ZO/26/2024 Wałbrzych dnia 25.10.2024 r.

Wykonawcy- wszyscy

Dotyczy: Usługa SOC na okres 12 miesięcy.

Specjalistyczny Szpital im. dra Alfreda Sokołowskiego w Wałbrzychu odpowiada na pytania Wykonawcy.

Pytanie nr 1.

Proszę o udostepnienie draftu umowy aktualnie preferowanego przez Państwa. Jest to niezbędny dokument w celu oszacowania ryzyka biznesowego.

Umowa zostanie przekazana po rozstrzygnięciu. Istotne jej elementy niezbędne do oszacowania znajdują się w OPZ.

Pytanie nr 2.
Prosimy o potwierdzenie: czy płatność za usługę będzie realizowana w cyklu miesięcznym, czy jednorazowo w ciągu 60 dni do dnia podpisania protokołu realizacji.

Płatność realizowana będzie miesięcznie

Pytanie nr 3.
Czy w ramach realizacji zadania zamawiający udostępni miejsce w środowisku IT pod Wirtualną Maszynę niezbędną do realizacji zadania.

Tak Zamawiający udostępni.

Pytanie nr 4.
IV. 4.
Ilość źródeł logów: minimum 100, maksimum 700. w tym serwery Windows, serwery Linuks (różne dystrybucje) oraz urządzenia sieciowe - zwracam się z prośbą o przekazanie informacji o ilości serwerów Windows, ilości serwerów Linuks oraz ilości urządzeń sieciowych.

Specjalistyczny Szpital im. dra Alfreda Sokołowskiego
ul. Alfreda Sokołowskiego 4
58-309 Wałbrzych
www.zdrowie.walbrzych.pl
szpitalsokolowski@zdrowie.walbrzych.pl

sekretariat 74 64 89 600
faks 74 64 89 746
centrala 74 64 89 742

Linux 24,Win 2016 5, Win 2019 1, Win 2022 27, 65 urządzeń sieciowych.

Pytanie nr 5.
IV. 9.
Czy jako uruchomienie usługi Zamawiający uznaje rozpoczęcie logowania do SIEM przez 2 (lub więcej) źródła logów danych, a jeżeli więcej to proszę o wskazanie tej liczby.

Rozpoczęcie działania usługi rozumie jako wykonanie wszystkich zadań określonych w OPZ.

Pytanie nr 6
Jaka jest przewidywana kwota na sfinansowanie tego zamówienia?

Zamawiający nie ma obowiązku udzielenia odpowiedzi co do kwoty szacowania. Postępowanie w ramach zamówień do 130 000 tys. zł.

Pytanie nr 7.
Czy mogą podać Państwo bardziej szczegółową listę źródeł logów: ilość komputerów, serwerów, urządzeń brzegowych, maszyny wirtualnych, aplikacji webowych, rozwiązań klasy XDR, AV, DLP, PAM innych, które mają zostać objęte usługą?

Komputerów 600, serwerów 57,urządzeń 65

Pytanie nr 8.
Czy w ramach uruchomienia łącza wspomnianego w punkcie IV. 5. zapewniacie Państwo po swojej stronie łącze 50 Mb/s, na potrzeby bezpiecznego, szyfrowanego łącza wypuszczonego do Internetu, które zostanie połączone z łączem usługodawcy o tej samej przepustowości, czy jest wymagane dostarczenie całkowicie osobnego łącza o wskazanych parametrach?

Tak Zamawiający zapewnia. Nie jest wymagane dostarczenie osobnego łącza.

Pytanie nr 9.

Czy do 30 dni od dnia podpisania umowy ma być uruchomiona pełna usługa? Czy po tym czasie zgodnie z wcześniej przedstawionym harmonogramem będzie możliwość do konfigurowania środowiska, aby zoptymalizować jego działanie?

Tak, uruchomiona pełne usługa.

Pytanie nr 10.
W związku z zadanymi pytaniami zwracam się z prośbą o przedłużenie terminu składania oferty do 30.10.2024r.

Specjalistyczny Szpital im. dra Alfreda Sokołowskiego
ul. Alfreda Sokołowskiego 4
58-309 Wałbrzych
www.zdrowie.walbrzych.pl
szpitalsokolowski@zdrowie.walbrzych.pl

sekretariat 74 64 89 600
faks 74 64 89 746
centrala 74 64 89 742

Termin ulega zmianie do 29.10.2024r

Pytanie nr 11.
Czy Zamawiający umożliwi lokowanie serwerów środowiska SIEM w datacenter spełniającym wymagania normy ISO/IEC27001 lokowanym w Polsce lub w Niemczech?

Wymagania dla data Center zostały określone i nie ulegają zmianom.

Pytanie nr 12.
Czy Zamawiający zapewni zasoby niezbędne pod utrzymanie komponentów kolektora logów dla środowiska SIEM (maszyna wirtualna o parametrach 8vcpu, 16gb ram, 500gb hdd)?

Tak Zamawiający zapewni.

Pytanie nr 13.
Czy Zamawiający umożliwi integrację źródeł danych poprzez protokół syslog oraz rozwiązanie agentowe?

Tak Zamawiający umożliwi.

Pytanie nr 14.
Jakie niedomyślne źródła danych Zamawiający przewiduje do integracji (protokół, nazwa źródła danych)?

Niedomyślnych źródeł danych nie przewidujemy.

Pytanie nr 15.
Czy Zamawiający wymaga od wykonawcy dostarczenia dedykowanego łącza symetrycznego do perymetru wykonawcy o przepustowości 50/50 (czy Zamawiający planuje wykorzystać istniejące, swoje łącze do zestawienia tunelu VPN)?

Zamawiający udostępni łącze.

Pytanie nr 16.
Jaki jest planowany zakres ilości hostów objętych skanowaniem podatności (ilość hostów eksponowanych publicznie, ilość hostów w sieci LAN)

Zakładamy min. 100 hostów objąć skanowaniem. Posiadamy 1 host publiczny.

Specjalistyczny Szpital im. dra Alfreda Sokołowskiego
ul. Alfreda Sokołowskiego 4
58-309 Wałbrzych
www.zdrowie.walbrzych.pl
szpitalsokolowski@zdrowie.walbrzych.pl

sekretariat 74 64 89 600
faks 74 64 89 746
centrala 74 64 89 742

Pytanie nr 17.
Czy Zamawiający udostępni formularz ofertowy na którym ma zostać złożona oferta?

Zamawiający nie udostępnia formularza ofertowego.

Pytanie nr 18.
Czy Zamawiający może przekazać wzór umowy, czy też zaakceptuje zawarcie umowy na wzorze wykonawcy?

Umowa zostanie przekazana po rozstrzygnięciu.

Pytanie nr 19.
Punkt IV.9 OPZ brzmi: wdrożenie, uruchomienie i przekazanie systemu do eksploatacji, uruchomienie usługi – w czasie zadeklarowanym przez usługodawcę, maksymalnie do 30 dni od zawarcia umowy;
Punkt 7 Zaproszenia – Termin realizacji zamówienia do 7 dni od złożenia zamówienia.
Prosimy o odpowiedź, który z powyższych parametrów jest prawidłowy (zakładamy, że wartość z OPZ)

Wartość w OPZ

Pytanie nr 20.
Jakie systemy bezpieczeństwa są stosowane przez Zamawiającego (firewall, system antywirusowy/EDR/XDR, system Antyspam/antyphishing, Proxy, PAM, DLP, NAC, WAF, VPN Gateway, IDS/IDP, SSL decryptor, HoneyPot, inne). Prosimy o podanie producentów oraz ilości systemów zabezpieczeń.

Fortigate, Eset Antywirus, Spamassasin

Pytanie nr 21.
Ile Centrów Przetwarzania Danych/serwerowni posiada Zamawiający.

Zamawiający posiada 3.

Pytanie nr 22.
Ilu użytkowników korzysta z infrastruktury IT Szpitala (wewnętrznych i zewnętrznych), prosimy o podanie ilości stacji roboczych i urządzeń mobilnych

Około 600.

Pytanie nr 23.
Czy Zamawiający korzysta w swojej infrastrukturze IT z następujących systemów (Active Directory/LDAP; DNS, PKI – prosimy o podanie ilości serwerów

Specjalistyczny Szpital im. dra Alfreda Sokołowskiego
ul. Alfreda Sokołowskiego 4
58-309 Wałbrzych
www.zdrowie.walbrzych.pl
szpitalsokolowski@zdrowie.walbrzych.pl

sekretariat 74 64 89 600
faks 74 64 89 746
centrala 74 64 89 742

Tak Zamawiający korzysta z AD i DNS, posiadamy 57 serwerów.

Pytanie nr 24.
Z jakiego systemu poczty elektronicznej korzysta Zamawiający

Zamawiający korzysta z IredMAil.

Pytanie nr 25.
Z jakich systemów zarządzania stacjami roboczymi/serwerami/urządzeniami mobilnymi korzysta Zamawiający

Zamawiający nie korzysta.

Pytanie nr 26.
Ile łączy do sieci Internet posiada Zamawiający, jaka jest przepustowość tych łączy

Zamawiający posiada 3 łącza, 1GB/1GB, 100MB/20MB, 300MB/100 MB

Pytanie nr 27.
Ile urządzeń aktywnych posiada sieć LAN/WAN Zamawiającego (routery, przełączniki); czy sieć LAN jest centralnie zarządzana.

Zamawiający posiada 65 urządzeń. Sieć nie jest centralnie zarządzana.

Pytanie nr 28.
Czy Zamawiający posiada sieć WLAN – prosimy o podanie ilości kontrolerów i Access Point'ów

Tak Zamawiający posiada sieć WLAN, 1 kontroler, 80

Pytanie nr 29.
Prosimy o doprecyzowanie co Zamawiający rozumie poprzez: "Wykonawca musi posiadać możliwość wykonywania identyfikacji zagrożeń w odniesieniu do systemów informacyjnych Zamawiającego;"
Zapis pozostaje bez zmian . Jest precyzyjny

Pytanie nr 30.
W punkcie IV, 4. Zamawiający określił liczbę źródeł logów na poziomie
100 do 700. Czy Zamawiający jest w stanie podać bardziej szczegółowo ilości systemów oraz urządzeń w celu obliczenia kosztu licencji?

Zamawiający nie jest w stanie podać bardziej szczegółowo ilości źródeł..

Pytanie nr 31.
W punkcie IV podpunkt 6. K. raportowanie incydentów poważnych w rozumieniu ustawy o Krajowym Systemie Bezpieczeństwa (Dz.U. z 2018 r. poz.
1560) do CSIRT NASK do 24h, - Czy Zamawiający potwierdza że to zamawiający będzie zgłaszał a po stronie wykonawcy jest przygotowanie informacji do zgłoszenia?

Tak Zamawiający potwierdza.

Pytanie nr 32.
Czy Zamawiający zgodzi się na przedłużenie terminu na wdrożenie na 60 dni aby umożliwić dokładną analizę oraz poprawne wdrożenie?

Zamawiający nie zgadza się na przedłużenie terminu.

Pytanie nr 33.
Co Zamawiający rozumie przez Termin realizacji zamówienia do 7 dni od złożenia zamówienia?

Zgodnie z OPZ 30 dni.

Pytanie nr 34a.
W nawiązaniu do zmiany opisu przedmiotu zamówienia opublikowanej 21.10.2024 r. wnosimy o przywrócenie pierwotnych zapisów. Prosimy również o wprowadzenie wymogów, aby posiadany certyfikat ISO 27001 był wystawiony w oparciu o akredytację Polskiego Centrum Akredytacji. Informujemy, iż certyfikat wystawiony bez akredytacji nie ma właściwie żadnej wartości. Praktycznie każdy może go sobie stworzyć i wydrukować samodzielnie.

Zapisy pozostają bez zmian.

Pytanie nr 34.
Czy dla norm 22301, 27017, 27018 akceptują Państwo wdrożenie równoważnych standardów w zakresie wpływającym na pracę SOC?

Zapisy pozostają bez zmian.

Pytanie nr 35.
Jaki jest cel posiadania certyfikatu ochrony elektromagnetycznej dla pomieszczeń SOC na poziomie SSoE2?

Specjalistyczny Szpital im. dra Alfreda Sokołowskiego
ul. Alfreda Sokołowskiego 4
58-309 Wałbrzych
www.zdrowie.walbrzych.pl
szpitalsokolowski@zdrowie.walbrzych.pl

sekretariat 74 64 89 600
faks 74 64 89 746
centrala 74 64 89 742

Zapisy pozostają bez zmian

Pytanie nr 36.
W związku z weryfikacją techniczną i procedurami Wykonawcy dla zatwierdzania ofert niestandardowych aby móc złożyć ofertę w postępowaniu Wykonawca prosi o przedłużenie terminu składania ofert do dnia 06.11.2024 roku. Czy Zamawiający wyrazi zgodę na przedłużenie terminu składania ofert ?

Termin ulega zmianie do 29.10.2024r

Pytanie nr 37.
Czy Zamawiający wyrazi zgodę na wydłużenie czasu wdrożenia do 90 dni od podpisania umowy aby zachować równość szans dla podmiotów uczestniczących w postępowaniu oraz utrzymania konkurencyjności ?

Zapisy pozostają bez zmian.

Pytanie nr 38.
Czy zmawiający wyraża zgodę na wycenienie funkcjonalności 3 linii SOC w trybie time and material(analiza malwere/ respose) ?

Zamawiający nie wyraża zgody.

Pytanie nr 39.
Proszę o zmianę zapisu dotyczącego „ W ramach podłączenia źródeł logów dostawca usługi uruchomi przesyłanie logów do SIEM, przygotuje sposób podłączania źródeł i przekaże go do Zamawiającego w celu realizacji pozostałych zasobów z tego samego typu". Wykonawca dostarczy instrukcje do uruchomienia funkcjonalności przesyłania logów do SIEM, która będzie dotyczyła również podłączania źródeł i przekaże go do Zamawiającego".

Zapisy pozostają bez zmian.

Pytanie nr 40.
Nawiązując do zapisu Zamawiającego „Wykonawca musi posiadać możliwość wykonywania zabezpieczania informacji potrzebnych do analizy powłamaniowej, pozwalających na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej, w tym informacji dotyczących: rodzajów usług kluczowych, na które incydent miał wpływ, liczby użytkowników usługi kluczowej, na których incydent miał wpływ, momentu wystąpienia i wykrycia incydentu oraz czas jego trwania, zasięgu geograficznego obszaru, którego dotyczy incydent poważny, wpływu incydentu na świadczenie usługi kluczowej przez innych

operatorów usług kluczowych i dostawców usług cyfrowych, przyczyny zaistnienia incydentu i sposobu jego przebiegu oraz skutków jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe na potrzeby postępowań prowadzonych przez organy ścigania.
„Czy zamawiający się zgadza się abym wykonawca zabezpieczał tylko wyłącznie logi, ze źródeł w ramach SIEM oraz wykonawca przekazał instrukcje, w jaki sposób zamawiający ma zabezpieczyć u siebie
materiały dowodowe? Elementy wsparcia analizy powłamaniowej byłyby wyceniane w trybie time and material.

Zapisy pozostają bez zmian

Pytanie nr 41.
Nawiązując do podpunktu zamawiającego „środowisko, na którym realizowana jest usługa SOC oraz SIEM będzie uruchomione na dedykowanym środowisku wysokiej dostępności H” Czy zamawiający wyrazi zgodę na realizacje usługi na środowisku wysokiej dostępności HA w ramach platformy MT?

Zamawiający nie wyraża. Zapisy pozostają bez zmian

Pytanie nr 42.
Nawiązując do podpunktu zmawiającego : „ilość źródeł logów: minimum 100, maksimum 700. w tym serwery Windows, serwery, Linuks (różne dystrybucje) oraz urządzenia sieciowych” Zachowując element konkurencyjności wykonawca prosi o wskazanie dokładnych parametrów ilości : źródeł do monitorowania oraz EPSów w celu złożenia oferty pod potrzeby zamawiającego.

Zapisy pozostają bez zmian

Pytanie nr 43.
W kwestii skanów podatności proszę o doprecyzowanie czy wymieniona usługa ma obejmować adresy IP publiczne czy lokalne też?

Lokalne też.

Pytanie nr 44.
Czy zmawiający wyraża zgodę na umiejscowienie kolektorów SIEMowych na 4 wirtualnych maszynach po swojej stronie ?

Zamawiający nie wyraża zgody.

Specjalistyczny Szpital im. dra Alfreda Sokołowskiego
ul. Alfreda Sokołowskiego 4
58-309 Wałbrzych
www.zdrowie.walbrzych.pl
szpitalsokolowski@zdrowie.walbrzych.pl

sekretariat 74 64 89 600
faks 74 64 89 746
centrala 74 64 89 742

Pytanie nr 45.

W dokumentach po zmianie pojawił się wymóg posiadania certyfikatów:
1. zgodności z normą PN-EN ISO/IEC 270018, która dotyczy kodeksu postępowania ochrony danych osobowych w chmurach obliczeniowych funkcjonujących jako podmioty przetwarzające dane osobowe,
2. zgodności z normą PN-EN ISO/IEC 27017, która zapewnia dostawcom usług w chmurze i klientom korzystającym z usług w chmurze kontrolę, wytyczne w zakresie stosowania zabezpieczeń podnoszących poziom bezpieczeństwa usług.
Wnioskujemy, iż normy te mają zastosowanie do rozwiązań chmurowych SOC. Prosimy więc o wyjaśnienie, że jeżeli wykonawca ma rozwiązanie nie oparte na chmurze publicznej zewnętrznego dostawcy, to te normy są nadprogramowe i niepotrzebne, gdyż nie będzie miało miejsca chmurowe przetwarzanie danych. Dane z infrastruktury klienta pobierane są przez szyfrowany kanał IPSEC. Tym samy prosimy o wykreślenie tych norm dla rozwiązań nie opartych na chmurze publicznej zewnętrznego dostawcy.

Zapisy pozostają bez zmian.

Kierownik Działu

Zamówień Publicznych i Zaopatrzenia

Małgorzata Słomiana

Dział Zamówień Publicznych i Zaopatrzenia

Sporządziła: Agnieszka Piasecka

nr tel.: 74/6489744