**Zamawiający udziela odpowiedzi na pytanie Wykonawcy o następującej treści:**

**Pytania:**

Dotyczy - Punktu III OPIS SZCZEGÓŁOWY OBOWIĄZKÓW WYKONAWCY ZWIĄZANYCH Z

ZAPEWNIENIEM CYBERBEZPIECZEŃSTWA ZAMAWIAJĄCEGO:

Zamawiający odpowiednio wskazuje w poniższych punktach, że wykonawca będzie:

➢ punkt 2 – prowadził całodobowy, codzienny monitoring bezpieczeństwa

teleinformatycznego Zamawiającego, w obu jego lokalizacjach, to jest w:

• lokalizacji biura spółki, mieszczącego się przy ul. Igielnej 13 (50-117) we

Wrocławiu,

• lokalizacji pionu eksploatacji, mieszczącego się w obiekcie szpitalnym przy ul.

Generała Fieldorfa (54-049) we Wrocławiu.

➢ punkt 3 – zamawiający w tym punkcie określa, że w ramach monitorowania

bezpieczeństwa teleinformatycznego, o którym mowa w punkcie 2 ma:

• wykonywać analizę bieżących polityk bezpieczeństwa i przedstawiać

koordynatorom umowy z ramienia Zamawiającego propozycji ich zmian wraz z

uzasadnieniem,

• analizować systemy informatyczne Zamawiającego pod względem ich

odporności na zagrożenia cyberbezpieczeństwa i wprowadzać niezbędne

zmiany konfiguracyjne, by zapewnić bezpieczeństwo teleinformatyczne i

prawidłowe działanie systemów oraz współpracujących z nimi urządzeń,

➢ punkt 5 – być odpowiedzialny za wykrywanie i obsługę incydentów przez 24 godziny

na dobę, 7 dni tygodniu przez 365 dni w roku,

➢ punkt 7 – ma prowadzić klasyfikację incydentów i wykrywanie podatności,

➢ punkt 9 – być odpowiedzialny za zabezpieczanie informacji potrzebnych do analizy

powłamaniowej na potrzeby postępowań prowadzonych przez organy ścigania

(CSIRT MON, CSIRT NASK lub CSIRT GOV)

➢ punkt 10, podpunkt 8 – przeprowadzać badanie systemów zabezpieczeń na

przełamanie lub omijanie zabezpieczeń za skanerów podatności zaktualizowanych o

bazy CVE.

Wykonawca wskazuje, iż w celu realizacji powyższych wymagań niezbędne jest

posiadanie narzędzi informatycznych typu SIEM, narzędzi do monitorowania (np. Zabbix,

Nagios, PRTG), skanerów podatności (np. Nessus, OpenVAS, Qualys), systemów

IDS/IPS, narzędzi do analizy powłamaniowej ( np. Wireshark, Volatility, Autopsy).

Dodatkowo ww. zapisy wskazują także, że aby wypełnić wymagania Zamawiającego

Wykonawca powinien świadczyć usługę SOC

W punkcie II Opis szczegółowy opieki administracyjnej nad infrastruktura IT punkt 3

(Informacje o sprzęcie/systemach/urządzeniach) wymieniają Państwo sprzęt i systemy

jakie będą podlegały opiece i administracji w ramach świadczonej usługi. Na liście tej

nie pojawiają się jednak wymienione powyżej narzędzia niezbędne do świadczenia

oczekiwanych usług z zakresu cybersecurity.

Wobec powyższego Wykonawca zwraca się z prośbą o udzielenie informacji czy

Zamawiający dysponuje narzędziami typu SIEM, narzędziami do monitorowania sieci,

skanerami podatności, systemów IDS/IPS, narzędzi do analizy po włamaniowej jeśli tak

to wnosimy o wskazanie jakimi narzędziami Zamawiający dysponuje. W przypadku gdy

Zamawiający nie dysponuje tego typu narzędziami prosimy o informację czy Wykonawca

ma uwzględnić wyżej wymienione narzędzia w wycenie.

Ponadto, w związku z tym, iż opisany zakres usługi w dużym stopniu pokrywa się z

zakresem usług świadczonych w ramach usługi SOC (Security Operations Center),

Wykonawca wnosi o dookreślenie czy Zamawiający oczekuje świadczenia takiej usługi.

**Odpowiedzi:**

Zamawiający nie wymaga prowadzenia przez Wykonawcę usługi SOC, ani na rzecz swoją, ani na rzecz operatora usługi kluczowej, jakim jest Szpital im. T. Marciniaka. Zakres wsparcia dla SOC operatora u.k. został omówiony w OPZ.

Zgodnie z zapisami OPZ, Zamawiający wymaga od Wykonawcy monitoringu cyberbezpieczeństwa oraz wsparcia w tym zakresie. Szczegółowo zaś w kwestiach poruszonych w pytaniach:

• całodobowy codzienny monitoring bezpieczeństwa nie jest tożsamy z usługą SOC, ma natomiast w swoim zakresie taki nadzór nad funkcjonowaniem sieci, by możliwe było wykrycie incydentu, udokumentowanie jego charakterystyki i dalsza obsługa zgodnie z zaleceniami Wykonawcy,

• analiza bieżących polityk bezpieczeństwa sprowadza się w istocie do aktualizacji wobec zmian przepisów oraz rekomendacji dobrych praktyk wobec ewoluujących zagrożeń i metod zabezpieczeń,

• obsługa incydentów powinna zapewniać możliwość podejmowania przewidzianych przepisami oraz wynikających z rekomendacji Wykonawcy czynności, przy czym nie jest wymagana ich realizacja przez 24/h 7 dni w tygodniu, a jedynie zdolność do udokumentowania / zabezpieczenia dowodów wszelkich incydentów w okresie obowiązywania umowy) (bez przerw, a więc bez utraty danych wymaganych w punktu widzenia potrzeb późniejszej obsługi tychże incydentów,

• Zamawiający dysponuje następującymi narzędziami wspomagającymi kontrolę nad cyberbezpieczeństwa:

a) narzędzie SIEM: SecureVisio (aktualna subskrypcja wygasa w czerwcu 2025 r. i nie będzie odnawiana),

b) skaner podatności: Nessus Tenable (aktualna subskrypcja wygasa w marcu 2025 r. i nie będzie odnawiana),

c) narzędzia IDS/IPS: UTM Fortigate, NOD32,

d) narzędzia analizy powłamaniowej: Fortianalizer (aktualna subskrypcja wygasa w grudniu 2025 r.) + SecureVisio (aktualna subskrypcja wygasa w czerwcu 2025 r. i nie będzie odnawiana)

• niezależnie od powyższego, w związku z kończącymi się subskrypcjami, o których mowa powyżej, Wykonawca powinien dysponować kompetencjami pozwalającymi na realizację przedmiotu zamówienia, a także narzędziami umożliwiającymi tę realizację, nie zakładając, że całość lub część tych narzędzi będzie miał Zamawiający.