DOTYCZY: **Usługi SOC (Security Operations Center): scentralizowane operacyjne centrum bezpieczeństwa pracujące w trybie 24/7 zajmujące się stałym monitorowaniem i analizą LOGów Zamawiającego i alarmów oraz reagowaniem na incydenty**

Opis Przedmiotu Zamówienia

Lp.	Wymagania minimalne:
1	Przedmiotem zamówienia jest świadczenie przez Wykonawcę usługi SOC w zakresie cyberbezpieczeństwa, w szczególności usługa ma polegać na: • wykonaniu analizy przedwdrożeniowej (przygotowawczej) z Zamawiającym, • zbieraniu i archiwizacji LOGów z określonych Źródeł Danych Zamawiającego w Analizatorze Wykonawcy, • uruchomienia Algorytmów w Analizatorze , które pozwalają na generowanie Alarmów a następnie ich kwalifikację jako Incydenty, • automatycznej analizie Alarmów i zdarzeń rejestrowanych w Źródłach Danych,- wynikiem automatycznej analizy ma być wykonanie zadań określonych w uzgodnionym na etapie wdrożenia Usługi scenariuszu reakcji przez personel Wykonawcy a następnie powiadomienie personelu Zamawiającego • ocenie poziomu krytyczności zdiagnozowanych Incydentów, • informowaniu i wydawaniu Zaleceń Mitygujących dla Zamawiającego, • przekazaniu Zamawiającemu cyklicznego Planowego raportu ze świadczonych Usług
2	W zakresie funkcjonalnym: • monitorowanie urządzeń zabezpieczających brzeg sieci na bazie urządzeń brzegowych firmy Fortinet • cykliczne skanowanie publicznych adresów IP (około 30 adresów) z częstotliwością 1 raz na dobę • cykliczne skanowanie wewnętrznych adresów IP (około 100 adresów) z częstotliwością skanów 1 raz na tydzień • zbieranie Logów oraz ich klasyfikacja i analiza • raport automatyczny • raport z komentarzem • analiza incydentów zlecona przez Zamawiającego rozliczana z dokładnością 1 godziny pracy analityka , której wynikiem będzie dokładna informacja co do przyczyny danego incydentu oraz sposobu zapobiegania incydentom takiego typu w przyszłości • ~~administracja firewall Fortigate zlecona przez Zamawiającego rozliczana z dokładnością 1 godziny pracy inżyniera~~ • ~~system komunikacji web~~ • szkolenie Security Awareness w formie wykładu zdalnego lub dostępu do materiałów wideo dla min. 10 osób (obejmujące wiedzę z zakresu zabezpieczenia stacji roboczych , systemów operacyjnych Windows, bezpieczeństwo urządzeń mobilnych, socjotechnika, prywatność informacji itp.) • spotkanie podsumowujące jeden raz na półrocze

	• retencja logów w okresie 1 miesiąca • indicator of compromise (IOC) generowany przez Wykonawcę – generowane na podstawie przeprowadzanych analiz • newsletter o zagrożeniach w postaci kanału RSS (Really Simple Syndication)
3	Wykaz ilościowy systemów/urządzeń przewidzianych do objęcia monitorowaniem: • systemy Microsoft Serwer (Active Directory (4 kontrolery), DHCP, DNS, Radius) – po jednym komplecie dla każdej z 2 lokalizacj~~e~~i • systemy VMware vCenter – do 5 szt (do 10 hostów) • pozostałe systemy Microsoft Windows Server – do 10 sztuk • systemy bezpieczeństwa (ESET Protect Server (2 instancje), Fortigate (2 klastry), Fortiweb (1 sztuka)) – dotyczy 2 lokalizacj~~e~~i • przełączniki sieciowe – do 100 sztuk (HP, Aruba) – nie zarządzane centralnie, • kluczowe stacje robocze – do 30 sztuk (z Windows 10, 11) Wyżej wymienione systemy generują lokalnie logi
4	Dostawa/realizacja przedmiotu zamówienia nastąpi: 12 miesięcy od daty podpisania umowy
5	Wymagania dodatkowe: • minimum 3-letnie doświadczenie w realizowaniu usługi SOC potwierdzone minimum 3 referencjami • posiadanie certyfikatu ISO 27001 ~~oraz~~(ISO 22301 dodatkowo punktowane)
6	Czas na wykonanie analizy przedwdrożeniowej maksymalnie do 30 dni od podpisania umowy
7	Czas trwania usługi 12 miesięcy od momentu uruchomienia wdrożonej usługi potwierdzonej protokołem powdrożeniowym