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, • 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 • skanowanie publicznych adresów IP • skanowanie wewnętrznych adresów IP • zbieranie Logów oraz ich klasyfikacja i analiza • raport automatyczny • raport z komentarzem • analiza incydentów zlecona przez Zamawiającego rozliczana z dokładnością 1 godziny pracy analityka • 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 • spotkanie podsumowujące jeden raz na półrocze • retencja logów w okresie 1 miesiąca • indicator of compromise (IOC) generowany przez Wykonawcę • newsletter o zagrożeniach w postaci kanału RSS (Really Simple Syndication)
3	Wykaz ilościowy systemów/urządzeń przewidzianych do objęcia monitorowaniem: • systemy Microsoft Serwer (Active Directory, DHCP, DNS, Radius) – 2 lokalizacje • systemy VMware vCenter – do 5 szt (do 10 hostów) • pozostałe systemy Microsoft Windows Server – do 10 sztuk • systemy bezpieczeństwa (ESET Protect Server, Fortigate, Fortiweb) – 2 lokalizacje

	• przełączniki sieciowe – do 100 sztuk • kluczowe stacje robocze – do 30 sztuk
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
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