Załącznik Nr 2 do ZO

OPIS PRZEDMIOTU ZAMÓWIENIA – wymagane minimalne parametry techniczne

WYMAGANIA OGÓLNE

Przedmiotem zamówienia jest wdrożenie usług i oprogramowania w postaci systemu wspomagającego monitorowanie i reagowanie na incydenty bezpieczeństwa SOC (Operacyjne Centrum Bezpieczeństwa)

Poniżej wyspecyfikowano minimalne parametry systemu, które należy dostarczyć w ramach realizacji przedmiotu zamówienia.

Wymagania ogólne:
Zamawiający wymaga, aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

- posiadane środowisko teleinformatyczne,
- posiadaną konfigurację sieci,
- posiadaną konfiguracją urządzeń dostępowych i punktów styku z siecią publiczną,
- konfigurację serwerów i stacji roboczych.

Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z konfiguracją dostarczanego oprogramowania:

1. Zapewnienie niezbędnej infrastruktury (sprzętu i oprogramowania)
2. Instalacja oraz konfiguracji oprogramowania.
3. Integracja z systemami Zamawiającego
4. Testy rozwiązania.
5. Instruktaż dla administratorów.
6. Dostarczenie dokumentacji
7. Świadczenie usług utrzymania systemu przez okres 12 miesięcy

Oczekiwany sposób realizacji usługi:

- Zdalne monitorowanie zdarzeń i zarządzanie systemem przy wykorzystaniu bezpiecznego połączenia.
  Instalacja rozwiązania na platformie wirtualnej,
- Prezentacja informacji nt. zagrożeń i/lub incydentów u Zamawiającego w formie dashboardów (bieżąca aktualizacja)
- Wskazanie oraz klasyfikacja poziomu zagrożenia/incydentu oraz zapewnienie dostępu do informacji pozwalających na sprawne zarządzenie zarejestrowanymi zdarzeniami.

Zakres działań linii wsparcia:

- ***Monitoring***
  Bieżące monitorowanie zgłoszeń i incydentów wykrytych przez system monitorowania bezpieczeństwa,
  Ustalenie typu i poziomu zagrożenia ze strony wykrytego zdarzenia,
  Wstępna analiza zagrożeń uznanych za incydenty, zgodnie z ustalonymi procedurami i scenariuszami uzgodnionymi z Zamawiającym.
- ***Zarządzanie incydentami:***
  Realizacja okresowych raportów podsumowujących ilość incydentów i czasy obsługi, w terminach ustalonych w zależności od wpływu i wagi zagrożeń na bezpieczeństwo Zmawiającego.

- ***Czas reakcji:***
  Usługa świadczona jest w trybie ciągłym tj. 365 dni w roku 24h na dobę.

Opis parametrów minimalnych dostarczanego oprogramowania:

1. System monitoringu infrastruktury IT (SOC)	
Lp.	***Wymagane minimalne parametry techniczne***
Użytkownicy	
1.	■ Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat. ■ Zapewnienia równoległego dostępu do systemu dla wielu użytkowników. ■ Ograniczania użytkownikom dostępu do wybranych grup hostów. ■ Możliwość logowania z wykorzystaniem mechanizmu 2FA
Monitorowanie	
1.	■ Monitorowanie infrastruktury z szczególnym uwzględnieniem urządzeń i systemów mających styk s siecią publiczną ■ Monitorowania serwerów fizycznych. ■ Monitorowania urządzeń sieciowych. ■ Monitorowania stanu połączeń. ■ Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów ■ Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń. ■ Wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu. ■ Monitorowanie przerw serwisowych dla hostów i usług. ■ Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK). ■ Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane i generowane poprzez www). ■ Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW. ■ Monitorowanie poprawności działania DNS. ■ Współpraca z systemami wtyczek Nagios/Zabbix służących do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Windows/Linux i Unix. ■ Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence) ■ Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe ■ Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących) ■ Wykrywanie niestabilnie działających usług. ■ Monitorowanie dostępności stron internetowych. ■ Konfigurację hierarchiczną.
Prezentacja	
1.	■ Prezentację stanu systemów i urządzeń ■ Przegląd historii zdarzeń ■ Możliwość konfiguracji dashboardów, wybór elementów. ■ Wizualizację stanu działania całej infrastruktury na jednym dashboardzie.
Powiadomienia	

1.	■ Globalne wyłączanie powiadomień. ■ Powiadamianie użytkownika o problemach przez e-mail. ■ Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie. ■ Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników. ■ Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług ■ Raporty okresowe
Konfiguracja	
1.	■ Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW ■ Automatyczna konfiguracja i działanie z REST-API ■ Integracja danych z różnych źródeł danych (JSON, XML, SNMP)
Kolektor logów	
1.	■ System posiada własny kolektor logów syslog ■ Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps ■ Za pomocą agentów potrafi przetwarzać logi tekstowe i logi WEvent ■ Klasyfikuje wiadomości bazując zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe.
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” jest uważany za OK, a status „niezsynchronizowany” 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 poziomu obciążenia ■ System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog ■ System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog.
SOC	
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 ■ W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie monitorowania zgodnie z opisanymi poniżej wymaganiami. - Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24 / 7 / 365 - Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji. - Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.

Dostęp do systemu

1.	• Komunikacja pomiędzy komponentami systemu odpowiadającymi za agregacji, retencję i wizualizację danych musi odbywać się w sposób szyfrowany z wykorzystaniem protokołu TLS w wersji minimum 1.3. • Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać proroków TLS w wersji minimum 1.3. • System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Safari • Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem. • System musi wspierać mechanizm logowania 2FA • System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników. • System musi posiadać dedykowany widok zarządzania użytkownikami i rolami. • System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only" oraz „pełny". Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
Raportowanie i Archiwizacja danych	
1.	• System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika. • Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny. • Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu. • Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich ówcześniejszego rozpakowania. • System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie. • Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
Wdrożenie	
1.	• Zakres oczekiwanych prac związanych z wdrożenie system: • Opracowanie harmonogramu wdrożenia systemu. • Przeprowadzenie przez Wykonawcę analizy przedwdrożeniowej oraz projektu wdrożenia. • Przeprowadzenie instalacji i konfiguracji komponentów systemu. • Podłączenie do systemu wskazanych przez Zamawiającego źródeł danych. • Do podłączonych źródeł Wykonawca musi skonfigurować reguły korelacyjne, raporty oraz dashboardy z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem. • Wykonawca na etapie analizy przedwdrożeniowej przedstawi do akceptacji Zamawiającego listę proponowanych reguł korelacyjnych, wizualizacji oraz dashboardów odnoszących się do źródeł danych.
Wymagania niefunkcjonalne	
1.	• Wykonawca dostarczy rozwiązanie w terminie 7 dni od podpisania umowy. • Wykonawca przeprowadzi szkolenia z zakresu użytkowania oraz administrowania systemem • Szkolenie musi być prowadzone w języku polskim. • Każdy uczestnik szkolenia otrzyma certyfikat ukończenia. • Szkolenie winno być realizowane na miejscu lub po uzgodnieniu z Zamawiającym w trybie online.

3. Wykonanie skanu podatności	
Lp.	**Wymagane minimalne parametry techniczne**

1.	■ Wykonanie skanów otwartych portów w całej adresacji publicznej audytowanego podmiotu. ■ Wykorzystanie dedykowanego oprogramowania do wykrywania podatności zasilonego najnowszą bazą znanych podatności. ■ Wykonanie skanów nieuwierzytelnionych. ■ Wykonanie raportu końcowego. **Planowanie (faza I)** ■ Rekonesans, kolekcja danych i pozyskiwanie informacji, mapowanie **Testy stabilności i dostępności infrastruktury sieciowej na styku z Internetem (faza II)** ■ Skan całej puli adresacji publicznej jednostki audytowanej ■ Testy ekspozycji systemów na styku z Internetem ■ Opcjonalne testy destabilizujące infrastrukturę sieciową typu Denial of Service ■ W sytuacji wykrycia mniejszej bądź większej liczby systemów niż w przyjętych w punkcie „założenia skali i architektury przyjęte w wycenie”, nastąpi spotkanie między ■ zamawiającym, a wykonawcą, które będzie miało na celu doprecyzowanie danych lub ■ przekazanie dodatkowych informacji wykonawcy

Dodatkowe informacje i wymagania:

a) o zamówienie będzie mógł się ubiegać Wykonawca, który posiada odpowiednie rozwiązania techniczne i personel oraz doświadczenie w zakresie realizacji usług z zakresu cyberbezpieczeństwa dla minimum 5 jednostek medycznych w ciągu ostatnich 3 lat.

b) Zamawiający zastrzega, że wszelkie prowadzone w ramach instalacji i uruchomienia usługi prace instalacyjne/rekonfiguracyjne oprogramowania u urządzeń mogą być realizowane w godzinach 8:00-16:00 w dni robocze, po uzyskaniu zgody i pod warunkiem zatwierdzenia ich ze strony Zamawiającego.

c) usługa wdrożenia zostanie wykonana w terminie do 7 dni od dnia zawarcia umowy i obejmować będzie realizację monitorowania bezpieczeństwa „Zdalny SOC” przez okres 12 miesięcy .