzyka dla transmisji danych.
- 7) Projektowanie polis inspekcji dostępu do zasobów.
- 8) Analiza ryzyka tworzonego przez użytkowników sieci, projektowanie polityki bezpiecznego używania komputera
- 9) Analiza ryzyka zarządzania sieci, projektowanie polityki bezpieczeństwa dla zarządzania siecią.
- 10) Sposoby wykorzystania kryptografii do zabezpieczania informacji.
- 11) Dystrybucja i zarządzanie certyfikatami, tworzenie struktury PKI

Czas szkolenia: min. 12 godzin

Część II: Analiza logów i ruchu sieciowego

- 1) Znaczenie monitorowania systemów informatycznych.
- 2) Logi w kontekście cyberbezpieczeństwa.
- 3) Monitorowanie aktywności użytkowników i aplikacji w systemie Windows.
- 4) Analiza logów w Windows Event Viewer: Security Logs, Application Logs.
- 5) Monitorowanie działań użytkowników w systemie Linux.

- 6) Wprowadzenie do hardeningu systemów Windows i Linux.
- 7) Analiza ruchu sieciowego - Wireshark.
- 8) Najlepsze praktyki w zakresie zabezpieczania systemów przed atakami.
- 9) Wprowadzenie do ESET Inspect jako narzędzia EDR
- 10) Praktyczne ćwiczenia w analizie logów ESET i identyfikacji zagrożeń.

Czas szkolenia: min. 5 godzin

Część III: Veeam Backup & Replication: Konfigurowanie, zarządzanie i odzyskiwanie(VMCE).

- 1) Opisanie strategii i narzędzi zabezpieczających serwer kopii zapasowych Veeam w celu uniknięcia nieautoryzowanego dostępu i wycieków danych.
- 2) Efektywna ochrona maszyn wirtualnych VMware i Hyper-V w oparciu o ściśle określone umowy SLA poprzez tworzenie zadań tworzenia kopii zapasowych.
- 3) Identyfikacja wykorzystania grup ochrony do automatyzacji instalacji agentów Veeam i ochrony obciążeń za pomocą zadań tworzenia kopii zapasowych agentów.
- 4) Analiza funkcji i ustawień, które umożliwiają optymalizację pamięci masowej kopii zapasowych, szybsze tworzenie kopii zapasowych i spójność danych.
- 5 Zapewnienie odzyskiwania danych i przestrzeganie reguły 3-2-1 dzięki zadaniom tworzenia kopii zapasowych.
- 6) Przypadki użycia Veeam Backup Enterprise Manager.
- 7) Integracja Veeam Backup and Replication z planem reagowania na incydenty.
- 8) Funkcje odzyskiwania Veeam Backup and Replication.
- 9) Jakie są implikacje różnych metod odzyskiwania i jaki jest właściwy wybór metody odzyskiwania?
- 10) Korzystanie z funkcji wykrywania złośliwego oprogramowania Veeam.
- 11) Dostęp do oprogramowania Veeam Backup - zajęcia praktyczne
- 12) Zabezpieczanie serwera Veeam Backup – zajęcia praktyczne
- 13) Możliwości Veeam Agent Backup – zajęcia praktyczne
- 14) Możliwości tworzenia kopii zapasowych danych nieustrukturyzowanych – zajęcia praktyczne

15) Tworzenie kopii zapasowych w drugiej lokalizacji i zarządzanie nimi – zajęcia praktyczne

16) Budowanie możliwości replikacji – zajęcia praktyczne

17) Testowanie kopii zapasowych maszyn wirtualnych – zajęcia praktyczne

Czas szkolenia: min. 25 godzin

Część IV: Cyberbezpieczeństwo systemów operacyjnych

1) Analiza i skanowanie w sieci.

2) Weryfikacja i wyszukiwanie dostępnych exploitów na aplikacje wykorzystywane w organizacji.

3) Ataki na systemy operacyjne Windows oraz Linux.

4) Ataki na aplikacje w systemach operacyjnych.

5) Ataki na bazy danych.

6) Ataki na przeglądarki internetowe.

7) Szybka identyfikacja możliwych ataków na systemy Windows i ich uniemożliwianie.

8) Szybka identyfikacja możliwych ataków na systemy Linux i ich uniemożliwianie.

9) Podstawowy Port knocking.

Czas szkolenia: min. 6 godzin

4. Wymagania ogólne dotyczące organizacji szkolenia:

1) Szkolenie stacjonarne w siedzibie Zamawiającego lub w miejscu ustalonym przez Wykonawcę w lokalizacji znajdującej się maksymalnie do 100 km od siedziby Zamawiającego. Zamawiający dopuszcza również możliwość przeprowadzenia szkolenia online w czasie rzeczywistym.

3) W szkoleniu będzie brało udział **2 osoby**. Szkolenia będą odbywać się w dni robocze, w godz. 7:00 – 16:00. Szkolenie będzie prowadzone w **języku polskim**. Szczegółowa data szkolenia będzie ustalana z Zamawiającym. **Każdy Uczestnik szkolenia otrzyma materiały szkoleniowe w języku polskim oraz certyfikat ukończenia szkolenia**

4) Wykonawca zobowiązuje się w terminie 7 dni od podpisania umowy dostarczyć Zamawiającemu:

- a) Proponowany zakres tematyczny,
- b) Dzienny

harmonogram szkolenia.

Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek w sporządzanej przez siebie dokumentacji szkoleniowej zgodnie z sugestiami Zamawiającego na każdym etapie realizacji zamówienia. Szkolenia mogą zostać przeprowadzone po akceptacji dokumentacji przez Zamawiającego.

5) W ramach organizacji szkolenia Wykonawca zapewni:

1. Materiały szkoleniowe, obejmujące szczegółowy zakres merytoryczny szkolenia i harmonogram dzienny szkolenia.
2. Właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych uczestnikowi. Zasady zostały określone w Podręczniku wnioskodawcy i beneficjenta Funduszy europejskich na lata 2021-2027 w zakresie informacji i promocji opublikowanym na stronie internetowej www.funduszeuropejskie.gov.pl
3. Wydanie uczestnikowi szkolenia zaświadczenia/certyfikatu o ukończeniu szkolenia.
4. Kadre trenerską posiadającą wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia.
5. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składa się:
 - a) Lista obecności uczestnika
 - b) Sporządzony przez trenera dziennik szkolenia, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

Wykonawca zobowiązany jest do przekazania dokumentacji szkolenia w formie papierowej.

6. Wykonawca ma obowiązek przestrzegania zasad równościowych podczas realizacji zamówienia, ze szczególnym uwzględnieniem przekazu równych szans kobiet i mężczyzn, informowania uczestników zajęć o współfinansowaniu projektu ze środków Unii Europejskiej,

6) Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia w tym materiałów szkoleniowych, zaświadczeń czy certyfikatów.