**Załącznik nr 2a do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA – ZADANIE 1**

Strony zgodnie stwierdzają, że na potrzeby niniejszego OPZ wraz z załącznikami i przyszłej Umowy dotyczącej opisanego zamówienia, wymienionym pojęciom nadają znaczenie określone poniżej, oraz że użyte w tekście poniżej wymienione pojęcia, rozumiane będą w sposób poniżej zdefiniowany. Dla podkreślenia, że pojęcia te rozumiane są w sposób zdefiniowany, ich pierwsze litery będą pisane w tekście wielką literą.

Strony ustalają następujące definicje:

1. **Zamawiający** – oznacza **Szpital Specjalistyczny w Pile im. Stanisława Staszica**
2. **Wykonawca** - podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez prowadzenia negocjacji na podstawie art. 275 pkt 1 Ustawy z dnia 11 września 2019r – prawo zamówień publicznych (Dz.U. 2023 poz. 1605 ze zm.).
3. **Strony** - podmioty bezpośrednio uczestniczące w umowie zawiązanej na podstawie rozstrzygnięcia podstępowania przetargowego.
4. **System informatyczny** - zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej.
5. **Infrastruktura sprzętowa -** znajdująca się w dyspozycji Zamawiającego, w tym stanowiąca jego własność oraz dostarczana w ramach realizacji przedmiotu zamówienia infrastruktura przetwarzania danych wszystkie połączenia, urządzenia fizyczne i oprogramowania aplikacyjne, które łącznie współpracując umożliwiają gromadzenie, przechowywanie, wytwarzanie danych i usług oraz udostępnianie danych i usług elektronicznych.
6. **Umowa** – umowa zawarta w ramach realizacji OPZ.
7. **SWZ –** Specyfikacja Warunków Zamówienia
8. **Gwarancja i Serwis** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie w oraz w projekcie umowy.
9. **Wada**- Należy przez to rozumieć Awarię, Błąd, Usterkę
10. **Awaria-** oznacza to Błąd, uniemożliwiający prawidłowe użytkowanie oprogramowania lub jego części, który nie prowadzi do zatrzymania eksploatacji oprogramowania.
11. **Błąd** - oznacza to powtarzalne działanie oprogramowania niezgodne z jego dokumentacją użytkową, uniemożliwiające wykonanie części jego funkcji.
12. **Usterka -** należy przez to rozumieć kategorię Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SWZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
13. **Szkolenie Administratora(ów)** – szkolenia użytkownika(ów) wskazanych przez Zamawiającego do pełnienia funkcji administratora infrastruktury sprzętowej.
14. **Zdalny Dostęp** – analogowe lub cyfrowe łącze wydajnej transmisji danych pomiędzy węzłem infrastruktury siedziby Wykonawcy, a węzłem infrastruktury zapewnianym przez Zamawiającego, umożliwiające realizować usługi serwisowe lub konfiguracyjne.
15. **Szczegółowy Harmonogram Realizacji Zadania** – szczegółowy terminarz realizacji przedmiotu Umowy wraz z podziałem na Etapy przygotowany przez Wykonawcę w terminie 14 dni roboczych od zawarcia umowy.
16. **Zadanie** – przedmiot zamówienia (przedmiot Umowy) wynikający łącznie z SWZ, Oferty Wykonawcy, Umowy.
17. **Protokół Odbiorczy** – protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego wykonanych przez Wykonawcę prac będących przedmiotem poszczególnych Etapów.
18. **Protokół Odbioru Końcowego-** Protokół, który po podpisaniu bez zastrzeżeń przez Zamawiającego, stanowi potwierdzenie wykonania i odbioru Przedmiotu Zamówienia.
19. **Protokół Dostawy-** Protokół, w którymZamawiający sprawdza ilości dostarczonego towaru i porównuje go ze stanem wykazanym w dokumentach towarzyszących dostawie.
20. **Protokół Usterek -** Protokół, w którym Zamawiający wskazuje zastrzeżenia co do zakresu i jakości wykonanych prac, które uniemożliwiają dokonanie odbioru wykonanych dostaw i prac.
21. **Protokół Uzgodnień** – dokument tworzony przez Wykonawcę i zatwierdzony przez Strony, na podstawie zapisu ze spotkania lub ustaleń zdalnych (mailowych, telefonicznych) z Zamawiającym. Dokument ten używany jest w trakcie prowadzenia analizy wymagań Zamawiającego i stanowi zobowiązanie obu Stron. Zamawiający zobowiązany jest, że wymagania zapisane w/w protokole nie zostaną zmienione, natomiast Wykonawca zobowiązany jest do realizacji zawartych w nim wymagań Zamawiającego. W przypadku zajścia konieczności wykonania zmian lub innych czynności niż te, które zostały opisane w Protokole Uzgodnień, należy utworzyć nowy Protokół Uzgodnień zawierający te zmiany. W Protokole Uzgodnień można zamieścić inne uzgodnienia, niezwiązane z wymaganiami projektu, tj. ustalenia organizacyjne.
22. **Dzień Roboczy** – każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
23. **Godziny Robocze** – godziny od 7:30 do 14:30 w każdym Dniu Roboczym.
24. **Czas Reakcji** – okres liczony od zaewidencjonowania Zgłoszenia Serwisowego do zmiany jego statusu na zarejestrowane.
25. **Czas Naprawy** - czas pomiędzy Zgłoszeniem Serwisowym a usunięciem/rozwiązaniem przyczyny jego zgłoszenia.
26. **Kierownik Zamawiającego** – osoba wyznaczona przez Zamawiającego, koordynująca całość przedmiotu danego pakietu, posiadająca odpowiednie pełnomocnictwa. W szczególności odpowiedzialna ze strony Zamawiającego za realizację przedmiotu zamówienia.
27. **Kierownik Wykonawcy** - osoba wyznaczona przez Wykonawcę do koordynacji realizacji prac danego zadania. Upoważniona do podpisywania Dokumentacji Projektu z ramienia Wykonawcy.
28. **HelpDesk (HD)** – narzędzie posiadające interfejs WWW służące do rejestracji zgłoszeń (potencjalnych problemów, usterek) oraz kontroli ich cyklu życia (tzw. Issue Tracking System lub Defect Tracking System). System HD udostępniony zostanie przez Wykonawcę dla Zamawiającego na czas realizacji przedmiotu zamówienia oraz w okresie jego gwarancji.

**OPIS RÓWNOWAŻNOŚCI:**

W przypadku gdy w dokumencie stanowiącym element opisu przedmiotu zamówienia pojawią się wskazania znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego dostawcę (jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub jego produktów), należy rozumieć, zgodnie z przepisem art. 99 ust. 5 ustawy Pzp, że zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób i w takich okolicznościach Zamawiający dopuszcza możliwość składania w ofercie rozwiązań równoważnych, wskazując, iż minimalne wymagania, jakim mają odpowiadać rozwiązania równoważne, to wymagania nie gorsze od parametrów wskazanych w tych dokumentach, a ich kryteria w celu oceny równoważności wskazane są w opisie przedmiotu zamówienia.

W przypadku, gdy Zamawiający opisuje przedmiot zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy, zamawiający dopuszcza rozwiązania równoważne opisywanym.

Wykonawcy mogą składać oferty zawierające rozwiązania równoważne w stosunku do przedmiotu zamówienia przedstawionego w SWZ – zgodnie z art. 101 ust. 4, 5 i 6 ustawy PZP, jednak są zobowiązani wykazać, że oferowane przez nich rozwiązania spełniają wymagania określone przez Zamawiającego. Równoważność pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów nie gorszych od założonych w niniejszym SWZ

Za równoważne uznaje się rozwiązania, jak również elementy, materiały, urządzenia o właściwościach funkcjonalnych i jakościowych takich samych, które zostały określone w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem. Przy czym istotne jest to, że produkt równoważny to produkt, który nie jest identyczny, tożsamy z produktem referencyjnym, ale posiada pewne, istotne dla Zamawiającego, zbliżone do produktu referencyjnego cechy i parametry.

Istotne dla Zamawiającego cechy i parametry, to takie, które pozwolą zachować wszystkim systemom, urządzeniom, wyrobom, parametry i cechy pozwalające przede wszystkim na prawidłową współpracę z innymi systemami i/lub urządzeniami i/lub wyrobami w sposób założony przez Zamawiającego oraz pozwalające przy tym uzyskać parametry nie gorsze od założonych w niniejszym załączniku. Ciężar udowodnienia równoważności spoczywa na Wykonawcy

Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowany przedmiot zamówienia spełnia wymagania określone przez Zamawiającego poprzez złożenie opisu zaoferowanych produktów wraz z wykazaniem cech równoważności w stosunku do wymagań opisanych przez Zamawiającego w niniejszym załączniku oraz podanie nazwy handlowej i producenta.

W celu wykazania cech równoważności Zamawiający dopuszcza załączenie do opisu etykiet, zdjęć, kart katalogowych itp., z dopiskiem której pozycji asortymentowej (jakiego sprzętu) dotyczy dana informacja z zastrzeżeniem, że z tych dokumentów muszą wynikać parametry co najmniej określone przez Zamawiającego w załącznikach do OPZ i dane identyfikujące produkt.

**DOSTAWA INFRASTRUKTURY OPROGRAMOWANIA**

Przedmiotem zamówienia jest oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych **w Szpitalu Specjalistycznym w Pile im. Stanisława Staszica** .

Poniżej wyspecyfikowano minimalne oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Wymagania ogólne:

* Całość dostarczanego oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
* Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).
* Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:
* posiadane środowisko domenowe,
* posiadaną konfigurację sieci wraz z jednostkami podległymi,
* posiadaną konfiguracją baz danych i backupów,
* konfigurację stacji roboczych.

**Opis parametrów minimalnych oprogramowania:**

Zamawiający wymaga, aby Wykonawca spełniała wymagania w zakresie:

|  |
| --- |
| 1. SYSTEM SIEM |
| **Minimalne parametry techniczne** |
| **Użytkownicy:**   1. Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat. 2. Zapewnienia równoległego dostępu do systemu dla wielu użytkowników. |
| **Analiza logów systemowych:**   1. Monitorowanie plików konfiguracyjnych 2. Skanowanie integralności plików 3. Analiza integralności rejestru 4. Analiza logów aplikacji systemowych 5. Analiza logów aplikacji internetowych 6. Analiza logów aplikacji na poziomie użytkownika 7. Analiza logów związanych z bazami danych 8. Analiza logów związanych z sieciami VPN 9. Analiza logów związanych z kontami użytkowników 10. Analiza logów związanych z kontami serwisowymi 11. Analiza logów związanych z kontami administratorów |
| **Detekcja ataków i zagrożeń:**   1. Wykrywanie prób włamania się (brute-force) 2. Wykrywanie prób ataku typu Man-in-the-Middle 3. Wykrywanie prób zmiany lub ataku na pliki systemowe 4. Wykrywanie prób wykorzystania podatności 5. Wykrywanie prób ataku typu SQL injection 6. Wykrywanie prób ataku typu Cross-Site Scripting (XSS) 7. Wykrywanie prób ataku typu zero-day 8. Wykrywanie prób ataku typu buffer overflow 9. Wykrywanie prób ataku typu DNS poisoning 10. Wykrywanie prób ataku typu DDoS (Denial-of-Service) |
| **Zbieranie logów z wielu źródeł:**   1. Zbieranie danych z systemów kontenerowych 2. Zbieranie danych z systemów wirtualizacji 3. Zbieranie danych z systemów kontroli wersji 4. Zbieranie danych z systemów monitorowania chmury 5. Zbieranie danych z systemów wirtualizacji 6. Zbieranie danych z systemów kontroli wersji 7. Zbieranie danych z platform IoT 8. Zbieranie danych z urządzeń mobilnych 9. Zbieranie danych z platform wirtualizacyjnych 10. Zbieranie danych z platform chmurowych |
| **Monitorowanie aktywności użytkowników:**   1. Monitorowanie aktywności użytkowników 2. Monitorowanie aktywności administratorów 3. Monitorowanie aktywności na poziomie portów i usług 4. Monitorowanie aktywności na poziomie interfejsów 5. Monitorowanie aktywności na poziomie protokołów |
| **Monitorowanie urządzeń sieciowych:**   1. Monitorowanie aktywności na poziomie protokołów sieciowych 2. Monitorowanie aktywności na poziomie protokołów aplikacji 3. Monitorowanie aktywności na poziomie protokołów transportowych 4. Monitorowanie aktywności na poziomie protokołów internetowych 5. Monitorowanie aktywności na poziomie protokołów telekomunikacyjnych |
| **Integracja z systemami monitorowania:**   1. Integracja z systemami monitorowania logów 2. Integracja z systemami monitorowania zachowań użytkowników 3. Integracja z systemami monitorowania aplikacji 4. Integracja z systemami monitorowania chmury 5. Integracja z systemami monitorowania IoT |
| **Zdalne monitorowanie agentów:**   1. Zdalne monitorowanie agentów w różnych środowiskach 2. Zdalne monitorowanie agentów na platformach IoT 3. Zdalne monitorowanie agentów w chmurze |
| **Wykrywanie nieautoryzowanego dostępu:**   1. Wykrywanie prób nieautoryzowanego dostępu 2. Wykrywanie prób podmiany binarnych 3. Wykrywanie prób podmiany tokenów uwierzytelniania 4. Wykrywanie prób podważenia integralności plików |
| **Ostrzeganie przed atakami:**   1. Ostrzeganie przed próbami włamania się na konta 2. Ostrzeganie przed próbami łamania haseł metodą bruteforce 3. Ostrzeganie przed próbami ataku typu SQL tampering 4. Ostrzeganie przed próbami ataku typu formjacking 5. Ostrzeganie przed próbami ataku typu clickjacking 6. Ostrzeganie przed próbami ataku typu formjacking 7. Ostrzeganie przed próbami ataku typu clickjacking 8. Ostrzeganie przed próbami ataku typu domain hijacking 9. Ostrzeganie przed próbami ataku typu URL poisoning 10. Ostrzeganie przed próbami ataku typu click injection 11. Ostrzeganie przed próbami ataku typu smart meter tampering 12. Ostrzeganie przed próbami ataku typu driverless car hacking 13. Ostrzeganie przed wykrytymi próbami ataku typu watering hole 14. Ostrzeganie przed wykrytymi próbami ataku typu zero-click exploit |
| **Integracja z różnymi systemami:**   1. Integracja z rozwiązaniami do zarządzania incydentami 2. Integracja z narzędziami do analizy ruchu sieciowego 3. Integracja z narzędziami do analizy zachowań malware'u 4. Integracja z narzędziami do analizy zachowań użytkowników 5. Integracja z narzędziami do analizy danych z urządzeń IoT 6. Integracja z narzędziami do analizy zachowań aplikacji 7. Integracja z narzędziami do analizy zachowań użytkowników na platformach chmurowych 8. Integracja z narzędziami do analizy zachowań użytkowników na platformach mobilnych 9. Integracja z narzędziami do analizy zachowań użytkowników na platformach IoT 10. Integracja z narzędziami do analizy zachowań użytkowników na platformach wirtualizacyjnych 11. Integracja z narzędziami do analizy zachowań użytkowników na platformach przemysłowych (OT) 12. Integracja z narzędziami do analizy zachowań użytkowników na platformach z systemami wbudowanymi 13. Integracja z narzędziami do analizy zachowań użytkowników na platformach autonomicznych pojazdów (AV) |
| **Monitorowanie aktywności sieciowej:**   1. Monitorowanie ruchu sieciowego 2. Monitorowanie aktywności na poziomie jądra systemu 3. Monitorowanie dostępów SSH 4. Monitorowanie aktywności sieciowych na poziomie interfejsów 5. Monitorowanie aktywności na poziomie protokołów 6. Monitorowanie aktywności na poziomie protokołu SMB/CIFS 7. Monitorowanie aktywności na poziomie protokołu RDP 8. Monitorowanie aktywności na poziomie protokołu POP3/IMAP 9. Monitorowanie aktywności na poziomie protokołu SMTP 10. Monitorowanie aktywności na poziomie protokołu DNS over HTTPS (DoH) 11. Monitorowanie aktywności na poziomie protokołu iSCSI (Internet Small Computer System Interface) 12. Monitorowanie aktywności na poziomie protokołu UPnP (Universal Plug and Play) 13. Monitorowanie aktywności na poziomie protokołu SIP-TLS (Session Initiation Protocol over Transport Layer Security) 14. Monitorowanie aktywności na poziomie protokołu DNS over HTTPS (DoH) 15. Monitorowanie aktywności na poziomie protokołu ICMPv6 (Internet Control Message Protocol version 6) 16. Monitorowanie aktywności na poziomie protokołu LLDP (Link Layer Discovery Protocol) 17. Monitorowanie aktywności na poziomie protokołu DHCP (Dynamic Host Configuration Protocol) 18. Monitorowanie aktywności na poziomie protokołu IGMP (Internet Group Management Protocol) 19. Monitorowanie aktywności na poziomie protokołu SCTP (Stream Control Transmission Protocol) 20. Monitorowanie aktywności na poziomie protokołu Thread (IPv6-based mesh networking protocol) 21. Monitorowanie aktywności na poziomie protokołu IPv6 over IPv4 tunneling 22. Monitorowanie aktywności na poziomie protokołu IP-in-IP (IP encapsulation) 23. Monitorowanie aktywności na poziomie protokołu SRTP (Secure Real-time Transport Protocol) 24. Monitorowanie aktywności na poziomie protokołu SAML (Security Assertion Markup Language) |
| **Reagowanie na ataki:**   1. Reagowanie na ataki w czasie rzeczywistym 2. Reagowanie na zablokowany dostęp do zasobów 3. Reagowanie na niepowodzenia uwierzytelniania 4. Reagowanie na zmiany uprawnień plików 5. Reagowanie na podejrzane aktywności na kontach użytkowników 6. Reagowanie na wykryte ataki typu phishing 7. Reagowanie na próby ataku typu Man-in-the-Middle 8. Reagowanie na próby manipulacji tokenami uwierzytelniania 9. Reagowanie na zmiany w konfiguracji firewalla 10. Reagowanie na podejrzane aktywności administratorów 11. Reagowanie na próby manipulacji logami zdarzeń 12. Reagowanie na wykryte próby ataku typu ransomware 13. Reagowanie na wykryte próby ataku typu drive-by download 14. Reagowanie na próby ataku typu cryptojacking 15. Reagowanie na wykryte próby ataku typu eavesdropping 16. Reagowanie na wykryte próby ataku typu steganografia 17. Reagowanie na wykryte próby ataku typu biometric data theft 18. Reagowanie na wykryte próby ataku typu data manipulation 19. Reagowanie na wykryte próby ataku typu supply chain attack 20. Reagowanie na wykryte próby ataku typu DNS poisoning 21. Reagowanie na próby ataku typu DDoS (Distributed Denial of Service) 22. Reagowanie na próby ataku typu DoS (Denial of Service) |
| **Wsparcie dla jednostek służby zdrowia:**   1. Monitorowanie logów aplikacji medycznych: System SIEM może analizować logi z aplikacji medycznych, bazy danych i systemów informatycznych w jednostkach służby zdrowia. Pozwala to na wykrywanie nieprawidłowych aktywności, prób nieautoryzowanego dostępu i innych zagrożeń. 2. Detekcja ataków na systemy IT: System SIEM oferuje zaawansowane mechanizmy detekcji intruzów, które pozwalają na wykrywanie zaawansowanych ataków, prób wykorzystania luk w zabezpieczeniach i innych zagrożeń. 3. Monitorowanie integralności plików: System SIEM pozwala na monitorowanie zmian w plikach systemowych, co może być istotne dla ochrony danych medycznych i zapobiegania nieautoryzowanym zmianom. 4. Wdrażanie polityk bezpieczeństwa: System SIEM umożliwia definiowanie i egzekwowanie polityk bezpieczeństwa w organizacji, co pozwala na utrzymanie odpowiedniego poziomu bezpieczeństwa. 5. Analiza ruchu sieciowego: System SIEM oferuje funkcje analizy ruchu sieciowego, dzięki czemu można wykrywać podejrzane aktywności i ataki, takie jak próby skanowania portów czy ataki DDoS. 6. Reagowanie na incydenty: System SIEM pozwala na definiowanie planów reagowania na różne typy incydentów, dzięki czemu personel odpowiedzialny za bezpieczeństwo może skutecznie reagować na zagrożenia. 7. Powiadomienia i alerty: System SIEM generuje alerty w czasie rzeczywistym, informując personel o potencjalnych zagrożeniach. Możliwe jest również konfigurowanie powiadomień e-mail lub SMS 8. Monitorowanie logów medycznych: System SIEM może analizować logi z systemów klasy HIS (Hospital Information System), RIS (Radiology Information System) i PASC (Picture Archiving and Communication System) używanych w środowisku medycznym. 9. Wykrywanie naruszeń związanych z danymi pacjentów: Dzięki analizie logów medycznych, System SIEM może wykryć próby nieautoryzowanego dostępu do danych pacjentów, zmiany w medycznych zapisach pacjentów lub próby wykradzenia danych medycznych. 10. Ochrona danych medycznych: System SIEM umożliwia monitorowanie integralności i poufności danych medycznych, co pozwala na reagowanie na zagrożenia związane z ochroną danych medycznych i zapewnienie zgodności z przepisami regulującymi ochronę danych w sferze medycyny. 11. System monitoruje krytyczne elementy systemu HIS:  * Komunikacja z platformą P1 * Komunikacji bramek HL7 * Komunikacja EWUŚ * Komunikacja KOWAL * Komunikacja AP-KOLCE * Funkcjonowanie Rejestru Zdarzeń Medycznych * Baza danych systemu HIS |
| **Tworzenie reguł korelacji:**   1. Możliwość definiowania reguł korelacji, które określają, jakie zdarzenia i logi mają być analizowane oraz w jaki sposób powiązywane, aby wykrywać zaawansowane zagrożenia i ataki. 2. Korelacja zdarzeń w czasie rzeczywistym: Silnik korelacji System SIEM działa w czasie rzeczywistym, co pozwala na wykrywanie ataków i zagrożeń w czasie rzeczywistym. 3. Korelacja wielu zdarzeń: Możliwość powiązania wielu zdarzeń i logów w celu identyfikacji bardziej złożonych aktywności i etapów ataków, które mogą obejmować różne komponenty infrastruktury. 4. Wykorzystywanie bazy wiedzy: Silnik korelacji wykorzystuje bazę wiedzy zawierającą informacje o znanych zagrożeniach i atakach, co pozwala na lepsze wykrywanie i identyfikację nowych incydentów. 5. Wykrywanie anomalii: Silnik korelacji może identyfikować anomalie w zachowaniach użytkowników, aplikacji i systemów, co może wskazywać na nieautoryzowany dostęp lub działania. 6. Wykorzystywanie heurystyk: Silnik korelacji System SIEM wykorzystuje zaawansowane heurystyki, aby identyfikować podejrzane aktywności i zachowania, nawet jeśli nie są to znane zagrożenia. 7. Personalizacja reguł i zapytań: Administratorzy mogą dostosowywać istniejące reguły i zapytania korelacji lub tworzyć własne, dopasowane do konkretnych potrzeb i wymagań organizacji. 8. Integracja z innymi źródłami danych: Możliwość integracji z dodatkowymi źródłami logów, co pozwala na analizę danych z różnych systemów i aplikacji, w tym również urządzeń IoT. 9. Generowanie alertów: Silnik korelacji może generować alerty i powiadomienia w czasie rzeczywistym, co pozwala na szybką reakcję na incydenty. 10. Raportowanie i analiza: Możliwość generowania raportów i analizy wykrytych zagrożeń oraz aktywności, co pozwala na lepsze zrozumienie sytuacji bezpieczeństwa i podejmowanie odpowiednich działań. 11. Ustalanie priorytetów: Możliwość przypisania priorytetów wykrytym incydentom na podstawie stopnia zagrożenia i znaczenia dla organizacji. 12. Uczenie maszynowe: Integracja z technologią uczenia maszynowego, która pozwala na automatyczną analizę danych i identyfikację nowych wzorców zachowań. 13. Korelacja zdarzeń między hostami: Możliwość powiązywania zdarzeń między różnymi hostami w celu wykrywania ataków na poziomie infrastruktury. 14. Filtracja zdarzeń: Możliwość definiowania reguł i filtrów, które pozwalają na wykluczenie zdarzeń bezpiecznych i skupienie się na tych bardziej podejrzanych. 15. Wielopoziomowa analiza: Możliwość przeprowadzania analizy na różnych poziomach infrastruktury, takich jak warstwa aplikacji, systemu operacyjnego, a także warstwa sieciowa. 16. Korelacja geolokacji: Możliwość powiązania zdarzeń z geolokacją, co pozwala na wykrywanie podejrzanych aktywności z różnych lokalizacji geograficznych. 17. Wsparcie dla różnych formatów logów: Silnik korelacji obsługuje różne formaty logów, co pozwala na integrację z wieloma aplikacjami i urządzeniami. 18. Detekcja ataków z wykorzystaniem wielu etapów: Możliwość wykrywania zaawansowanych ataków, które obejmują wiele etapów i etapów przeprowadzenia ataku. 19. Skalowalność: Silnik korelacji System SIEM jest skalowalny, co pozwala na analizę dużych ilości danych w środowiskach o dużej infrastrukturze. 20. Integracja z narzędziami SIEM: Możliwość integracji silnika korelacji System SIEM z innymi narzędziami SIEM, co pozwala na kompleksowe zarządzanie bezpieczeństwem i analizę zagrożeń. |
| **Raportowanie:**   1. Raporty na żądanie: Możliwość generowania raportów w czasie rzeczywistym na żądanie użytkownika w oparciu o określone zapytania i dane logów. 2. Automatyczne generowanie raportów: Możliwość zaplanowania i automatycznego generowania raportów na określone interwały czasowe, co pozwala na regularne monitorowanie i analizę aktywności. 3. Wybór zakresu czasowego: Możliwość wyboru zakresu czasowego dla raportu, aby skupić się na określonym przedziale czasowym. 4. Analiza zdarzeń bezpieczeństwa: Raportowanie i analiza zdarzeń bezpieczeństwa, które pozwalają na identyfikację podejrzanych aktywności, prób ataków i incydentów. 5. Wykrywanie anomalii: Raportowanie wykrytych anomalii w zachowaniach użytkowników, aplikacji czy systemów, co może wskazywać na nieprawidłowe lub nieautoryzowane działania. 6. Raporty o wydajności: Możliwość generowania raportów dotyczących wydajności i dostępności infrastruktury, które pozwalają na monitorowanie stanu systemów i urządzeń. 7. Raporty o atakach DDoS: Raportowanie prób ataków typu Distributed Denial of Service (DDoS) w celu zrozumienia potencjalnych ataków na infrastrukturę. 8. Raporty o próbach ataków brute-force: Generowanie raportów o próbach ataków brute-force na konta użytkowników czy aplikacje, które mogą wskazywać na próby złamania haseł. 9. Raporty o próbach ataków XSS i SQL injection: Raportowanie prób ataków typu Cross-Site Scripting (XSS) i SQL Injection, które mogą stanowić zagrożenie dla aplikacji webowych. 10. Raporty o próbach ataków RCE: Generowanie raportów o próbach ataków typu Remote Code Execution (RCE), które pozwalają na zdalne wykonanie kodu na systemie. 11. Personalizacja raportów: Możliwość personalizacji raportów, aby uwzględnić specyficzne wymagania i potrzeby organizacji. 12. Raportowanie na różnych poziomach: Możliwość generowania raportów na różnych poziomach abstrakcji, takich jak raporty ogólne, raporty szczegółowe czy raporty na poziomie hosta czy użytkownika. 13. Formatowanie raportów: Możliwość formatowania raportów, aby były czytelne i czytelnie przedstawiały wyniki analiz. 14. Raporty o zgodności: Generowanie raportów o zgodności z różnymi standardami i regulacjami dotyczącymi bezpieczeństwa, takimi jak GDPR, HIPAA, czy PCI-DSS. 15. Eksport danych: Możliwość eksportu danych z raportów do różnych formatów, takich jak PDF, CSV czy HTML. 16. Raporty na poziomie zarządczym: Możliwość generowania raportów na poziomie zarządczym, które pozwalają na przedstawienie kluczowych wskaźników i wyników dla kierownictwa. 17. Wykresy i diagramy: Możliwość przedstawienia wyników raportów za pomocą wykresów i diagramów, co ułatwia wizualizację danych i analizę trendów. 18. Raporty o monitorowaniu aktywności użytkowników: Generowanie raportów o aktywnościach użytkowników, co pozwala na kontrolę i audyt działań użytkowników. 19. Zautomatyzowane generowanie raportów bezpieczeństwa: Możliwość zautomatyzowanego generowania raportów dotyczących bezpieczeństwa w celu przestrzegania wymogów regulacji i standardów. |
| **Aktywny parser logów z rożnych systemów :**   1. Zbieranie logów w czasie rzeczywistym: System SIEM posiada agenty logowania (System SIEM Agents), które mogą zbierać logi z różnych systemów i aplikacji. Te agenty mogą działać w czasie rzeczywistym, pozwalając na monitorowanie aktywności na bieżąco. 2. Normalizacja logów: System SIEM normalizuje logi z różnych źródeł do jednolitego formatu, co ułatwia analizę i detekcję zagrożeń. Dzięki temu, nawet jeśli logi pochodzą z różnych systemów i mają różne formaty, System SIEM pozwala na ich spójną analizę. 3. Wykorzystanie reguł i detekcja w czasie rzeczywistym: System SIEM pozwala na konfigurację zaawansowanych reguł detekcji, które pozwalają na identyfikację niebezpiecznych aktywności w czasie rzeczywistym. Kiedy zdarzenie spełnia kryteria reguły, System SIEM generuje alert, który może być natychmiastowo obsłużony przez personel bezpieczeństwa. 4. Integracja z Elastic Stack: System SIEM można zintegrować z Elastic Stack, co pozwala na zaawansowaną analizę logów przy użyciu narzędzi takich jak Elasticsearch, Logstash i Kibana. Elastic Stack jest w stanie przetwarzać ogromne ilości logów w czasie rzeczywistym i umożliwia zaawansowane filtrowanie, sortowanie i analizę danych. 5. Skalowalność: System SIEM jest skalowalne, co oznacza, że można go rozbudować, aby obsługiwać duże ilości logów z różnych źródeł w czasie rzeczywistym. |
| **Poczta elektroniczna:**   1. Analiza logów serwera poczty elektronicznej: System SIEM jest w stanie monitorować logi generowane przez serwery pocztowe, takie jak Microsoft Exchange, Postfix, czy Sendmail. Dzięki temu możliwe jest wykrycie podejrzanych aktywności, takich jak próby nieudanych logowań, wysyłania dużej ilości e-maili w krótkim czasie (możliwe znaki kompromitacji konta), czy ataki typu "brute-force" mające na celu przejęcie konta pocztowego. 2. Wykrywanie prób phishingu: System SIEM może analizować zawartość e-maili i załączników w poszukiwaniu potencjalnie szkodliwych linków, które mogą prowadzić do stron phishingowych. Jeśli wykryte zostaną podejrzane adresy URL, System SIEM może generować alert, umożliwiając administratorowi podjęcie odpowiednich działań. 3. Monitorowanie zmian konfiguracji: System SIEM pozwala monitorować zmiany w konfiguracji serwera poczty elektronicznej. W przypadku nieautoryzowanych zmian, takich jak dodawanie nowych kont użytkowników lub zmiana ustawień przekierowań, System SIEM może wygenerować alert, informując o potencjalnym naruszeniu bezpieczeństwa. |
| **Sandbox:**   1. Analiza zachowania plików: System SIEM może integrować się z rozwiązaniami do analizy zachowania plików w sandboxie. Po uruchomieniu podejrzanego pliku w bezpiecznym środowisku, dane z analizy w sandboxie są przesyłane do System SIEM w celu identyfikacji podejrzanych aktywności. 2. Wykrywanie zaawansowanych zagrożeń: Dzięki analizie zachowania plików, System SIEM może wykryć nowe, nieznane wcześniej zagrożenia, które omijają tradycyjne metody wykrywania, takie jak sygnatury antywirusowe. |
| **Skanery podatności:**   1. Integracja z narzędziami do skanowania podatności: System SIEM może integrować się z różnymi narzędziami do skanowania podatności, takimi jak Nessus czy OpenVAS. Po przeprowadzeniu skanowania podatności, wyniki są przesyłane do System SIEM w celu analizy i identyfikacji słabych punktów w infrastrukturze. 2. Wykrywanie zagrożeń wynikających z podatności: System SIEM może analizować wyniki skanowania podatności w celu identyfikacji potencjalnych zagrożeń i generowania alertów w przypadku wystąpienia znanych podatności, które mogą być wykorzystane przez atakujących. |
| **Możliwe działania proaktywne w ramach SIEM (na podstawie dodatkowych zamówień):**   1. Wykonywanie skanów podatności 2. Stałe aktualizacje zabezpieczeń i łatek oprogramowania 3. Wdrażanie mechanizmów zwiększających odporność na ataki 4. Edukacja użytkowników w zakresie bezpieczeństwa informatycznego 5. Analiza trendów i nowych zagrożeń w cyberprzestrzeni 6. Wdrażanie technologii zwiększających wykrywalność ataków 7. Ocena ryzyka i zarządzanie bezpieczeństwem informacji 8. Tworzenie planów reagowania na incydenty i awarie 9. Wdrażanie polityk bezpieczeństwa w organizacji 10. Monitorowanie mediów społecznościowych pod kątem zagrożeń 11. Współpraca z innymi organizacjami w celu wymiany informacji o zagrożeniach 12. Tworzenie świadomości kultury bezpieczeństwa w całej organizacji 13. Opracowanie strategii audytów bezpieczeństwa i weryfikacji zgodności 14. Zarządzanie i zapewnienie bezpieczeństwa informacji to proces ciągły, który wymaga podejmowania działań zarówno reaktywnych, jak i proaktywnych. Wszystkie te obszary funkcjonalne wspólnie tworzą całościowe podejście do zapobiegania incydentom bezpieczeństwa i minimalizowania ryzyka wystąpienia zagrożeń w środowisku informatycznym. |
| **Gwarancja i serwis**   1. Oprogramowanie ma być objęte minimum 36 miesięcznym gwarancją dla wszystkich funkcji. 2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. 3. Aktualizacje dostarczonego Systemu SIEM do nowych wersji oprogramowania. 4. Szkolenia administratorów on-line z nowych funkcjonalności, 5. Usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania Systemem, bieżące aktualizacje dokumentacji technicznej dla Systemu, 6. Przyjmowania zgłoszeń serwisowych przez dedykowany serwisowy moduł internetowy oraz mail 24/7 7. Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24 /7/365, zgodnie z określonymi poniżej warunkami SLA 8. Zgłoszenia i Incydenty są klasyfikowane na podstawie potencjalnego wpływu na Klienta. wykorzystywane są 4 poziomy klasyfikacji, jak przedstawiono w poniższej tabeli:  |  |  |  |  | | --- | --- | --- | --- | | Poziom | Opis | Zagrożenie | Przykład | | Krytyczny | Niezbędne natychmiastowe działanie | * Przerwa w działaniu serwera/systemu | Wyciek danych | | złagodzić obecne złośliwe oprogramowanie | * Brak odbioru danych z lokalizacja klienta |  | | Działalność |  |  | | 3 | Wysokie prawdopodobieństwo incydentu, jeśli | * Znaczące zmiany w SIEM | Brak potwierdzenia | | nie podejmuje się działań zapobiegawczych | * wskazanie natężenia ruchu danych obniżona wydajność potencjał |  | | 2 | Niski potencjalny incydent | * Użytkownik nie zaktualizował hasła w wymaganym odstępie czasu | Znaleziony wirus na stacji roboczej | | 1 | Aktywności utrzymaniowe lub informacyjne | - | Raport |   w oparciu o klasyfikację i rodzaj zdarzenia/zgłoszenia wsparcie reaguje zgodnie z poniższymi interwałami.   |  |  |  |  | | --- | --- | --- | --- | | Poziom | Opis | Zagrożenie | SLA | | Krytyczny | 1 godzina | 1 godzina | 96% | | 3 | 24 godziny | 2 godziny | 96% | | 2 | 72 godziny | 8 godzin | 96% | | 1 | 5 dni | 24 godzin | 96% | |
| **Dodatkowe wymagania:**   1. Producent Systemu SIEM musi posiadać certyfikacje w zakresie: ŚWIADCZENIA USŁUGI SECURITY OPERATION CENTER - REAGOWANIE NA ZAGROŻENIA CYBERBEZPIECZEŃSTWA, zgodnie z normą ISO ISO/IEC 27001:2017 – załączyć do oferty. 2. W celu zabezpieczenia danych krytycznych przetwarzanych w systemie HIS Zamawiającego (system Eskulap, którego producentem jest Nexus Polska Sp. z o.o.), Wykonawca zobowiązany jest dołączyć do oferty potwierdzenie, że posiada uprawnienia lub autoryzację Nexus Polska lub zrealizuje przedmiot zamówienia w obszarze dotyczącym ingerencji w dane przetwarzane przez system Eskulap, nie naruszając postanowień licencyjnych i gwarancyjnych dla systemu medycznego Eskulap i będzie gwarantował jego poprawne monitorowanie po zakończeniu prac integracyjnych – załączyć do oferty. |

**UWAGA: do oferty należy dołączyć materiały pozwalające Zamawiającemu zapoznać się z oferowanymi produktami.**

**Dokument należy uzupełnić, podpisać i załączyć do oferty.**