**Załącznik nr 2 do SWZ**

**Część nr 6**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

## **1. Przedmiot zamówienia**

1.1. Przedmiotem zamówienia jest **dostawa, instalacja, konfiguracja oraz wdrożenie systemu klasy Security Information and Event Management (SIEM)** w infrastrukturze Zamawiającego, wraz ze szkoleniem administratorów oraz zapewnieniem wsparcia serwisowego.

1.2. System SIEM ma służyć do centralnego gromadzenia, przechowywania, analizy i korelacji logów oraz zdarzeń bezpieczeństwa z urządzeń i systemów teleinformatycznych Zamawiającego, w związku z realizacją inwestycji: „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia – Inwestycja D1.1.2”.

**2. Wymagania dla Systemu Zbierania Logów**

Wymagane jest dostarczenie centralnego systemu zbierania logów kompatybilnego z posiadanym systemem UTM Zamawiającego oraz spełniającego poniższe wymagania minimalne:

Rozwiązanie musi zostać dostarczone w postaci platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie Linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących Hypervisorach: VMware ESX/ESXi wersje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, 2025; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

**Interfejsy, Dysk:**

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności min. 3 TB.

**Parametry wydajnościowe:**

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

**Wymagania minimalne dla systemu:**

1. W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące incydenty na urządzeniach sieciowych Zamawiającego
2. Rozwiązanie musi realizować pełną funkcjonalność w środowisku teleinformatycznym Zamawiającego (instalacja lokalna / on-premise), bez konieczności przekazywania logów i danych eksploatacyjnych do środowisk chmurowych poza infrastrukturę Zamawiającego.
3. Architektura rozwiązania musi być oparta o fizyczne lub wirtualne sondy monitorujące, których rolą jest odbieranie kopii ruchu sieciowego, generowanie alarmów oraz/lub metadanych o zdarzeniach, przygotowanie przechwyconych plików do dalszej analizy oraz przekazywanie przetworzonych danych do urządzenia administracyjnego.
4. Architektura rozwiązania musi być oparta także o fizyczne urządzenie administrujące, którego rolą jest zarządzanie sondami, włącznie z regułami detekcji, sygnaturami i nadzorem stanu, dogłębna analiza odebranych plików, prezentacja wyników detekcji, a także przekazywanie danych do rozwiązań stron trzecich
5. Platformy muszą obsługiwać szyfrowanie dysków w standardzie LUKS.
6. Rozwiązanie musi wspierać implementację na środowisku wirtualnym takim jak m.in. VMWare, Hyper-V, Proxmox, KVM, OVM, OVF.
7. Licencja na zakup i serwis oprogramowania musi bazować na ilości aktywnie występujących w ruchu sieciowym adresów IP. Ilość adresów, objętych monitorowaniem: do 400.
8. Musi posiadać moduły zabezpieczone połączeniem (HTTPS) w przeglądarce
9. Konsola rozwiązania musi zawierać informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, sygnatury czasowe.
10. Konsola rozwiązania musi szacować poziom ryzyka dla każdego wykrytego zagrożenia oraz musi dawać możliwość tagowania zdarzeń i załączania opisu (notatek).
11. Konsola musi mieć wbudowane filtrowanie pomocą parametrów min.: data, agent lub poziom reguły (priorytet).
12. Konsola musi umożliwiać grupowanie takich samych zdarzeń w ramach jednego wpisu oraz podawać liczbę wystąpień identycznego zdarzenia
13. Konsola musi umożliwiać wyświetlanie zdarzeń pogrupowanych na podstawie opisu reguły wraz z liczbą ich wystąpienia.
14. Konsola musi umożliwiać wyświetlenie wyników w postaci tabeli, w której jest możliwość sortowania wyników.
15. Konsola musi umożliwiać wyświetlenie dla każdego wiersza dodatkowych opcji: podgląd ostatniego zdarzenia, usunięcie grupy zdarzeń oraz dodanie zdarzeń do grupy ignorowanych.
16. Konsola musi umożliwiać ustawienie liczby wyświetlanych wierszy.
17. Konsola musi umożliwiać utworzenie zgłoszenia z dowolnego zdarzenia. Dla każdego zgłoszenia musi być możliwość nadania tytułu oraz opisu ułatwiającego szukanie, identyfikację.
18. Konsola musi umożliwiać zmianę statusu zgłoszeń.
19. Konsola musi wyświetlać zgłoszenia w dedykowanym panelu.
20. Zgłoszenia muszą być przechowywane w lokalnej bazie danych.
21. Konsola musi posiadać dedykowany widok dla utworzonych zgłoszeń.
22. Z poziomu konsoli musi być dostępna opcja zmiany statusu zgłoszenia.
23. Rozwiązanie musi obsługiwać silniki detekcji takie jak Analiza Shellcode i Powershell, tj. detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wywoływania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach.
24. Rozwiązanie musi umożliwiać analizowanie całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń.

**Zakres funkcjonalny**

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

1. **Logowanie**
2. Podgląd logowanych zdarzeń w czasie rzeczywistym.
3. Możliwość przeglądania logów historycznych z funkcją filtrowania.
4. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
   1. Listę najczęściej wykrywanych ataków.
   2. Listę najbardziej aktywnych użytkowników.
   3. Listę najczęściej wykorzystywanych aplikacji.
   4. Listę najczęściej odwiedzanych stron www.
   5. Listę krajów, do których nawiązywane są połączenia.
   6. Listę najczęściej wykorzystywanych polityk Firewall.
   7. Informacje o realizowanych połączeniach IPSec.
5. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
6. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
7. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
8. **Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
6. **Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System musi korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   * Malware.
   * Aplikacje sieciowe.
   * email.
   * IPS.
   * Traffic.
   * Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
5. Funkcję zarządzania zdarzeniami z automatyzacją zadań, która może być konfigurowalna za pomocą playbooków składających się z reakcji i sekwencji zautomatyzowanych działań.
6. **Zarządzanie**
7. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
   1. Proces uwierzytelniania administratorów musi być realizowany w oparciu o lokalną bazę, Radius, LDAP, PKI.
8. System musi umożliwiać zdefiniowanie co najmniej 2 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

**Serwisy i licencje**

1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2. Wsparcie: System musi być objęty serwisem producenta przez okres min. 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
3. Funkcja analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach powinna być licencjonowana na okres min. 36 miesięcy.
4. Funkcja zarządzania zdarzeniami z automatyzacją zadań powinna być licencjonowana na okres min. 36 miesięcy

**Zakres wdrożenia**

1. Wykonawca dostarczy system, zainstaluje i skonfiguruje.
2. Zamawiający może wymagać skonfigurowania dodatkowych parametrów systemu, jeśli podczas wdrożenia zajdzie taka potrzeba.
3. Zamawiający wymaga, aby wdrożenie przeprowadził inżynier posiadający certyfikat techniczny producenta oferowanego rozwiązania, potwierdzający kompetencje z zakresu wdrażania systemów.
4. Wykonawca przed przystąpieniem do wdrożenia przygotuje harmonogram wdrożenia.

**Instruktaże**

Zamawiający wymaga przeprowadzenia instruktaży dla swoich administratorów zgodnie z poniższym opisem:

1. Instruktaż podstawowy (wdrożeniowy) – odbędzie się w trakcie wdrożenia i konfiguracji systemu w siedzibie Zamawiającego, jego przedstawiciele będą uczestniczyć w wykonywanych pracach.
2. Instruktaż powdrożeniowy musi zawierać elementy warsztatowe i opierać się na zadaniach praktycznych. Musi być przygotowany w wersji oprogramowania zastosowanej podczas wdrożenia.
3. Instruktaże muszą być prowadzone przez praktyka posiadającego co najmniej 3-letnie doświadczenie w zakresie wdrażania systemów oraz posiadającego certyfikat inżynierski w zakresie administracji.
4. **Wymagania dla Systemu Analizy Logów**

### W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.

### Rozwiązanie musi zostać dostarczone w postaci maszyn wirtualnej instalowanych w środowisku Vmware lub Windows Hyper-V

### Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach.

### Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.

### Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.

### Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.

### Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.

### Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.

### Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).

### Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.

### Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie. –

### Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).

### Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.

### Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).

### Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów)

### Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.

### Rozwiązanie musi umożliwiać tworzenie statycznych raportów.

### Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF.

### Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.

### Rozwiązanie musi umożliwiać tworzenie własnych raportów.

### Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.

### Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.

**Wymagania systemowe**

1. Liczba zdarzeń na sekundę (EPS): min. 9 500
2. Możliwość zarządzania logami: min. 3 lata
3. Liczba obsługiwanych urządzeń min. 600
4. Liczba zapisu zdarzeń na dobę: min 12000 MB
5. System logów musi wspierać hiperwizory: Vmware ESXi, Microsoft HyperV oraz Proxmox

**3. Wymagania dla Systemu SIEM.**

1. W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące incydenty na urządzeniach sieciowych Zamawiającego
2. Rozwiązanie musi w pełni realizować swoją funkcjonalność lokalnie (instalacja on-prem)
3. Architektura rozwiązania musi być oparta o fizyczne lub wirtualne sondy monitorujące, których rolą jest odbieranie kopii ruchu sieciowego, generowanie alarmów oraz/lub metadanych o zdarzeniach, przygotowanie przechwyconych plików do dalszej analizy oraz przekazywanie przetworzonych danych do urządzenia administracyjnego.
4. Architektura rozwiązania musi być oparta także o fizyczne urządzenie administrujące, którego rolą jest zarządzanie sondami, włącznie z regułami detekcji, sygnaturami i nadzorem stanu, dogłębna analiza odebranych plików, prezentacja wyników detekcji, a także przekazywanie danych do rozwiązań stron trzecich. Minimalne wymagania dla urządzenia administrującego:

* obudowa rack max. 2U dla min. 8 dysków
* procesor w architekturze x86, ilość rdzeni dla procesora min. 12. Wynik wydajności procesora zainstalowanego w oferowanym serwerze powinien przekraczać 173 punktów baseline w teście SPECrate®2017\_int\_base opublikowanym na stronie [www.spec.org](http://www.spec.org/) dla konfiguracji 2-procesorowej
* Min. 96 GB pamięci RAM w max. 4 modułach
* kontroler RAID z min. 8GB pamięci cache oraz podtrzymaniem bateryjnym lub min. 8GB pamięci cache typu flash
* dostępna powierzchnia dyskowa min. 38TB w RAID 5, min. 1,9 TB SSD w min. RAID 1
* karta sieciowa 2-portowa min. 10Gbit SFP+ wraz z modułami umożliwiającymi podłączenie do przełączników LAN Zamawiającego
* karta sieciowa 2-portowa min. 1Gbit RJ45
* dwa redundantne zasilacze Hot-Swap
* moduł zdalnego zarządzania poprzez konsolę graficzną wraz z licencją na min. 3 lata
* min. 3 lata gwarancji w miejscu instalacji, rozpoczęcie naprawy NBD

1. Platformy muszą obsługiwać szyfrowanie dysków w standardzie LUKS.
2. Rozwiązanie musi wspierać implementację na środowisku wirtualnym takim jak m.in. VMWare, Hyper-V, Proxmox, KVM, OVM, OVF.
3. Serwer dedykowany musi posiadać redundantne zasilanie oraz musi być objęty 3 letnim okresem gwarancyjnym w miejscu instalacji.
4. Sonda musi posiadać co najmniej 4 porty monitorujące i muszą być w stanie przetworzyć dane dla maksymalnego odbieranego ruchu sieciowego na poziomie 4Gb/s.
5. Serwer dedykowany musi obsługiwać do 3 900 zdarzeń na sekundę, musi przechowywać do 9 milionów zdarzeń, musi mieć możliwość detekcji malware, a także musi analizować przy pomocy silnika detekcji shellcode/powershell do 3 na sekundę.
6. Licencja na zakup i serwis oprogramowania musi bazować na ilości aktywnie występujących w ruchu sieciowym adresów IP. Ilość adresów, objętych monitorowaniem: do 400.
7. Musi posiadać moduły zabezpieczone połączeniem (HTTPS) w przeglądarce
8. Konsola rozwiązania musi zawierać informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, sygnatury czasowe.
9. Konsola rozwiązania musi szacować poziom ryzyka dla każdego wykrytego zagrożenia oraz musi dawać możliwość tagowania zdarzeń i załączania opisu (notatek).
10. Rozwiązanie musi obsługiwać silniki detekcji takie jak Analiza Shellcode i Powershell, tj. detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wywoływania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach.
11. Rozwiązanie musi umożliwiać analizowanie całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń.

**4. Wymagania dla konsoli systemu SIEM**

1. Konsola zarządzającą umożliwiająca grupowanie takich samych zdarzeń w ramach jednego wpisu oraz wyświetlająca liczbę wystąpień identycznego zdarzenia.
2. Konsola posiadającą możliwość tworzenia i śledzenia zgłoszeń.
3. Konsola umożliwiająca stworzenie zgłoszenia z dowolnego zdarzenia.
4. Konsola posiadająca dedykowany widok dla utworzonych zgłoszeń.

**5. Moduł EDR (Endpoint Detection and Response).**

Wykonawca wraz z system SIEM może dostarczyć moduł Endpoint Detection and Response wraz z centralną konsolą zarządzającą dla min. 300 urządzeń (adresów IP) oraz gwarancją i wsparciem technicznym na okres min. 36 miesięcy. Minimalne wymagania dla moduł EDR:

1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS umożliwiający bezproblemową współpracę z systemem antywirusowym do ochrony stacji roboczych, użytkowanym przez Zamawiającego.
2. Rozwiązanie musi zawierać centralną konsolę administracyjną umożliwiającą monitorowanie oraz wizualizację zebranych danych z zarządzanych urządzeń.
3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej.
4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
6. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, nazwę komputera, grupę, użytkownika.
7. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, rozmiar pliku.
8. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne lub niebezpieczne.
9. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.
10. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania komend zdalnych.
11. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
12. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
13. Rozwiązanie musi umożliwiać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
14. Rozwiązanie musi zapewniać integrację z przynajmniej takimi systemami jak: konsola programu antywirusowego, moduł EDR.
15. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: numer seryjny, informacje o systemie, procesor, pamięć RAM, karty sieciowe.
16. Serwer administracyjny musi posiadać możliwość tworzenia grup komputerów.
17. Rozwiązanie musi zapewniać korzystanie z min. 100 szablonów raportów, przygotowanych przez producenta lub własnych raportów tworzonych przez administratora.
18. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email oraz do dziennika syslog.
19. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami.
20. Rozwiązanie musi informować administratora o niezainstalowanych aktualizacjach systemowych.

**6.** **Oprogramowanie do monitorowania infrastruktury informatycznej.**

W celu zapewnienia ciągłości działania kluczowych elementów infrastruktury IT Zamawiającego należy zainstalować, skonfigurować system umożliwiający aktywny monitoring stanu pracy serwerów, macierzy, urządzeń sieci LAN/WAN, aplikacji, baz danych, zasilaczy awaryjnych. System musi wykrywać awarie, problemy lub spadek wydajności systemów, usług oraz wysyłać alerty zdefiniowanymi kanałami komunikacji. W ramach realizacji zadania Wykonawca dostarczy system objęty gwarancją i wsparciem technicznym na okres min. 36 miesięcy. Wykonawca podłączy wszystkie wymagane systemy wskazane przez Zamawiającego. System musi spełniać poniższe wymagania minimalne:

|  |  |
| --- | --- |
| 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. |
| Monitorowanie | |
| 2 | * Monitorowania serwerów fizycznych. * Monitorowania urządzeń sieciowych. * Monitorowania stanu połączeń. * Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów * Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux. * Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych. * Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń. * Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu. * Grupowanie hostów. * Definiowanie planowanych przerw serwisowych dla hostów i usług. * Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK). * Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych). * Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www). * Monitorowanie serwerów za pomocą agentów * Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server. * Monitorowanie Active Directory. * Monitorowanie serwerów plików, udziałów sieciowych. * Monitorowanie statusu serwerów Apache. * Monitorowanie baz danych: * ORACLE, * MySQL, * Postgress. * MSSQL Server * DB2 * Monitorowanie urządzeń przez następujące protokoły: * SNMP, * WMI, * IPMI. * Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW. * Monitorowanie poprawności działania DNS. * Monitorowanie środowiska VMware. * Monitorowanie środowiska Hyper-V. * Monitorowanie środowisk Proxmox * Monitorowanie działania serwera czasu NTP. * Monitorowanie offsetu czasu na serwerach. * Monitorowanie ping - czasy odpowiedzi, straty pakietów. * Monitorowanie zajętości miejsca na poszczególnych partycjach. * Monitorowanie obciążenia dysków. * Monitorowanie wykorzystania pamięci RAM. * Monitorowanie obciążenia CPU. * Monitorowanie logów systemowych Windows. * Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia. * Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane. * Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach 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, np. z kilku lokalizacji/oddziałów). * Wykrywanie niestabilnie działających usług. * Monitorowanie dostępności stron internetowych. * Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń). |
| Prezentacja | |
| 3 | * Prezentację stanu urządzeń na mapie. * Prezentację danych na dashboardach. * Elastyczną konfigurację dashboardów, wybór elementów. * Wizualizację stanu działania całej infrastruktury na jednym dashboardzie. * Tworzenie indywidualnych dashboardów przez użytkowników |
| Powiadomienia | |
| 4 | * 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 |
| Konfiguracja | |
| 5 | * Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW * Automatyczna konfiguracja i działanie z REST-API * Centralne zarządzanie agentami * Integracja danych z różnych źródeł danych (JSON, XML, SNMP) |
| Monitoring bazy danych systemu HIS | |
| 6 | 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 * Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości |
| Kolektor logów | |
| 7 | * System posiada własny kolektor logów syslog * Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps * Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event * Klasyfikuje wiadomości bazując zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe. |
| Cyberbezpieczeństwo | |
| 8 | * 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 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. * 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. |
| Monitoring | |
| 9 | W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT:   * Serwer fizyczny – do 8 sztuk * maszyna wirtualna Windows / Linux / hosty – do 25 sztuk * serwer AD – do 4 sztuk * Macierze / NASy – do 4 sztuk * Przełącznik rdzeniowy – do 2 sztuk * Przełącznik dostępowy (LAN) – do 15 sztuk * Zasilacz awaryjny (UPS) – do 4 sztuk * Serwer bazodanowy - 1 sztuki * Serwer Backupu - 1 sztuka * W ramach usługi wykonawca monitoruje krytyczne systemy Zamawiającego: * Baza danych systemu systemu szpitalnego: Oracle. * System HIS, ERP, PACS |

**7. Poufność, bezpieczeństwo informacji i dane osobowe**

7.1. Wykonawca zobowiązany jest do zachowania w poufności wszelkich informacji uzyskanych w związku z realizacją przedmiotu zamówienia, w szczególności informacji dotyczących infrastruktury teleinformatycznej Zamawiającego, konfiguracji systemów, treści logów, danych osobowych i danych medycznych pacjentów oraz innych informacji stanowiących tajemnicę przedsiębiorstwa lub tajemnicę prawnie chronioną.

7.2. Przed dopuszczeniem do realizacji prac osoby wyznaczone przez Wykonawcę do udziału w wykonywaniu zamówienia zobowiązane są podpisać oświadczenie/umowę o zachowaniu poufności, zgodnie ze wzorem stanowiącym załącznik nr 1 do niniejszego OPZ lub do umowy.

7.3. Wykonawca nie jest uprawniony do wykorzystywania informacji uzyskanych w związku z realizacją zamówienia w jakimkolwiek innym celu niż wykonanie umowy, ani do udostępniania tych informacji osobom trzecim bez uprzedniej pisemnej zgody Zamawiającego, chyba że obowiązek udostępnienia wynika wprost z przepisów prawa.

7.4. Dane (w tym logi i zrzuty ekranów) pozyskane w ramach realizacji usług serwisowych, w szczególności z wykorzystaniem zdalnego dostępu, które zawierają informacje dotyczące środowiska Zamawiającego, nie mogą być przenoszone ani przechowywane poza środowiskiem Zamawiającego, z wyjątkiem przypadków wyraźnie zaakceptowanych przez Zamawiającego na piśmie.

7.5. W przypadku, gdy w związku z realizacją zamówienia dochodzi do przetwarzania danych osobowych w rozumieniu przepisów o ochronie danych osobowych, strony zawrą odrębną umowę powierzenia przetwarzania danych osobowych, zgodnie z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) oraz przepisami krajowymi.

7.6. Po zakończeniu realizacji zamówienia (lub wcześniej, na żądanie Zamawiającego) Wykonawca zobowiązany jest do zwrotu lub trwałego usunięcia wszelkich danych, informacji i nośników zawierających informacje Zamawiającego, o ile ich dalsze przechowywanie nie wynika z bezwzględnie obowiązujących przepisów prawa. Fakt usunięcia danych Wykonawca potwierdzi stosownym protokołem.

7.7. Postanowienia niniejszego punktu pozostają w mocy także po wygaśnięciu lub rozwiązaniu umowy, przez okres co najmniej 5 lat, a w zakresie danych osobowych – przez okres wymagany przepisami prawa.

**8. Termin realizacji zamówienia**

8.1. Realizacja całości przedmiotu zamówienia, obejmująca w szczególności:

1) dostawę, instalację, konfigurację i uruchomienie produkcyjne systemu klasy SIEM oraz systemu zbierania i analizy logów,

2) wykonanie niezbędnych testów działania i odbiorów końcowych,

3) przeprowadzenie wszystkich wymaganych instruktaży / szkoleń dla administratorów Zamawiającego,musi zostać zakończona w terminie do dnia **15 maja 2026 r.**

8.2. Szczegółowy harmonogram realizacji prac zostanie uzgodniony pomiędzy Zamawiającym a Wykonawcą po podpisaniu umowy, przy czym nie może on wykraczać poza termin określony w pkt 9.1.