**Załącznik nr 1 do zapytania ofertowego**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Przeprowadzenie czterech szkoleń z zakresu kompleksowego bezpieczeństwa i ochrony sieci komputerowej z wykorzystaniem rozwiązań firmy Fortinet**

CPV: 80550000-4 - Usługi szkolenia w dziedzinie bezpieczeństwa

Przedmiotem zamówienia jest przeprowadzenie czterech szkoleń z zakresu kompleksowego bezpieczeństwa i ochrony sieci komputerowej z wykorzystaniem rozwiązań firmy Fortinet, jn.:

1. Szkolenie nr 1 - kompleksowe bezpieczeństwo sieci komputerowej – min. 21 h w podziale na 3 dni robocze.
2. Szkolenie nr 2 - administrowanie urządzeniem klasy UTM - min. 21 h w podziale na 3 dni robocze.
3. Szkolenie nr 3 – kompleksowe bezpieczeństwo poczty elektronicznej – min. 14 h w podziale na 2 dni robocze.
4. Szkolenie nr 4 – administracja urządzeniem do logowania zdarzeń, bezpieczeństwo i zarządzanie logami oparte na analizie – min. 6 h.
5. **Wymagania ogólne dotyczące organizacji szkoleń:**
6. Szkolenia odbędą w formie zdalnego wykładu połączonego z ćwiczeniami warsztatowymi wykonywanymi zdalnie.
7. Termin realizacji: **60 dni** od dnia podpisania umowy.
8. W każdym szkoleniu weźmie udział 3 stałych pracowników Powiatowego Urzędu Pracy w Ostródzie.
9. Szkolenia będą odbywać się w dni robocze, w godz. 8.00 - 15.00.
10. Szkolenia będą prowadzone w języku polskim.
11. Wykonawca zobowiązuje się w terminie 14 dni od dnia podpisania umowy dostarczyć Zamawiającemu do akceptacji:
12. proponowany harmonogram szkoleń
13. szczegółowy zakres merytoryczny szkoleń
14. Wykonawca przygotuje w wersji papierowej, w 2 egzemplarzach, certyfikaty ukończenia szkolenia - oryginał dla uczestnika, kopię potwierdzoną za zgodność z oryginałem dla Zamawiającego wraz z listą odbioru certyfikatów przez uczestników szkolenia. Wzór certyfikatu Zamawiający przekaże Wykonawcy na minimum 5 dni przed rozpoczęciem pierwszego szkolenia.
15. Wykonawca zapewnia uczestnikom szkoleń materiały szkoleniowe w języku polskim. Prezentacje na szkolenia oraz materiały szkoleniowe będą sporządzone zgodnie ze standardami dostępności.

9.Wykonawca jest zobowiązany do załączenia do faktury raportu z platformy szkoleniowej potwierdzający listę uczestników szkolenia.

1. Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia, w tym koszty wydruku i przekazania certyfikatów o ukończeniu szkolenia, o których mowa w ust. 7.
2. **Szczegółowa tematyka szkoleń**

**Szkolenie nr 1 - kompleksowe bezpieczeństwo sieci komputerowej**

Kompleksowe bezpieczeństwo sieci z wykorzystaniem urządzeń klasy UTM FortiGate – poziom podstawowy:

1. Minimalne wymagania dotyczące programu szkolenia:
2. Fizyczna budowa urządzeń FortiGate
3. Wstępna konfiguracja urządzenia FortiGate

* Tryby pracy NAT/Transparent
* Konfiguracja sieci i routingu
* System Dashboard i moduły systemu
* Administracja urządzeniem (WWW, CLI)

1. Polityki zapory sieciowej

* Koncepcja firewall w urządzeniach FortiGate
* Tworzenie obiektów dla reguł firewall
* Translacja adresów NAT i Virtual IP
* Internet Service Database

1. Inspekcja ruchu SSL i metody dystrybucji certyfikatów
2. Omówienie trybów pracy urządzenia – Proxy i Flow
3. Logowanie i powiadomienia
4. Korzystanie z FortiCloud
5. FortiView
6. Wprowadzenie do Security Fabric

* Fabric Connectors

1. Konfiguracja funkcji ochronnych (profile bezpieczeństwa)

* Ochrona antywirusowa i integracja z FortiSandbox
* Content Disarm and Reconstruction
* Filtrowanie antyspamowe
* System IPS / DoS Policy
* Kontrola ruchu WWW / blokowanie URL / DNS Filter
* Kontrola aplikacji
* Reputacja klienta
* Data Leakage Prevention (DLP)
* Web Application Firewall (WAF)

1. Optymalizacja ruchu sieciowego (kształtowanie pasma)
2. Konfiguracja połączeń SSL VPN
3. Konserwacja i bieżąca obsługa systemu
4. Minimalny czas trwania szkolenia 21 h podzielonych na 3 dni robocze.

**Szkolenie nr 2 - administrowanie urządzeniem klasy UTM**

Administrowanie urządzeniem klasy UTM FortiGate – poziom zaawansowany.

1. Minimalne wymagania dotyczące programu szkolenia:
2. Architektura urządzenia
3. VDOM - Wirtualizacja w obrębie urządzenia

* Wykorzystanie trybów pracy NAT / Transparent

1. Zaawansowana konfiguracja sieci i routingu

* Tworzenie sieci VLAN
* Routing dynamiczny
* Pojęcie Policy Routingu
* SD-WAN - Load Balancing oraz redundancja łącz Internetowych

1. Uwierzytelnianie użytkowników

* Integracja z usługami katalogowymi – FSSO
* Tworzenie reguł firewall w oparciu o grupy użytkowników
* Konta użytkowników gości
* Dwuskładnikowa autoryzacja – FortiToken

1. Identyfikacja urządzeń
2. Endpoint Control

* Integracja z aplikacją FortiClient

1. Cooperative Security Fabric

* Integracja urządzeń z portfolio Fortinet
* Automatyzacja

1. Wirtualne sieci prywatne - VPN

* IPSec VPN site-to-site, client-to-site
* VXLAN
* ADVPN

1. Diagnostyka i rozwiązywanie problemów
2. Konfiguracja urządzeń do pracy w klastrze HA

* Tryby pracy klastra
* Topologia połączeń i konfiguracja urządzeń

1. Minimalny czas trwania szkolenia 21 h podzielonych na 3 dni robocze.

**Szkolenie nr 3 – kompleksowe bezpieczeństwo poczty elektronicznej**

Wykorzystania urządzenia FortiMail do ochrony poczty elektronicznej.

1. Minimalne wymagania dotyczące programu szkolenia:
2. Przegląd modeli oraz podstawowe tryby pracy urządzeń FortiMail
3. Protokół SMTP i zagrożenia sieciowe z nim związane
4. Podstawowa konfiguracja urządzenia

* Konfiguracja trybu pracy
* Ustawienia sieciowe
* Administracja domeną pocztową
* Listy dostępowe
* Ustawienia logowania i raportowania

1. Mechanizmy zabezpieczające wykorzystywane przez urządzenie

* Etapy analizy wiadomości
* Zastosowanie profili
* Polityki bezpieczeństwa
* Opcje uwierzytelniania

1. Zaawansowana konfiguracja profili

* Metody blokowania niechcianych wiadomości
* Konfiguracja uwierzytelniania (SMTP, IMAP, POP3, RADIUS)
* Synchronizacja z bazą LDAP
* Filtrowanie zawartości
* Wykorzystanie profili TLS

1. Administrowanie kwarantanną
2. Wykorzystanie sieciowych pamięci masowych
3. Archiwizacja wiadomości
4. Analiza logów i raportów
5. Budowa klastra HA, omówienie możliwych konfiguracji
6. Zaawansowana konfiguracja i rozwiązywanie problemów

* Wykorzystanie CLI
* Podnoszenie wersji firmware
* Eksport konfiguracji

1. Minimalny czas trwania szkolenia 14 h podzielonych na 2 dni robocze.

**Szkolenie nr 4 – administracja urządzeniem do logowania zdarzeń, bezpieczeństwo i zarządzanie logami oparte na analizie**

Administrowania urządzeniem FortiAnalyzer.

1. Minimalne wymagania dotyczące programu szkolenia:
2. FortiAnalyzer - architektura

* Rola w infrastrukturze
* Tryby pracy i wstępna konfiguracja

1. Zarządzanie monitorowanymi urządzeniami

* Koncepcja ADOM (Administrative Domains)
* Dodawanie urządzeń
* Bezpieczna komunikacja

1. Konfiguracja opcji systemowych

* Wstępna konfiguracja
* Zarządzanie logami i archiwizacja
* Backup i przywracanie po awarii
* Aktualizacja firmware
* Zarządzanie dyskiem

1. Logowanie i monitorowanie zdarzeń

* Przeglądanie logów i mechanizmy wyszukiwania
* Integralność logów
* FortiView
* Fetcher Management

1. FortiSOC

* Indicator of Compromise
* Event Handlers
* Outbreak Alerts
* Playbooks

1. Wprowadzenie do raportowania

* Projektowanie i przeglądanie raportów
* Dataset – zapytania do bazy danych

1. Diagnostyka i rozwiązywanie problemów – sniffer. ADOM rebuild
2. ~~Minimalny czas trwania szkolenia 14 h podzielonych na 2 dni robocze.~~
3. Minimalny czas trwania szkolenia 6 h zrealizowanych w 1 dniu roboczym.