Załącznik nr 1 do SWZ

Nr postępowania: WIR.271.5.2025

**OPIS PRZEDMIOTU ZAMÓWIENIA – Zadanie 2 obszar kompetencyjny**

**Pozycja 1. Szkolenia dla administratora z zarządzania UTM i pozostałych systemów**

**Opis techniczny zamówienia – Szkolenie dla Administratora z zarządzania UTM i pozostałych wdrożonych systemów**

**1. Cel szkolenia**

Celem szkolenia jest podniesienie kwalifikacji Administratora IT w zakresie zarządzania i konfiguracji UTM oraz pozostałych wdrożonych systemów bezpieczeństwa IT w ramach projektu „Cyberbezpieczny Urząd”. Uczestnik zdobędzie wiedzę oraz praktyczne umiejętności niezbędne do skutecznej administracji i monitorowania środowiska IT, zapewniając ochronę przed cyberzagrożeniami.

**2. Zakres szkolenia**

Szkolenie obejmuje kompleksowe omówienie i praktyczne zastosowanie funkcji systemów wdrożonych w ramach projektu. Zakres tematyczny obejmuje:

**I. Zarządzanie UTM (Unified Threat Management)**

* Instalacja i konfiguracja systemu UTM.
* Tworzenie i zarządzanie politykami bezpieczeństwa.
* Konfiguracja filtrowania treści i kontrola ruchu sieciowego.
* Analiza logów i alertów bezpieczeństwa.
* Ochrona przed atakami DDoS oraz IPS (Intrusion Prevention System).
* Konfiguracja VPN dla pracowników urzędu.

**II. Zarządzanie systemem ochrony poczty e-mail**

* Implementacja i konfiguracja systemu ochrony poczty.
* Ochrona przed phishingiem i malware.
* Filtrowanie wiadomości spamowych.
* Wykrywanie i blokowanie podejrzanych załączników.
* Zabezpieczenie komunikacji e-mail (DKIM, SPF, DMARC).

**III. System DLP (Data Loss Prevention)**

* Wdrożenie polityk ochrony danych przed wyciekiem.
* Monitorowanie i analiza przepływu informacji w sieci.
* Konfiguracja zasad dostępu do poufnych danych.
* Audyt i raportowanie naruszeń polityki bezpieczeństwa.

**IV. System zarządzania podatnościami VA/PM Inspekt EDR & 2FA**

* Skanowanie systemów pod kątem podatności.
* Wdrożenie systemu Endpoint Detection & Response (EDR).
* Konfiguracja dwuetapowego uwierzytelniania (2FA).
* Analiza i reagowanie na incydenty bezpieczeństwa.

**V. Macierz dyskowa i systemy backupu**

* Administracja nową macierzą dyskową z SSD.
* Implementacja polityk backupowych z wykorzystaniem taśm LTO-8.
* Zabezpieczenie kopii zapasowych przed atakami ransomware.
* Strategia odzyskiwania danych w przypadku awarii.

**VI. System wirtualizacji i serwer HA**

* Instalacja i konfiguracja nowego serwera do wirtualizacji.
* Integracja z istniejącym klastrem HA (High Availability).
* Migracja maszyn wirtualnych między hostami.
* Monitorowanie i optymalizacja wydajności serwerów.

**VII. Rozwiązanie do bezpiecznego udostępniania danych**

* Implementacja polityki bezpiecznego udostępniania danych osobowych.
* Zastosowanie szyfrowanych linków do przesyłania informacji.
* Audyt dostępu i analiza logów użytkowników.

**VIII. Ochrona stacji roboczych**

* Wdrożenie rozwiązań zabezpieczających przed ransomware.
* Aktualizacja polityk antywirusowych i endpoint security.
* Automatyzacja aktualizacji i monitorowanie podatności.

**IX. Monitoring i audyt systemów**

* Tworzenie raportów bezpieczeństwa.
* Wykrywanie i analiza zagrożeń w czasie rzeczywistym.
* Integracja systemów SIEM do centralnego monitorowania incydentów.

**3. Forma szkolenia**

* **Typ szkolenia**: stacjonarne lub online (w zależności od preferencji).
* **Czas trwania**: minimum **5 dni szkoleniowych** (40 godzin dydaktycznych).
* **Liczba uczestników**: 1 osoba (Administrator IT).
* **Materiały szkoleniowe**: wersja elektroniczna i papierowa.
* **Certyfikat ukończenia**: wydany po pomyślnym zakończeniu szkolenia.

**4. Wymagania wobec wykonawcy**

1. **Doświadczenie** – min. **4 lata doświadczenia** w szkoleniach z zakresu cyberbezpieczeństwa.
2. **Certyfikowanyi trenerzy** – z certyfikatem w zakresie zarządzania UTM
3. **Dostęp do środowiska testowego** – zapewnienie symulacji realnych scenariuszy cyberataków.

**5. Termin realizacji**

Zgodnie z postanowieniami zawartymi w projekcie umowy.