**Załącznik nr 2 – Opis przedmiotu zamówienia**

***OPIS PRZEDMIOTU ZAMÓWIENIA***

***„Podniesienie poziomu bezpieczeństwa systemów teleinformatycznych”***

1. **Wstęp**

Beneficjentem projektu jest Powiatowy Publiczny Zakład Opieki Zdrowotnej w Rydułtowach i Wodzisławiu Śląskim. Celem nadrzędnym projektu jest dalsze podniesienie poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawcy zgodnie z Zarządzeniem nr 8/2023/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 16 stycznia 2023r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa teleinformatycznego u świadczeniodawców (z późn. zm.)

**2.1 Podstawa opracowania**

1. Obowiązujące na dzień wydania opracowania normy i przepisy,
2. Uzgodnienia dokonane przez Zamawiającego,
3. Wiedza techniczna, doświadczenie oraz najlepsze praktyki wykorzystywane w realizacji projektów informatycznych.

**2.2 Założenia projektu**

Celem realizacji projektu opisanego w niniejszym OPZ jest podniesienie poziomu bezpieczeństwa systemów teleinformatycznych Powiatowego Publicznego Zakładu Opieki Zdrowotnej w Rydułtowach i Wodzisławiu Śląskim

**2.3 Zakres projektu**

**Przedmiot zamówienia obejmuje:**

1. Rozwój systemu kopi zapasowych
2. Biblioteka taśmowa
3. Serwer testowania kopii zapasowych oraz testowych odtworzeni kopii
4. Rozwój posiadanego systemu antywirusowego do rozwiązania Endpoint Detection and Response
5. Zakup systemu filtrowania poczty email
6. System SIEM
7. Zastosowanie rekomendacji po audytowych: Zestawy komputerowe

Zakres dla poszczególnych w/w punktów wraz z wytycznymi pod względem wymogów technicznych, funkcjonalno-użytkowych oraz organizacyjnych opisano w dalszej części niniejszego opracowania.

**UWAGA!**

Wykonawca będzie wykonywał prace w czynnym obiekcie – Szpital na czas prowadzenia przez Wykonawcę prac nie zostanie zamknięty i będzie funkcjonował w normalnym trybie.

**UWAGA!**

Wszystkie podane w niniejszym OPZ wymiary oraz wielkości ilościowe są danymi określonymi na podstawie ustaleń dokonanych przez Zamawiającego. Uszczegółowienie tych danych winno być zawarte w kompleksowej Dokumentacji Projektowej, której sporządzenie jest obowiązkiem Wykonawcy wyłonionego w postępowaniu przetargowym.

1. **Wytyczne ogólne dla dokumentacji projektowych**

W poniższych punktach znajdują się wytyczne, które należy zastosować podczas przygotowywania dokumentacji projektowych dla wszystkich systemów informatycznych:

1. W projektach wykonawczych Wykonawca powinien wyszczególnić wszystkie niezbędne roboty instalacyjne wraz z niezbędnymi ekspertyzami dotyczącymi niniejszego projektu.
2. Dokumentacja projektowa powinna umożliwiać etapową realizację prac, pozwalając w trakcie tych prac na bezpieczne użytkowanie istniejącego sprzętu informatycznego.
3. Zabezpieczenia, o których mowa w niniejszym dokumencie, powinny uwzględniać ochronę przed czynnikami losowymi oraz przed nieumyślnym i umyślnym działaniem człowieka. W dokumentacjach projektowych należy więc założyć współdziałanie systemów infrastruktury, systemów informatycznych i procedur administracyjnych.
4. Zaproponowane przez Wykonawcę rozwiązanie powinno cechować się jak najwyższą efektywnością energetyczną.
5. W dalszych rozdziałach niniejszego dokumentu znajdują się normy, których stosowanie jest obowiązkiem Wykonawcy.
6. Dokumentacje projektowe muszą być wykonane oraz zatwierdzone przez wykwalifikowany personel posiadający właściwe uprawnienia projektowe z danej branży.
7. Dokumentację projektową należy przygotować w trzech egzemplarzach w wersji papierowej oraz jednej wersji elektronicznej na płycie CD/DVD.
8. Wszystkie projekty muszą być opracowywane w porozumieniu z Zamawiającym i przez niego zatwierdzone oraz pisemnie dopuszczone do realizacji. Termin na akceptację dokumentacji projektowej przez Zamawiającego wynosi 3 dni robocze od dnia jej złożenia przez Wykonawcę.
9. Wymagania ogólne:
10. Całość dostarczanego sprzętu i oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
11. Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
12. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
13. Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
14. Wszystkie urządzenia muszą posiadać oznakowanie CE.
15. Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
16. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
17. Wymagane jest, aby dostarczony sprzęt był gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
18. Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).
19. Wykonawca po zainstalowaniu i skonfigurowaniu sprzętu i oprogramowania będzie miał obowiązek przeprowadzenia instruktażu dla administratorów Zamawiającego w zakresie konfiguracji i zarządzania dostarczonego sprzętu oraz oprogramowania.

***Opis przedmiotu zamówienia (OPZ)***

**I. Rozwój systemu kopi zapasowych:**

1. **Biblioteka taśmowa:**

|  |  |  |
| --- | --- | --- |
| Lp. | WYMAGANIA MINIMALNE | POTWIERDZENIE WYKONAWCY SPEŁNIENIA WARUNKU (WPISAĆ TAK/NIE |
|  | Obudowa przystosowana do montażu w standardowej szafie rack 19’’. Maksymalna wysokość oferowanego rozwiązania - 3U. |  |
|  | Biblioteka taśmowa musi być wyposażona w min. 1 napęd taśmowy LTO8 z interfejsem FC min. 8 Gbit/s. |  |
|  | Biblioteka taśmowa musi mieć możliwość rozbudowy do min. 8 napędów taśmowych. |  |
|  | Biblioteka musi być wyposażona w nie mniej niż 20 slotów na taśmy i posiadać możliwość rozbudowy do co najmniej 100 slotów na taśmy. |  |
|  | Biblioteka musi być wyposażona w przynajmniej 3 sloty wejścia/wyjścia, umożliwiający wymianę taśm bez konieczności wyłączania urządzenia. |  |
|  | Biblioteka musi być wyposażona w czytnik kodów kreskowych. |  |
|  | Biblioteka musi być wyposażona w komplet magazynków na taśmy, tak by możliwa była pełna obsada biblioteki taśmami LTO. |  |
|  | Możliwość zdalnego zarządzania biblioteką poprzez interfejs WWW. |  |
|  | Możliwość monitorowania stanu biblioteki i napędów. |  |
|  | Biblioteka musi posiadać panel sterowania oraz wyświetlacz informujący o błędach urządzenia, aktywności napędów. |  |
| Wymagania dodatkowe | | |
|  | Do biblioteki należy dostarczyć:  - niezbędne kable zasilające,  - taśmę LTO 8 – 10szt.  - taśmę czyszczącą – 1szt.  - przewód światłowodowy – 1szt. |  |
|  | Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu. |  |
|  | Wszystkie oferowane urządzenia muszą być fabrycznie nowe. |  |
|  | Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. |  |
|  | Urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz. |  |
|  | Oferowane produkty (urządzenia, sprzęty) w przedmiotowym postępowaniu o udzielenie zamówienia publicznego muszą spełniać wymagania norm CE,  tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE. |  |
|  | Urządzanie musi być objęta minimum 24 miesięczną gwarancją (kryterium oceny oferty) |  |
|  | Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji. |  |
|  | Karta FC dual port 16Gb kompatybilna z posiadanym serwerem backupu Fujitsu RX2540 M6 |  |

1. **Serwer testowania kopii zapasowych oraz testowych odtworzeni kopii:**

|  |  |  |
| --- | --- | --- |
| Lp. | WYMAGANIA MINIMALNE | POTWIERDZENIE WYKONAWCY SPEŁNIENIA WARUNKU (WPISAĆ TAK/NIE |
|  | obudowa do montażu w szafie typu rack |  |
|  | zasilanie redundantne, przynajmniej 2 zasilacze typu HotPlug |  |
|  | płyta główna z możliwością zainstalowania minimum dwóch procesorów |  |
|  | zegar procesora minimum 2,6 GHz |  |
|  | Zainstalowany min 1 procesor minimum ośmiordzeniowy klasy x86 dedykowane do pracy w serwerach, zaprojektowane do pracy w układach wieloprocesorowych |  |
|  | pamięć minimum 256GB ECC DIMM, rozszerzalna, z zabezpieczeniem typu: ECC |  |
|  | dyski minimum 2x 1,9TB SSD skonfigurowane w RAID1 , 4x2,4TB 10K 4x8TB 7.2K |  |
|  | sieć minimum 2x16Gb FC, 2x10Gb SFP+ SR |  |
|  | z przodu obudowy: 1x USB 3.0, 1x USB 2.0 |  |
|  | z tyłu obudowy: 2x USB 3.0, , 1x DB-15 |  |
|  | Zarządzanie:   * Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania * Monitoring statusu i zdrowia systemu * Logowanie zdarzeń * Umożliwiający Update systemowego firmware * Umożliwiający zdalną konfigurację serwera * Monitoring i możliwość ograniczenia poboru prądu * Zdalne włączanie/wyłączanie/restart * Przekierowanie konsoli szeregowej przez IPMI * Zrzut ekranu w momencie zawieszenia system * Możliwość przejęcia zdalnego ekranu 1920x1200, 60 Hz,16 bpp * Zdalny dostęp do serwera * Możliwość zdalnej instalacji systemu operacyjnego * Alerty Syslog * Przekierowanie konsoli szeregowej przez SSH * Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera * Możliwość mapowania obrazów ISO z lokalnego dysku operatora * Możliwość mapowania obrazów ISO przez HTTPS * Możliwość jednoczesnej pracy użytkowników przez wirtualną konsolę * Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3 |  |
|  | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID |  |
|  | Serwerowy system operacyjny umożliwiający uruchomienie min 4 maszyn wirtualnych z usługą iis. |  |
|  | gwarancja: minimum 24 m-ce, 1YNBD, producenta (kryterium oceny oferty) |  |

**II. Rozwój posiadanego systemu antywirusowego do rozwiązania Endpoint Detection and Response**

W związku z posiadaniem przez Zamawiającego systemu antywirusowego ESET zamawiający oczekuje rozwoju posiadanego oprogramowania do funkcji systemu EDR – licencje dostarczane w ramach zamówienia będą realizacją rozbudowy posiadanego już systemu ESET.

Ilość szt. Licencji nie mniej niż – 300 szt.

Dostęp do aktualizacji systemu bezpieczeństwa powinien być nie krótszy niż 12 miesięcy.

**III. Zakup systemu filtrowania poczty email**

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

# **Ogólne funkcje systemu ochrony poczty**

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 70 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 50 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Prevention)
18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

# **Kontrola antywirusowa i ochrona przed malware**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.

# **Kontrola antyspamowa**

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

# **Ochrona przed atakami na usługę poczty**

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

# **Funkcje logowania i raportowania**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

# **Funkcje pracy w trybie wysokiej dostępności (HA)**

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

# **Aktualizacje sygnatur, dostęp do bazy spamu**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

# **Zarządzanie**

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

# **Certyfikaty**

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

# **Serwisy i licencje**

System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

# **Gwarancja oraz wsparcie**

1. System musi być objęty serwisem producenta przez okres minimum 24 miesięcy (kryterium oceny oferty), upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie .

**IV. System SIEM:**

|  |
| --- |
| **WYMAGANIA MINIMALNE** |
| **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 24 miesięcznym gwarancją dla wszystkich funkcji. 2. W okresie obowiązywania licencji 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 |  | |  | 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 | Znaleziony wirus na stacji roboczej | |  |  | hasła w wymaganym odstępie czasu |  | |  |  |  |  | | 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% |   **Informacje dodatkowe:**   1. Producent Systemu SIEM posiada certyfikacje w zakresie: ŚWIADCZENIA USŁUGI SECURITY OPERATION CENTER - REAGOWANIE NA ZAGROŻENIA CYBERBEZPIECZEŃSTWA, zgodnie z normą ISO ISO/IEC 27001:2017- załączyć do oferty |

# **V. Zastosowanie rekomendacji po audytowych:**

## **Zestaw komputerowy 35 szt. o parametrach:**

|  |  |  |
| --- | --- | --- |
| **WYMAGANIA MINIMALNE** | | **POTWIERDZENIE WYKONAWCY SPEŁNIENIA WARUNKU (WPISAĆ TAK/NIE** |
| Komputer stacjonarny | |  |
| Obudowa | Small Form Factor |  |
| Taktowanie procesora | 3.4 GHz |  |
| Liczba rdzeni | 4 |  |
| Liczba wątków | 8 |  |
| Zainstalowana pamięć RAM | 16GB |  |
| Rodzaj pamięci | DDR4 |  |
| Częstotliwość szyny pamięci | 3200 MHz |  |
| Typ dysku | SSD |  |
| Pojemność SSD | 256 GB |  |
| Format szerokości SSD | M.2 |  |
| Interfejs dysku SSD | PCI-Express |  |
| Model karty graficznej | zintegrowana |  |
| Porty wideo | 1 x HDMI |  |
| 1 x DisplayPort |  |
| Interfejs sieciowy | 1 x 10/100/1000 Mbit/s |  |
| Wi-Fi 802.11a/b/g/n/ac |  |
| Bluetooth |  |
| Napęd optyczny | DVD-RW |  |
| Czytnik kart pamięci | Tak |  |
| Porty USB | 4 x USB 2.0 Type-A |  |
| 4 x USB 3.0 Type-A |  |
| Pozostałe porty we/wy | 1 x Audio (Line-out) |  |
| 1 x Audio (Combo) |  |
| 1 x RJ-45 |  |
| Gniazda rozszerzeń | 1 x PCIe 3.0 x 1 |  |
| 1 x PCIe 3.0 x 16 |  |
| Moc zasilacza | 180 W |  |
| Kolor | Czarny |  |
| System operacyjny | w najnowszej wersji dedykowany do dostarczanego komputera z możliwością integracji z ActiveDirectory |  |
| Akcesoria | Klawiatura multimedialna USB |  |
| Mysz optyczna |  |
| Informacje o gwarancji | 3 lata w systemie min. door to door, lub ONSITE |  |
| Monitor | |  |
| Przekątna ekranu | Min. 23.8'' |  |
| Typ matrycy | VA |  |
| Powierzchnia matrycy | Matowa |  |
| Technologia podświetlania | Diody LED |  |
| Rozdzielczość | 1920 x 1080 (FHD 1080) |  |
| Czas reakcji | 8 ms |  |
| Jasność | 250 cd/m² |  |
| Kontrast statyczny | 3 000:1 |  |
| Kontrast dynamiczny | 3 000:1 |  |
| Częstotliwość odświeżania | 60 Hz |  |
| Kąt widzenia poziomy | 178 ° |  |
| Kąt widzenia pionowy | 178 ° |  |
| Ilość kolorów | 16,7 mln |  |
| Gniazda we/wy | 1 x 15-pin D-Sub |  |
| 1 x HDMI |  |
| TCO Certified | Tak |  |
|  | Energy Star |  |
| EPEAT |  |
| Certyfikat CE (znak CE) - Wszystkie dostarczone urządzenia muszą być oznakowane znakiem CE zgodnie z wymogami deklaracji zgodności WE wystawionej przez producenta lub jego upoważnionego przedstawiciela, w celu potwierdzenia zgodności z dyrektywami Nowego Podejścia lub równoważnymi |  |
| Standard VESA | 100 x 100 |  |
| Akcesoria w zestawie | Kabel HDMI |  |
| Kolor | Czarny |  |
| Informacje o gwarancji | 3 lata w systemie door to door lub ONSITE |  |