

INW.271.28.2026

załącznik nr 1A do zapytania ofertowego

## OPIS PRZEDMIOTU ZAMÓWIENIA

### I. Nazwa przedmiotu zamówienia:

Szkolenie specjalistyczne z zakresu cyberbezpieczeństwa dla informatyka JST

### II. Nazwa i adres Zamawiającego:

Gmina Kutno

ul. Wincentego Witosa 1 99-300 Kutno

NIP: 7752406122

### III. Szczegółowy zakres przedmiotu zamówienia

Przedmiotem zamówienia jest organizacja i przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla pracowników IT jednostek samorządu terytorialnego (JST).

Uczestnik otrzyma imienny certyfikat potwierdzający udział w szkoleniu. Szkolenie prowadzone będzie w języku polskim.

Wykonawca zobowiązany jest do:

- 1) zapewnienia wykwalifikowanego trenera/trenerów z doświadczeniem w szkoleniach dla administracji publicznej;
- 2) prowadzenia dokumentacji szkolenia (plan szkolenia podpisany przez trenera, certyfikat uczestnictwa);
- 3) dostosowania treści i formy szkolenia do poziomu wiedzy uczestników oraz specyfiki JST.

Liczba uczestników: 1

#### **IV. Zakres szkolenia:**

##### **1. Część I – Szkolenie z zakresu obsługi systemu Windows Server z uwzględnieniem Active Directory**

Szkolenie powinno obejmować w szczególności następujące zagadnienia:

###### **1) Wprowadzenie do Windows Server**

- a) architektura systemu Windows Server,
- b) instalacja i konfiguracja Windows Server 2019/2022,
- c) podstawowe role i funkcje systemu.

###### **2) Active Directory – podstawy i architektura**

- a) koncepcja katalogu Active Directory,
- b) struktura logiczna: lasy, domeny, jednostki organizacyjne,
- c) struktura fizyczna: kontrolery domeny, replikacja, serwery globalne.

###### **3) Zarządzanie użytkownikami i grupami**

- a) tworzenie, modyfikacja i usuwanie kont użytkowników i grup,
- b) delegowanie uprawnień,
- c) polityki haseł i zasady bezpieczeństwa.

###### **4) Group Policy (GPO)**

- a) tworzenie i stosowanie zasad grupowych,
- b) konfiguracja ustawień bezpieczeństwa i aplikacji,
- c) planowanie i zarządzanie politykami w dużych środowiskach.

###### **5) Zarządzanie zasobami i uprawnieniami**

- a) udostępnianie folderów i drukarek,
- b) zarządzanie uprawnieniami NTFS i udziałów sieciowych,
- c) mechanizmy kontroli dostępu.

###### **6) Bezpieczeństwo i ochrona środowiska AD**

- a) mechanizmy logowania i audytu,
- b) zabezpieczenie kontrolerów domeny,
- c) backup i odtwarzanie Active Directory.

###### **7) Replikacja i wysoka dostępność AD**

- a) konfiguracja replikacji,
- b) rozwiązywanie problemów z replikacją,
- c) monitoring usług AD.
- d) Integracja AD z innymi usługami

- e) DNS i DHCP w kontekście Active Directory,
- f) integracja z usługami pocztowymi i aplikacjami biznesowymi.

#### **8) Praktyczne ćwiczenia**

- a) wdrożenie kontrolera domeny,
- b) konfiguracja jednostek organizacyjnych i zasad GPO,
- c) zarządzanie użytkownikami, grupami i uprawnieniami,
- d) symulacja awarii i odtwarzanie systemu.

#### **Czas trwania szkolenia**

Szkolenie musi obejmować **łącznie minimum 24 godziny dydaktyczne** (1 godzina dydaktyczna = 45 minut), realizowane w formule online.

Zajęcia powinny być podzielone na **bloki szkoleniowe** w wymiarze **3 - 4 godzin dydaktycznych każdy**, tak aby zapewnić uczestnikowi komfort nauki i możliwość praktycznego przećwiczenia zagadnień.

Harmonogram bloków zostanie uzgodniony pomiędzy Wykonawcą, a Zamawiającym przed rozpoczęciem szkolenia.

## **2. Część II – Szkolenie z zakresu obsługi i administracji systemu FortiAnalyzer-VM**

Szkolenie powinno obejmować w szczególności następujące zagadnienia:

### **1) Wprowadzenie do FortiAnalyzer**

- a) rola FortiAnalyzer w architekturze bezpieczeństwa,
- b) omówienie funkcjonalności systemu,
- c) przegląd interfejsu użytkownika,
- d) modele wdrożeń (on-premise, VM).

### **2) Instalacja i konfiguracja FortiAnalyzer-VM**

- a) wymagania systemowe i środowiskowe,
- b) instalacja maszyny wirtualnej,
- c) konfiguracja podstawowa (sieć, dostęp administracyjny),
- d) aktualizacje systemu (firmware).

### **3) Integracja z urządzeniami Fortinet**

- a) dodawanie urządzeń (FortiGate, FortiMail, FortiWeb itd.),
- b) konfiguracja przesyłania logów,
- c) zarządzanie urządzeniami (Device Manager),
- d) synchronizacja konfiguracji.

### **4) Zarządzanie logami**

- a) rodzaje logów (traffic, event, security, system),
- b) retencja i archiwizacja logów,
- c) filtrowanie i wyszukiwanie logów,
- d) analiza zdarzeń bezpieczeństwa.

**5) Analiza zdarzeń i incydentów**

- a) korelacja zdarzeń,
- b) identyfikacja zagrożeń,
- c) analiza ruchu sieciowego,
- d) wykrywanie anomalii i incydentów.

**6) Raportowanie**

- a) tworzenie raportów standardowych i niestandardowych,
- b) harmonogramowanie raportów,
- c) eksport raportów,
- d) interpretacja wyników.

**7) Alerty i automatyzacja**

- a) konfiguracja alertów,
- b) powiadomienia e-mail,
- c) automatyczne reakcje na zdarzenia,
- d) integracja z systemami SIEM/SOC.

**8) Zarządzanie użytkownikami i dostępem**

- a) role i uprawnienia,
- b) konta administratorów,
- c) integracja z LDAP/AD.

**9) Bezpieczeństwo i dobre praktyki**

- a) zabezpieczenie dostępu do systemu,
- b) backup i odtwarzanie konfiguracji,
- c) zarządzanie przestrzenią dyskową,
- d) optymalizacja wydajności.

**10) Praktyczne ćwiczenia**

- a) konfiguracja środowiska,
- b) analiza rzeczywistych logów,
- c) tworzenie raportów,
- d) symulacja incydentów bezpieczeństwa.

**Czas trwania szkolenia**

Szkolenie powinno obejmować **łącznie minimum 16 godzin dydaktycznych** (1 godzina dydaktyczna = 45 minut), realizowane w formule online.

Zajęcia powinny być podzielone na **bloki szkoleniowe** w wymiarze **3 - 4 godzin dydaktycznych każdy**, tak aby zapewnić uczestnikowi komfort nauki i możliwość praktycznego przećwiczenia zagadnień.

Harmonogram bloków zostanie uzgodniony pomiędzy Wykonawcą a Zamawiającym przed rozpoczęciem szkolenia.

**V. Forma szkolenia**

Szkolenie realizowane w formule online (na żywo) Szkolenie zostanie zrealizowane w formie zdalnej (online), przy wykorzystaniu platformy do wideokonferencji umożliwiającej interaktywny udział uczestników w czasie rzeczywistym.