Załącznik nr 2 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Strony zgodnie stwierdzają, że na potrzeby niniejszego OPZ wraz z załącznikami i przyszłej Umowy dotyczącej opisanego zamówienia, wymienionym w niniejszym paragrafie 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 **Zespół Opieki Zdrowotnej w Brodnicy**
2. **Wykonawca -** podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w sprawie zamówienia publicznego
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. W skład systemu wchodzą najczęściej elementy: Sprzęt komputerowy, Oprogramowanie narzędziowe, Oprogramowanie dziedzinowe.
5. **Systemy medyczne** - systemy klasy HIS (Hospital Information System), RIS (Radiology Information System) i PACS (Picture Archiving and Communication System) używanych w środowisku medycznym, przechowujące dane o udzielonych świadczeniach medycznych i stanie zdrowia pacjentów.
6. **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.
7. **Umowa** – umowa zawarta w ramach realizacji OPZ.
8. **SWZ –** Specyfikacja Warunków Zamówienia
9. **Gwarancja i Serwis Oprogramowania** – 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.
10. **System Komunikacyjny** – infrastruktura telekomunikacyjna, sieciowa, systemy separacji, systemy bezpieczeństwa oraz certyfikaty serwerów WWW, obejmujące elementy lokalnej sieci komputerowej, łącza i urządzenia rozległej sieci transmisji danych oraz urządzenia komutacji pakietów wraz z ich oprogramowaniem, odpowiedzialne za obsługę HIS.
11. **Oprogramowanie Narzędziowe** – elementy oprogramowania zainstalowane na Sprzęcie Komputerowym, obejmujące w szczególności:
	* + systemy operacyjne (np. Windows, LINUX, UNIX),
		+ system zarządzania bazą danych (SZBD), zwane też oprogramowaniem bazodanowym (np. MSSQL, Oracle),
		+ oprogramowanie służące do administracji i zarządzania Sprzętem Komputerowym, systemem operacyjnym i systemem zarządzania bazą danych,
		+ oprogramowanie komunikacyjne umożliwiające podłączenie stacji dostępowych do serwera bazy;
12. **Szkolenie Administratora(ów)** – szkolenia użytkownika(ów) wskazanych przez Zamawiającego do pełnienia funkcji administratora infrastruktury sprzętowej.
13. **Systemy Zewnętrzne** – systemy z którymi docelowo współpracować będzie wdrażany system.
14. **Wdrożenie** – etap cyklu życia systemu informatycznego, polegający na instalacji i dostosowaniu oprogramowania do wymagań Zamawiającego oraz testowaniu i uruchomieniu systemu informatycznego.
* Podstawowe etapy procesu wdrożenia:
* Przygotowanie dokumentacji,
* Przygotowanie i skonfigurowanie infrastruktury technicznej,
* Zainstalowanie i skonfigurowanie systemu informatycznego do eksploatacji,
* Testowanie systemu,
* Uruchomienie produkcyjne systemu.
1. **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.
2. **Zadanie** – przedmiot zamówienia (przedmiot Umowy) wynikający łącznie z SWZ, Oferty Wykonawcy, Umowy.
3. **Etap** – główny element części Zadania, stanowiący funkcjonalną całość, podlegająca odrębnym odbiorom. Każdy Etap stanowi odrębną część (rozdział) niniejszego OPZ.
4. **Protokół Odbiorczy** – protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego wykonanych przez Wykonawcę prac będących przedmiotem poszczególnych Etapów.
5. **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.
6. **Dzień Roboczy** – każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
7. **Godziny Robocze** – godziny od 7:30 do 14:30 w każdym Dniu Roboczym.
8. **Kierownik Zamawiającego** – osoba wyznaczona przez Zamawiającego, koordynująca całość przedmiotu danego pakietu, posiadająca odpowiednie pełnomocnictwa. W szczególności odpowiedzialna ze strony Zamawiającego za realizację przedmiotu zamówienia.
9. **Kierownik Wykonawcy** - osoba wyznaczona przez Wykonawcę do koordynacji realizacji prac danego zadania. Upoważniona do podpisywania Dokumentacji Projektu z ramienia Wykonawcy.
10. **Elektroniczny System Zgłoszeń (ESZ)** – 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 ESZ udostępniony zostanie przez Wykonawcę dla Zamawiającego na czas realizacji przedmiotu zamówienia oraz w okresie jego gwarancji.

**DOSTAWA INFRASTRUKTURY OPROGRAMOWANIA – SYSTEM TYPU SIEM**

Przedmiotem zamówienia jest dostawa oprogramowania typu SIEM podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych w Zespole Opieki Zdrowotnej w Brodnicy.

Poniżej wyspecyfikowano minimalne parametry oprogramowania oraz usług, które należy dostarczyć lub wdrożyć 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 oprogramowania i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

* posiadane środowisko domenowe,
* posiadaną konfigurację sieci wraz z wdrożoną w ramach postępowania segmentacją VLAN, oraz strefą DMZ,
* posiadaną konfiguracją baz danych i backupów,
* konfigurację stacji roboczych.

**Opis parametrów minimalnych dostarczanej infrastruktury oraz oprogramowania**

**1. System SIEM.**

System klasy SIEM w ramach funkcjonalności związanej z zarządzaniem informacjami i zdarzeniami w zakresie bezpieczeństwa systemów informatycznych musi spełniać poniższe minimalne wymagania:

System typu SIEM w ramach swojej funkcjonalności związanej z zarządzaniem informacjami i zdarzeniami w zakresie bezpieczeństwa systemów informatycznych musi posiadać możliwość:

1. Monitorowania serwerów fizycznych.

2. Monitorowania urządzeń sieciowych.

3. Monitorowania stanu połączeń.

4. Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów

5. Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux.

6. Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych.

7. Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń.

8. Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu.

9. Definiowanie planowanych przerw serwisowych dla hostów i usług.

10. Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).

11. Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych).

12. Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).

13. Monitorowanie serwerów za pomocą agentów

14. Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server.

15. Monitorowanie Active Directory.

16. Monitorowanie serwerów plików, udziałów sieciowych.

17. Monitorowanie statusu serwerów Apache.

18. Monitorowanie baz danych: ORACLE, MySQL, Postgress, MSSQL Server.

19. Monitorowanie urządzeń przez następujące protokoły: SNMP, WMI, IPMI.

20. Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW.

21. Monitorowanie poprawności działania DNS.

22. Monitorowanie środowisk wirtualizacyjnych: Vmware, Hyper-V.

23. Monitorowanie działania serwera czasu NTP.

24. Monitorowanie offsetu czasu na serwerach.

25. Monitorowanie ping - czasy odpowiedzi, straty pakietów.

26. Monitorowanie zasobów serwerów w zakresie: obciążenia CPU, wykorzystania pamięci RAM, obciążenia dysków, zajętości miejsca na poszczególnych partycjach.

27. Monitorowanie logów systemowych Windows.

28. Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia.

29. Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix.

30. Wykrywanie niestabilnie działających usług.

31. Monitorowanie dostępności stron internetowych.

32. Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń).

**Użytkownicy:**

1. System umożliwia utworzenia wielu użytkowników systemu monitorowania infrastruktury IT bez dodatkowych opłat.

2. System zapewnia równoległy dostępu dla wszystkich użytkowników równocześnie (brak współdzielonych licencji).

3. Możliwość konfiguracji uprawnień dla użytkownika w postaci ograniczania dostępu dla wybranych grup hostów lub usług.

**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 zarządzania (interfejsów zarządzających) serwerami, macierzami (np. iRMC, iDRAC itp.)

2. Zbieranie danych z systemów zainstalowanych na serwerach fizycznych

3. Zbieranie danych z systemów wirtualizacji (Vmware, Hyper-V)

4. Zbieranie danych z systemów operacyjnych (Linux, Windows, Windows Server)

5. Zbieranie danych z systemów kontenerowych

6. Zbieranie danych z systemów typy EDR (Zamawiający obecnie wykorzystuje ESET XDR)

7. Zbieranie danych z urządzeń dostępowych UTM

8. Zbieranie danych z systemów kontroli wersji

9. Zbieranie danych z systemów monitorowania chmury

10. Zbieranie danych z platform IoT

11. 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 podmian 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

**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 ICMPv6 (Internet Control Message Protocol version 6)

15. Monitorowanie aktywności na poziomie protokołu LLDP (Link Layer Discovery Protocol)

16. Monitorowanie aktywności na poziomie protokołu DHCP (Dynamic Host Configuration Protocol)

17. Monitorowanie aktywności na poziomie protokołu IGMP (Internet Group Management Protocol)

18. Monitorowanie aktywności na poziomie protokołu SCTP (Stream Control Transmission Protocol)

19. Monitorowanie aktywności na poziomie protokołu Thread (IPv6-based mesh networking protocol)

20. Monitorowanie aktywności na poziomie protokołu IPv6 over IPv4 tunneling

21. Monitorowanie aktywności na poziomie protokołu IP-in-IP (IP encapsulation)

22. Monitorowanie aktywności na poziomie protokołu SRTP (Secure Real-time Transport Protocol)

23. 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)

**System SIEM realizuje monitoring usług związanych z udzielaniem świadczeń zdrowotnych:**

1. Monitorowanie logów aplikacji medycznych z systemów klasy HIS (Hospital Information System), RIS (Radiology Information System) i PACS (Picture Archiving and Communication System) używanych w środowisku medycznym. Analiza logów z aplikacji medycznych, baz danych tych systemów i systemów informatycznych w jednostkach służby zdrowia pozwala na wykrywanie nieprawidłowych aktywności, prób nieautoryzowanego dostępu do danych medycznych i innych zagrożeń w tym prób wykradzenia danych medycznych.

2. System SIEM monitoruje krytyczne elementy systemu HIS (usługi komunikacyjne odpowiedzialne za ciągłość udzielania świadczeń medycznych):

1. Komunikacja z platformą P1
2. Komunikacji bramek HL7
3. Komunikacja EWUŚ
4. Komunikacja KOWAL
5. Komunikacja AP-KOLCE
6. Funkcjonowanie Rejestru Zdarzeń Medycznych
7. Baza danych systemu HIS

4. System monitoruje bazę danych Oracle szpitalnego systemu medycznego w zakresie co najmniej:

1. Instance state
2. Version
3. Jobs
4. Locks
5. Processes
6. Number of active sessions
7. Recovery area
8. Log switch activity
9. General tablespace information
10. Tablespaces performance
11. Long active sessions
12. Undo retention
13. Checkpoint and online backup state
14. Custom SQLs
15. RMAN backup status
16. RMAN backups
17. ASM disk groups
18. Apply and transport lag of Oracle Data-Guard

**Dodatkowo system umożliwia dodawanie własnych zapytań SQL i monitorowanie zwracanych wartości.**

**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 Systemu 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.

**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. Zamawiający obecnie wykorzystuje do skanowania podatności sieci wewnętrznych LAN system Greenbone.

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 30 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. W okresie obowiązywania gwarancji mają być zapewnione 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- Złagodzenie skutków powstałego zagrożenia (złośliwe oprogramowanie)- przywrócenie ciągłości działania usług | * Przerwa w działaniu serwera/systemu medycznego
* Brak wymiany danych z lokalizacją Zamawiającego
 | - Brak dostępu do systemu medycznego- niedziałające usługi P1 |
| 3 | - Wysokie prawdopodobieństwo incydentu- podejmowanie działań zapobiegawczych | * Znaczące zmiany w SIEM – alerty
* wskazanie wzrostu natężenia ruchu danych
* obniżona wydajność potencjału usług
 | - Informacje o problemach z wydajnością systemów |
| 2 | - Niski potencjalny incydent- działania zapobiegawcze | * Brak wymaganych aktualizacji
* Użytkownik nie zaktualizował hasła w wymaganym odstępie czasu
 | Znaleziony wirus na stacji roboczej |
| 1 | Aktywności utrzymaniowe lub informacyjne | - | Raport |

|  |  |  |  |
| --- | --- | --- | --- |
| 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. Wykonawca w celu zabezpieczenia danych krytycznych przetwarzanych w systemie HIS Zamawiającego zobowiązany jest dołączyć do oferty potwierdzenie, że posiada zgodę producenta systemu HIS na dostęp do monitorowania bazy danych lub autoryzację producenta systemu medycznego, z którego obecnie korzysta Zamawiający lub zrealizował przedmiot zamówienia w obszarze dotyczącym ingerencji w dane przetwarzane przez system medyczny Zamawiającego nie naruszając postanowień licencyjnych i gwarancyjnych dla systemu medycznego Eskulap i gwarantował jego poprawne monitorowanie po zakończeniu prac integracyjnych.

Powyższe zobowiązanie wynika z konieczności monitoringu krytycznych elementów systemu HIS przez system SIEM.

Zamawiający posiada stanowisko producenta systemu HIS (system Eskulap – producent Nexus Polska Sp. z o.o.) w sprawie dostępu do struktur baz danych na potrzeby monitoringu– załączyć do oferty.

W ramach instalacji systemu SIEM Wykonawca podłączy do zainstalowanego systemu elementy infrastruktury Zamawiającego wymienione poniżej (monitorowanie krytycznych elementów infrastruktury IT):

* Serwery fizyczne będące hostami wirtualizacyjnymi – 5 szt.,
* Serwery fizyczne na których jest zainstalowany system operacyjny (bez witualizacji) – 1 szt.,
* Serwery wirtualne - 26 szt.,
* Macierze - 3 szt.,
* Przełączniki SAN - 2 szt.,
* Przełączniki LAN - 35 szt.,
* Serwer Backupu - 1 szt.,
* Bibliotekę taśmowa LTO - 1 szt.,
* Macierz NAS - 1 szt.,
* Serwerów aplikacji – 2 szt.
* JBOS - 1 szt.,
* Usługi IIS - 3 szt.,
* Kontenery docker - 1 szt.,
* serwer AD - 2 szt.,
* usługę skanowania podatności Greenbone – 1 szt.

Miejscowość ............................. data .......................

 ..............................................................................

 podpis i pieczęć składającego oświadczenie(osoba/y uprawniona/e)