**Załącznik nr 2 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Definicje:

1. **Zamawiający** – oznacza **Pałuckie Centrum Zdrowia Spółka z o. o.**
2. **Wykonawca** - podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez prowadzenia negocjacji na podstawie art. 275 pkt 1 Ustawy z dnia 11 września 2019r – prawo zamówień publicznych (Dz.U. 2023 poz. 1605 ze zm.).
3. **Strony** - podmioty bezpośrednio uczestniczące w umowie zawiązanej na podstawie rozstrzygnięcia podstępowania przetargowego.
4. **Umowa** – umowa zawarta w ramach realizacji OPZ.
5. **SWZ –** Specyfikacja Warunków Zamówienia
6. **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.
7. **Wada**- Należy przez to rozumieć Awarię, Błąd, Usterkę
8. **Awaria-** oznacza to Błąd, uniemożliwiający prawidłowe użytkowanie oprogramowania/ sprzętu lub jego części, który nie prowadzi do zatrzymania eksploatacji oprogramowania lub możliwości korzystania ze sprzętu.
9. **Błąd** - oznacza to powtarzalne działanie oprogramowania/sprzętu niezgodne z jego dokumentacją użytkową, uniemożliwiające wykonanie części jego funkcji.
10. **Usterka -** należy przez to rozumieć kategorię Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SWZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
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. **Protokół Odbiorczy** – protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego wykonanych przez Wykonawcę prac będących przedmiotem poszczególnych Etapów.
13. **Protokół Odbioru Końcowego-** Protokół, który po podpisaniu bez zastrzeżeń przez Zamawiającego, stanowi potwierdzenie wykonania i odbioru Przedmiotu Zamówienia.
14. **Protokół Dostawy-** Protokół, w którymZamawiający sprawdza ilości dostarczonego towaru i porównuje go ze stanem wykazanym w dokumentach towarzyszących dostawie.
15. **Protokół Usterek -** Protokół, w którym Zamawiający wskazuje zastrzeżenia co do zakresu i jakości wykonanych prac, które uniemożliwiają dokonanie odbioru wykonanych dostaw i prac.
16. **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.
17. **Dzień Roboczy** – każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
18. **Godziny Robocze** – godziny od 7:30 do 14:30 w każdym Dniu Roboczym.
19. **Czas Reakcji** – okres liczony od zaewidencjonowania Zgłoszenia Serwisowego do zmiany jego statusu na zarejestrowane.
20. **Czas Naprawy** - czas pomiędzy Zgłoszeniem Serwisowym a usunięciem/rozwiązaniem przyczyny jego zgłoszenia.
21. **HelpDesk (HD)** – narzędzie posiadające interfejs WWW służące do rejestracji zgłoszeń (potencjalnych problemów, usterek) oraz kontroli ich cyklu życia (tzw. Issue Tracking System lub Defect Tracking System). System HD udostępniony zostanie przez Wykonawcę dla Zamawiającego na czas realizacji przedmiotu zamówienia oraz w okresie jego gwarancji.

**DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ ORAZ OPROGRAMOWANIA**

Przedmiotem zamówienia jest podniesienie poziomu cyberbezpieczeństwa Szpitala.

Wymagania ogólne:

* Całość dostarczanego sprzętu i oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
* 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.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
* 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.
* Wszystkie urządzenia muszą posiadać oznakowanie CE.
* Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
* Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
* Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
* Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).

Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

* posiadane środowisko domenowe,
* posiadaną konfigurację sieci wraz z jednostkami podległymi,
* posiadaną konfiguracją baz danych i backupów,
* konfigurację stacji roboczych.

# Rozwój systemu kopi zapasowych poprzez:

1. **Zakup biblioteki taśmowej o parametrach:**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | *Wymagane minimalne parametry techniczne* | *Wymóg do spełnienia (warunek graniczny)* | *OFEROWANE PARAMETRY TECHNICZNE – podaje Wykonawca**Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr**NIE – wykonawca nie spełnia konkretnego parametru* |
|  | Obudowa przystosowana do montażu w standardowej szafie rack 19’’. Maksymalna wysokość oferowanego rozwiązania - 3U. | TAK |  |
|  | Biblioteka taśmowa musi być wyposażona w min. 1 napęd taśmowy LTO8 z interfejsem FC min. 8 Gbit/s. | TAK |  |
|  | Biblioteka taśmowa musi mieć możliwość rozbudowy do min. 8 napędów taśmowych. | TAK |  |
|  | Biblioteka musi być wyposażona w nie mniej niż 20 slotów na taśmy i posiadać możliwość rozbudowy do co najmniej 100 slotów na taśmy. | TAK |  |
|  | Biblioteka musi być wyposażona w przynajmniej 3 sloty wejścia/wyjścia, umożliwiający wymianę taśm bez konieczności wyłączania urządzenia. | TAK |  |
|  | Biblioteka musi być wyposażona w czytnik kodów kreskowych. | TAK |  |
|  | Biblioteka musi być wyposażona w komplet magazynków na taśmy, tak by możliwa była pełna obsada biblioteki taśmami LTO. | TAK |  |
|  | Możliwość zdalnego zarządzania biblioteką poprzez interfejs WWW. | TAK |  |
|  | Możliwość monitorowania stanu biblioteki i napędów. | TAK |  |
|  | Biblioteka musi posiadać panel sterowania oraz wyświetlacz informujący o błędach urządzenia, aktywności napędów. | TAK |  |
| Wymagania dodatkowe |
|  | Do biblioteki należy dostarczyć:- niezbędne kable zasilające,- taśmę LTO 8 – 20szt. - taśmę czyszczącą – 1szt.- przewód światłowodowy – 1szt. | TAK |  |
|  | Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu. | TAK |  |
|  | Wszystkie oferowane urządzenia muszą być fabrycznie nowe. | TAK |  |
|  | Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. | TAK |  |
|  | Urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.  | TAK |  |
|  | 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. | TAK |  |
|  | Urządzanie musi być objęta 36 miesięczną gwarancją  | TAK |  |
|  | Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji.  | TAK |  |

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

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | *Wymagane minimalne parametry techniczne* | *Wymóg do spełnienia (warunek graniczny)* | *OFEROWANE PARAMETRY TECHNICZNE – podaje Wykonawca**Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr**NIE – wykonawca nie spełnia konkretnego parametru* |
|  | obudowa do montażu w szafie typu rack | TAK |  |
|  | zasilanie redundantne, przynajmniej 2 zasilacze typu HotPlug | TAK |  |
|  | płyta główna z możliwością zainstalowania minimum dwóch procesorów | TAK |  |
|  | zegar procesora minimum 2,6 GHz | TAK |  |
|  | Zainstalowany min 1 procesor minimum ośmiordzeniowy klasy x86 dedykowane do pracy w serwerach, zaprojektowane do pracy w układach wieloprocesorowych | TAK |  |
|  | pamięć minimum 256GB ECC DIMM, rozszerzalna, z zabezpieczeniem typu: ECC | TAK |  |
|  | dyski minimum 2x 1,9TB SSD skonfigurowane w RAID1 , 4x2,4TB 10K 4x8TB 7.2K | TAK |  |
|  | sieć minimum 2x16Gb FC, 2x10Gb SFP+ SR | TAK |  |
|  | z przodu obudowy: 1x USB 3.0, 1x USB 2.0 | TAK |  |
|  | z tyłu obudowy: 2x USB 3.0, , 1x DB-15 | TAK |  |
|  | 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
 | TAK |  |
|  | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID | TAK |  |
|  | Serwerowy system operacyjny umożliwiający uruchomienie min 4 maszyn wirtualnych z usługą iis. |  |  |
|  | gwarancja: min. 36 m-cy, 3YNBD, producenta | TAK |  |

# Rozwój systemu bezpieczeństwa poczty:

**Wymagania ogólne systemu**

1. System musi posiadać konsolę zarządzającą dostępną przez przeglądarkę internetową.
2. System musi umożliwiać dostęp do konsoli osobno poprzez http oraz https
3. System musi mieć możliwość implementacji wewnątrz i na zewnątrz struktury informatycznej organizacji, powinien funkcjonować niezależnie od pozostałych jej elementów.
4. Rozwiązanie musi wspierać filtrację dla serwerów znajdujących się wewnątrz i na zewnątrz struktury informatycznej danej organizacji.
5. System musi być dostępny w postaci pliku ISO pozwalającym na instalację na serwerze fizycznym, jak też w wersji na maszyny wirtualne ze wsparciem dla następujących środowisk: VMWare, Citrix, MS Hyper-V.
6. Interfejs rozwiązania musi wspierać kilka języków i posiadać także polskojęzyczny interfejs.
7. System musi zawierać główny pulpit, na którym będą wyświetlane podstawowe informacje takie jak:
	1. Stan systemu w tym zużycie CPU, RAM, pamięci dyskowej
	2. Wersję systemu i bieżącą datę
	3. Informacje o typie aktualnie używanego procesora
	4. Informacje o stanie skanerów antywirusowych
	5. Wykres przedstawiający informacje zbiorcze na temat procesowania wiadomości
	6. Informacje z ostatnich siedmiu dni w formie listy lub/i wykresu przedstawiające liczbę zablokowanych wiadomości, liczbę wystąpień wirusów, liczbę zablokowanych załączników i innych odrzuceń
	7. Listy najpopularniejszych nadawców wirusów i spamu oraz najpopularniejszych wirusów wykrytych przez silniki antywirusowe
8. System musi w widocznym miejscu zawierać sekcje poświęconą wsparciu technicznemu umożliwiającą utworzenie bezpiecznego połączenia z suportem producenta.
9. Konsola zarządzająca musi mieć możliwość dostosowywania wyglądu, personalizacji kolorystyki interfejsu i umieszczenia logo firmy.
10. System musi mieć możliwość obsługi certyfikatów SSL.
11. System musi mieć możliwość importu certyfikatów.
12. System musi mieć możliwość obsługi TLS.
13. System musi mieć funkcjonalność szyfrowania emaili kluczem prywatnym, i odszyfrowywania ich u odbiorcy kluczem publicznym, tak zwane DKIM
14. System musi mieć możliwość uwierzytelniania nadawcy poprzez określone mechanizmy, nie mniej niż SPF, DMARC, ARC.
15. System musi mieć możliwość wykonywania kopii zapasowych konfiguracji zarówno automatycznych na serwerze FTP lub w chmurze amazona, jak i na żądanie, a także możliwość importu takiej konfiguracji.
16. System musi obsługiwać zdalny Syslog, osobny dla logów dotyczących maili i osobny dla logów dotyczących inferface’u oraz zmian w systemie
17. System musi wspierać SNMP v2c oraz v3
18. System musi mieć możliwość pracy w klastrze (dwóch lub więcej węzłów).
19. Aktualizacja systemu musi odbywać się poprzez konsolę webową, oraz nie może mieć wpływu na działanie samego systemu (tj. żadna wiadomość mailowa nie zostanie utracona). W przypadku aktualizacji systemów działających w klastrze, musi istnieć możliwość uruchomienia tych procesów oddzielnie (np. w przypadku gdyby aktualizacja okazała się wadliwa)

**Moduł antyspamowy**

1. System musi posiadać wbudowany silnik antyspamowy.
2. System musi mieć umożliwiać korzystanie z zewnętrznych baz RBL, dowolnie definiowanych przez administratora.
3. System musi mieć możliwość tworzenia przez administratora białej listy adresów IP nadawcy, pomijanych podczas filtracji RBL.
4. System musi mieć możliwość wyłączania filtracji RBL dla poszczególnych domen podpiętych do rozwiązania.
5. System musi mieć możliwość sprawdzenia poprawności odbiorcy danej wiadomości, w trybie co najmniej: dynamicznym (weryfikacja na serwerze docelowym), LDAP, listę dozwolonych odbiorców oraz poprzez wyrażenia regularne.
6. System musi być wspierany samouczącą się bazą danych Bayes’a.
7. System musi obsługiwać Passive OS Fingerprinting oraz mechanizm Penpals i analizę Botnetów.
8. System musi posiadać konfigurowalną szarą listę, z możliwością jej włączenia i wyłączenia
9. System musi pozwalać na zdefiniowanie języków, w których to muszą być napisane wiadomości, by pomyślnie przeszły weryfikację
10. System musi umożliwiać tworzenie białych i czarnych list, opartych na adresach email oraz nazwach domen. Listy powinny być traktowane globalnie, per domena i osobno dla każdego użytkownika.
11. System musi umożliwiać tworzenie białych i czarnych list, opartych na adresach IP serwerów pocztowych nadawcy.
12. System musi mieć możliwość indywidualnego ustalania wysokości progu filtrowania wiadomości przez moduł antyspamowy dla domen jak i również dla określonych aliasów pocztowych.
13. System musi mieć możliwość rozczytywania skróconych wersji URLi
14. System musi mieć możliwość dodawania konfigurowalnych stopek do maili wychodzących, które potwierdzą że zostały one przefiltrowane przez tenże system

**Moduł antywirusowy**

1. System musi zawierać dwa niezależnie działające silniki antywirusowe zewnętrznego dostawcy.
2. System musi mieć możliwość całkowitego wyłączenia silnika antywirusowego.
3. System musi samoczynnie aktualizować bazę danych dla wbudowanego silnika antywirusowego. Baza musi być aktualizowana minimum, co godzinę.

**Moduł kontroli treści**

1. System musi umożliwiać blokowanie wybranych przez administratora rozszerzeń i nazw plików.
2. System musi umożliwiać blokowanie co najmniej następujących rozszerzeń plików:

ade, adp, bat, chm, cmd, com, cpl, dll, doc, exe, hta, ins, isp, jar, js, jse, lib, lnk, mde, msc, msp, mst, pif, scr, sct, shb, sys, vb, vbe, vbs, vxd, wsc, wsf, wsh

1. System musi umożliwiać blokowanie co najmniej następujących typów MIME:

application/ecmascript, application/javascript, application/x-javascript,

application/x-msdos-program, application/x-msdownload, text/ecmascript,

text/javascript

1. Wykrywanie i blokowanie rozszerzenia załącznika typu wykonywalnego powinno być odporne na zmianę nazwy i rozszerzenia, również w przypadku skompresowanego archiwum.
2. System musi umożliwiać blokowanie zabezpieczonych hasłem archiwów.
3. System musi umożliwiać tworzenie własnych reguł filtracji.
4. System musi umożliwiać kontrolę treści opartej na słowniku lub wyrażeniu regularnym (przykładowo blokowanie wiadomości z numerami kard kredytowych, numerami PESEL czy też innymi danymi określanymi jako wrażliwe).
5. Wszystkie wyżej wymienione funkcje powinny być dostępne dla filtracji wiadomości wychodzących i przychodzących.
6. System musi posiadać mechanizm przepisywania linków w wiadomościach, automatycznie kierujący odbiorcę na serwery zewnętrzne, które kategoryzują strony internetowe pod kątem zagrożeń:
	1. Funkcjonalność można ustawić osobno dla domeny i dla użytkownika systemu
	2. Można tworzyć wyjątki dla domen stron internetowych, które mają być nie przepisywane, osobno dla całej domeny pocztowej oraz użytkowników systemu.
	3. Funkcjonalność powinna pozwalać na edycję wyświetlanej strony z informacją o blokadzie, minimum o treść wyświetlanej informacji oraz o wyświetlane logo.

**Moduł powiadamiania użytkowników**

1. System musi posiadać moduł powiadamiający adresata bądź odbiorcę wiadomości o podjętych przez system akcjach.
2. System musi powiadamiać o zablokowanych wiadomościach w tym wiadomościach zablokowanych przez moduł antyspamowy, antywirusowy czy moduł kontroli treści.
3. Wiadomości powinny być edytowalne i wysyłane do odbiorcy lub/i nadawcy.

**Kwarantanna**

1. System musi posiadać mechanizm kwarantanny.
2. System musi zawierać wbudowaną wyszukiwarkę.
3. System musi generować raporty kwarantanny
	1. Raporty kwarantanny powinny być generowane automatycznie lub na żądanie
	2. Raporty kwarantanny powinny być personalizowane (w tym podmiana logo producenta)
	3. Raporty powinny być generowane dla użytkowników systemu pocztowego.
	4. W przypadku współpracy z serwerami pocztowymi Microsoft Exchange, raport powinien być generowany dla użytkownika tylko raz, uwzględniając jego wszystkie aliasy.
4. System musi umożliwić dostęp do kwarantanny poprzez interfejs przeglądarki internetowej dla każdego użytkownika indywidualnie z możliwością dopasowania odpowiednich uprawnień.
5. System musi umożliwić uwierzytelnianie użytkownika za pośrednictwem wewnętrznej bazy, LDAP, w oparciu o bazę kont na docelowym serwerze pocztowym (POP3, IMAP), lub bazy SQL.

**Pozostałe funkcjonalności**

1. System musi mieć możliwość tworzenie wielu administratorów o zróżnicowanym poziomie uprawnień.
2. System musi mieć możliwość tworzenia grup domen przyporządkowanych odpowiednim administratorom.
3. System musi posiadać funkcję kontroli ilości przetwarzanych wiadomości dla ruchu przychodzącego i wychodzącego.
4. System musi umożliwiać wyświetlanie statystyk dotyczących aktualnego użycia licencji (liczby unikalnych kont mailowych, przez które przechodzą wiadomości).
5. System musi umożliwiać manualne ustawienie równocześnie pracujących procesów SMTP w celu optymalizacji wydajności rozwiązania względem platformy, na której jest zainstalowane.
6. System musi posiadać moduł kontroli jakości, który pozwoli zdefiniować ograniczenia odnoszące się do co najmniej:
	1. ilości maili, które mogą zostać wysłane z określonej jednostce czasu
	2. zbiorczego rozmiaru maili, które mogą zostać wysłane w określonej jednostce czasu
7. System musi mieć możliwość ujednolicenia aliasów emailowych
8. System powinien mieć możliwość konfiguracji raportów generowanych użytkownikom tak, aby mogły być generowane na żądanie (z opcją wyłączenia tej opcji przez administratora)
9. Dostarczony system musi zostać zainstalowany d0 100 użytkowników Zamawiającego
10. Okres aktualizacji minimum 2 lata.

# Segmentacja i rozbudowa sieci :

1. **Przełącznik rdzenia sieci 2 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | *Wymagane minimalne parametry techniczne* | *Wymóg do spełnienia (warunek graniczny)* | *OFEROWANE PARAMETRY TECHNICZNE – podaje Wykonawca**Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr**NIE – wykonawca nie spełnia konkretnego parametru* |
| 1 | 4 x 10GBase-T/SFP+ Combo IEEE 802.3ae | TAK |  |
| 2 | Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). | TAK |  |
| 3 | Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. | TAK |  |
| 4 | 20 x SFP+ IEEE 802.3ae/802.3ae;- porty SFP+ muszą obsługiwać również moduły SFP 1000Base-X IEEE 802.3z; | TAK |  |
| 5 | Konsola szeregowa RS-232 oraz dedykowany port Ethernet do zarządzania Out-of-Band. | TAK |  |
| 6 | Port dla zewnętrznych czujników zdarzeń i port dla zewnętrznego element wykonawczego wyzwalanego po wystąpieniu alarmu. | TAK |  |
| 7 | Łączenie urządzeń w stosy o wielkości co najmniej 4 jednostek. Awaria żadnego pojedynczego urządzenia nie może spowodować przerwania pracy stosu. Praca w topologii pierścienia. Przepustowość magistrali stosu co najmniej 80 Gb/s. Port-Channel oraz Mirroring ruchu przy użyciu dowolnych portów w stosie. | TAK |  |
| 8 | Zasilanie AC 230V. Zamontowane min 2 zasilacze. | TAK |  |
| 9 | Pojemność przełączania nie mniej, niż 480 Gb/s. Wydajność przełączania nie mniej niż 357 Mp/s. | TAK |  |
| 10 | Architektura nieblokującą (wire-speed). | TAK |  |
| 11 | Pojemność tablicy MAC nie mniej, niż 48K. Możliwość wprowadzenia co najmniej 1020 wpisów statycznych. | TAK |  |
| 12 | Ilość RAM nie mniej, niż 512 MB. Pamięć Flash - nie mniej niż 128 MB. | TAK |  |
| 13 | Obsługa ramek Jumbo o rozmiarze co najmniej 12280 B. | TAK |  |
| 14 | Bufor pakietów nie mniej, niż 4 MB. | TAK |  |
| 15 | Temperatura pracy w zakresie co najmniej od -5C do 50 stopni Celsjusza. | TAK |  |
| 16 | Ochrona przeciwprzepięciową na portach miedzianych co najmniej do 1 kV. | TAK |  |
| 17 | MTBF > 140000 godzin. | TAK |  |
| 19 | Funkcjonalności warstwy 2 | TAK |  |
| 20 | IGMP Snoopingv3- obsługa nie mniej, niż 510 grup multicast w tym co najmniej 64 grup statycznych. | TAK |  |
| 21 | MLD Snoopingv2- obsługa nie mniej, niż 250 grup multicast w tym co najmniej 64 grup statycznych. | TAK |  |
| 22 | Możliwość uwierzytelniania przyłączania do grup multicast. | TAK |  |
| 23 | Możliwość wybiórczego filtrowania zapytań IGMP oraz wybiórczego filtrowania zapytań MLD. | TAK |  |
| 24 | IEEE 802.1D, 802.1w, 802.1s (co najmniej 64 instancji). Funkcja 802.1Q Restricted Role oraz 802.1Q Restricted TCN. | TAK |  |
| 25 | Wykrywanie pętli w L2 dla przyłączonych urządzeń bez protokołu rodziny STP. | TAK |  |
| 26 | Tworzenie interfejsów Port-Channel - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie z obsługą LACP. | TAK |  |
| 27 | LLDP (802.1AB) oraz LLDP-MED. | TAK |  |
| 28 | ERPS (ITU-T G.8032) w wersji co najmniej 2. Jednoczesna obsługa co najmniej 14 pierścieni. | TAK |  |
| 29 | DHCP Relay w tym opcji 60 i 61 oraz opcji 82. DHCP Relay dla IPv6. | TAK |  |
| 30 | Port monitoring/mirroring/span. Możliwość monitorowania tylko wybranego ruchu oraz monitorowania ruchu na port w innym przełączniku (RSPAN). | TAK |  |
| 31 | Obsługa klastrów MS NLB. | TAK |  |
| 33 | Obsługa sieci VLAN | TAK |  |
| 34 | 802.1Q VLAN, co najmniej 4094, 802.1v GVRP, QinQ VLAN, VLAN Translation, w tym klasyfikacja co najmniej wg adresów MAC, adresów IP, CVID, priorytetu 802.1p, protokołu IP i portu. | TAK |  |
| 35 | Multicast VLAN (MVR) - co najmniej co najmniej 5 takich sieci VLAN. | TAK |  |
| 36 | Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. | TAK |  |
| 37 | Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. | TAK |  |
| 38 | Urządzenie powinno umożliwiać tworzenie VLANów, które będą zapewniały funkcjonalność tworzenia wielu grup portów w ramach których porty będą mogły się komunikować, ale zablokowana będzie komunikacja pomiędzy portami w różnych grupach oraz wszystkie grupy będą mogły komunikować się z grupą portów wspólnych. Wszystkie porty należące do takich VLANów powinny pozostać nietagowane. | TAK |  |
| 39 | Przełącznik powinien obsługiwać także sieci VLAN oparte o podsieci IP - co najmniej 510 wpisów. | TAK |  |
| 40 | Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN. | TAK |  |
| 41 | Powinna istnieć możliwość liczenia w pakietach przepływającego przez VLAN ruchu. | TAK |  |
| 43 | Funkcjonalności warstwy 3 | TAK |  |
| 44 | Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 256 takich interfejsów. | TAK |  |
| 45 | Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv6 na urządzeniu - co najmniej 256 takich interfejsów; oraz możliwość utworzenia wielu interfejsów IP na pojedynczej skonfigurowanej sieci VLAN - co najmniej 256 takich interfejsów. | TAK |  |
| 46 | Musi istnieć możliwość skonfigurowania specjalnego interfejsu IP, który jest cały czas dostępny w sieci niezależnie od pozostałej konfiguracji przełącznika. | TAK |  |
| 47 | Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą odpowiadanie na zapytania ARP w imieniu urządzenia znajdującego się w innej podsieci VLAN. | TAK |  |
| 48 | Przełącznik musi posiadać funkcjonalność Gratuitous ARP. | TAK |  |
| 49 | Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci. | TAK |  |
| 50 | Urządzenie musi posiadać również funkcjonalność umożliwiającą przekazywanie zapytań DNS do odpowiednich serwerów DNS w sieci (wewnętrznych lub zewnętrznych). | TAK |  |
| 51 | Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 96 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP. Serwer DHCP musi mieć możliwość przydzielania dowolnych opcji DHCP. | TAK |  |
| 52 | Serwer DHCP musi także obsługiwać delegację prefiksów DHCPv6. | TAK |  |
| 53 | Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 1K wpisów oraz umożliwiać wprowadzenie co najmniej 512 wpisów statycznych. | TAK |  |
| 54 | Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 32250 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 16128 takich tras dla IPv6. | TAK |  |
| 55 | Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 4090 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 1024 takich tras dla IPv6. | TAK |  |
| 56 | Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 250 takich tras) oraz dla IPv6 (co najmniej 120 tras). | TAK |  |
| 57 | Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4 oraz dla IPv6. | TAK |  |
| 58 | Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery. | TAK |  |
| 59 | Przełącznik musi być wyposażony w funkcjonalność umożliwiającą trasowanie ruchu w różnych kierunkach w zależności od zawartości pakietów (np. na podstawie adresu źródłowego IP lub protokołu IP). | TAK |  |
| 60 | Przełącznik musi umożliwiać redystrybucję tras routingu pomiędzy różnymi protokołami routingu skonfigurowanymi na urządzeniu. | TAK |  |
| 61 | Urządzenie powinno umożliwiać konfigurację protokołów routingu dynamicznego: RIP v1 i v2, RIPng. | TAK |  |
| 62 | Urządzenie powinno obsługiwać także protokół umożliwiający utworzenie wirtualnego routera i zapewniającego dostępność sieci zewnętrznej po awarii jednego z urządzeń fizycznych bez potrzeby specjalnej rekonfiguracji klientów w sieci. Protokół powinien wspierać adresację IPv6. | TAK |  |
| 64 | Quality of Service | TAK |  |
| 65 | Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, adresu IPv6, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. | TAK |  |
| 66 | Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu. | TAK |  |
| 67 | W przypadku wykrycia ruchu iSCSI, urządzenie powinno również być w stanie obsługiwać ten ruch ze skonfigurowanym dla niego priorytetem, WRR, DRR, WDRR. | TAK |  |
| 68 | Urządzenie powinno obsługiwać tzw. CIR. | TAK |  |
| 69 | Przełącznik powinien umożliwiać kontrolę kongestii ruchu WRED. | TAK |  |
| 70 | Przełącznik powinien posiadać obsługę powiadamiania o kongestii zgodnie z IEEE 802.1Qau, a także obsługiwać Flow Control zgodnie ze standardem 802.1Qbb i posiadać wsparcie dla alokowania przepustowości pomiędzy klasami ruchu zgodnie ze standardem 802.1Qaz. | TAK |  |
| 71 | Urządzenie powinno umożliwiać limitowanie pasma osobno dla każdej klasy ruchu (kolejki na porcie fizycznym) z granulacją co najwyżej 64 kb/s. | TAK |  |
| 72 | Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. | TAK |  |
| 73 | Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. | TAK |  |
| 74 | Powinna istnieć funkcjonalność limitowania pasma dla określonego typu ruchu (np. odbywającego się na danym porcie TCP lub UDP) z granulacją nie większą, niż 64 kb/s. | TAK |  |
| 76 | Filtrowanie ruchu | TAK |  |
| 77 | Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, adres IPv6, zawartość pola DSCP, typ protokołu, flagi protokołu TCP, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 dla ruchu wejściowego i wyjściowego z portów przełącznika, a także umożliwiać tworzenie statystyk dla ACL i mieć możliwość uruchamiania reguł ACL wg kalendarza. | TAK |  |
| 78 | Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN. | TAK |  |
| 79 | Musi istnieć też możliwość niezależnej filtracji ruchu kierowanego do procesora przełącznika w celu jego dodatkowej ochrony. | TAK |  |
| 81 | Funkcje bezpieczeństwa | TAK |  |
| 82 | Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 12K takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. | TAK |  |
| 83 | Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. | TAK |  |
| 84 | Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. | TAK |  |
| 85 | Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. | TAK |  |
| 86 | Przełącznik musi umożliwiać współpracę z serwerem RADIUS w celu realizacji tzw. Accountingu dla przyłączonych użytkowników. | TAK |  |
| 87 | Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. | TAK |  |
| 88 | Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. | TAK |  |
| 89 | Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. | TAK |  |
| 90 | Urządzenie musi współpracować z funkcjonalnością Microsoft NAP w celu wymuszenia separacji maszyn nie będących w zgodzie z obowiązującą polityką bezpieczeństwa w sieci oraz z funkcjonalnością DHCP NAP. | TAK |  |
| 91 | Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC, jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. | TAK |  |
| 92 | Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). | TAK |  |
| 93 | Urządzenie powinno posiadać możliwość filtrowanie protokołu sieci LAN NetBIOS. |  |  |
| 94 | Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. | TAK |  |
| 95 | Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci. | TAK |  |
| 96 | Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU. | TAK |  |
| 97 | Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. | TAK |  |
| 98 | Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 1 pps), Multicast (z krokiem minimalnym co najwyżej 1 pps), Broadcast (z krokiem minimalnym co najwyżej 1 pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie. | TAK |  |
| 99 | Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast. | TAK |  |
| 101 | Zarządzanie | TAK |  |
| 102 | Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. | TAK |  |
| 103 | Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. | TAK |  |
| 104 | Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. | TAK |  |
| 105 | Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. | TAK |  |
| 106 | Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet - również poprzez adres IPv6. | TAK |  |
| 107 | W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. | TAK |  |
| 108 | Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. | TAK |  |
| 109 | Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON oraz RMONv2 i obsługiwać protokół sFlow. | TAK |  |
| 110 | Urządzenie musi obsługiwać protokół 802.1ag umożliwiający zdalne wykrywanie przerw połączeń w sieci oraz protokół Y.1731. | TAK |  |
| 111 | Przełącznik musi obsługiwać protokół 802.3ah umożliwiający separację domeny Ethernet operatora od sieci Ethernet klienta. |  |  |
| 112 | Urządzenie musi posiadać funkcję wykrywania połączeń jednokierunkowych. | TAK |  |
| 113 | Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. | TAK |  |
| 114 | Urządzenie musi posiadać wbudowanego klienta DHCP i DHCPv6 oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. | TAK |  |
| 115 | Przełącznik powinien posiadać wbudowanego klienta SMTP. | TAK |  |
| 116 | Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. | TAK |  |
| 117 | Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6 oraz musi wspierać protokół synchronizacji czasu zgodny z IEEE1588. | TAK |  |
| 118 | Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. | TAK |  |
| 119 | Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci. | TAK |  |
| 120 | Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego oraz wspierać traceroute dla IPv6. | TAK |  |
| 121 | Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6. | TAK |  |
| 122 | Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia. | TAK |  |
| 123 | Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC. | TAK |  |
| 124 | Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane. | TAK |  |
| 125 | Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware oraz wielu wersji konfiguracji. | TAK |  |
| 126 | Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików. | TAK |  |
| 127 | Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet). | TAK |  |
| 128 | Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach oraz wykrywanie długości linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych. | TAK |  |
| 131 | Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania. | TAK |  |

1. **Przełącznik dostępowy 16 szt.**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | *Wymagane minimalne parametry techniczne* | *Wymóg do spełnienia (warunek graniczny)* | *OFEROWANE PARAMETRY TECHNICZNE – podaje Wykonawca**Wymogi dotyczące opisu oferowanych parametrów:**TAK – wykonawca spełnia konkretny parametr**NIE – wykonawca nie spełnia konkretnego parametru* |
| 1 | 48 x 1000Base-T IEEE 802.3ab | TAK |  |
| 2 | Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). | TAK |  |
| 3 | Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. | TAK |  |
| 4 | 4 x SFP+ IEEE 802.3ae/802.3ae;- porty SFP+ muszą obsługiwać również moduły SFP 1000Base-X IEEE 802.3z; | TAK |  |
| 5 | Konsola szeregowa RS-232. | TAK |  |
| 6 | Łączenie urządzeń w stosy o wielkości co najmniej 6 jednostek. Awaria żadnego pojedynczego urządzenia nie może spowodować przerwania pracy stosu. Praca w topologii pierścienia. Przepustowość magistrali stosu co najmniej 40 Gb/s. Port-Channel oraz Mirroring ruchu przy użyciu dowolnych portów w stosie. | TAK |  |
| 7 | Zasilanie AC 230V. | TAK |  |
| 8 | Pojemność przełączania nie mniej, niż 176 Gb/s. Wydajność przełączania nie mniej niż 130 Mp/s. | TAK |  |
| 9 | Architektura nieblokującą (wire-speed). |  |  |
| 10 | Pojemność tablicy MAC nie mniej, niż 16K. Możliwość wprowadzenia co najmniej 510 wpisów statycznych. | TAK |  |
| 11 | Ilość RAM nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB. | TAK |  |
| 12 | Obsługa ramek Jumbo o rozmiarze co najmniej 9210 B. | TAK |  |
| 13 | Bufor pakietów nie mniej, niż 3 MB. | TAK |  |
| 14 | Temperatura pracy w zakresie co najmniej od -5C do 50 stopni Celsjusza. | TAK |  |
| 15 | MTBF > 410000 godzin. | TAK |  |
| 16 | Obudowa urządzenia powinna być wyposażona w mocowanie umożliwiające przypięcie zabezpieczenia fizycznego typu Kensington Lock. | TAK |  |
| 17 | Funkcjonalności warstwy 2 | TAK |  |
| 18 | IGMP Snoopingv3- obsługa nie mniej, niż 510 grup multicast w tym co najmniej 256 grup statycznych. | TAK |  |
| 19 | MLD Snoopingv2- obsługa nie mniej, niż 31 grup multicast w tym co najmniej 31 grup statycznych. | TAK |  |
| 20 | IEEE 802.1D, 802.1w, 802.1s (co najmniej 16 instancji). Funkcja 802.1Q Restricted Role oraz 802.1Q Restricted TCN. | TAK |  |
| 21 | Wykrywanie pętli w L2 dla przyłączonych urządzeń bez protokołu rodziny STP. | TAK |  |
| 22 | Tworzenie interfejsów Port-Channel - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie z obsługą LACP. | TAK |  |
| 23 | LLDP (802.1AB) oraz LLDP-MED. | TAK |  |
| 24 | ERPS (ITU-T G.8032) w wersji co najmniej 1. Jednoczesna obsługa co najmniej 1 pierścieni. | TAK |  |
| 25 | DHCP Relay w tym opcji 60 i 61 oraz opcji 82, DHCP Local Relay + opcja 82. DHCP Relay dla IPv6. | TAK |  |
| 26 | Port monitoring/mirroring/span. Możliwość monitorowania tylko wybranego ruchu. |  |  |
| 27 | Obsługa sieci VLAN | TAK |  |
| 28 | 802.1Q VLAN, co najmniej 4094, 802.1v GVRP. | TAK |  |
| 29 | Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. | TAK |  |
| 30 | Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN. | TAK |  |
| 31 | Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN. | TAK |  |
| 32 | Funkcjonalności warstwy 3 | TAK |  |
| 33 | Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 16 takich interfejsów. | TAK |  |
| 34 | Przełącznik musi posiadać funkcjonalność Gratuitous ARP. | TAK |  |
| 35 | Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci. | TAK |  |
| 36 | Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 10 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP. |  |  |
| 37 | Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 0,5K wpisów oraz umożliwiać wprowadzenie co najmniej 256 wpisów statycznych. | TAK |  |
| 38 | Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 510 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 256 takich tras dla IPv6. | TAK |  |
| 39 | Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 60 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 32 takich tras dla IPv6. | TAK |  |
| 40 | Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 60 takich tras) oraz dla IPv6 (co najmniej 30 tras). | TAK |  |
| 41 | Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4. | TAK |  |
| 42 | Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery. | TAK |  |
| 43 | Quality of Service | TAK |  |
| 44 | Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. | TAK |  |
| 45 | Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR. | TAK |  |
| 46 | Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. | TAK |  |
| 47 | Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. | TAK |  |
| 48 | Filtrowanie ruchu | TAK |  |
| 49 | Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza. | TAK |  |
| 50 | Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN. | TAK |  |
| 51 | Funkcje bezpieczeństwa | TAK |  |
| 52 | Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 120 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. | TAK |  |
| 53 | Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. | TAK |  |
| 54 | Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. | TAK |  |
| 55 | Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. | TAK |  |
| 56 | Urządzenie musi wspierać funkcję umożliwiającą zmianę przypisanych z serwera RADIUS uprawnień bez rozłączania ponownego uwierzytelniania przyłączonego klienta. | TAK |  |
| 57 | Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. | TAK |  |
| 58 | Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. | TAK |  |
| 59 | Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. | TAK |  |
| 60 | Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 250 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. | TAK |  |
| 61 | Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). | TAK |  |
| 62 | Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. | TAK |  |
| 63 | Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany. | TAK |  |
| 64 | Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci. | TAK |  |
| 65 | Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU. | TAK |  |
| 66 | Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. | TAK |  |
| 67 | Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Multicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Broadcast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie. | TAK |  |
| 68 | Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast. | TAK |  |
| 69 | Zarządzanie |  |  |
| 70 | Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. | TAK |  |
| 71 | Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. | TAK |  |
| 72 | Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia. | TAK |  |
| 73 | Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. | TAK |  |
| 74 | W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. | TAK |  |
| 75 | Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. | TAK |  |
| 76 | Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. | TAK |  |
| 77 | Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow. | TAK |  |
| 78 | Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. | TAK |  |
| 79 | Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. | TAK |  |
| 80 | Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. | TAK |  |
| 81 | Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6. | TAK |  |
| 82 | Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. | TAK |  |
| 83 | Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci. | TAK |  |
| 84 | Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego. | TAK |  |
| 85 | Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6, a także umożliwiać przeglądanie tablicy adresów MAC. | TAK |  |
| 86 | Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia. | TAK |  |
| 87 | Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia. | TAK |  |
| 88 | Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC. | TAK |  |
| 89 | Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane. | TAK |  |
| 90 | Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware. | TAK |  |
| 91 | Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików. | TAK |  |
| 92 | Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet). | TAK |  |
| 93 | Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych. | TAK |  |
| 94 | Pozostałe | TAK |  |
| 95 | Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania. | TAK |  |
| 96 | Gwarancja przez cały czas produkcji urządzenia oraz przez co najmniej 5 lat po jej zakończeniu. | TAK |  |

1. **Wyposażenie dodatkowe :**
2. 70 szt wkładka SFP+ SR kompatybilna wraz z potrzebnymi patchcordami światłowodowymi
3. Oprogramowanie producenta sprzętu do monitoringu dostarczonych przełączników

1. **System Siem**

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

|  |  |  |  |
| --- | --- | --- | --- |
| Poziom | Opis | Zagrożenie | Przykład |
| Krytyczny | Niezbędne natychmiastowe działanie | * Przerwa w działaniu serwera/systemu
 | Wyciek danych |
| złagodzić obecne złośliwe oprogramowanie | * Brak odbioru danych z lokalizacja klienta
 |  |
| Działalność |  |  |
| 3 | Wysokie prawdopodobieństwo incydentu, jeśli | * Znaczące zmiany w SIEM
 | Brak potwierdzenia |
| nie podejmuje się działań zapobiegawczych | * wskazanie natężenia ruchu danych obniżona wydajność potencjał
 |  |
| 2 | Niski potencjalny incydent | * Użytkownik nie zaktualizował hasła w wymaganym odstępie czasu
 | Znaleziony wirus na stacji roboczej |
| 1 | Aktywności utrzymaniowe lub informacyjne | - | Raport |

w oparciu o klasyfikację i rodzaj zdarzenia/zgłoszenia wsparcie reaguje zgodnie z poniższymi interwałami.

|  |  |  |  |
| --- | --- | --- | --- |
| Poziom | Opis | Zagrożenie | SLA |
| Krytyczny | 1 godzina | 1 godzina | 96% |
| 3 | 24 godziny | 2 godziny | 96% |
| 2 | 72 godziny | 8 godzin | 96% |
| 1 | 5 dni | 24 godzin | 96% |

 |
| **Dodatkowe wymagania:**1. Producent Systemu SIEM musi posiadać certyfikacje w zakresie: ŚWIADCZENIA USŁUGI SECURITY OPERATION CENTER - REAGOWANIE NA ZAGROŻENIA CYBERBEZPIECZEŃSTWA, zgodnie z normą ISO ISO/IEC 27001:2017 – załączyć do oferty.
2. W celu zabezpieczenia danych krytycznych przetwarzanych w systemie HIS Zamawiającego (system Eskulap, którego producentem jest Nexus Polska Sp. z o.o.), Wykonawca zobowiązany jest dołączyć do oferty potwierdzenie, że posiada uprawnienia lub autoryzację Nexus Polska lub zrealizuje przedmiot zamówienia w obszarze dotyczącym ingerencji w dane przetwarzane przez system Eskulap, nie naruszając postanowień licencyjnych i gwarancyjnych dla systemu medycznego Eskulap i będzie gwarantował jego poprawne monitorowanie po zakończeniu prac integracyjnych – załączyć do oferty.
 |

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

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