DOTYCZY: Usługi **monitorowania środowiska pracy Zintegrowanego Systemu Informatycznego Zamawiającego firmy Asseco Poland (ZSI)**

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest usługa monitorowania środowiska pracy Zintegrowanego Systemu Informatycznego InfoMedica/AMMS (ZSI) Zamawiającego. Monitorowanie ma przeciwdziałać powstawaniu różnego typu awarii poprzez wcześniejsze przeprowadzenie optymalizacji działania ZSI.

Monitorowaniem musi być objęte kompleksowo całe oprogramowanie tzn. samo oprogramowanie, serwer, na którym działa, system operacyjny danego serwera oraz współpraca sieci LAN z tym serwerem.

Zamawiający informuje, że posiada aktualnie wdrożoną usługę monitoringu środowiska pracy ZSI realizowaną przez firmę Asseco Poland. W przypadku gdy usługa monitoringu będzie świadczona z wykorzystaniem innego oprogramowania niż aktualnie wykorzystywane przez Zamawiającego Wykonawca zobowiązany będzie do wdrożenia nowego oprogramowania zgodnie z minimalnymi wymaganiami opisanymi poniżej.

Lp.	Wymagania minimalne:
1	Przedmiotem zamówienia jest świadczenie przez Wykonawcę usługi monitorowania środowiska pracy w zakresie ZSI Zamawiającego wraz z całym środowiskiem niezbędnym do poprawnego działania wszystkich usług realizowanych przez system, w szczególności usługa ma polegać na: • kompleksowym monitoringu całego środowiska niezbędnego do poprawnego działania wszystkich usług realizowanych przez ZSI • dostarczeniu i wdrożeniu niezbędnego oprogramowania monitorującego środowisko pracy ZSI, wraz ze wszystkimi niezbędnymi licencjami (jeżeli będą konieczne) Zamawiający poprzez monitorowanie części opisanej jako InfoMedica rozumie monitorowanie tylko bazy danych bez monitorowania aplikacji na stacjach końcowych • diagnostyce, analizie oraz przeprowadzeniu konfiguracji parametrów środowiska systemowego (systemów operacyjnych na których posadowione jest monitorowane środowisko) wynikających z wykrytych problemów, oraz przekazaniu rekomendacji w formie raportu z przeprowadzonych działań • diagnostyce, analizie oraz przeprowadzeniu konfiguracji parametrów serwerów aplikacyjnych wynikających z wykrytych problemów, oraz przekazaniu rekomendacji w formie raportu z przeprowadzonych działań • diagnostyce, analizie oraz przeprowadzeniu konfiguracji parametrów serwerów bazodanowych aplikacyjnych wynikających z wykrytych problemów oraz przekazaniu rekomendacji w formie raportu z przeprowadzonych działań • diagnostyce, analizie oraz przeprowadzeniu konfiguracji parametrów oprogramowania aplikacyjnego/dziedzinowego wynikająca z wykrytych problemów, oraz przekazaniu rekomendacji w formie raportu z przeprowadzonych działań
	Raport z przeprowadzonych działań musi zostać przekazany Zamawiającemu niepóźnej niż do 5 dni roboczych od momentu wystąpienia nieprawidłowości. W przypadku wystąpienia złożonych problemów czas dostarczenia raportu może zostać wydłużony, jednakże Zamawiający każdorazowo musi zostać poinformowaniu o takim fakcie

	Zamawiający informuje, że rozumie „nieprawidłowość" jako zdiagnozowany incydent, który został zakwalifikowany jako istotny problem dotyczący wydajności lub awarii wpływający bezpośrednio lub pośrednio na prawidłową pracę systemu ZSI, dla którego zostały podjęte czynności diagnostyczne lub naprawcze.
	Zamawiający wymaga, aby raporty, o których mowa powyżej zawierały minimum następujące informacje: a. Data rozpoczęcia i zakończenia działania b. Kategoria (baza danych, aplikacja, system operacyjny, platforma, email, zadanie) c. Temat zadania /przeprowadzonego działania d. Opis realizacji zadania Zamawiający dopuszcza przekazywanie raportów w formie wiadomości e-mail
	dostęp do Inżynierów Systemowych w godzinach od 8:00 – 16:00
	Szkolenie personelu Zamawiającego z zakresu wdrożonego oprogramowania monitorowania środowiska pracy
2	Minimalne wymagania funkcjonalne dla oprogramowania monitorującego środowisko pracy ZSI: • autonomiczny moduł monitoringu zintegrowany z panelem administracyjnym systemu AMMS • automatyczny proces przekazywania / synchronizowania wprowadzonych zmian konfiguracyjnych w module monitoringu systemu AMMS do niezależnego modułu wykonawczego monitoringu • musi udostępniać interfejs do edycji parametrów systemu monitoringu (m.in. adresów URL agentów, parametrów poczty SMTP, tokenów SMS i serwerów Proxy • musi umożliwiać dodawanie, edycję i usuwanie danych serwerów poddawanych monitoringowi • musi pozwalać na definiowanie i weryfikację dostępności adresów zewnętrznych platform integracyjnych (np. NFZ, e-zdrowie) • musi umożliwiać ręczne wprowadzanie i monitorowanie komponentów działających wewnątrz sieci szpitala (np. Serwera Integracji) • musi zapewniać konfigurację monitorowania instancji baz danych Oracle. • musi umożliwiać zarządzanie wysyłką powiadomień alarmowych poprzez e-mail oraz wiadomości SMS. • centralna i automatyczna rejestracja zdarzeń serwerów aplikacyjnych i bazodanowych, • centralna i automatyczna rejestracja plików logowania serwerów aplikacyjnych i bazodanowych • centralna i automatyczna rejestracja zdarzeń występujących w systemach operacyjnych • centralna i automatyczna rejestracja wybranych zdarzeń w systemach dziedzinowych uruchomionych na serwerach aplikacyjnych • automatyczna rejestracja zdarzeń w trybie 24/7/365 • ustawienie czasu retencji przechowywanych danych historycznych

	• przegląd danych za pomocą centralnej konsoli dostępnej z przeglądarek internetowych, • przegląd danych za pomocą typów wykresów: słupkowy, kołowy, wykres w czasie, tabela, zegarowy, histogram • przegląd danych historycznych • przegląd w czasie rzeczywistym wskazanych zdarzeń reprezentujących stan środowiska systemowego, aplikacyjnego i bazodanowego, • przegląd w czasie rzeczywistym wybranych zdarzeń w systemach uruchomionych na serwerach aplikacyjnych • natychmiastowa wysyłka powiadomień o ostrzeżeniach i awariach • przekazywanie powiadomień w zależności od przyjętych wartości krytycznych dla zdarzeń • przekazywanie powiadomień za pomocą komunikatora działającego na platformie mobilnej
3	Dostarczone oprogramowanie monitorujące musi posiadać licencję typu 'otwartego' (bez limitu monitorowanych urządzeń, hostów, systemów itp.), umożliwiającą Zamawiającemu samodzielne i bezpłatne dodawanie dowolnej liczby nowych systemów/serwerów do platformy monitoringu. Na dzień uruchomienia systemu, Wykonawca skonfiguruje i obejmie monitoringiem bazowym 27 systemów/serwerów składających się obecnie na ZSI
4	Wymagania dodatkowe: • w przypadku świadczenia usługi przez Wykonawcę niebędącego producentem oprogramowania ZSI, Wykonawca musi przedstawić oświadczenie, że może świadczyć usługi w w/w zakresie diagnostyki oraz konfiguracji ZSI • usługi mogą być wykonywane jedynie przez tych Wykonawców, którzy posiadają niezbędną wiedzę i doświadczenie oraz dysponują odpowiednim potencjałem technicznym i osobami zdolnymi do należytego wykonania zamówienia.
5	Czas trwania usługi 24 /36 miesięcy od momentu uruchomienia wdrożonej usługi potwierdzonej protokołem powdrożeniowym, płatność za usługę w okresach miesięcznych
VII WYMAGANIA DOTYCZĄCE CYBERBEZPIECZEŃSTWA	
1.	Instalacja krytycznych patchy bezpieczeństwa dla dostarczonego oprogramowania – w ciągu 14 dni od publikacji poprzez oficjalne kanały producenta oprogramowania np. Biuletyny Bezpieczeństwa, Wewnętrzne systemy dystrybucji poprawek, Bazy wiedzy producenta
2	Przechowywanie logów dostępu przez minimum 90 dni, Wykonawca zobowiązany będzie do udostępnienia ich na żądanie Zamawiającego w przypadku incydentu
3.	Wykonawca jest zobowiązany do niezwłocznego powiadomienia Zamawiającego o usuniętych lub zredukowanych podatnościach bezpieczeństwa, wraz z zaleceniami dotyczącymi zabezpieczenia systemów oraz informacjami o zmianach w Oprogramowaniu Aplikacyjnym oraz do współpracy w zakresie ograniczenia wpływu na funkcjonowanie Oprogramowania Aplikacyjnego."
4.	Wykonawca jest zobowiązany w przypadku wystąpienia incydentu obejmującego dostarczone oprogramowanie zapewnić wsparcie gwarancyjne w zakresie udostępnienia logów systemowych, które są dostępne i przechowywane w bazie danych.
5.	Zamawiający w okresie gwarancji może przeprowadzić coroczne badanie ankietowe Wykonawcy, które będzie miało na celu zweryfikowanie czy personel Wykonawcy świadczy usługi gwarancyjne zgodnie z procedurami bezpieczeństwa oraz czy systemy lub infrastruktura Wykonawcy chronią prawidłowo powierzone dane.

	Badanie ankietowe będzie zawierało następujące pytania: 1. Czy wyznaczono osoby (osobę) odpowiedzialną za zarządzanie bezpieczeństwem informacji? Jeśli tak, to prosimy o podanie danych kontaktowych. 2. Czy została wdrożona polityka bezpieczeństwa informacji zgodna z ISO 27001 lub równoważna? 3. Czy prowadzony jest formalny rejestr ryzyk i proces jego regularnej aktualizacji? 4. Czy realizowane są cykliczne szkolenia pracowników z bezpieczeństwa? 5. Czy organizacja posiada certyfikaty potwierdzające zgodność (ISO 27001, ISO 22301, SOC 2 lub inne)? Jeśli tak, to prosimy o podanie, które. 6. Czy w ostatnich 2 latach przeprowadzono u Wykonawcy audyt bezpieczeństwa (wewnętrzny/zewnętrzny)? 7. Czy został wdrożony proces zapewnienia zgodności z NIS2 (raportowanie incydentów, ochrona danych osobowych)? 8. Czy pracownicy mający dostęp do systemów przechodzą proces weryfikacji (np. NDA)? 9. Czy stosowane są zasady minimalnych uprawnień i segregacji obowiązków? 10. Czy stosowane są MFA dla wszystkich zdalnych dostępów? 11. Czy wdrożony jest proces monitorowania dostępu do danych i systemów (logowanie, audyt)? 12. Czy wdrożony został formalny plan reagowania na incydenty bezpieczeństwa (IRP)? 13. Czy powołany został zespół reagowania na incydenty? 14. Czy prowadzona jest analiza przyczyn incydentów i raport działań naprawczych? 15. Czy w ciągu ostatnich 3 lat wystąpił incydent poważny/wyciek danych i jakie działania naprawcze wdrożono? 16. Czy wykorzystuje się z podwykonawców w świadczeniu usług dla Zamawiającego? 17. Czy wprowadzony został proces oceny bezpieczeństwa podwykonawców (np. ankiety, audyty)? 18. Czy umowy z podwykonawcami zawierają klauzule bezpieczeństwa (np. RODO) 19. Czy dostawcy Wykonawcy mają obowiązek raportowania incydentów bezpieczeństwa w określonym czasie? 20. Czy zostały przygotowane plany ciągłości działania (BCP) i odtwarzania po awarii (DRP)? 21. Jakie są gwarantowane czasy odtworzenia (RTO, RPO) dla usług świadczonych dla Zamawiającego? 22. Czy regularnie testowane są scenariusze awaryjne? 23. Czy przygotowana jest redundancja dla kluczowych usług (data center, łącza, zasilanie)?
6.	W przypadku wystąpienia zaleceń po przeprowadzeniu badania ankietowego Wykonawca ma obowiązek ich wdrożenia w terminie 30 dni od daty ich otrzymania.