SPZZOZ.ZP/14/2024 Przasnysz, 20.02.2024 r.

Do wszystkich,
którzy pobrali zapytanie

Dotyczy: zapytania ofertowego na świadczenie usług w zakresie cyberbezpieczeństwa w rozumieniu art. 14 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa dla SPZZOZ w Przasnyszu

Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Przasnyszu na otrzymane pytania udziela odpowiedzi:

Pyt. 1

Zapytanie ofertowe, Rozdział III, Umowa, §2

Prosimy o potwierdzenie, że przedmiotem zamówienia jest zobowiązanie Wykonawcy do świadczenia na rzecz Zamawiającego usługi SOC (Security Operations Center).
Jednocześnie prosimy o potwierdzenie, że Zamawiający uzna za spełnione świadczenie usługi SOC jeśli Wykonawca w ramach realizacji przedmiotu zamówienia zapewni poniższe warunki i zakres świadczenia usługi:
System monitoringu infrastruktury IT i usługa SOC:

I. MINIMALNE WYMAGANIA TECHNICZNE

1. **Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat.**
2. **Zapewnienia równoległego dostępu do systemu dla wielu użytkowników.**
3. **Ograniczania użytkownikom dostępu do wybranych grup hostów.**

II. Monitorowanie

1. **Monitorowania serwerów fizycznych.**
2. **Monitorowania urządzeń sieciowych.**
3. **Monitorowania stanu połączeń.**
4. **Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów**
5. **Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux.**
6. **Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych.**
7. **Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń.**
8. **Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu.**
9. **Grupowanie hostów.**

10. Definiowanie planowanych przerw serwisowych dla hostów i usług.
11. Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).
12. Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych).
13. Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).
14. Monitorowanie serwerów za pomocą agentów
15. Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server .
16. Monitorowanie Active Directory.
17. Monitorowanie serwerów plików, udziałów sieciowych.
18. Monitorowanie statusu serwerów Apache.
19. Monitorowanie baz danych:
– ORACLE,
– MySQL,
– Postgress.
– MSSQL Server
– DB2
20. Monitorowanie urządzeń przez następujące protokoły:
– SNMP,
– WMI,
– IPMI.
21. Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW.
22. Monitorowanie poprawności działania DNS.
23. Monitorowanie środowiska VMware.
24. Monitorowanie środowiska Hyper-V.
25. Monitorowanie działania serwera czasu NTP.
26. Monitorowanie offsetu czasu na serwerach.
27. Monitorowanie ping - czasy odpowiedzi, straty pakietów.
28. Monitorowanie zajętości miejsca na poszczególnych partycjach.
29. Monitorowanie obciążenia dysków.
30. Monitorowanie wykorzystania pamięci RAM.
31. Monitorowanie obciążenia CPU.
32. Monitorowanie logów systemowych Windows.
33. Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia.
34. Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane.
35. Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix.
36. Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence)

37. **Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe**
38. **Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów).**
39. **Wykrywanie niestabilnie działających usług.**
40. **Monitorowanie dostępności stron internetowych.**
41. **Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń).**

III. Prezentacja

1. **Prezentację stanu urządzeń na mapie.**
2. **Prezentację danych na dashboardach.**
3. **Elastyczną konfigurację dashboardów, wybór elementów.**
4. **Wizualizację stanu działania całej infrastruktury na jednym dashboardzie.**
5. **Tworzenie indywidualnych dashboardów przez użytkowników**

IV. Powiadomienia

1. **Globalne wyłączanie powiadomień.**
2. **Powiadamianie użytkownika o problemach przez e-mail.**
3. **Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie.**
4. **Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników.**
5. **Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług**

V. Konfiguracja

1. **Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW**
2. **Automatyczna konfiguracja i działanie z REST-API**
3. **Centralne zarządzanie agentami**
4. **Integracja danych z różnych źródeł danych (JSON, XML, SNMP)**

VI. Monitoring bazy danych systemu HIS

1. **Możliwość monitorowania bazy danych systemu HIS w zakresie co najmniej:**

- **Instance state**
- **Version**
- **Jobs**
- **Locks**
- **Processes**
- **Number of active sessions**
- **Recovery area**
- **Log switch activity**
- **General tablespace information**
- **Tablespaces performance**
- **Long active sessions**
- **Undo retention**
- **Checkpoint and online backup state**
- **Custom SQLs**

- **RMAN backup status**
- **RMAN backups**
- **ASM disk groups**
- **Apply and transport lag of Oracle Data-Guard**

2. Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości

VII. Kolektor logów

1. System posiada własny kolektor logów syslog

2. Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps

3. Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event

4. Klasyfikuje wiadomości bazując na zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe.

VIII. Cyberbezpieczeństwo

1. System monitoruje urządzenia klasy UTM minimum w zakresie:

- **wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika**
- **monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany" ustawienie stanu na OK, a status „niezsynchronizowany" na CRIT.**
- **monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz" (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda" (1).**
- **monitoruje aktualną liczbę sesji na urządzeniu**
- **monitoruje liczbę dostępnych tuneli IPSec VPN**
- **monitoruje wykrywanie wirusów i szybkość blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika.**
- **monitoruje poziom wykorzystania procesora**
- **Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne.**

2. System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog

3. System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog.

IX. Warunki świadczenia usługi

1. Operacyjne Centrum Bezpieczeństwa; centrum kompetencyjne, które zajmować się będzie monitorowaniem infrastruktury teleinformatycznej, analizą zdarzeń, detekcją zagrożeń bezpieczeństwa i reagowaniem na wykryte incydenty naruszające bezpieczeństwo teleinformatyczne chronionych organizacji za pomocą analizy zbieranych logów z urządzeń, systemów IT oraz aplikacji, korelacją zdarzeń i detekcją zagrożeń oraz odpowiednią reakcję na pojawiające się incydenty

2. W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie monitorowania zgodnie z opisanymi poniżej wymaganiami.

3. Aktualizacje dostarczonego Systemu SOC do nowych wersji oprogramowania przez okres 12 miesięcy.

4. Szkolenia administratorów on-line z nowych funkcjonalności,

5. Usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania Systemem, bieżące aktualizacje dokumentacji technicznej dla Systemu,

6. Przyjmowania zgłoszeń serwisowych przez dedykowany serwisowy moduł internetowy oraz mail 24/7

7. Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24/7/365, zgodnie z określonymi poniżej warunkami SLA

8. Zgłoszenia i Incydenty są klasyfikowane na podstawie potencjalnego wpływu na Klienta. Wykorzystywane są 4 poziomy klasyfikacji, jak przedstawiono w poniższej tabeli:

Poziom	Opis	Zagrożenie	Przykład
Krytyczny	Niezbędne natychmiastowe działanie złagodzić obecne złośliwe oprogramowanie Działalność	- Przerwa w działaniu serwera/systemu - Brak odbioru danych z lokalizacja klienta	Wyciek danych
3	Wysokie prawdopodobieństwo incydentu, jeśli nie podejmuje się działań zapobiegawczych	- Znaczące zmiany w SIEM - wskazanie natężenia ruchu danych obniżona wydajność potencjał	Brak potwierdzenia
2	Niski potencjalny incydent	- Użytkownik nie zaktualizował hasła w wymaganym odstępie czasu	Znaleziony wirus na stacji roboczej
1	Aktywności utrzymaniowe lub informacyjne	-	Raport

9. W oparciu o klasyfikację i rodzaj zdarzenia/zgłoszenia wsparcie reaguje zgodnie z poniższymi interwałami.

Poziom	Opis	Zagrożenie	SLA
Critical	1 godzina	1 godzina	96%
3	24 godziny	2 godziny	96%
2	72 godziny	8 godzin	96%
1	5 dni	24 godzin	96%

10. W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT:

– Serwery 5…… szt.,

- **Macierze ……. szt.,**
- **Przełączniki LAN …….. szt.,**
- **Serwer Backupu ……. szt.,**
- **Bibliotekę taśmowa LTO …….sztuka**
- **serwer AD …… szt.**
- **UPS ……**

W przypadku instalacji przez Zamawiającego nowego rozwiązania będącego jednym z powyższych elementów musi ono zostać objęte systemem monitorowania w ramach usługi SOC.

11. W ramach usługi wykonawca monitoruje krytyczne elementy systemu HIS:
- **Monitorowanie komunikacji z platformą P1**
- **Monitorowanie komunikacji EWUŚ**
- **Monitorowanie bazy danych systemu HIS**

12. Producent Systemu SOC musi posiadać certyfikacje w zakresie: ŚWIADCZENIA USŁUGI SECURITY OPERATION CENTER - REAGOWANIE NA ZAGROŻENIA CYBERBEZPIECZEŃSTWA, zgodnie z normą ISO ISO/IEC 27001:2017

Odp. Zamawiający potwierdza. W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT:
- *Serwery 5 szt.,*
- *Macierze 1 szt.,*
- *Przełączniki LAN 25 szt.,*
- *Serwer Backupu 1 szt.,*
- *Bibliotekę taśmowa LTO 0 sztuka*
- *serwer AD 2 szt.*
- *UPS 1*

Pyt. 2

Zapytanie ofertowe, Rozdział III, pkt 7

Prosimy o potwierdzenie, że Zamawiający dopuszcza Elektroniczny System Obsługi Zgłoszeń udostępniany przez Wykonawcę tj. HelpDesk- narzędzie do komunikacji Stron w zakresie realizacji Umowy. Prosimy o potwierdzenie, że przyjmowanie zgłoszeń następuje poprzez narzędzie Helpdesk dostępne pod adresem www: ……., zgodnie z regulaminem dostępnym na stronie Wykonawcy, a w przypadku braku dostępności narzędzia HelpDesk za pomocą Telefonu serwisowego pod nr ……bądź e-maila:……

Odp. Zamawiający dopuszcza.

Pyt. 3

Zapytanie ofertowe, wzór umowy

Prosimy o ujednolicenie nazewnictwa stosowanego w dokumentacji postępowania bądź potwierdzenie, że Zamawiający zwany jest zamiennie jako Zleceniodawca.

Odp. Zamawiający potwierdza.

Pyt. 4
Zapytanie ofertowe, Rozdział V, pkt 1, tiert 2, załącznik nr 2, Oświadczenie Wykonawcy Zamawiający specyfikuje zapis: dysponuje pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty, zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi. Prosimy o potwierdzenie, że Zamawiamy interpretując zapis ma na myśli miejsce, które jest zabezpieczone poprzez odpowiednie środki techniczne i organizacyjne stosowane przez Wykonawcę oraz jego Personel pozwalające na zapewnienie cyberbezpieczeństwa Zamawiającemu.
Odp. Zamawiający potwierdza.

Pyt. 5

Zapytanie ofertowe, Rozdział V, pkt. 3.

Zgodnie z treścią wymogu dotyczącego spełniania warunków udziału w postepowaniu Wykonawcy, którzy biorą udział w postępowaniu muszą pkt 3: posiadać doświadczenie, polegające na tym, iż Wykonawca w ciągu ostatnich 3 lat, dla min 2 podmiotów świadczył lub świadczy usługę realizacji wymagań nałożonych na podmiot wyznaczony na operatora usług kluczowych, zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa. – zał. 5 oraz pkt 4: posiadać doświadczenie, polegające na tym, iż w ciągu ostatnich 3 lat, dla min. 3 podmiotów świadczył lub świadczy usługę Security Operation Center (SOC).

Prosimy o usuniecie wymagania treści pkt 3. Wykonawca wskazuje w tej sytuacji, iż tak sformułowany warunek jest nieproporcjonalny do przedmiotu zamówienia, a nadto biorąc pod uwagę niewielką na rynku liczbę zamówień obejmujących łącznie wszystkie ww. elementy mający charakter dyskryminujący z uwagi na to, że uniemożliwia on ubieganie się o to zamówienie podmiotom posiadającym doświadczenie wystarczające do prawidłowego wykonania zamówienia.

W tym kontekście wskazujemy, że przy założeniu chęci weryfikacji przez Zamawiającego doświadczenia Wykonawców w zakresie świadczenia usługi realizacji wymagań nałożonych na podmiot wyznaczony na operatora usług kluczowych zwracamy się z wnioskiem o ograniczenie takiego wymagania w ten sposób, aby wystarczające było wykazanie się warunkiem udziału w postępowaniu określonym w pkt 4 tj.: posiadanym doświadczeniem, polegające na tym, iż w ciągu ostatnich 3 lat, dla min. 3 podmiotów świadczył lub świadczy usługę Security Operation Center (SOC) lub wnosimy o modyfikacje zapisów na: posiadanym doświadczeniem, polegające na tym, iż w ciągu ostatnich 3 lat, dla min. 5 podmiotów świadczył lub świadczy usługę Security Operation Center (SOC), w tym 2 usługi realizowane były lub są na rzecz podmiotów wyznaczony na operatora usług kluczowych.

Biorąc bowiem pod uwagę powyższe Zamawiający, który dba o zapewnienie odpowiedniego poziomu konkurencji, winien rozważyć dostosowanie stawianych przez siebie wymogów do rzeczywistej sytuacji na rynku i określić ww. warunek udziału w postępowaniu tak, aby z jednej strony skala wymagania nie była zbyt mała (po to, aby wybrany Wykonawca dawał rękojmię należytego wykonania umowy), ale z drugiej strony aby wymagania nie były zbyt wygórowane (po to aby w sposób bezrefleksyjny nie wykluczyć z postępowania podmiotów posiadających niezbędną wiedzę i doświadczenie i mogących zrealizować przedmiot zamówienia na warunkach konkurencyjnych w stosunku do tych bardzo nielicznych podmiotów posiadających referencje o parametrach zgodnych z określonymi przez Zamawiającego w aktualnej treści zapytania ofertowego warunkami).

Odp. Szpital został wyznaczony na OUK, dlatego wymaga od potencjalnych podmiotów realizujących usługi objęte zamówieniem doświadczenia w tym zakresie. Jednym z wymagań nakładanych na podmiot OUK, zgodnie z ustawą, jest zapewnienie monitorowania 24/7 (SOC). Zamawiający wymaga doświadczenia w realizacji ww usług dla podmiotów z obszaru ochrony zdrowia.

Pyt. 6
Zapytanie ofertowe, Rozdział VII
Prosimy o potwierdzenie, że wykonawca wraz z ofertą winien złożyć oświadczenie o niepodleganiu wykluczeniu na podstawie art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

Odp. Zamawiający nie wymaga powyższego oświadczenia. .

Pyt. 7
Załącznik nr 1, Rozdział II, pkt c)
Prosimy o dostosowanie zakresu formularza ofertowego do przedmiotu zapytania ofertowego.
Odp. Zamawiający pozostawia formularz ofertowy bez zmian.

Pyt. 8
Załącznik nr 1, Rozdział II, pkt c), Załącznik nr 4, Umowa § 6 ust. 2
Zgodnie z dokumentacją zapytania ofertowego, Zamawiający określa limitów godzin jakie Wykonawca winien wliczyć w swojej kalkulacji dla Usługii II i III linii wsparcia (po 8 roboczogodzin dla każdej usługi). W związku z powyższym prosimy o potwierdzenie, że po przekroczeniu limitu godzin dla usługi II i IIII linii wsparcia w okresie rozliczeniowym koszt roboczogodziny będzie fakturowany według stawki zaoferowanej przez Wykonawcę w ofercie. Prosimy również o wykreślenie możliwości wpisania pozycji: Koszt godziny roboczej wsparcia po przekroczeniu limitu dla usługi I linii wsparcia, zgodnie z dokumentacją zapytania ofertowego Zamawiający określa limit godzin w tej kategorii jako nieokreślony.

Odp. Zamawiający potwierdza.

Pyt. 9
Załącznik nr 1, Rozdział II, pkt d)
Prosimy o potwierdzenie, że Zamawiający dopuszcza podpisanie umowy w formie elektronicznej, tj. kwalifikowanym podpisem elektronicznym, które to jest równoważny w skutkach z podpisaniem umowy w formie pisemnej (podpisanie własnoręcznym podpisem).

Odp. Zamawiający dopuszcza.

Pyt. 10
Załącznik nr 4, Umowa, §1, definicje, Harmonogram
Prosimy o potwierdzenie, że poprzez definicje: Harmonogram Zamawiający rozumie przedstawione w załącznikach do umowy zasady i warunki wykonania usług.

Odp. Zamawiający potwierdza.

Pyt. 11
Załącznik nr 4, Umowa, §1, definicje, Podwykonawcy
Prosimy o poprawę oczywistej omyłki pisarskiej i modyfikacje definicji na: Podwykonawcy – podmioty inne niż Pracownicy Wykonawcy, którymi Wykonawcy posługuje się przy świadczeniu Usług

Odp. Zamawiający poprawia omyłkę pisarską.

Pyt. 12
Załącznik nr 4, Umowa, §3 ust. 4.
Prosimy o poprawę oczywistej omyłki pisarskiej i wskazanie poprawnego odniesienia jakim jest §11 do umowy.

Odp. Zamawiający poprawia omyłkę pisarską.

Pyt. 13
Załącznik nr 4, Umowa, §3 ust. 5
Prosimy o potwierdzenie, ze udzielanie bieżących informacji nt. realizowanego przedmiotu umowy będzie odbywać się na wyraźną prośbę Zamawiającego.

Odp. Zamawiający potwierdza.

Pyt. 14
Załącznik nr 4, Umowa, §4
Prosimy o dodanie zapisów dotyczących zobowiązania Zamawiającego do:

- **zapewnienia Wykonawcy zdalnego dostępu do infrastruktury sieciowej niezbędnej o wykonywania usługi;**
- **informowania na bieżąco Wykonawcy o wszelkich zmianach i sytuacjach, które mogłyby wpłynąć na sposób wykonania usługi;**
- **do pisemnego powiadomienia Wykonawcy o wszelkich zmianach w monitorowanej infrastrukturze.**

Odp. Zamawiający wyraża zgodę.

Pyt. 15
Załącznik nr 4, Umowa, §5 ust. 1, § 12 ust. 4
Prosimy o potwierdzenie, że w przypadku udzielenia pozytywnej odpowiedzi na Pytanie nr 1 Wykonawcy, szczegółowe zasady wykonywania Usług zawarte są będą w Załączniku pn. System monitoringu infrastruktury IT i usługa SOC.

Odp. Zamawiający potwierdza.

Pyt. 16
Załącznik nr 4, Umowa, §5 ust. 3
Prosimy o potwierdzenie, że warunki realizacji usług zdalnych będą obowiązywały wówczas, kiedy Zamawiający udostępni bezpieczne połączenie zdalne. W przypadku braku takiego dostępu warunki realizacji usług mogą się przedłużać i tym samym mogą być niedochowane co nie będzie miało odzwierciedlenia w konsekwencjach dochowania terminów realizacji określonych dla Wykonawcy.
Odp. Zamawiający potwierdza.

Pyt. 17
Załącznik nr 4, Umowa, §5 ust. 4.
Prosimy o potwierdzenie, że Zamawiający zaakceptuje również poniższe rodzaje połączeń zdalnego dostępu:
1. Udostępnienie terminala - zapewni bezpieczny sposób komunikacji z siecią poprzez udostępnienie bezpiecznego terminala;
2. Udostępnienie portu do bazy danych – zapewni bezpieczny sposób komunikacji z siecią poprzez udostępnienie IP i portu pozwalającego na komunikację z bazą danych.
3. Udostępnienie dostępu poprzez aplikację Team Viewer.
4. Udostępnienie dostępu przez narzędzie AnyDesk.
Prosimy również o potwierdzenie, że Zamawiający udostępni Wykonawcy politykę bezpieczeństwa przed podpisaniem umowy w celu zapoznania się ze stosowanymi środkami technicznymi i organizacyjnymi stosowanymi przez Zamawiającego.

Odp. Zamawiający wyraża zgodę tylko na udostępnienie dostępu przez narzędzie AnyDesk, jednocześnie Zamawiający potwierdza, że udostępni Wykonawcy politykę bezpieczeństwa po podpisaniem umowy z Wykonawcą.

Pyt. 18
Załącznik nr 4, Umowa, §5 ust. 5
Prosimy o potwierdzenie, że lista osób Wykonawcy będzie mogła być aktualizowana podczas trwania umowy na adres email wskazany przez Zamawiającego.

Odp. Zamawiający potwierdza.

Pyt. 19
Załącznik nr 4, Umowa, § 6 ust. 3

Prosimy o wyjaśnienie jakie zasady wystawiania faktur i płatności mają dla wynagrodzenia w zakresie wykupionych dodatkowych godzin.
Odp. Wszelkie dodatkowe opłaty wynikające ponad zakres godzin z umowy będą fakturowane oddzielnie po akceptacji przez Zamawiającego.

Pyt. 20
Załącznik nr 4, Umowa, §6 ust. 5
1. Wykonawca zwraca uwagę na fakt, że przepisy prawa nie przewidują instytucji „prawidłowej" faktury VAT, a zatem to Zamawiający może określić jakie elementy faktury VAT będą dla niego istotne, poza tymi które wynikają z przepisów prawa. Prosimy zatem o wprowadzenie do umowy zapisów definiujących prawidłową dla tej umowy fakturę VAT, która zostanie przez Zamawiającego przyjęta do rozliczeń Stron lub wykreślenie sformułowania: „prawidłowa".
Odp. Zamawiający wykreśla sformułowanie „prawidłowa".

2. Prosimy Zamawiającego o skrócenie terminu płatności z 60 dni do 30 dni od daty dostarczenia do Zamawiającego poprawnie wystawionej zgodnie z postanowieniami umownymi i przepisami prawa faktury VAT. Powszechną praktyką w świadczeniu usług jest stosowanie 30-dniowego terminu płatności.
Prosimy o dokonanie stosownych zmian w dokumentacji postępowania.

Odp. Zamawiający nie wyraża zgody.

Pyt. 20
Załącznik nr 4, Umowa, §6
Prosimy o zgodę na dodanie poniższych zapisów w zakresie wystawiania ustrukturyzowanych FV:

1. „Wykonawca może wystawiać ustrukturyzowane faktury elektroniczne w rozumieniu przepisów ustawy z dnia 9 listopada 2018r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz. U. z 2020 r. poz. 1666, dalej – „Ustawa o Fakturowaniu").

2. W przypadku wystawienia faktury, o której mowa w ust. 1, Wykonawca jest obowiązany do wysłania jej do Zamawiającego za pośrednictwem Platformy Elektronicznego Fakturowania (dalej – „PEF"), podając numer PEPPOL (NIP) ……..…….

3. Wystawiona przez Wykonawcę ustrukturyzowana faktura elektroniczna winna zawierać elementy, o których mowa w art. 6 Ustawy o Fakturowaniu, a nadto faktura ta, lub załącznik do niej musi zawierać numer Umowy i zamówienia, których dotyczy.

4. Za chwilę doręczenia ustrukturyzowanej faktury elektronicznej uznawać się będzie chwilę wprowadzenia prawidłowo wystawionej faktury, zawierającej wszystkie elementy, o których mowa w ustępie powyżej, do konta Zamawiającego na PEF, w sposób umożliwiający Zamawiającemu zapoznanie się z jej treścią.

Uzasadnienie: Na podstawie aktualnych przepisów ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno – prywatnym (Dz. U. 2020, poz. 1666) na Zamawiających zostały nałożone obowiązki związane z odbieraniem od Wykonawcy faktur elektronicznych za pośrednictwem platformy elektronicznego fakturowania.

Odp. Zamawiający wyraża zgodę.

Pyt. 21
Załącznik nr 4, Umowa, §7 ust. 2, załącznik nr 1 do umowy § 3 ust. 3 oraz ust. 4, załącznik nr 2, § 4 ust. 8
Prosimy o potwierdzenie, że podstawą naliczenia ewentualnej kary będzie miesięczna opłata netto określona w § 6 ust 1.

Odp. Zamawiający potwierdza.

Pyt. 22
Załącznik nr 4, Umowa, §10 ust. 2
Prosimy o modyfikacje zapisów: W przypadku rozwiązania lub wypowiedzenia Umowy przez Zamawiającego z przyczyn niezależnych od Wykonawcy lub przez Wykonawcę z przyczyn dotyczących Zamawiającego, Zamawiający zapłaci Wykonawcy karę umowną w wysokości 30% Wynagrodzenia należnego Wykonawcy za okres w którym usługi miały być wykonywane. Kara umowna płatna jest w terminie 7 dni od dnia pisemnego rozwiązani Umowy.

Odp. Zamawiający pozostawia zapis bez zmian.

Pyt. 23
Załącznik nr 4, Umowa, §12 ust. 2
Prosimy o modyfikacje zapisu: Ewentualne spory w relacjach z Wykonawcą o roszczenia cywilnoprawne w sprawach, w których zawarcie ugody jest dopuszczalne zostaną poddane mediacjom lub innemu polubownemu rozwiązaniu sporu, przed Sądem Polubownym przy Prokuratorii Generalnej Rzeczypospolitej Polskiej, wybranym mediatorem albo osobą prowadzącą inne polubowne rozwiązanie sporu. W przypadku braku możliwości ich polubownego załatwienia oraz w przypadku gdy zawarcie ugody będzie niedopuszczalne, spory wynikłe z niniejszej umowy będzie rozstrzygał sąd powszechny, właściwy dla siedziby Zamawiającego.

Odp. Zamawiający wyraża zgodę na modyfikację zapisu.

Pyt. 24
Załącznik nr 1 – Usługa utrzymania systemu SIEM § 1
Prosimy o wskazanie jakich integracji w ramach zapytania ofertowego Zamawiający oczekuje.

Odp. Lista serwerów do monitorowania po podpisaniu umowy. Są to systemy dziedzinowe kluczowe do działania szpitala takie jak: HIS, RIS, PACS oraz inne działające w zakładzie.

Pyt. 25

Zwracamy się z prośbą, o wydłużenie terminu złożenia oferty. Obecny termin 2024-02-23 jest za krótki do sporządzenia wyceny licencji i oszacowania środowiska (hosting).

Odp. Zamawiający nie wyraża zgody.

Pyt. 26

Czy Wykonawca będzie świadczyć usługę hostingu dla wdrożonego już systemu SIEM, czy wykonawca ma wdrożyć system SIEM samodzielnie?

Odp. Wykonawca ma wdrożyć system SIEM samodzielnie.

Pyt. 27

Czy Zamawiający jest w stanie określić wymagane zasoby pod system SIEM - jest to konieczne to oszacowania kosztów oferty.

Odp. Zamawiający nie jest w stanie określić.

Pyt. 28

Ile scenariuszy bezpieczeństwa/reguł korelacyjnych jest obecnie wdrożonych w systemie SIEM?

Odp. Szpital nie udziela informacji których ujawnienie może prowadzić do udostępnienia informacji o zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów.

Pyt. 29

Ile incydentów krytycznych i wysokich występuje dziennie?

Odp. Szpital nie udziela informacji których ujawnienie może prowadzić do udostępnienia informacji o zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów.

Pyt. 30

Czy Zamawiający jest wstanie określić ilość występujących dziennie EPS lub wolumen logów trafiających do systemu SIEM określonych w GB.

Odp. Zamawiający nie jest w stanie określić.

Pyt. 31

Jaki System SIEM jest obecnie wykorzystywany przez Zamawiającego - jest to konieczne do oszacowania pracochłonności oraz kompetencji po stronie Wykonawcy

Odp. Zamawiający nie posiada własnego systemu SIEM .

Pyt. 32

Czy Wykonawca powinien raportować występujące incydenty w aplikacji Zamawiającego? Jeżeli tak, jaki system obsługi zgłoszeń posiada Zamawiający?

Odp. Zamawiający nie posiada aplikacji, incydenty prosi o przesyłanie za pomocą emaila.

Pyt. 33

Usługa linii L3 wsparcia - administracja i strojenie platform bezpieczeństwa Zamawiającego ? Prosimy o sprecyzowanie, jakich systemów bezpieczeństwa używa aktualnie Zamawiający? Jakich czynności administracyjnych wymaga klient?

Odp. systemy bezpieczeństwa: firewall, klient antywirusowy. Czynności administracyjne: przegląd i aktualizacja polityki bezpieczeństwa.

Pyt. 34

Czy Zamawiający może podać źródła danych i ich ilości, którymi zasilany jest system SIEM (np. Firewall, Chmura, AV, etc)

Odp. Firewall + serwery (około 6 szt.)

Pyt. 35

Prosimy o sprecyzowanie czy Termin Wykonania Zamówienia (12 miesięcy) dotyczy długości trwania umowy czy czasu, który ma Wykonawca na wdrożenie usługi ?

Odp. Termin dotyczy długości trwania umowy.

Pyt. 36

Czy zamawiający udzieli informacji na temat ilości posiadanych skrzynek pocztowych w celu oszacowania ceny platformy elearningowej?

Odp. Obecnie posiadamy 150 skrzynek z planami rozszerzenia.

Z poważaniem:

mgr Zbigniew Makowski

Dyrektor SPZZOZ

Sporządziła:
Magdalena Krzykowska
st. insp. ds. zamówień publicznych
i eksploatacji sprzętu
tel. 29 75 34 405