załącznik nr 3 do Umowy cz.1

Szczegółowy Opis Przedmiotu Zamówienia

Nazwa: **Szkolenie administratorów systemów informatycznych z Fortinet® realizowane na rzecz Rządowego Centrum Bezpieczeństwa.**

1. **Przedmiot zamówienia obejmuje szkolenie z systemu firmy Fortinet® obejmujące:**
   - FortiGate;
   - FortiAnalyzer;
   - FortiMail;
   - FortiAuthenticator**;**

1.1. Wymagany zakres szkolenia FortiGate:

Szkolenie powinno obejmować co najmniej następujące zagadnienia:

- architektura urządzenia;
- omówienie sposobu działania urządzenia FortiGate:
  - ✓ jak urządzenie przetwarza ruch;
  - ✓ polityki zapory sieciowej:
    - koncepcja firewall w urządzeniach FortiGate;
    - tworzenie obiektów dla reguł firewall;
    - translacja adresów NAT i Virtual IP;
    - internet Service Database;
- inspekcja ruchu SSL i metody dystrybucji certyfikatów;
- omówienie trybów pracy urządzenia – Proxy i Flow;
- logowanie i powiadomienia;
- wprowadzenie do Security Fabric, Fabric Connectors.
- konfiguracja funkcji ochronnych (profile bezpieczeństwa):
  - ✓ ochrona antywirusowa i integracja z FortiSandbox;
  - ✓ system IPS / DoS Policy;
  - ✓ kontrola ruchu WWW / blokowanie URL;
  - ✓ DNS Filter;
  - ✓ kontrola aplikacji;
  - ✓ optymalizacja ruchu sieciowego (kształtowanie pasma).
- VDOM - wirtualizacja w obrębie urządzenia;
- wykorzystanie trybów pracy NAT / Transparent;
- zaawansowana konfiguracja sieci i routingu,
  - ✓ tworzenie sieci VLAN;
  - ✓ SD-WAN - Load Balancing oraz redundancja łącz Internetowych;
- uwierzytelnianie użytkowników:
  - ✓ integracja z usługami katalogowymi – FSSO;
  - ✓ tworzenie reguł firewall w oparciu o grupy użytkowników;

- ✓ konta użytkowników gości;
- ✓ dwuskładnikowa autoryzacja – FortiToken.

- wirtualne sieci prywatne – VPN, IPSec VPN site-to-site, client-to-site;
- konfiguracja urządzeń do pracy w klastrze HA, tryby pracy klastra, topologia połączeń i konfiguracja urządzeń;
- możliwości diagnostyczne urządzenia, możliwości CLI, Sniffer jako podstawowe narzędzie, debug flow;
- podejście do analizy problemów - jak być gotowym;
- diagnostyka VPN, diagnostyka zapory, diagnostyka routingu.

1.2. Wymagany zakres szkolenia FortiAnalyzer:

Szkolenie powinno obejmować co najmniej następujące zagadnienia:

- ✓ 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.

- administracja:
  - ✓ konta i uprawnienia administracyjne;
  - ✓ monitorowanie zdarzeń i zadań;
  - ✓ domeny administracyjne;
  - ✓ konfiguracja dysków RAID.
- rejestracja urządzeń:
  - ✓ lista urządzeń;
  - ✓ dodawanie nowych urządzeń;
  - ✓ Disk Quota;
  - ✓ diagnostyka i rozwiązywanie problemów komunikacyjnych;
  - ✓ zarządzanie zarejestrowanymi urządzeniami.
- logi i archiwa:
  - ✓ przetwarzanie i przeglądanie logów;
  - ✓ przeszukiwanie logów;
  - ✓ agregacja logów;
  - ✓ przekazywanie logów;
  - ✓ przywracanie logów;
  - ✓ archiwizacja logów;
  - ✓ alerty;
  - ✓ archiwizacja,
  - ✓ kwarantanna.
- alarmowanie i system SOC:
  - ✓ tworzenie alarmów;

  - ✓ tworzenie event handlerów;
  - ✓ zarządzanie incydentami bezpieczeństwa;
  - ✓ wykorzystanie automatyzacji Playbooków.
- raporty:
  - ✓ tworzenie i generowanie raportów;
  - ✓ zapytania SQL,
  - ✓ wykresy;
  - ✓ przeglądanie raportów;
  - ✓ kalendarz raportów.
- mechanizmy dodatkowe:
  - ✓ konfiguracja systemu Indicator of Compromise;
  - ✓ implementacja FortiGuard Outbreak Alert service;
  - ✓ wykorzystanie asystenta AI.

1.3. Wymagany zakres szkolenia FortiMail:

Szkolenie powinno obejmować co najmniej następujące zagadnienia:
- wstępna konfiguracja FortiMail w trybie Gateway:
  - ✓ Zasada działania DNS;
- konfiguracja chronionej domeny:
  - ✓ pojedynczy serwer pocztowy;
  - ✓ loadbalancing na wiele serwerów pocztowych.
- obsługa SMTP przez FortiMail:
  - ✓ fortimail jako MTA dla poczty przychodzącej i wychodzącej;
  - ✓ weryfikacja adresów odbiorców;
  - ✓ fortiMail jako proxy dla sesji uwierzytelnionych.
- konfiguracja i omówienie reguł Access Control;
- opracowanie niezbędnych polityk do poprawnej obsługi ruchu;
- omówienie zasad działania reguł:
  - ✓ ip policies;
  - ✓ recipient policies.
- analiza logów;
- troubleshooting;
- omówienie i konfiguracja profilu sesji;
- profile antyspamowe dla ruchu przychodzącego;
- antyspam dla ruchu wychodzącego;
- relay host;
- profile antywirusowe:
  - ✓ omówienie oraz konfiguracja integracji z FortiSandbox.
- profile kontroli treści;
- DLP;
- Block / Safe listy;
- filtry Bayesa;
- ochrona przed Blacklistingiem;
- kwarantanna;
- integracja z LDAP;

- archiwizacja poczty w oparciu o polityki;
- szyfrowanie poczty w oparciu o polityki (IBE);
- raportowanie;
- przechowywanie poczty na zewnętrznych zasobach;
- konfiguracja HA;
- tworzenie kopi zapasowej oraz jej odtwarzanie;

1.4. Wymagany zakres szkolenia FortiAuthenticator:

Szkolenie powinno obejmować co najmniej następujące zagadnienia:

- wprowadzenie do FortiAuthenticator.
- architektura rozwiązania.
- instalacja i wstępna konfiguracja.
- zarządzanie użytkownikami i grupami.
- integracja z:
  - ✓ Microsoft Active Directory,
  - ✓ LDAP,
  - ✓ RADIUS,
  - ✓ TACACS+.
- konfiguracja metod uwierzytelniania:
  - ✓ hasła,
  - ✓ tokeny sprzętowe i programowe,
  - ✓ FortiToken,
  - ✓ certyfikaty cyfrowe,
  - ✓ FIDO2 (jeżeli wspierane przez wykorzystywaną wersję).
- konfiguracja MFA.
- zarządzanie certyfikatami:
  - ✓ lokalny urząd certyfikacji,
  - ✓ import i eksport certyfikatów,
  - ✓ CSR,
  - ✓ odwoływanie certyfikatów (CRL).
- integracja z:
  - ✓ FortiGate,
  - ✓ FortiClient,
  - ✓ FortiManager,
  - ✓ FortiAnalyzer,
  - ✓ innymi urządzeniami wykorzystującymi RADIUS/TACACS+.
- portal użytkownika.
- Single Sign-On (FSSO).
- logowanie i raportowanie.
- backup i odtwarzanie konfiguracji.
- aktualizacja systemu.
- diagnostyka i troubleshooting.

1.5. Pozostałe wymagania dotyczące szkoleń firmy Fortinet:

- liczba osób przewidzianych do każde szkolenie – min. 3 osoby;
- poziom zaawansowania – średni;
- minimalny czas trwania każdego ze szkoleń Fortinet – 2 dni robocze;
- łączna liczba godzin szkoleniowych na każde szkolenie: minimum 12 godzin zegarowych;
- sugerowany harmonogram - 2 kolejne dni robocze na każde szkolenie, w godzinach dostosowanych do standardowego dnia pracy (np. 9:00-16:00/16:30 z przerwami);
- harmonogram szkoleń do uzgodnienia z Zamawiającym;
- termin szkolenia – po uzgodnieniu z Zamawiającym.

1.5.1. Wykonawca zapewni:
- ✓ materiały szkoleniowe w języku polskim lub angielskim;
- ✓ instrukcje do laboratoriów;
- ✓ prezentacje;
- ✓ dokumentację techniczną;
- ✓ dostęp do środowiska laboratoryjnego na czas szkolenia;
- ✓ indywidualne środowisko laboratoryjne dla każdego uczestnika.

1.5.2. Forma szkolenia – online lub stacjonarne, obejmująca ćwiczenia praktycznie na środowisku testowym Wykonawcy, oraz:
- ✓ w przypadku szkolenia stacjonarnego poza siedzibą/miejscowość siedziby Zamawiającego, zapewnienie całodziennego wyżywienia oraz noclegu (dwa noclegi na dwa dni szkolenia);
- ✓ po zakończeniu szkolenia uczestnik otrzyma imienny certyfikat potwierdzający ukończenie szkolenia z zakresu administracji i obsługi urządzeń Fortinet® z każdego szkolenia niezależnie;

1.5.3. Wykonawca zapewni każdemu uczestnikowi możliwość kontaktu z trenerem (np. poprzez e mail) przez okres minimum 14 dni kalendarzowych po zakończeniu szkolenia, w celu uzyskania odpowiedzi na pytania dotyczące zakresu odbytego szkolenia;

1.5.4. Zamawiający nie wymaga szkolenia autoryzowanego;