Załącznik nr 2

Szczegółowy opis przedmiotu zamówienia (SOPZ)

1. Przedmiotem zamówienia są szkolenia dla kadry zarządzającej i informatyków Starostwa Powiatowego w Tomaszowie Mazowieckim w ramach projektu dofinansowanego w konkursie grantowym „Cyberbezpieczny Samorząd” w ramach programu Fundusze Europejskie na Rozwój Cyfrowy (FERC).
2. W zakres zadania nr 2 wchodzą **„Szkolenia specjalistyczne dla informatyków w zakresie zastosowanych środków bezpieczeństwa”** (6 szkoleń). Do przedmiotowych szkoleń należą:
   2.1. Szkolenie „Szkolenie ESET Protect Administrator” (przeznaczone dla 1 uczestnika), dalej zwane także *Szkoleniem nr 1*.
   2.2. Szkolenie „Szkolenie Eset Inspect XDR” (przeznaczone dla 1 uczestnika), dalej zwane także *Szkoleniem nr 2*.
   2.3. Szkolenie „Szkolenie FortiGate Essentials” (przeznaczone dla 2 uczestników), dalej zwane także *Szkoleniem nr 3*.
   2.4. Szkolenie „Szkolenie FortiGate Advanced” (przeznaczone dla 2 uczestników), dalej zwane także *Szkoleniem nr 4*.
   2.5. Szkolenie „Szkolenie FortiAnalyzer” (przeznaczone dla 2 uczestników), dalej zwane także *Szkoleniem nr 5*.
   2.6. Szkolenie „Szkolenie FortiManager” (przeznaczone dla 1 uczestnika), dalej zwane także *Szkoleniem nr 6*.
3. Wykonawca zobowiązany będzie do przeprowadzenia szkoleń w terminie do 10.04.2026r.
4. Szkolenia prowadzone będą przez Wykonawcę:
   4.1. w przypadku *Szkoleń nr 1 i nr 2*, w trybie online, podczas którego prowadzący będzie do dyspozycji uczestników przez cały czas trwania szkolenia;
   4.2. w przypadku *Szkoleń nr 3, nr 4, nr 5 i nr 6,* w trybie online/hybrydowym (tj. uczestnik szkolenia pracuje na fizycznym urządzeniu testowym FortiGate 200F, które udostępniane jest przez Wykonawcę na czas szkolenia, zdalnie łączy się ze specjalistą prowadzącym. Dostarczenie i zwrot sprzętu przesyłką kurierską na koszt Wykonawcy).
5. Szkolenia prowadzone będą przez kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.

   Szkolenia nr 1 i nr 2 prowadzone będą przez certyfikowanego specjalistę (m.in. Certyfikat ESET Managed Client Security Professional).

   Szkolenia nr 3, nr 4, nr 5 i nr 6 prowadzone będą przez certyfikowanego specjalistę (m.in. Certyfikat Fortinet Certified Professional, Fortinet Certified Solution Specialist).
6. Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego dziennego harmonogramu prac oraz zakresu merytorycznego szkolenia, dostarczonego przez Wykonawcę Zamawiającemu nie później niż 3 dni przed rozpoczęciem szkolenia.
7. Szkolenia odbędą się:

7.1. w przypadku *Szkoleń nr 1 i nr 2* w trybie online dla 1 uczestnika każde. Minimalny czas trwania każdego szkolenia to 6 godzin zegarowych w zakresie godzinowym 8:00 - 20:00 w dni robocze (tj. poniedziałek-piątek);

7.2. w przypadku *Szkoleń nr 3 i nr 4* w trybie online/hybrydowym dla 2 uczestników każde. Minimalny czas trwania każdego szkolenia to 6 godzin zegarowych w zakresie godzinowym 8:00 - 20:00 w dni robocze (tj. poniedziałek-piątek);

7.3. w przypadku *Szkolenia nr 5* w trybie online/hybrydowym dla 2 uczestników. Minimalny czas trwania szkolenia to 8 godzin zegarowych w zakresie godzinowym 8:00 - 20:00 w dni robocze (tj. poniedziałek-piątek);

7.4. w przypadku *Szkolenia nr 6* w trybie online/hybrydowym dla 1 uczestnika. Minimalny czas trwania szkolenia to 8 godzin zegarowych w zakresie godzinowym 8:00 - 20:00 w dni robocze (tj. poniedziałek-piątek);

8. Szkolenia muszą być prowadzone w języku polskim.

9. Uczestnik po każdym szkoleniu otrzymuje certyfikat ukończenia szkolenia.

10. W ramach organizacji szkoleń Wykonawca zapewni:

10.1. Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej/elektronicznej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na własność. 2 egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.

10.2. Warunki pracy uczestników i Wykonawcy w trakcie trwania szkolenia zgodne z przepisami bezpieczeństwa i higieny pracy.

10.3. Prezentacje multimedialne, tablice i inne artykuły niezbędne do prowadzenia szkolenia.

10.4. Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.

10.5. Prowadzenie dokumentacji wszystkich szkoleń w jednakowy sposób. Na dokumentację szkolenia składają się:

10.5.1. Lista odbioru potwierdzona przez Uczestników szkolenia, imiennych certyfikatów potwierdzających uczestnictwo w szkoleniu.

10.5.2. Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

10.6. Dla każdego uczestnika szkolenia, wydrukowany imienny certyfikat potwierdzający uczestnictwo w szkoleniu.

10.7. **Programy szkoleń.**

10.7.1. Program szkolenia „Szkolenie ESET Protect Administrator”:

10.7.1.1. Omówienie aktualnej wersji programu ESET

- Nowości w wersji 12
- Architektura oraz komponenty
- Wymagania instalacji

10.7.1.2. Migracja ze starszych wersji do 12

10.7.1.3. Instalacja środowiska ESET

- Instalacja serwera zarządzającego
- Instalacja modułu zarządzającego urządzeniami mobilnymi
- Instalacja konsoli zarządzającej
- Instalacja skanera sieciowego wykrywającego nieautoryzowane komputery

10.7.1.4. Zarządzanie środowiskiem ESET

- Omówienie opcji dostępnych z poziomu interfejsu administratora,
- Omówienie opcji dostępnych z poziomu interfejsu użytkownika,
- Podstawowa konfiguracja serwera zarządzającego,
- Instalacja agentów zarządzających,
- Instalacja produktów zabezpieczających,
- Administracja grupami statycznymi,
- Administracja grupami dynamicznymi,
- Konfiguracja i dystrybucja polityk

10.7.1.5. Raportowanie środowiskiem ESET

- Analiza dzienników zdarzeń
- Generowanie przykładowych raportów

10.7.1.6. Różnica między lokalnym serwerem ESET PROTECT a ESET PROTECT Cloud

10.7.2. Program szkolenia „Szkolenie Eset Inspect XDR”:

10.7.2.1. Extended Detection & Response (XDR) – wprowadzenie

- Czym jest XDR i jak wpisuje się w model wielowarstwowej ochrony?
- Różnice między EPP, EDR i XDR na przykładzie rozwiązań ESET
- Korzyści z wdrożenia XDR: szerszy kontekst zagrożeń, korelacja zdarzeń, szybsze decyzje
- Rola ESET INSPECT w architekturze XDR

10.7.2.2. Omówienie funkcji ESET INSPECT

- Przegląd interfejsu i głównych modułów systemu
- Kluczowe możliwości: monitorowanie zachowań, wykrywanie anomalii, reagowanie na incydenty
- Sposoby prezentacji danych – zdarzenia, incydenty, kontekst użytkownika i maszyny
- Mechanizmy skanowania zachowań i detekcji offline/online

10.7.2.3. Architektura i wdrożenie serwera ESET INSPECT

- Wymagania sprzętowe i systemowe
- Modele wdrożeniowe: standalone vs. integracja z ESET PROTECT
- Rola serwera, bazy danych i komunikacji z agentami
- Planowanie pojemności i optymalizacja dla większych środowisk
- Najczęstsze błędy wdrożeniowe i jak ich uniknąć

10.7.2.4. Instalacja i konfiguracja ESET INSPECT CONNECTOR

- Instalacja komponentu łączącego agenta ESET z serwerem INSPECT
- Konfiguracja źródeł danych i synchronizacji z ESET PROTECT
- Przegląd parametrów komunikacyjnych i zasady działania agenta
- Testowanie poprawności połączenia i diagnozowanie problemów

10.7.2.5. Generowanie i analiza detekcji

- Praktyczne zadania: ręczne wywoływanie detekcji w kontrolowanym środowisku
- Praca z konsolą ESET INSPECT: filtrowanie, sortowanie, tworzenie widoków
- Interpretacja alertów – kontekst, priorytetyzacja, korelacja zdarzeń
- Analiza śladów ataku – od nietypowych procesów po komunikację sieciową

10.7.2.6. Tworzenie reguł i automatyzacja reakcji (warsztat)

- Składnia i logika reguł detekcji – warunki, wyjątki, działania
- Tworzenie reguł dostosowanych do środowiska klienta
- Automatyczne działania: powiadomienia, blokady, zgłoszenia do systemu ticketowego
- Scenariusze automatycznej reakcji w oparciu o klasy incydentów

10.7.2.7. Raportowanie i eksport danych

- Tworzenie raportów na potrzeby audytu, zarządu i zespołów SOC
- Personalizacja raportów i automatyczne generowanie zestawień
- Eksport danych do SIEM / integracja z narzędziami typu SOAR
- API i możliwości automatyzacji raportowania w dużych środowiskach

10.7.3. Program szkolenia „Szkolenie FortiGate Essentials”:

10.7.3.1. Konfiguracja trybów pracy urządzenia (transparentny/sniffer lub router/NAT)
10.7.3.2. Zarządzanie aktualizacjami oraz backup
10.7.3.3. Budowa i optymalizacja reguł zapory sieciowej
10.7.3.4. Konfiguracja systemu wykrywania włamań (IDS/IPS)
10.7.3.5. Monitorowanie wykorzystania aplikacji i blokowanie malware/ransomware
10.7.3.6. Konfiguracja modułu filtrowania stron www
10.7.3.7. Konfiguracja profili antyspam
10.7.3.8. Zarządzanie wyciekiem danych DLP
10.7.3.9. Konfiguracja wielu łączy internetowych WAN
10.7.3.10. Raportowanie i analiza zdarzeń (FortiView, FortiCloud)

10.7.4. Program szkolenia „Szkolenie FortiGate Advanced”:

10.7.4.1. FortiOS - zmiany i nowości – zmiany i nowości
10.7.4.2. Zaawansowana konfiguracja wielu łącz internetowych – SD WAN
10.7.4.3. Konfiguracja połączeń tunelowych Site-to-Site IPsec VPN
10.7.4.4. Zarządzanie dostępem zdalnym SSL- VPN w oparciu o dwu stopniowe metody uwierzytelniania
10.7.4.5. Instalacja i konfiguracja aplikacji FortiClient
10.7.4.6. Zarządzanie mechanizmami routingu
10.7.4.7. Konfiguracja systemy ochrony przed atakami DDoS
10.7.4.8. Zaawansowana analiza logów i zdarzeń (FortiAnalyzer, FortiCloud)
10.7.4.9. Diagnostyka i rozwiązywanie problemów

10.7.5. Program szkolenia „Szkolenie FortiAnalyzer”:

10.7.5.1. Wprowadzenie i wstępna konfiguracja FortiAnalyzer

- Możliwości FortiAnalyzer
- Rodzina produktów FortiAnalyzer
- Logowanie i raporty — zasada działania
- Ustawienia fabryczne, interfejs zarządzania

- Konfiguracja ustawień sieciowych
- Backup i odtwarzanie konfiguracji
- Komunikacja ze środowiskiem chmury publicznej

10.7.5.2. Administracja
- Konta i uprawnienia administracyjne
- Monitorowanie zdarzeń i zadań
- Domeny administracyjne
- Konfiguracja dysków RAID

10.7.5.3. Rejestracja urządzeń
- Lista urządzeń
- Dodawanie nowych urządzeń
- Disk Quota
- Diagnostyka i rozwiązywanie problemów komunikacyjnych
- Zarządzanie zarejestrowanymi urządzeniami

10.7.5.4. Logi i archiwa
- Przetwarzanie i przeglądanie logów
- Przeszukiwanie logów
- Agregacja logów
- Przekazywanie logów
- Przywracanie logów
- Archiwizacja logów
- Alerty
- Archiwizacja
- Kwarantanna

10.7.5.5. Alarmowanie i system SOC
- Tworzenie alarmów
- Tworzenie event handlerów
- Zarządzanie incydentami bezpieczeństwa
- Wykorzystanie automatyzacji Playbooków

10.7.5.6. Raporty
- Tworzenie i generowanie raportów
- Zapytania SQL
- Wykresy
- Przeglądanie raportów
- Kalendarz raportów

10.7.5.7. Mechanizmy dodatkowe
- Konfiguracja systemu Indicator of Compromise
- Implementacja FortiGuard Outbreak Alert service
- Wykorzystanie asystenta AI

10.7.6. Program szkolenia „Szkolenie FortiManager”

10.7.6.1. Kluczowe funkcjonalności FortiManagera

10.7.6.2. Zrozumienie technologii FortiManager API oraz meta fields

10.7.6.3. Implementacja domen administracyjnych (Adom)

10.7.6.4. Konfiguracja trybów współdzielonej pracy workspace oraz workflow

10.7.6.5. Wykorzystanie szablonów w zarządzaniu grupami urządzeń

10.7.6.6. Identyfikacja statusu urządzeń i zarządzanie wersjami historycznymi ustawień

10.7.6.7. Zarządzanie politykami firewall w zakresie wielu urządzeń FortiGate. Wykorzystanie paczek polityk oraz obiektów dynamicznych.
10.7.6.8. Wykorzystanie ADOMu globalnego w celu zarządzania grupami FortiGate
10.7.6.9. Zarządzanie Fortinet Security Fabric poprzez narzędzia FortiManagera
10.7.6.10. Implementacja opcji wysokiej dostępności HA, odtwarzania i przywracania kopii zapasowej FortiManagera
10.7.6.11. Obsługa centralnej aktualizacji oprogramowania FortiOS na jednostkach FortiGate
10.7.6.12. Wykorzystania FortiManagera w rolu lokalnego serwera FortiGuard
10.7.6.13. Diagnostyka i rozwiązywanie problemów

10.8. Wynagrodzenie za realizację zakończonej usługi, przekazane będzie po prawidłowym wykonaniu usługi i przekazaniu Zamawiającemu dokumentacji określonej w punkcie 10.5.

10.9. Uwagi dotyczące przetwarzania danych.

Wykonawca realizując przedmiot zamówienia jest zobligowany do zachowania w tajemnicy wszelkich informacji pozyskanych w sposób bezpośredni lub pośredni, dotyczących Powiatu Tomaszowskiego i pracowników Starostwa Powiatowego w Tomaszowie Maz., a w szczególności danych osobowych, informacji technicznych, ekonomicznych lub organizacyjnych. Zobowiązanie do zachowania poufności dotyczy wszelkich informacji udzielonych ustnie, pisemnie drogą elektroniczną lub w inny sposób w odpowiedzi na zapytania Wykonawcy w trakcie realizacji zadań szkoleniowych i jest bezterminowe.

Warunkiem podpisania umowy na realizację przedmiotu zamówienia będzie podpisanie z Zamawiającym oddzielnej umowy dotyczącej powierzenia przetwarzania danych osobowych.