Załącznik nr1.

Opis przedmiotu zamówienia

I. **Przedmiotem zamówienia jest:**

Świadczenie usługi SOC (Security Operation Center) dla Specjalistycznego Szpitala im. dra Alfreda Sokołowskiego w Wałbrzychu, polegającej na monitorowaniu, analizowaniu i reagowaniu na incydenty związane z cyberbezpieczeństwem w modelu usługowym (dostawca usługi zapewnia po swojej stronie wymaganą infrastrukturę, oprogramowanie i niezbędne zasoby) wraz z udostępnieniem systemu klasy SIEM (Security Information and Event Management) oraz skanera podatności przez okres 12 miesięcy zgodnie z poniższymi wymaganiami:

II. **Wymagania formalne wobec wykonawcy:**

- Posiadanie certyfikatu na zgodność działań z normą PN-EN ISO/IEC 27001 System zarządzania bezpieczeństwem informacji przez cały okres obowiązywania umowy;
- Wykonywanie usługi SOC, o której jest mowa w OPZ zgodnie z wymaganiami Ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa w zakresie wsparcia Operatorów Usług Kluczowych, rozporządzeniem Ministra Cyfryzacji z dnia 4 grudnia 2019r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo;
- Podejmowanie działań i procesów operacyjnych zgodnie z wymogami norm PN-EN ISO/IEC 27001 lub równoważne, PN-EN ISO 22301 lub równoważne oraz dokumentem RFC 2350 publikowanym przez organizację Internet Engineering Task Force (IETF);
- Posiadanie ubezpieczenia OC w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną min. 3 000 000 zł przez cały okres obowiązywania umowy.

III. **Wymagania formalne wobec wykonawcy wynikające z rozporządzenia ministra cyfryzacji z dnia 4 grudnia 2019 r w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo:**

- Wykonawca musi posiadać, utrzymywać i aktualizować system zarządzania bezpieczeństwem informacji spełniającym wymagania Polskiej Normy PN-EN ISO/IEC 27001 w zakresie obejmującym co najmniej świadczone usługi;
- Wykonawca musi zapewnić ciągłość działania usługi obsługi incydentu oraz wsparcia operatora usługi kluczowej z czasem reakcji adekwatnym do charakteru usługi kluczowej;
- Posiadać i udostępniać deklarację swojej polityki działania w zakresie określonym dokumentem RFC 2350.
- Wykonawca musi zapewnić przez cały okres obowiązywania umowy z Zamawiającym dysponować personelem posiadający umiejętności, o których mowa w par. 1 ust. 1 pkt 4 rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.
- Wykonawca musi posiadać możliwość wykonywania identyfikacji zagrożeń w odniesieniu do systemów informacyjnych Zamawiającego;

- Wykonawca musi posiadać możliwość wykonywania wykrywania przełamania lub ominięcia zabezpieczeń systemu informacyjnego Zamawiającego, prowadzenia analizy powłamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego operatora usługi kluczowej;
- 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;
- Wykonawca musi dysponować prawem do wyłącznego korzystania z pomieszczenia lub zespołu pomieszczeń, w których będzie realizowana usługa SOC, a pomieszczenia te muszą posiadać odpowiedni poziom zabezpieczeń fizycznych zgodny z w/w rozporządzeniem.
- Wykonawca musi dysponować redundantnymi środkami łączności umożliwiającymi prawidłową i bezpieczną wymianę informacji z podmiotami, dla których świadczą usługi SOC oraz właściwym CSiRT.
- Inne wynikające z rozporządzenia.

IV. <u>W skład usługi będzie wchodzić:</u>

1. monitorowanie bezpieczeństwa wraz z identyfikacją niebezpiecznych zdarzeń w ramach SOC w trybie ciągłym: 24/7/365,
2. uruchomienie środowiska SIEM (Security Information and Event Management) posiadanego, administrowanego i uruchomionego w infrastrukturze Wykonawcy
3. środowisko, na którym realizowana jest usługa SOC oraz SIEM będzie uruchomione na dedykowanym środowisku wysokiej dostępności HA
4. ilość źródeł logów: minimum 100, maksimum 700. w tym serwery Windows, serwery Linuks (różne dystrybucje) oraz urządzenia sieciowe,
5. zestawienie, zabezpieczenie i obsługa połączenia w relacji Zamawiający do SOC poprzez uruchomienie łącza szyfrowanej transmisji danych w technologii VPN IP MPLS lub VPN IP SEC o minimalnej przepustowości 50/50 Mbps realizowane na koszt usługodawcy,
6. realizowanie zadań w ramach opłaty abonamentowej - w szczególności:
   a. reagowanie na podejrzenia i obsługa zidentyfikowanych incydentów,
   b. ilość incydentów: możliwość obsługi co najmniej 15/24h,
   c. analiza incydentów i ich klasyfikowanie,
   d. zarządzanie incydentami,
   e. raportowania incydentów,
   f. opracowanie i obsługa scenariuszy monitorowania i reagowania,
   g. SLA o notyfikacji – do 60 min. od zidentyfikowania incydentu,
   h. minimalny gwarantowany poziom incydentu a czas reakcji:
      - incydent krytyczny – do 60 min,
      - incydent niekrytyczny – do 240 min,
   i. klasyfikacja (poziomy) incydentów uzgadniane będą w ramach wdrożenia i opracowywania scenariuszy monitorowania i reagowania,
   j. kanały komunikacji obejmujące notyfikację: e-mail i kontakt telefoniczny,
   k. raportowanie incydentów poważnych w rozumieniu ustawy o Krajowym Systemie Bezpieczeństwa (Dz.U. z 2018 r. poz. 1560) do CSIRT NASK do 24h,
   l. skanowanie podatności – infrastruktura krytyczna,

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

m. tworzenie rekomendacji bezpieczeństwa na podstawie incydentów bezpieczeństwa – dotyczących działań związanych z powstrzymaniem incydentu oraz zalecanych środkach naprawczych.

7. składowanie logów i dostęp w ramach zasobów dostawcy usługi, zlokalizowane w Polsce, w trybie wysokiej dostępności HA. Okres przechowania – minimum 6 miesięcy,
8. przedstawienie analizy przedwdrożeniowej i harmonogramu realizacji,
9. wdrożenie, uruchomienie i przekazanie systemu do eksploatacji, uruchomienie usługi – w czasie zadeklarowanym przez usługodawcę, maksymalnie do 30 dni od zawarcia umowy,
10. zapewnienie wsparcia grupy projektowej i dedykowanego kierownika projektu,
11. niezbędne licencje na uruchomienie systemu bezpieczeństwa.
12. 30h konsultacji specjalistów w zakresie organizacji/dostosowania monitorowanego środowiska.

W ramach analizy przedwdrożeniowej dostawca usługi przeprowadzi analizę źródeł logów oraz określi sposób ich parsowania w SIEM, przeprowadzi analizę potrzebnych i dostępnych informacji do utworzenia reguł bezpieczeństwa dla systemu SIEM, określi wykonalności scenariuszy na podstawie dostępnych danych oraz analizę potencjalnych dodatkowych scenariuszy, wstępnie określi sposób reagowania na poszczególne podejrzenia incydentów.

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.

Dostawca usługi przeprowadzi wstępne strojenie i implementację reguł bezpieczeństwa, a rezultatem tych prac będzie działające parsowanie logów oraz zaimplementowane uzgodnione reguły. Dostawca usługi przeprowadzi strojenie systemu SIEM w celu zmniejszenia ilości fałszywych alarmów.

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