**Opis Przedmiotu Zamówienia: Świadczenie usług utrzymania środowiska SIEM/SOC posiadanego przez Zamawiającego**

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** - Dolnośląski Szpital Specjalistyczny im. T. Marciniaka - Centrum Medycyny Ratunkowej ul. Gen. Augusta Emila Fieldorfa 2, 54-049 Wrocław
2. **Wykonawca** – podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w wyniku przeprowadzonego Zapytania Ofertowego.
3. **Strony** - podmioty bezpośrednio uczestniczące w umowie zawiązanej na podstawie rozstrzygnięcia podstępowania przetargowego.
4. **Oprogramowanie** - Całość instrukcji i procedur (programów) oraz powiązanych z nimi danych umożliwiających komputerom i innym programowalnym urządzeniom wykonywanie określonych funkcji..
5. **Umowa** – umowa zawarta w ramach realizacji OPZ.
6. **SWZ –** Specyfikacja Warunków Zamówienia
7. **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.
8. **SIEM** - (ang. Security Information and Event Management) mówi, iż jest to informatyczny system bezpieczeństwa, składający się z rozmaitych komponentów. Istotą jego działania jest monitorowanie oraz analiza ruchu sieciowego i zdarzeń, celem efektywnego wykrywania zagrożeń cybernetycznych oraz łagodzenia skutków cyberataków.
9. **SOC –** (ang. Security Operations Center) to model outsourcingu usług związanych z monitorowaniem, analizą i reagowaniem na zagrożenia bezpieczeństwa informatycznego. W tym modelu zewnętrzny dostawca zapewnia kompleksowe usługi centrum operacji bezpieczeństwa (SOC) dla organizacji, wykorzystując zaawansowane narzędzia, technologie i wykwalifikowany personel.
10. **Szkolenie Administratora(ów)** – szkolenia użytkownika(ów) wskazanych przez Zamawiającego do pełnienia funkcji administratora Oprogramowania
11. **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.
12. **Zadanie** – przedmiot zamówienia (przedmiot Umowy) wynikający łącznie z SWZ, Oferty Wykonawcy, Umowy.
13. **Dzień Roboczy** – każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.

**DOSTAWA OPROGRAMOWANIA**

Przedmiotem zamówienia jest świadczenie usług utrzymania posiadanego przez Zamawiającego systemu Zarządzania Informacjami i Zdarzeniami Bezpieczeństwa (SIEM) oraz Centrum Operacji Bezpieczeństwa (SOC) – obejmujące obsługę incydentów bezpieczeństwa, raportowanie, regularne aktualizacje, konserwację, wsparcie techniczne oraz monitorowanie działania do 31.01.2026r

Zamawiający, zgodnie z decyzją Ministra Zdrowia został ustanowiony operatorem usługi kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz.U. poz. 1560). Usługa kluczowa to udzielenie świadczenia opieki zdrowotnej przez podmiot leczniczy oraz obrót i dystrybucja produktów leczniczych.

Najważniejszym elementem krajowego systemu cyberbezpieczeństwa są tzw. Operatorzy Usług Kluczowych, czyli dostawcy ważnych usług zależnych od systemów informacyjnych w tym szpitale, które te są zobowiązane m.in. do szacowania ryzyka dla swoich usług kluczowych, zbierania informacji o zagrożeniach i podatnościach, stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego oraz zgłaszania incydentów poważnych do tzw. CSIRT-ów (tj. Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego), jak również do Zamawiającego w formie tekstowej, na wskazane adresy e-mail oraz głosowej, na wskazane numery telefonów.

W związku z powyższym Zamawiający w ramach realizacji przedmiotu zamówienia wymaga wsparcia technicznego oraz dostępu do aktualizacji dla posiadanej licencji SIEM oraz świadczenia usługi SOC od dnia 01.05.2025r. do 31.05.2026r.

Poniżej wyspecyfikowano parametry oprogramowania, które objęte jest świadczeniem usług utrzymania środowiska posiadanego przez Zamawiającego:

**Opis parametrów oprogramowania:**

|  |  |
| --- | --- |
| WYMAGANE MINIMALNE/PARAMETRY TECHNICZNE | POTWIERDZENIE WYKONAWCY SPEŁNIENIA WARUNKU(WPISAĆ TAK/NIE) |
| **Parametry techniczne posiadanego przez Zamawiającego systemu SIEM**  |  |
| **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. Wykonywanie skanów podatności
2. 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.
3. 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. Stałe aktualizacje zabezpieczeń i łatek oprogramowania
2. Wdrażanie mechanizmów zwiększających odporność na ataki
3. Edukacja użytkowników w zakresie bezpieczeństwa informatycznego
4. Analiza trendów i nowych zagrożeń w cyberprzestrzeni
5. Wdrażanie technologii zwiększających wykrywalność ataków
6. Ocena ryzyka i zarządzanie bezpieczeństwem informacji
7. Tworzenie planów reagowania na incydenty i awarie
8. Wdrażanie polityk bezpieczeństwa w organizacji
9. Monitorowanie mediów społecznościowych pod kątem zagrożeń
10. Współpraca z innymi organizacjami w celu wymiany informacji o zagrożeniach
11. Tworzenie świadomości kultury bezpieczeństwa w całej organizacji
12. Opracowanie strategii audytów bezpieczeństwa i weryfikacji zgodności
13. 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 gwarancją dla wszystkich funkcji od dnia 01.05.2025r. do dnia 31.01.2026r
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. Instruktaż dla administratorów demonstrujący sposób zarządzania środowiskiem.
5. Szkolenia administratorów on-line z nowych funkcjonalności.
6. Usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania Systemem, bieżące aktualizacje dokumentacji technicznej dla Systemu,
7. Przyjmowania zgłoszeń serwisowych przez dedykowany serwisowy moduł internetowy oraz mail 24/7
8. Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24 /7/365, zgodnie z określonymi poniżej warunkami SLA
9. 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% |

 |  |

|  |  |
| --- | --- |
| WYMAGANE MINIMALNE/PARAMETRY TECHNICZNE | POTWIERDZENIE WYKONAWCY SPEŁNIENIA WARUNKU(WPISAĆ TAK/NIE) |
| System monitoringu infrastruktury IT i usługa SOC  |  |
|  | MINIMALNE WYMAGANIA TECHNICZNE |  |
|  | 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 |  |
|  | 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 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 |  |
|  | 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 |  |
|  | 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 |  |
|  | Konfiguracja 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 |  |
|  | 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 |  |
|  | 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 na zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe. |  |
|  | Cyberbezpieczeństwo |  |
|  | 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” ustawienie stanu na OK, a status „niezsynchronizowany” na 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. |  |
|  | Warunki świadczenia usługi |  |
|  | Operacyjne Centrum Bezpieczeństwa; centrum kompetencyjne, które zajmować się będzie monitorowaniem infrastruktury teleinformatycznej, analizą zdarzeń, detekcją zagrożeń bezpieczeństwa i reagowaniem na wykryte incydenty naruszające bezpieczeństwo teleinformatyczne chronionych organizacji za pomocą analizy zbieranych logów z urządzeń, systemów IT oraz aplikacji, korelacją zdarzeń i detekcją zagrożeń oraz odpowiednią reakcję na pojawiające się incydenty.  |  |
|  | W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie monitorowania zgodnie z opisanymi poniżej wymaganiami. |  |
|  | Przyjmowania zgłoszeń serwisowych przez dedykowany serwisowy moduł internetowy oraz mail 24/7. |  |
|  | Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24/7/365, zgodnie z określonymi poniżej warunkami SLA |  |
|  | 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 |  |
|  | Działalność | lokalizacja klienta |  |
| 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** |
|  |  |  |  |
| Critical | 1 godzina | 1 godzina | 96% |
| 3 | 24 godziny | 2 godziny | 96% |
| 2 | 72 godziny | 8 godzin | 96% |
| 1 | 5 dni | 24 godzin | 96% |

|  |  |  |
| --- | --- | --- |
|  | W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT: |  |
|  | * Serwery 64 szt.,
 |  |
|  | * Macierze 6 szt.,
 |  |
|  | * Przełączniki LAN 55 szt.,
 |  |
|  | * Serwer Backupu 2 szt.,
 |  |
|  | * Bibliotekę taśmowa LTO 1 sztuka
 |  |
|  | * serwer AD 2 szt.
 |  |
|  | W przypadku instalacji przez Zamawiającego nowego rozwiązania będącego jednym z powyższych elementów musi ono zostać objęte systemem monitorowania w ramach usługi SOC. |  |
|  | Producent Systemu SOC musi posiada certyfikacje w zakresie: ŚWIADCZENIA USŁUGI SECURITY OPERATION CENTER - REAGOWANIE NA ZAGROŻENIA CYBERBEZPIECZEŃSTWA, zgodnie z normą ISO ISO/IEC 27001:2017 |  |

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

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