Załącznik nr 1 do SWZ

Szczegółowy Opis Przedmiotu Zamówienia

Spis treści

Spis treści 2
1. Zakres realizacji Przedmiotu Zamówienia 3
   1.1 Dostawy w ramach Przedmiotu Zamówienia 3
   1.2 Usługi w ramach Przedmiotu Zamówienia 3
2. Organizacja wdrożenia 4
3. Specyfikacja techniczna 4
   3.1 Specyfikacja ilościowa 4
   3.2 Specyfikacja Oprogramowania 5
      3.2.1 Wymagania ogólne 5
      3.2.2 System NAC 5
      3.2.3 System SIEM 9
      3.2.4 System wyniesionej kopii zapasowej 11
4. Spis tabel 13

1. Zakres realizacji Przedmiotu Zamówienia

1.1 Dostawy w ramach Przedmiotu Zamówienia

W ramach Przedmiotu Zamówienia konieczna jest dostawa:

1) System typu Network Access Control (NAC)
2) System typu Security Information and Event Management (SIEM)
3) Kompletnego systemu kopii zapasowej wraz z niezbędnymi licencjami

1.2 Usługi w ramach Przedmiotu Zamówienia

W ramach Przedmiotu Zamówienia Wykonawca zrealizuję następujące usługi:

1) Dla wszystkich systemów Wykonawca przeprowadzi z udziałem Zamawiającego wstępną analizę i przedstawi projekt wdrożenia poszczególnych aplikacji, który będzie zawierał co najmniej:
   a) Ogólny opis wdrażanych aplikacji
   b) Zestawienie dostarczanych licencji
   c) Opis środowiska instalacji (dostarczany sprzęt, Ilość maszyn wirtualnych, systemy operacyjne itp.)
   d) Ogólny projekt i założenia wdrożeniowe dla każdego oprogramowania
2) Dla systemu NAC
   a) Dostawa oprogramowania dla Zamawiającego zgodnego z opisem z punktu 3.2.2
   b) Instalacja i wdrożenie sprzętu oraz oprogramowania opisanego w pkt 3.2.2
   c) Wykonawca przeprowadzi szkolenie dla administratora systemu dla grupy maksymalnie 2 osobowej z obsługi dostarczanego oprogramowania (dopuszczalna forma wideokonferencji)
3) Dla systemu SIEM
   a) Dostawa oprogramowania dla Zamawiającego zgodne z opisem z punktu 3.2.3
   b) Instalacja i wdrożenie oprogramowania opisanego w pkt 3.2.3
   c) W trakcie wdrożenia Wykonawca zainstaluje, skonfiguruje i przygotuje dostarczane oprogramowanie do połączenia ze źródłami danych o zdarzeniach znajdującymi się w infrastrukturze teleinformatycznej Zamawiającego oraz zapewni wsparcie w zakresie definiowania reguł monitorowania.
   d) Wykonawca przeprowadzi szkolenie dla personelu Zamawiającego dla grupy maksymalnie 6-osobowej z zakresu obsługi dostarczonego oprogramowania oraz zapewni dostęp do dokumentacji technicznej rozwiązania.
   e) Wykonawca zapewni asystę techniczną po uruchomieniu oprogramowania.
4) Systemu wyniesionej kopii zapasowej
   a) Dostawa oprogramowania dla Zamawiającego zgodnego z opisem z punktu 3.2.4
   b) Instalacja i wdrożenie oprogramowania opisanego w pkt 3.2.4
   c) Udostępnienie serwera kopii zapasowej po stronie Wykonawcy oraz wsparcie w konfiguracji łącza po stronie Zamawiającego (konfiguracje sprzętu sieciowego Zamawiającego przeprowadza Zamawiający)
   d) Opracowanie i skonfigurowanie scenariuszy kopii zapasowych
   e) Wykonawca przeprowadzi szkolenie dla administratora systemu dla grupy maksymalnie 2 osobowej z obsługi dostarczanego oprogramowania (dopuszczalna forma wideokonferencji)
5) Przeprowadzi testy działania systemów
6) Opracuje dokumentacje powykonawczą

2. Organizacja wdrożenia

1) Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i chorych, tzn. organizacja prac powinna przede wszystkim zapewniać bezpieczeństwo przebywających w oddziałach pracowników i chorych

3. Specyfikacja techniczna

W niniejszym dziale przedstawiono minimalne wymagania dotyczące Oprogramowania. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.
Wymagania ogólne:

1. Całość dostarczanego oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producenta.
2. Dostarczane oprogramowanie musi zostać dostarczonej w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).

3.1 Specyfikacja ilościowa

Tabela 1 Specyfikacja ilościowa

LP.	NAZWA	LICZBA
1.	System typu Network Access Control (NAC)	1 komplet
2.	System typu Security Information and Event Management (SIEM)	1 komplet
3.	Systemu wyniesionej kopi zapasowej wraz z niezbędnymi licencjami	1 komplet

3.2 Specyfikacja Oprogramowania

3.2.1 Wymagania ogólne

1) Wykonawca jest odpowiedzialny za zaprojektowanie, dostawy licencji i wdrożenie Oprogramowania ściśle dostosowanego jakościowo i ilościowo do wymagań
2) Oprogramowanie dostarczane przez Wykonawcę będzie zaprojektowane, dostarczone, skonfigurowane i wdrożone „pod klucz" przez Wykonawcę

3.2.2 System NAC

System do kontroli dostępu musi charakteryzować się co najmniej następującymi cechami:

Tabela 2 Wymagania dotyczące systemu NAC

LP.	WYMAGANIA OGÓLNE
1.	Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)
2.	System musi odsługiwać minimum 500 urządzeń klienckich (w tym gości) Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia
3.	Praca na dedykowanym fizycznym appliance
4.	Musi posiadać wbudowany serwer Radius oraz TACACS +
5.	Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym: • Cisco Systems • Fortinet • Microsoft • Alcatel-lucent Enterprise • Huawei Networks • Extreme Networks • PaloAlto Networks • Producenta posiadanych przez Zamawiającego urządzeń firm: Hewlett Packard Enterprise i Aruba Networks
6.	System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera. W szczególności musi współpracować w tym zakresie z posiadanymi przez Zamawiającego kontrolerami Aruba 7205
7.	System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego. W szczególności musi współpracować w tym zakresie z posiadanymi przez Zamawiającego kontrolerami Aruba 7205
8.	Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
9.	Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych: • Microsoft Active Directory • Radius • Kerberos • LDAP • ODBC • Współpraca z serwerami tokenów

10.	Musi obsługiwać metody profilowania • DHCP • TCP • MAC OUI • SNMP • Cisco device sensor
11.	Musi Wspierać protokoły • Radius, Radius CoA, TACACS +, web authentication, SAML v2.0 • EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS) • PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD) • TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP) • EAP-TLS • PAP, CHAP, MSCHAPv1 i v2, EAP-MD5 • NAC, Microsoft NAP • Windows machine authentication • MAC Auth • Audit (role oparte na porcie oraz skanowanie podatności) • OCSP (Online Certificate Status Protocol) • SNMP generic MIB, SNMP private MIB • CEF (Common Event Format), LEEF (Log Event Extended Format) • TLS 1.2
12.	Musi posiadać funkcje integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami
13.	Musi posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (500). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.

14.	System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności
	• Samodzielna rejestracja klientów gościnnych w oparciu o:
	  ○ Adres e-mail
	  ○ Numer telefonu (wiadomość SMS)
	  ○ Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)
	• Logowanie w oparciu o portale społecznościowe
	• Funkcja integracji z systemami trzecimi poprzez API
	• Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową
	• Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych.
	• Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
	• Funkcja personalizacji strony gościnnej

15.	Musi posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Licencja pozwalająca na obsługę co najmniej 200 urządzeń typu BYOD.
16.	Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działu IT
17.	System musi wspierać obsługę następujących systemów operacyjnych

	• MS Windows • Mac OS X • iOS • Android • Chromebook • Ubuntu
18.	Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci
19.	Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej
20.	Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
21.	Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID
22.	Funkcja tworzenia unikalnych certyfikatów dla urządzeń.
23.	Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń
24.	Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Licencja pozwalająca na obsługę co najmniej 200 końcówek klienckich.

25.	System kontroli końcówek klienckich musi mieć następujące funkcjonalności
	• System musi wspierać następujące systemy operacyjne
	  ○ Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)
	  ○ Apple Mac OS X 10.7 i nowsze
	  ○ Red HAT Enterprise Linux 4 i nowsze
	  ○ CentOS 4 (Community Enterprise Operating System) i nowsze
	  ○ Fedora Core 5 i nowsze
	  ○ SUSE linux 10.x i nowsze
	• Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall
	• Wyświetlanie informacji on-line o statusie monitorowanych końcówek
	• System powinien obsługiwać agenta w formie
	  ○ Stałej (Presistent Agent)
	  ○ Tymczasowej (Dissolvabe Agent)
	  ○ Agenta NAP

26.	3 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
27.	Zaoferowany system kontroli dostępu musi tworzyć spójny ekosystem z posiadanymi przez Zamawiającego przełącznikami, kontrolerami i punktami dostępowymi marki Aruba Networks. W szczególności muszą posiadać wspólny, autoryzowany przez ich producentów punkt serwisowy realizujący kompleksową pomoc techniczną dla całego rozwiązania
28.	Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań

29.	Oferta musi zawierać kompletne zestawianie numerów katalogowych produktów i wszystkich jego dodatkowych składników umożliwiających ich jednoznaczną identyfikację u producenta sprzętu

3.2.3 System SIEM

Tabela 3 Specyfikacja systemu SIEM

LP.	WYMAGANIA OGÓLNE
1.	Oprogramowanie musi zainstalowane na serwerach Zamawiającego.
2.	Oprogramowanie jest zgodne z adekwatnymi przepisami prawa oraz w okresie wsparcia dostawcy gwarantuje stałą, pełną zgodność wszelkich realizowanych funkcji/algorytmów rozliczeń/formatów sprawozdań z obowiązującym prawem, dostosowywanie oprogramowania do zmian przepisów obowiązującego odbywa się z odpowiednim wyprzedzeniem.
3.	Oprogramowanie jest dostarczone przez oferenta i nie narusza praw licencyjnych innych osób i podmiotów
4.	Oprogramowanie posiada graficzny interfejs użytkownika.
5.	Oprogramowanie posiada wbudowany mechanizm autoryzacji i mechanizmy zabezpieczające przed nieautoryzowanym dostępem.
6.	Oprogramowanie posiada funkcjonalność zarządzania i administrowania uprawnieniami, w szczególności: mechanizm nadawania uprawnień funkcjonalnych do poszczególnych obszarów każdemu użytkownikowi.
7.	Oprogramowanie umożliwia monitorowanie stanów i zmian parametrów podstawowych systemów wykorzystywanych w zbudowanej infrastrukturze teleinformatycznej Zamawiającego.
8.	Oprogramowanie umożliwia stworzenie reguł bezpieczeństwa dla dedykowanych i najbardziej prawdopodobnych scenariuszy i wektorów ataków.
9.	Oprogramowanie umożliwia monitorowanie i analizę zdarzeń w systemach i sieci teleinformatycznej Zamawiającego.
10.	Oprogramowanie umożliwia korelację danych między różnymi systemami i realizacja założonych scenariuszy.
11.	Oprogramowanie umożliwia generowanie alarmów na podstawie określonych reguł.
12.	Oprogramowanie wysyła powiadomienie ostrzegawcze na adres e-mail użytkownika na podstawie określonych reguł.
13.	Oprogramowanie posiada możliwość wyświetlania szczegółowych informacji o danych zdarzeniach.
14.	Oprogramowanie zapewnia możliwość konfigurowania dashboardów.
15.	Oprogramowanie posiada moduł zapewniający dostęp do aktualnych informacji o podatnościach systemów teleinformatycznych Zamawiającego
16.	Oprogramowanie pozwala na przeszukiwanie bazy podatności systemów informatycznych.
17.	Oprogramowanie możliwość wyświetlania szczegółowych informacji, o podatnościach systemów IT
18.	Oprogramowanie pozwala na generowanie raportów dotyczących podatności na bazie zdefiniowanych zapytań w formacie co najmniej XLS i PDF
19.	Oprogramowanie posiada możliwość automatycznego generowania raportów wysyłanych na adres email w regularnych odstępach czasu na bazie zdefiniowanych przez danego użytkownika zapytań.
20.	Oprogramowanie posiada możliwość prowadzenia rejestru aktywów teleinformatycznych Zamawiającego.

21.	Oprogramowanie zapewnia możliwość przechowywania logów przez czas zdefiniowany przez Zamawiającego.
22.	Wykonawca zapewni wsparcie techniczne dla dostarczonego rozwiązania przez okres 36-miesiecy od daty podpisania protokołu odbioru obejmujące: • Dostęp do poprawek i nowych wersji oprogramowania • Dostęp do dokumentacji technicznej

3.2.4 System wyniesionej kopii zapasowej

1. Zamawiający oczekuje dostarczenie jednego, kompletnego systemu backupu spełanijącego wszystkie poniższe wymagania. Nie dopuszcza się dostarczenia wielu odrębnych, zintegrowanych rozwiązań.
2. Zamawiający wymaga, aby dostarczony system był w pełni kompatybilny z posiadanym przez Zamawiającego system kopii zapasowej tj. Veeam Backup & Replication Enterprise Plus.
3. Zamawiający wymaga dostarczenia systemu umożliwiającego wykonywanie wyniesionych kopii zapasowych serwerów z co najmniej 8 procesorami lub umożliwiające wykonywanie kopii zapasowych co najmniej (wskazując możliwość zamienną):20 maszyn wirtualnych lub 20 fizycznych serwerów
4. Dostarczany system musi zapewniać możliwość automatycznego wykonywania wyniesionej kopii zapasowej danych, co oznacza przesyłanie i składowanie kopii poza siedzibą Zamawiającego w okresie nie krótszym niż 3 lata od daty podpisania Umowy.
5. W celu realizacji automatycznego wykonywania wyniesionej kopii zapasowej danych, Zamawiający wymaga udostępnienia:
   a) Infrastruktury udostepniającej przestrzeń dyskową na składowanie kopii zapasowych w Centrum Przetwarzania danych spełniającym, co najmniej następującego wymagania:
      1. Centrum Przetwarzania Danych musi posiadać aktywne elementy infrastruktury IT zapewniające pracę w modelu n+1;
      2. Centrum Przetwarzania Danych musi posiadać redundantne wewnętrzne linie dystrybucji energii elektrycznej obsługujące macierze dyskowe;
      3. Centrum Przetwarzania Danych musi posiadać redundantne wewnętrzne linie chłodu równolegle obsługujące macierze dyskowe;
      4. Centrum Przetwarzania Danych musi posiadać możliwość, odłączania każdego elementu linii dystrybucji energii elektrycznej i chłodu w celu poddania czynnością serwisowy, tak aby nie zakłócić normalnej pracy urządzeń dwuzasilaczowych;
      5. Centrum Przetwarzania Danych musi posiadać wdrożoną strefową kontrolę dostępu w oparciu o karty zbliżeniowe lub rozwiązanie równoważne;
      6. Centrum Przetwarzania Danych musi posiadać całodobową ochronę fizyczną z rejestracją kamer monitoringu wizyjnego na zewnątrz i wewnątrz budynku;
      7. Centrum Przetwarzania Danych musi być zlokalizowane na terenie Polski;
      8. Centrum Przetwarzania Danych musi posiadać niezależne strefy pożarowe oraz system wczesnej detekcji dymu i ognia, a pomieszczenie ze sprzętem IT muszą być wyposażone w zautomatyzowaną aparaturę gaśniczą;
      9. Centrum Przetwarzania Danych musi mieć zapewnione zasilanie z dwóch niezależnych linii energetycznych oraz rezerwowe zasilanie realizowane przy pomocy UPS oraz agregatu prądotwórczego;
      10. Centrum Przetwarzania Danych musi posiadać UPS'y pracujące w nadmiarowej konfiguracji (co najmniej N+1), zapewniając nieprzerwane zasilanie macierzy dyskowej;
      11. Centrum Przetwarzania Danych musi pozwalać, aby dystrybucja energii elektrycznej do macierzy dyskowej odbywała się z wykorzystaniem minimum dwóch niezależnych torów zasilania, z minimum jednym torem gwarantowanym (podtrzymanie zasilania z wykorzystaniem UPS i agregatu prądotwórczego);
      12. Centrum Przetwarzania Danych musi posiadać Certyfikat Ochrony Elektromagnetycznej wydany przez Agencję Bezpieczeństwa Wewnętrznego.

   b) Przestrzeni dyskowej na składowanie kopii zapasowej o wielkości 10 TB z możliwością zwiększenia do, co najmniej 100 TB (zwiększenie pojemności powyżej 10 TB nie jest elementem oferty i nie podlega wycenie), w oparciu o wysokodostępną macierz dyskową spełniającą poniższe wymagania:
      1. Macierz musi posiadać wbudowaną funkcjonalność sprzętowej deduplikacji;
      2. Macierz musi pozwalać na tworzenia kopii zapasowych z wykorzystaniem transmisji wielostrumieniowej

3. Macierz musi posiadać redundancję wszystkich komponentów – brak pojedynczego punktu awarii. W przypadku awarii kontrolera, automatyczne przełączanie wystawianych zasobów na inny kontroler, którego wydajność jest nie mniejsza niż tego, który uległ awarii.
4. Macierz musi posiadać możliwość rozbudowy w trakcie jej pracy (online);
5. Rozłożenie dysków w macierzy musi zapewniać redundancję pozwalającą na nieprzerwaną pracę i dostęp do wszystkich danych w sytuacji awarii pojedynczego komponentu sprzętowego typu: dysk, półka dyskowa, kontroler, zasilacz;
6. Macierz musi posiadać możliwość aktualizacji firmware trybie online, bez zauważalnego zanikania ścieżek dostępu do zasobów dyskowych macierzy

c) Łącza internetowe symetryczne o przepustowości nie mniejszej niż 1 Gb/s do infrastruktury, na której składowane będą wyniesione kopie zapasowe. Wykonawca nie zapewnia łącza po stronie Zamawiającego.

2. Komunikacja pomiędzy Zamawiającym, a miejscem składowania danych wyniesionych musi odbywać się z wykorzystaniem bezpiecznego połączenia (co najmniej SSL lub IPSec)
3. Zamawiający wymaga, aby system przechowywania wyniesionych kopii zapasowych po stronie Wykonawcy nie umożliwiał przesłania niezaszyfrowanej kopii zapasowej do wyniesionego miejsca składania danych.
4. Zamawiający może zażądać wskazania dokładnej lokalizacji fizycznej urządzeń przetwarzania i składowania danych (z dokładnością do adresu i szafy w Centrum Danych).
5. Awaryjne odtwarzanie danych z wyniesionego miejsca składowania danych musi odbywać się automatycznie za pomocą lokalnego interfejsu systemu kopii zapasowych Zamawiającego, bez udziału pracowników Wykonawcy.
6. Wykonawca zapewni panel usługi systemu kopii wyniesionych, który posiada co najmniej poniższe funkcjonalności:
   a) Zdalne monitorowanie i zarządzanie kopiami zapasowymi za pomocą jednego internetowego interfejsu użytkownika.
      1. Zabezpieczenie dostępu do Panelu Zarządzania z wykorzystaniem protokołu SSL oraz dwuskładnikowego uwierzytelniania MFA (użytkownik, hasło i token).
      2. Prezentacja stanu realizowanych oraz historycznych zadań backupu oraz możliwość eksportowania tych danych do pliku tekstowego.
      3. Możliwość uruchamiania, zatrzymywania, powtarzania, włączania i wyłączania zadań backupu oraz pobierania rejestru zdarzeń.
      4. Obsługa alarmów dotyczących zadań backupowych oraz stanu systemu oraz eksportowania ich do pliku tekstowego.
   b) Raportowanie i rozliczenia zapewniające pełny wgląd w czasie rzeczywistym w zasoby zaangażowane do przechowywania kopii zapasowych.
      1. Możliwość konfigurowania indywidualnych raportów przez Zamawiającego oraz ich edytowania i usuwania.
      2. Sprawdzanie poziomu wykorzystania przydzielonej bezpiecznej przestrzeni dyskowej.
      3. Wyświetlanie statystyki dotyczącej liczby serwerów, stacji roboczych i wirtualnych maszyn obsługiwanych przez system.

4. Spis tabel

Tabela 1 Specyfikacja ilościowa 4
Tabela 2 Wymagania dotyczące systemu NAC 5
Tabela 3 Specyfikacja systemu SIEM 9