Załącznik nr 2

Szczegółowy opis Przedmiotu Zamówienia, opis parametrów technicznych i dodatkowych wymagań Zamawiającego

SPIS TREŚCI

1. PRZEDMIOT ZAMÓWIENIA

Wspierana i aktualizowana w ramach Przedmiotu Zamówienia infrastruktura teleinformatyczna nazywana będzie dalej w dokumencie Systemem, a poszczególne części Przedmiotu Zamówienia nazywane Obszarami (w ich skład wchodzą poszczególne Podsystemy) oznaczane będą kodami/mnemonikami:

Kod / mnemonik	Obszar
I_NET	sieć szkieletowa
I_WIFI	sieci bezprzewodowa
I_SEC	bezpieczeństwo sieci i zasobów teleinformatycznych
I_UC	system łączności
I_CPD	Centrum Przetwarzania Danych
I_MGMT	zarządzanie zasobami IT

1.1. Przedmiotem Zamówienia jest:

1. Przedłużenie gwarancji i wsparcia producenta wskazanych Podsystemów do końca roku 2020.
2. Wdrożenie rozwiązań zastępczych dla wskazanych, opisanych w dalszej części przedmiotu zamówienia, Podsystemów wraz z gwarancją i wsparciem producenta do końca roku 2020.
3. Przygotowanie dokumentacji powykonawczej uwzględniającej konfigurację, procedury (między innymi: dostępu, konfiguracji, tworzenia kopii zapasowych i odzyskiwania z nich danych) hasła itp. nowych podsystemów.
4. Gwarancja i wsparcie wykonawcy na System do końca roku 2020.
5. Szkolenie personelu IT

1.2. Ogólne wymagania dla Przedmiotu Zamówienia:

1. 1. Dla opisanego w ramach Przedmiotu Zamówienia Systemu wymagane jest zapewnienie przez Wykonawcę gwarancji i opieki technicznej (serwisu i wsparcia technicznego) do 31.12.2020 r. (zamawiający planuje, że umowa będąca efektem niniejszego postępowania zawarta będzie od dnia 01.10.2017 r.) Usługi gwarancyjne, opieka techniczna oraz szkolenia muszą być świadczone w języku polskim.
2. W przypadku nowych Podsystemów Wykonawca musi uwzględnić w kosztach realizacji:
   2.1. Dostawę, montaż, instalację, podłączenie, uruchomienie dostarczanych urządzeń wraz z niezbędnym osprzętem, a w szczególności: akcesoriami, osprzętem montażowo-instalacyjnym (stelaże, kable przyłączeniowe i zasilające, przewody, patchcordy, przejściówki, opaski, itp),
   2.2. W przypadku rozwiązań wirtualnych, opisanych w dalszej części przedmiotu zamówienia, koszty urządzeń oraz licencji związanych z wirtualizacją wdrażanych Podsystemów.
   2.3. Wszystkie dodatkowe licencje dotyczące uruchomienia i działania Podsystemu – w tym te na współpracujących urządzeniach/Podsystemach,
   2.4. Zaimplementowanie ustawień i polityk z dotychczasowych podsystemów, które zastąpią nowe podsystemy.
   2.5. Konfigurację i integrację z innymi powiązanymi Podsystemami Zamawiającego,

2.6. Zapewnienie szkoleń personelu IT Zamawiającego (szczegółowe wymagania w tym zakresie opisane są w dalszej części niniejszego dokumentu)

3. Wszystkie dostarczone urządzenia i systemy muszą być: nowe, posiadać gwarancję producenta, zamontowane, zainstalowane, skonfigurowane i uruchomione zgodnie z wymaganiami niniejszej specyfikacji, ofertą i dokumentacją projektowo-wykonawczą. Wszystkie dostarczone produkty muszą być wyposażone we wszystkie niezbędne komponenty, podzespoły i licencje.

2. WARUNKI WDROŻENIA I FAZY RELIZACYJNEJ

Warunki wdrożenia i fazy realizacyjnej:

1. Zamawiający przewiduje etapową realizację prac z odbiorami po uruchomieniu każdego Podsystemu.
2. Wdrożenie nowego Podsystemu powiązane być musi z integracją z Podsystemami, z którymi współpracował dotychczasowy Podsystem i z przeniesieniem dotychczasowych konfiguracji, ustawień, polityk itp.
3. Wykonawca zobowiązany jest do przedstawienia niezwłocznie po podpisaniu umowy planowanego harmonogramu prac i planu migracji do nowych podsystemów, aby:
   3.1. Przewidywać możliwość równoległej realizacji zadań w kilku lokalizacjach i/lub obszarach
   3.2. Zapewnić w maksymalnym stopniu ciągłość działalności statutowej Zamawiającego
   3.3. Minimalizować uciążliwość prac poprzez wcześniejsze uzgadnianie z Zamawiającym terminów (dni, godzin) ich realizacji (w ramach przyjętego harmonogramu)

   Harmonogram musi zostać zatwierdzony przez Zamawiającego.
4. Wykonawca zobowiązany jest do oznaczenia zainstalowanych urządzeń i połączeń za pomocą etykiet z kodami przyjętymi przez Zamawiającego.
5. Miejsca (pomieszczenia) wykonywania prac muszą zostać uporządkowane i przywrócone do stanu nie gorszego niż przed ich rozpoczęciem
6. Odbiory po zakończeniu każdego z etapów i odbiór końcowy przeprowadzone będą po wykonaniu testów akceptacyjnych i zakończeniu ich pozytywnym wynikiem, potwierdzane każdorazowo, obustronnie podpisanym bezusterkowym protokołem odbioru.

3. DOKUMENTACJA POWYKONAWCZA

Wymagania dotyczące dokumentacji powykonawczej:

1. Dokumentacja powykonawcza dotycząca nowych systemów powinna zawierać dokładny opis Podsystemu oraz niezbędne schematy i instrukcje - ostateczne wersje (wraz z komentarzami) plików konfiguracyjnych urządzeń i oprogramowania.
2. Kody na opisach i schematach w dokumentacji powykonawczej muszą być zgodne z faktycznymi oznaczeniami na etykietach urządzeń i połączeń.
3. W trakcie odbioru końcowego Wykonawca przekaże Zamawiającemu 1 egzemplarz dokumentacji powykonawczej w wersji papierowej i 1 egzemplarz w wersji elektronicznej.

4. OGÓLNE WYMAGANIA DLA STOSOWANYCH PRODUKTÓW

Ogólne wymagania Zamawiającego dla stosowanych produktów o ile wymagania szczegółowe dla produktów opisanych w dalszej części dokumentu nie stanowią inaczej:

1. Wymagane jest, aby dostarczany sprzęt był fabrycznie nowy, kompletny i pochodził z legalnego kanału sprzedaży.
2. Wymagane jest aby dostarczany sprzęt był wyprodukowany nie wcześniej niż 6 miesięcy przed dniem zawarcia Umowy dotyczącej Przedmiotu Zamówienia.
3. Urządzenia muszą posiadać tylko oryginalne komponenty i nie dopuszcza się stosowania zamienników. Wyjątkiem jest sytuacja, w której stosowanie zamienników jest dopuszczone przez producenta i nie wpływa na obsługę serwisową urządzeń – *w takim przypadku przed podpisaniem umowy wykonawca zobowiązany jest dostarczyć oświadczenie podpisane przez producenta, który wskazuje jakie elementy zamienne są dopuszczalne do użycia bez wpływu na obsługę serwisową w autoryzowanym kanale serwisowym. Oświadczenie musi być sporządzone w oryginale bądź w postaci kopii potwierdzonej za zgodność z oryginałem przez Wykonawcę.*
4. Wymagane jest zastosowanie redundantnego (co najmniej w układzie 1:1) zasilania i wentylacji/chłodzenia we wszystkich urządzeniach posiadających taką opcję
5. W przypadku licencji ograniczonych w czasie wymagane jest zapewnienie ich co najmniej na czas taki, jak oferowany okres serwisu zgodnie z wybranymi przez Wykonawcę warunkami opisanymi w podrozdziale „Warunki serwisu, gwarancji, wsparcia technicznego” rozdziału „Kryteria oceny ofert”.

5. SZKOLENIA

Dla każdego z wdrożonych Podsystemów Wykonawca zapewni dwa rodzaje szkoleń:

1. Autoryzowane – realizowane przez autoryzowane centrum szkoleniowe danego producenta
2. Autorskie – w formie instruktaży/warsztatów przeprowadzanych w trakcie wdrożenia przez Wykonawcę (mogą być zrealizowane w oparciu o sprzęt i oprogramowanie dostarczone w ramach zamówienia)

przy czym:

1. Szkolenia muszą być przeprowadzone, w języku polskim
2. Dla osób biorących udział w szkoleniu zostaną zapewnione materiały szkoleniowe w formie drukowanej i elektronicznej, w języku polskim
3. W przypadku szkoleń odbywających się w siedzibie Zamawiającego oraz poza siedzibą Zamawiającego wszelkie koszty związane ze szkoleniem pokrywa Wykonawca
4. Zakresy (tematyka) szkoleń autoryzowanych i liczba biorących w nich udział osób opisane są w rozdziałach dotyczących poszczególnych obszarów
5. Liczba osób objętych szkoleniami autorskimi nie powinna być mniejsza od 6, a wymagane czasy ich trwania opisane są w rozdziałach dotyczących poszczególnych obszarów
6. Szczegółowy harmonogram szkoleń zostanie ustalony z wykonawcą wybranym do realizacji zamówienia niezwłocznie po podpisaniu umowy, przy czym szkolenie autorskie powinno być zrealizowane nie później niż 1 miesiąc po uruchomieniu danego

Podsystemu, szkolenie autoryzowane zaś przynajmniej 3 miesiące po uruchomieniu Podsystemu, ale nie później niż po 6 miesiącach.

6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE

1. Gwarancje i serwisy producenta muszą być dostarczone w postaci subskrypcji rejestrowanych bezpośrednio na Zamawiającego i umożliwiać:
   a. Możliwość zakładania zgłoszeń serwisowych bezpośrednio u producenta,
   b. Bezpośredni dostęp do bazy wiedzy i pomocy technicznej TAC producenta Możliwość bezpośredniego pobierania aktualizacji oprogramowania z bazy producenta
   c. Możliwość monitorowania statusu zgłoszeń w systemie producenta
   d. Możliwość korzystania z serwisu producenta nawet w przypadku gdy Wykonawca utraci autoryzację producenta lub nie będzie zdolny do świadczenia serwisu
2. W przypadku dostarczania innej formy serwisu należy przed podpisaniem umowy dostarczyć oświadczenie producenta potwierdzające, iż przejmuje on wszelkie obowiązki dotyczące świadczenia serwisu w przypadku niewywiązywania się Wykonawcy z zakresu umowy dotyczącego danego producenta.
3. Dla produktów które mają być objęte przedłużeniem gwarancji na powyższych warunkach Wykonawca w terminie do 30 dni od daty podpisania umowy dostarczy dokument potwierdzający wykupienie u producenta gwarancji oraz wsparcia technicznego minimum do 31.12.2020r. W przypadku stwierdzenia po upływie 30 dni braku tego dokumentu, Zamawiający naliczy karę umowną oraz będzie przysługiwało mu prawo odstąpienia od umowy.
4. Dobór odpowiedniego pakietu serwisowego producenta leży w gestii Wykonawcy. Zamawiający dopuszcza aby serwisy producentów posiadały mniej restrykcyjny czas usuwania awarii, pod warunkiem iż Wykonawca zapewni usuwanie awarii na warunkach określonych w SIWZ. Zamawiający wymaga aby okres serwisu pokrywał się z czasem trwania umowy.
5. Usługi serwisu, gwarancji i wsparcia technicznego muszą być świadczone w języku polskim.

6.1. Definicje

Incydent – sytuacja, w której Zamawiający powinien skontaktować się z Wykonawcą w celu uzyskania pomocy w rozwiązaniu zaistniałego problemu.

Zgłoszenie serwisowe – powiadomienie Wykonawcy o wystąpieniu incydentu.

Gotowość serwisowa – czas (dni, godziny), w którym Wykonawca przyjmuje i rejestruje zgłoszenia serwisowe.

Czas reakcji – czas pomiędzy dokonaniem zgłoszenia serwisowego przez Zamawiającego, a momentem rozpoczęcia przez Wykonawcę prac nad usuwaniem problemu będącego przyczyną incydentu.

Czas naprawy – czas od chwili dokonania zgłoszenia serwisowego przez Zamawiającego do chwili usunięcia problemu będącego przyczyną incydentu.

Okres serwisu – czas świadczenia usług serwisu, gwarancji i wsparcia technicznego Wykonawcy i Producenta liczony od dnia obioru końcowego.

Rozwiązanie tymczasowe – dokonana przez Wykonawcę zmiana konfiguracji urządzenia i/lub oprogramowania, i/lub stworzenie procedury, i/lub wykonanie określonych czynności mających doprowadzić do przywrócenia działania Systemu i/lub uszkodzonej jego części i/lub funkcji, w zakresie umożliwiającym jego działanie i eksploatację do czasu usunięcia problemu będącego przyczyną incydentu.

Błąd systemowy – incydent, który może usunąć wyłącznie producent sprzętu i/lub oprogramowania.

6.2. Klasyfikacja incydentów

W opisie warunków świadczenia usług gwarancyjnych i serwisowych stosowana będzie następująca klasyfikacja incydentów (awarii, usterek, błędów):

Klasy incydentów	Opis	Możliwe rodzaje incydentu
A – Krytyczny	Sieć telekomunikacyjna Zamawiającego lub główne aplikacje usługowe nie funkcjonują, co ma krytyczny wpływ na działalność statutową Zamawiającego, o ile usługi nie zostaną szybko przywrócone.	System nie działa. Awaria całej sieci, przerwa w działaniu krytycznych elementów sieci lub krytycznych aplikacji. Awaria wszystkich elementów tworzących układ redundantny. Incydent skutkujący odpowiedzialnością prawną, spowodowaną niewydolnością wynikłą z niedostępności sieci lub aplikacji. Brak możliwości zastosowania rozwiązania tymczasowego.
B – Wysoki	Sieć lub aplikacje nie ulegają całkowitej awarii, ale skuteczność (dostępność, wydajność, bezpieczeństwo) działania sieci telekomunikacyjnej lub głównych aplikacji usługowych jest znacznie obniżona, co ma istotny wpływ na działalność statutową Zamawiającego.	Incydent, który w znaczący sposób wpływa niekorzystnie na dostępność sieci lub aplikacji. Awaria jednego z dwu lub dwu z kilku elementów tworzących układ redundantny. Działający destrukcyjnie, powtarzający się incydent, który wywiera poważne, lecz tymczasowe skutki. Znaczące braki w wydajności. Brak możliwości natychmiastowego zastosowania rozwiązania tymczasowego.
C – Średni	Skuteczność (dostępność, wydajność, bezpieczeństwo) działania sieci lub aplikacji jest wyraźnie obniżona, ale większość działań przebiega nieprzerwanie lub ujawnił się błąd utrudniający działanie Systemu w zakresie pełnej funkcjonalności.	Zidentyfikowane incydenty, które ustępują bez interwencji albo mogą być skutecznie ominięte w wyniku działania Zamawiającego lub dzięki zastosowaniu rozwiązania tymczasowego. Uszkodzenie jednego z kilku elementów tworzących układ redundantny.
D – Niski	Skuteczność (dostępność, wydajność, bezpieczeństwo) działania sieci lub aplikacji jest nieznacznie obniżona lub użytkownicy potrzebują informacji lub pomocy, związanych z możliwościami produktu, instalacją systemu lub konfiguracją.	Incydenty nienaglące, o małym znaczeniu, zapytanie techniczne lub prośba o informacje.

6.3. Zgłaszanie incydentów

Wykonawca zapewni następujące warunki zgłaszania incydentów poprzez prowadzenie ich rejestru:

1. Zgłoszenia serwisowe muszą być przyjmowane przez co najmniej następujące kanały: telefon, e-mail, WWW

2. Każdemu zgłoszeniu musi zostać nadany unikalny numer (identyfikator), pozwalający na jego jednoznaczną identyfikację
3. Zgłoszenie musi zawierać datę, opis incydentu wraz z jego klasyfikacją, dane osoby zgłaszającej, dane osoby prowadzącej obsługę gwarancyjną lub serwisową
4. Wykonawca zapewni Zamawiającemu dostęp do systemu śledzenia stanu obsługi zgłoszenia. Dostęp ten musi być możliwy poprzez następujące kanały komunikacyjne: telefon, e-mail, WWW
5. Lista osób upoważnionych ze strony Zamawiającego do dokonywania zgłoszeń będzie określona w załączniku do protokołu odbioru końcowego.

6.4. Rodzaje usług

W ramach świadczeń gwarancyjnych i serwisowych przewiduje się następujące rodzaje usług:

Nazwa	Opis
DIAGNOSTYKA	Zdalne diagnozowanie Systemu w przypadku zgłoszenia jego nieprawidłowej pracy. W ramach usługi wykonywane będą diagnozy incydentów, które nie trwają ciągle, nie dają się odtworzyć lub wystąpiły w przeszłości i należy zbadać powód ich wystąpienia. Wykonawca musi zapewnić dostęp do bezpłatnych narzędzi diagnostycznych producenta.
WSPARCIE	Wsparcie techniczne w zakresie rozwiązywania problemów związanych z funkcjonowaniem Systemu, gotowość do podjęcia działań związanych z usuwaniem awarii, błędów i/lub wymianą uszkodzonych elementów Systemu. W ramach usługi rozwiązywany będzie problem, który trwa ciągle lub daje się odtworzyć. Usługa w swoim zakresie musi obejmować zarówno działania zdalne jak i prace na miejscu. Jeśli działania zdalne nie rozwiążą problemu, interwencja jest przeprowadzana na miejscu. Usługa powinna obejmować odtworzenie środowiska w przypadku dostarczenia przez Zamawiającego kopii zapasowych plików konfiguracyjnych. W przypadku wystąpienia błędu systemowego, Wykonawca będzie współpracował z producentem błędnie działającego elementu systemu w celu jego usunięcia. Wykonawca musi zapewnić dostęp do baz wiedzy i przewodników konfiguracyjnych producenta.
NAPRAWA	Dostawa części zamiennych, naprawa lub wymiana uszkodzonego urządzenia na urządzenie sprawne i wolne od wad przez specjalistę Wykonawcy (nie dotyczy urządzeń końcowych np. aparaty telefoniczne, punkty dostępowe, terminale wideo, monitory). Zastępowane urządzenie lub część zamienna będzie po zgłoszeniu wysłane/a do Zamawiającego.
ZAMIANA	Zamiana wadliwie działających urządzeń końcowych Systemu wraz z dostawą nowych urządzeń końcowych wolnych od wad. Koszty przesyłek związanych z usługą (w obie strony) pokrywa Wykonawca. W przypadku braku możliwości zamiany, Wykonawca zobowiązuje się do dostarczenia ekwiwalentnego urządzenia.
AKTUALIZACJA	Dostarczanie aktualizacji oprogramowania objętego Umową zgodnie z udzielonymi licencjami i polityką wsparcia oprogramowania przez jego producenta obejmujące nowsze wersje (upgrade) oraz poprawki (update/patch). W przypadku wystąpienia błędu systemowego oprogramowania Wykonawca opracuje obejścia zgłoszonych problemów i zgłosi problem do producenta w celu uzyskania modyfikacji oprogramowania. Przez cały okres trwania Umowy Wykonawca zapewni dostęp do dedykowanych, oferowanych przez producenta subskrypcji wymaganych do działania oprogramowania (np. sygnatury AV, IPS).
ASYSTA	Wsparcie telefoniczne dla administratorów Zamawiającego świadczone przez Wykonawcę w zakresie obsługi, administracji, konfiguracji oprogramowania i urządzeń dostarczonych w ramach Systemu.
KONFIGURACJA	Zdalne wykonywanie zmian w konfiguracji Systemu.
STROJENIE	Wykonywanie zmian w konfiguracji Systemu w siedzibie Zamawiającego.
PRZEGLĄD	Okresowy przegląd polegający na zbadaniu stanu oprogramowania i stanu technicznego urządzeń, zebraniu z rejestrów i logów informacji o błędach oraz wartościach parametrów obciążenia poszczególnych elementów Systemu, analizie zebranych informacji i przeprowadzeniu korekt z niej wynikających.
OPTYMALIZACJA	Okresowy przegląd i monitorowanie Systemu w celu optymalizacji jego działania oraz poprawy dostępności, wydajności i bezpieczeństwa zakończony sporządzeniem raportu zawierającego diagnozy, wytyczne, zalecenia i rekomendacje w tym zakresie oraz przeprowadzenie korekt wynikających z raportu.

WARSZTATY	Transfer wiedzy w postaci dodatkowych warsztatów/szkoleń z zakresu zaawansowanej administracji serwisowanych technologii dla zespołu IT Zamawiającego prowadzonych przez certyfikowanych specjalistów Wykonawcy. Wspieranie zespołu IT Zamawiającego poprzez konsultacje w rozwiązywaniu pojawiających się w trakcie eksploatacji systemu problemów dotyczących złożonych zagadnień technicznych oraz w celu podniesienia stopnia dostępności, wydajności i bezpieczeństwa systemów informatycznych Zamawiającego. Tematyka warsztatów/szkoleń , konsultacji i ich terminy będą wcześniej uzgadniana pomiędzy stronami.

W przypadku świadczenia usług gwarancyjnych i/lub serwisowych Zamawiający nie ponosi żadnych dodatkowych kosztów, w tym związanych z dojazdem i zakwaterowaniem pracowników Wykonawcy.

6.5. Parametry i warunki świadczenia usług

W opisie stosowane są następujące oznaczenia:
g – godzina robocza tj. godzina w czasie od 8:00 do 16:00 w dni robocze liczona dla jednego specjalisty
gz – godzina zegarowa
d – dzień roboczy tj. dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy liczony dla jednego specjalisty
dk – dzień kalendarzowy
t – tydzień kalendarzowy
m – miesiąc kalendarzowy
x – ilość przez określony czas (np. 8g x 5d oznacza: po 8 godzin roboczych każdego dnia przez każde 5 dni roboczych tj. łącznie 40 godzin roboczych w ciągu 5 dni roboczych) w trakcie całego okresu serwisowego
/ – ilość na dany okres (np. 8g / 5d oznacza: 8 godzin roboczych rozłożonych na każde 5 dni roboczych tj. łącznie 8 godzin roboczych do wykorzystania w ciągu każdych 5 dni roboczych) w trakcie całego okresu serwisowego.

6.5.1. Usługi reaktywne

Wymagane są następujące parametry i warunki świadczenia usług reaktywnych tj. związanych z awariami Systemu (minimalny poziom wsparcia określony jest przy każdym Podsystemie) przez cały okres trwania umowy tj. do 31.12.2020 r.

Obszary	Usługi reaktywne	Klasy incydentów	Warianty pakietów świadczenia usług		
			Parametry	Podstawowy	Rozszerzony
I_NET I_SEC I_WIFI* I_UC* I_CPD I_MGMT	DIAGNOSTYKA WSPARCIE NAPRAWA ZAMIANA AKTUALIZACJA	A – Krytyczny	Gotowość serwisowa Czas reakcji Czas naprawy Okres serwisu	8g x 5d / 1t 2g 8g 39m	24gz x 7dk / 1t 1gz 6gz 39m
		B – Wysoki	Gotowość serwisowa Czas reakcji Czas naprawy Okres serwisu	8g x 5d / 1t 2g 12g 39m	24gz x 7dk / 1t 1gz 8gz 39m
		C – Średni	Gotowość serwisowa Czas reakcji Czas naprawy Okres serwisu	8g x 5d / 1t 4g 16g 39m	24gz x 7dk / 1t 2gz 12gz 39m
		D – Niski	Gotowość	8g x 5d / 1t	24gz x 7dk / 1t

			serwisowa Czas reakcji Czas naprawy Okres serwisu	8g 48g 39m	8gz 40gz 39m
I_WIFI** I_UC**	DIAGNOSTYKA ZAMIANA AKTUALIZACJA	C – Średni	Gotowość serwisowa Czas reakcji Czas naprawy Okres serwisu	8g x 5d / 1t 12g 32g 39m	24gz x 7dk / 1t 8gz 24gz 39m
		D – Niski	Gotowość serwisowa Czas reakcji Czas naprawy Okres serwisu	8g x 5d / 1t 16g 48g 39m	24gz x 7dk / 1t 12gz 32gz 39m

*) Kontrolery, serwery

**) Urządzenia terminalne tj. telefony, przystawki, punkty dostępowe, terminale wideo, monitory

6.5.2. **Usługi proaktywne**

Wymagane są następujące parametry i warunki świadczenia usług proaktywnych tj. związanych z eksploatacją Systemu (minimalny poziom wsparcia określony jest przy każdym Podsystemie)przez cały okres trwania umowy tj. do 31.12.2020 r.

Obszary	**Usługi proaktywne**	**Warianty pakietów świadczenia usług**		
		Parametry	**Podstawowy**	**Rozszerzony**
I_NET I_SEC I_WIFI I_UC I_CPD I_MGMT	ASYSTA	Gotowość serwisowa Ilość Okres serwisu	8g x 5d / 1t 1g / 1m 39m	8g x 5d / 1t 4g / 1m 39m
	WSPARCIE	Gotowość serwisowa Ilość Okres serwisu	8g x 5d / 1t 3d / 6m 39m	8g x 5d / 1t 9d / 6m 39m
	KONFIGURACJA	Gotowość serwisowa Ilość Okres serwisu	8g x 5d / 1t 6g / 6m 39m	8g x 5d / 1t 18g / 6m 39m
	STROJENIE	Gotowość serwisowa Ilość Okres serwisu	8g x 5d / 1t 4g / 6m 39m	8g x 5d / 1t 12g / 6m 39m
	PRZEGLĄD	Gotowość serwisowa Ilość Okres serwisu	8g x 5d / 1t 2 razy w roku 39m	8g x 5d / 1t 2 razy w roku 39m
	OPTYMALIZACJA	Gotowość serwisowa Ilość Okres serwisu	8g x 5d / 1t 4g / 6m 39m	8g x 5d / 1t 12g / 6m 39m
	WARSZTATY	Gotowość serwisowa Ilość Okres serwisu	8g x 5d / 1t 3d / 6m 39m	8g x 5d / 1t 5d / 6m 39m

Terminy i zakresy (konkretne problemy, zagadnienia, tematy) usług proaktywnych będą wcześniej (w ramach czasu gotowości) uzgadniane obustronnie z wykonawcą wybranym do realizacji zamówienia.

6.5.3. **Usługi dodatkowe**

W przypadku gdy konieczne wsparcie ze strony Wykonawcy będzie przekraczało limity godzinowe opisane w tabeli z punktu 6.5.2. Zamawiający dopuszcza dokupienie godzin pracy serwisanta (zdalnych, lub lokalnych .) zgodnie z ceną określoną przez Wykonawcę w

ofercie. Zamawiający nie ponosi żadnych dodatkowych kosztów związanych z dojazdem i zakwaterowaniem pracowników Wykonawcy))

7. WYMAGANIA DLA OBSZARÓW

7.1. Zestawienie Podsystemów i obszarów Systemu objętego postępowaniem – stan do 30.09.2017r

Kod / mnemonik	Podsystem / podobszar	Producent	Model	Nr kat.	Ilość*		Minimalnie wymagany poziom wsparcia:
I_NET							
I_NET-SW_CORE	Przełączniki rdzeniowe typu	Juniper Networks	EX 4500	EX4500-40F-VC1-FB	4	kpl	Rozszerzony
I_NET-FW_CORE	Centralne zapory sieciowe	Juniper Networks	SRX 3600	SRX3600BASE-AC	2	kpl	Rozszerzony
I_NET-GW	Bramy/routery dostępowe/brzegowe	Juniper Networks	MX 80	MX80-T-AC	2	kpl	Rozszerzony
I_NET-DWDM	System zwielokrotniania łączy optycznych DWDM	Microsens	10G Transport Platform	MS430504M	8	kpl	Podstawowy
I_WIFI							
I_WIFI-CTRL	System zarządzania siecią WiFi – kontrolery i zapory sieciowe	Meru Networks	Meru MC4200	MC4200	2	szt	Podstawowy
I_SEC							
I_SEC-VPN_SSL	System zdalnego dostępu VPN SSL	Juniper Networks	Secure Access 4500	SA4500	2 (100 jednoczesnych sesji)	2	Podstawowy
I_SEC-VPN_GRE	System zdalnego dostępu VPN IPsec/GRE	Juniper Networks	SRX650	SRX650-BASE-SRE6-645AP	2	kpl	Podstawowy
I_SEC-FW_EXT	Zewnętrzne zapory sieciowe, system ochrony przed intruzami, filtrowania treści i ochrony ruchu HTTP(S)	PaloAlto Networks	PA-5050	PAN-PA-5050	2	kpl	Rozszerzony
I_SEC-CF_MAIL	System filtrowania treści i ochrony ruchu SMTP	McAfee	Email Security 3400	EMS-3400-BI	2	kpl	Podstawowy
I_SEC-SIEM	System zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem	Juniper Networks	STRM 5000	JA-STRM5000-A2-BSE	3	kpl	Rozszerzony
I_SEC-ADM_AUTH	System uwierzytelniania administratorów	RSA EMC	SecurID Appliance 130	RSA-0010500	2 kpl (licencje dla 25 użytkowników)	2	Podstawowy
I_UC							
I_UC-VG	Bramy głosowe	Cisco	2951 Integrated Services Router	C2951-VSEC/K9	2	kpl	Podstawowy
I_CPD							
I_CPD-BLD_CHASS	Obudowy serwerów kasetowych – chassis	IBM	BladeCenter H	88524TG	2	kpl	Rozszerzony

I_CPD-BLD_SRV	Serwery kasetowe	IBM	BladeCenter HS22	7870C6G	12	kpl	Rozszerzony
I_CPD-SW_FC	Przełączniki Fibre Channel sieci SAN	IBM	Express IBM System Storage SAN24B-4	249824E	2	kpl	Rozszerzony
I_CPD-DA	Macierz dyskowa	IBM	Storwize V7000 Disk Control Enclosure Storwize V7000 Disk Expansion Enclosure	2076-124 2076-212	1	kpl	Rozszerzony
I_CPD-TL	Biblioteka taśmowa	IBM	TS3200 Tape Library Model L4U Driveless	35734UL	1	kpl	Podstawowy
I_CPD-DR_DA	System zapewnienia ciągłości działania – macierz dyskowa	IBM	IBM Storwize V7000 Disk Control Enclosure	2076-124	1	kpl	Rozszerzony
I_CPD-BKP_SRV	System kopii zapasowych – serwer	IBM	System x3650M3	7945H4G	1	kpl	Rozszerzony
I_MGMT							
I_MGMT-NMS	Centralny system monitorowania infrastruktury teleinformatycznej	Zenoss	Core	ZENOSSCORE	1	kpl	Podstawowy

7.2. Sieć szkieletowa [I_NET]

Wymagane jest zapewnienie wsparcia producenta dla Podsystemów posiadanych przez Zamawiającego do końca roku 2020, oraz aktualizacja rozwiązań sieciowych posiadanych przez Zamawiającego pozwalających na dalszą rozbudowę i zapewniające wsparcie producenta do końca roku 2020.

7.2.1. Przełączniki rdzeniowe [I_NET-SW_CORE]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	4
Producent	Juniper Networks
Model	4500
Numer katalogowy	EX4500-40F-VC1-FB
Numery seryjne	GX0215478832, GX0212140928, GX0212140988, GX0212140997

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Przedłużenie gwarancji i serwisu producenta do 31.12.2020 r.
2.	Udzielenie Wsparcia technicznego wykonawcy do 31.12.2020 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE.

7.2.2. Centralne zapory sieciowe [I_NET-FW_CORE]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	2
Producent	Juniper Networks
Model	SRX 3600
Numer katalogowy	SRX3600BASE-AC
Numery seryjne	AB1112AA0022, AB0812AA0031

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach.
2.	Wymagania Ogólne 1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 3. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania administratorów do poszczególnych instancji systemu. 4. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. **Redundancja, monitoring i wykrywanie awarii** 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej (co najmniej dwóch urządzeń). 3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 4. Monitoring stanu realizowanych połączeń VPN. 5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. 6. System realizujący funkcję Firewall musi być wyposażony w redundantne zasilacze AC. **Interfejsy, Dyski:** 1. System realizujący funkcję Firewall musi dysponować minimum 16 portami Gigabit Ethernet RJ-45, 16 gniazdami SFP 1 Gbps, 8 gniazdami SFP+ 10Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 4096 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System realizujący funkcję Firewall musi być wyposażony w co najmniej dwa dyski twarde o pojemności minimum 240 GB każdy. **Parametry wydajnościowe:** 1. W zakresie Firewall'a obsługa nie mniej niż 12 mln. jednoczesnych połączeń oraz 300 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 80 Gbps dla pakietów 512 B. 3. Przepustowość modułu Kontroli Aplikacji: nie mniej niż 16 Gbps. 4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 50 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 13 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 5 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES256-SHA1) dla ruchu http – minimum 10 Gbps. **Funkcje Systemu Bezpieczeństwa:** W ramach dostarczonego systemu musi istnieć możliwość realizacji wszystkich poniższych funkcji. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych, programowych lub w postaci dodatkowych licencji: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Analiza ruchu szyfrowanego protokołem SSL oraz SSH.
10. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
11. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

Polityki, Firewall

1. System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.
2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
4. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    - Wsparcie dla IKE v1 oraz v2.
    - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM)
    - Obsługa protokołu Diffiego-Hellman grup 19 i 20
    - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
    - Tworzenie połączeń typu Site-to-site oraz Client-to-Site.
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
    - Mechanizm „Split tunneling” dla połączeń Client-to-Site
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
    - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
    - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
3. Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej.
4. Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
    - Routingu statycznego
    - Policy Based Routingu
    - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2800 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, Botnet.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, Dynamic DNS, proxy avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. **Logowanie:** 1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG. **Certyfikaty** Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: • ICSA lub EAL4 dla funkcji Firewall • ICSA lub NSS Labs dla funkcji IPS • ICSA dla funkcji: SSL VPN, IPSec VPN **Serwisy i licencje** W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) IPS do dnia 31.12.2020 r. **Gwarancja oraz wsparcie** 1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta do dnia 31.12.2020 r. polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

7.2.3. System zwielokrotniania łączy optycznych [I_NET-DWDM]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	8
Producent	Microsens
Model	10G Transport Platform
Numer katalogowy	MS430504M
Numery seryjne	00001365, 00001389, 00001366, 00001369, 00001356, 00001384, 00001371, 00001374

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Przedłużenie gwarancji i serwisu producenta do 31.12.2020 r.
2.	Udzielenie Wsparcia technicznego wykonawcy do 31.12.2020 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE.

7.2.4. Szkolenia

7.2.4.1. Szkolenia autoryzowane

Wymagane jest zapewnienie szkoleń autoryzowanych o tematyce:

Tematyka	Liczba osób – pracowników Zamawiającego
I_NET	
Centralne zapory sieciowe [I_NET-FW_CORE] 1. Wstęp do UTM 2. Logowanie i monitoring 3. Konfiguracja polityk firewalla 4. NAT – Translacja adresów sieciowych 5. Lokalne uwierzytelnianie użytkowników 6. SSL VPN 7. Wstęp do IPSec-VPN 8. Explicit Proxy 9. Skanowanie antywirusowe 10. Filtr stron WWW 11. Kontrola aplikacji 12. Konfiguracja Routingu 13. Wirtualne domeny (VDOM) 14. Transparentny tryb pracy 15. High Availability 16. Zaawansowana konfiguracja IPSec VPN 17. Intrusion Prevention System – IPS 18. Operacje oparte na certyfikatach 19. Ochrona przed wyciekiem danych – DLP 20. Diagnostyka 21. Przyspieszenie sprzętowe – chipy ASIC 22. Ipv6	5

7.2.4.2. Szkolenia autorskie

Wymagane jest zapewnienie szkoleń autorskich dla następujących podsystemów/podobszarów:

Kod / mnemonik	Podsystem / podobszar	Czas trwania [dni]
I_NET		
I_NET-FW_CORE	Centralne zapory sieciowe	2

Zakres szkolenia powinien obejmować funkcje i konfiguracje zastosowane we wdrożonym u Zamawiającego Podsystemie.

7.3. Sieć bezprzewodowa [I_WIFI]

Wymagana jest aktualizacja rozwiązań sieci WIFI posiadanych przez Zamawiającego pozwalających na dalszą rozbudowę i zapewniające wsparcie producenta do końca roku 2020.

7.3.1. System zarządzania siecią WIFI [I_WIFI-CTRL]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	2
Producent	Meru Networks
Model	Meru MC4200
Numer katalogowy	GP230
Numery seryjne	6381, 6382

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o

	następujących parametrach.
2.	Zamawiający wymaga dostarczenia **2 szt**. kontrolerów sieci bezprzewodowej do pracy w klastrze active-pasive. Każdy z kontrolerów musi obsługiwać min 500 punktów dostępowych WiFi. Ze względu na posiadaną przez zamawiającego infrastrukturę sieci bezprzewodowej kontrolery muszą współpracować z aktualnie posiadanymi punktami dostępowymi Meru AP832i, Meru AP832e, AP1010, AP1020.

Parametry sieciowe	
DHCP	• Zintegrowany serwer DHCP
VLANy	• Mapowanie SSID do VLANu • Wsparcie dla dynamicznego przydzielania VLANów
Routing	• Wsparcie dla tras statycznych
Multicast	• Konwersja multicast do unicast • IGMP snooping
GRE	• Wsparcie dla tuneli GRE
Przesyłanie danych	• Scentralizowane – ruch tunelowany do kontrolera • Rozproszone – ruch przełączany lokalnie na porcie AP
Zarządzanie	
Dostęp administracyjny	• HTTPS • SSH, Telnet oraz konsola • SNMP (V1,V2c, V3)
Monitoring	• Punktów dostępowych (radio, kanał) – status, użycie, wykorzystanie • Klientów – siła sygnału, SNR, nazwa użytkownika, adres IP, typ urządzenia, nazwa polityki firewall'a, wykorzystanie przepustowości, kontrola aplikacji • Wykrywanie obcych punkty dostępowe • Hierarchia sieci kratowych • Monitorowanie stanu zdrowia sieci bezprzewodowej, trendy klientów, przeciążone AP, nadmierne błędy RF
Centralne zarządzanie	• Zarządzanie wszystkimi funkcjami system z poziomu kontrolera • Centralne raportowanie, analiza i trendy działania sieci z wykorzystaniem centralnego systemu zarządzania
Rozwiązywanie problemów	• Zdalny kolektor pakietów pochodzących z sieci bezprzewodowej • Kolektor pakietów pochodzących z sieci przewodowej • Funkcjonalność Station-log - Kontroler musi umożliwiać diagnostykę stacji końcowych oraz punktów dostępowych w czasie rzeczywistym, oraz udostępniać podgląd logów z aktywności stacji końcowych
Zdalne punkty dostępowe	
Zdalne punkty dostępowe	• Możliwość instalacji punktu dostępowego w zdalnej lokalizacji od kontrolera, poprzez łącze WAN • Możliwość szyfrowania ruchu danych poprzez 3DES • Kontroler musi zapewniać funkcje koncentratora VPN dla zdalnie podłączonych punktów dostępowych
Niedostępność kontrolera	• Podtrzymanie podłączenia dla zasocjowanych stacji na wypadek niedostępności kontrolera • Możliwość rozgłoszenia zapasowego SSID na czas niedostępności kontrolera
Układ wysokiej dostępności	
	• Kontroler musi zapewniać mechanizmy wysokiej dostępności, w tym układ N+1, dla minimum pięciu aktywnych kontrolerów
Sieć Kratowa	
Topologia	• Sieci kratowe typu Multi-hop • Wsparcie dla wielu instancji sieci kratowych
Punkty pośredniczące	• Konfigurowalna liczba punktów pośredniczących (tzw. hop count)
Most	• Mosty typu Point-to-Multipoint
Zarządzanie	• Poprzez interfejs graficzny kontrolera
Uwierzytelnianie	
Metody uwierzytelnienia - użytkownicy	• IEEE 802.1x (EAP, Cisco-LEAP, PEAP, EAP-TLS,EAP-TTLS, EAP-SIM,EAP-AKA) • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS • RFC 3579 RADIUS wsparcie dla EAP • RFC 3580 IEEE 802.1x RADIUS Guidelines • RFC 3748 Extensible Authentication Protocol • WEP64 – 64-bit Web Equivalent Privacy • WEP128 – 128 bit WEP • WPA (Wi-Fi Protected Access) Personal & Enterprise • WPA2 (Personal & Enterprise) – 802.11i standard • Uwierzytelnienie w oparciu o MAC adres • Uwierzytelnienie w oparciu o MAC adres via RADIUS

		• Uwierzytelnienie w oparciu o certyfikat dla stacji BYOD
	Serwery uwierzytelniające	• Lokalna baza użytkowników, RADIUS, TACACS+ do logowania lokalnego • Zewnętrzne serwery uwierzytelniające – Microsoft Active Directory, Microsoft RADIUS server, Cisco ACS Server, FreeRADIUS , Interlink RADIUS, Steel Belted Radius.
	Protokoły szyfrowania	• CCMP/AES • TKIP • TLS
	Captive Portal	• Uwierzytelnienie w oparciu o wewnętrzną lub zewnętrzną bazę użytkowników • W pełni konfigurowalna strona powitalna • Wsparcie dla wielu stron powitalnych • Przekierowanie na zewnętrzny captive portal • Przekierowanie na konkretną stronę po uwierzytelnieniu
	Użytkownicy typu „gość”	• Konfigurowalny czas wygaśnięcia konta • Konfigurowalny czas włączenia konta • Integracja z zewnętrznymi captive portal’ami
	RF and Performance Management	
	ARRP (Automatic Radio Resource Provisioning)	• Automatyczne nadawanie kanałów nadawczych dla punktów dostępowych
	Planowanie ARRP	• Konfigurowalne (włącz/wyłącz) • Możliwość określenia zakresów czasowych dla włączonego ARRP
	802.11N HT20 oraz HT40 802.11ac 80Mhz	• Wsparcie dla modeli 802.11ac • Wsparcie dla modeli 802.11n
	Sterowanie Pasmem	• Równoważenie obciążenia stacji pomiędzy dwoma częstotliwościami 2.4GHz i 5GHz
	Automatyzacja pokrycia sygnałem	• Automatyczne zwiększenie mocy nadawczych TX punktów dostępowych na wypadek awarii któregoś z punktów dostępowych
	Planowanie sieci	• Predykcyjne planowanie RF • Dynamiczne mapy w trybie czasu rzeczywistego • Site Survey
	Obce punkty dostępowe	
	Skanowanie	• W pełnym wymiarze czasu lub w tle
	Korelacja danych z sieci Ethernet	• Możliwość wykrycia czy obce punkty dostępowe widziane są w sieci Ethernet
	Supresja obcych punktów dostępowych	• Konfigurowalne opcje dla manualnej lub automatycznej supresji obcych punktów dostępowych • Supresja obcych punktów dostępowych uniemożliwiająca podłączenie się stacji roboczych
	Logowanie zdarzeń	• Syslog zdarzeń związanych z obcymi punktami dostępowymi
	Mobilność oraz BYOD	
	Identyfikacja urządzeń	• Rozróżnienie urządzeń pracowniczych i obcych • Identyfikacja i klasyfikacja typów urządzeń, informacji o producencie, typie i wersji systemu operacyjnego
	Kontrola Aplikacji	• Kontrola aplikacji na warstwie L7 z wykorzystaniem ponad 600 sygnatur • Możliwość detekcji, nadawania priorytetów lub blokowania aplikacji
	QoS	• Wsparcie dla QoS • Nadawanie znaczników QoS na podstawie kontroli aplikacji • Zachowywanie znaczników QoS w sieci przewodowej i bezprzewodowej • Nadawanie priorytetu transmisji najważniejszych aplikacji biznesowych w sieci bezprzewodowej
	Polityki QoS	• Nadawanie polityk QoS oraz firewall bazując na informacjach o urządzeniu i użytkowniku końcowym

	Roaming	• Kontroler musi umożliwiać rozwiązanie w którym z punktu widzenia użytkownika grupa punktów dostępowych podłączonych do kontrolera, rozgłaszająca daną sieć bezprzewodową, jest widziana jako pojedyncze urządzenie (BSSID) dla pasma 2,4 GHz lub 5GHz, zapewniając brak ponownego uwierzytelnienia i asocjacji podczas przełączania pomiędzy punktami dostępowymi • Fast Roaming - 2-3ms pomiędzy punktami dostępowymi • 802.11i fast-roam back • 802.11i fast-associate in advance • PMK caching na tym samym kontrolerze i w obrębie grupy mobilnej
	Funkcje Analityczne	• Kontroler musi umożliwiać kolekcję danych pochodzących z interfejsów radiowych oraz modułów Bluetooth dla zewnętrznych systemów analitycznych
	Analiza Spektrum	
		• Kontroler musi umożliwiać funkcje skanera pasma, analizatora widma w oparciu o zarządzane punkty dostępowe bez konieczności stosowania dodatkowych sond
	Wsparcie dla IPv6	
	Klienci	• Wsparcie dla klientów IPv6
	Wi-Fi Alliance	
	Certyfikacje Wi-Fi Alliance	• Certyfikacja Wi-Fi Alliance (802.11a/b/g/n/d/h, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM™ Power Save).
		• 802.11a, 802.11b, 802.11g, 802.11n (2x2 MIMO), 802.11n (3x3 MIMO), 802.11n with Automatic Power Save Delivery (UAPSD), 802.11n with HT40 support, 802.11ac • 802.11e & WME/WMM Multimedia Extensions, Block ACK, NoAck, 4 priority queues • 802.11h • 802.11i (TKIP/AES), 802.1x
	Parametry wydajnościowe	
		• Konfiguracja co najmniej 64 profili bezpieczeństwa • Konfiguracja co najmniej 64 serwerów radius • Konfiguracja co najmniej 8 zewnętrznych captive portal'i
		• Lokalna baza użytkowników typu gość – min. 300
		• Konfiguracja co najmniej 64 profili sieci bezprzewodowych (SSID) • Konfiguracja co najmniej 5 zapasowych SSID
		• Konfiguracja co najmniej 64 grup punktów dostępowych
		• Konfiguracja co najmniej 512 tuneli GRE oraz vlanów
		• Kontroler musi obsługiwać co najmniej 500AP oraz 6200 klientów sieci bezprzewodowej. Jeżeli do obsługi punktów dostępowych wymagane są licencje, to muszą być one dostarczone wraz z kontrolerem do obsługi 500AP.
	Parametry Fizyczne	
	Wymiary	• Obudowa rack 1U
	Porty	• Kontroler powinien być wyposażony przynajmniej w cztery porty 10/100/1000 Base-T Ethernet, cztery porty SFP, dwa porty SFP+ oraz port konsoli (RJ45)
	Pamięć	• Kontroler musi być wyposażony w przynajmniej 2 dyski SSD o pojemności 240GB
	Zasilanie	• Kontroler musi być wyposażony w dwa redundantne zasilacze sieciowe o mocy 300W

Zakres usług związanych z siecią WiFi obejmuje co najmniej:

- Przeniesienie używanych obecnie (ok. 150szt.) AP (Access Point) Meru 832i, 832e, 1010, 1020 z istniejącego kontrolera na dostarczany nowy klaster kontrolerów,
- Analiza obecnej konfiguracji i rozmieszczenia fizycznego poszczególnych AP (w sumie ok. 370szt.),
- Dostosowanie rozmieszczenia fizycznego poszczególnych AP do pracy sieci WiFi opartej o dwa niezależne klastry kontrolerów (m.in. rozplanowanie kanałów tak aby zachować pokrycie radiowe i zniwelować ewentualne zakłócenia). Spodziewana jest konieczność fizycznej relokacji przynajmniej części AP,
- Rekonfiguracja obecnych i konfiguracja nowych kontrolerów tak aby zachować spójność sieci bezprzewodowej w zakresie rozgłaszanych SSID, polityki konfiguracji i dostępu,
- Świadczenie usługi serwisu i gwarancji zgodnie z warunkami niniejszego postępowania.

3.	Dostarczenie, uruchomienie, konfiguracja, integracja z kontrolerami Zamawiającego **10** punktów dostępowych sieci WIFI i następujących parametrach.
4.	Punkty dostępowe: 1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwuzakresowe moduły radiowe pracujące w paśmie 2,4 GHz oraz 5 GHz, obsługujące standardy pracy IEEE 802.11 a/b/g/n/ac oraz szerokości kanałów 20/40/80 MHz. 2. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej umożliwiając automatyczne podłączenie, pobieranie oprogramowania oraz konfiguracji, a także wspierać tryb, w

	którym z punktu widzenia użytkownika grupa access-pointów rozgłaszająca daną sieć bezprzewodową, jest widziana jako pojedyncze urządzenie (BSSID) dla pasma 2,4 GHz lub 5GHz. 3. Punkt dostępowy musi mieć możliwość pracy obu modułów radiowych na paśmie 5GHz. 4. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy. 5. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 1dBm. 6. Punkt dostępowy musi umożliwiać zasilanie poprzez kabel sygnałowy Ethernet zgodnie ze standardem IEEE 802.3af. 7. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych: a. Tunelowy b. Bridge c. Mesh d. Tunel VPN do kontrolera. 8. Wsparcie dla QoS: 802.11E, Dynamic WMM rate adaptation, konfigurowalne polityki QoS per użytkownik/aplikacja. 9. Wsparcie dla SNMP. 10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, 802.11i, 802.1X (EAP-TLS, EAP-TTLS, PEAP, LEAP, EAP-FAST, EAP-SIM, EAP-AKA, and EAP-MD5). 11. Punkt dostępowy musi posiadać 6 wbudowanych anten pracujących w trybie 3x3 MIMO, z parametrami co najmniej: a. 2,4-2,5 GHz 3 dBi kącie wiązki azymut 195 ° elewacja 98° b. 4,9 -5,9 GHz 4 dBi kącie wiązki azymut 190 ° elewacja 100° 12. Praca w trybie MIMO 3X3:3SS. 13. Przepustowość punktu dostępowego w trybie pracy obu modułów radiowych na paśmie 5GHz: min 2.6 Gbps. 14. Obsługa standardów: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac. 15. Obsługiwane szerokości kanałów: 20 Mhz, 40 Mhz, 80 Mhz. 16. Obsługiwane modulacje: IEEE Std 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, IEEE Std 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, IEEE Std 802.11b: BPSK, QPSK, CCK 17. Wsparcie dla następujących technologii: a. Supported transmit beam-forming (TxBF) b. IEEE Std 802.11ac standard c. IEEE Std 802.11n/ac z Orthogonal Frequency Division Multiplexing (OFDM) d. EEE Std 802.11b z Direct Sequence Spread Spectrum (DSSS) e. IEEE Std 802.11ac z 20/40/80 MHz (VHT20/40/80) kanałem f. IEEE Std 802.11n z 40 MHz (HT40) kanałem g. IEEE Std 802.11a/g z 20 MHz kanałem h. IEEE Std 802.11b z 22 MHz kanałem 18. Ilość obsługiwanych klientów per moduł radiowy: min 128. 19. Ilość obsługiwanych BSSID per moduł radiowy: min. 64. 20. Punkt dostępowy musi być wyposażony w trzykolorową diodę sygnalizującą stan pracy urządzenia. 21. Punkt dostępowy musi być wyposażony w następujące interfejsy: a. Dwa gniazda Ethernet 10/100/1000 Mbps Base-T (przynajmniej jedno gniazdo PoE) oraz jedno gniazdo typu downlink dla innych urządzeń sieciowych b. Port konsolowy c. Przycisk reset 22. Punkt dostępowy musi być wyposażony w złącze typu Kensington. 23. Punkt dostępowy musi pracować w temperaturach z zakresu 0-50'C oraz wilgotności 5-95%. 24. Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance: WiFi certified IEEE Std 802.11a/b/g/n (ac). 25. Punkt dostępowy musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji.

7.3.2. Szkolenia

7.3.2.1. Szkolenia autoryzowane

Wymagane jest zapewnienie szkoleń autoryzowanych o tematyce:

Tematyka	Liczba osób – pracowników Zamawiającego
I_WIFI	
Podstawy Technologii radiowych • fale radiowe, modulacja, anteny • pasmo 2,4GHz oraz 5 GHz • technika MIMO • standardy sieci bezprzewodowej 802.11 • architektura sieci 802.11 • planowanie sieci bezprzewodowej r Koncepcja kontrolera bezprzewodowego	3

• architektura cienkiego klienta w sieci bezprzewodowej • konfiguracja kontrolera sieci bezprzewodowej • konfiguracja Virtual AP w konfiguracji • topologia Mesh • protokół CAPWAP Identyfikacja urządzeń • koncepcja Bring Your Own Device (BYOD) • polityki bazujące na urządzeniach Zaawansowane uwierzytelnianie • konfiguracja uwierzytelniania i szyfrowania w sieciach bezprzewodowych • Fast Roaming • local/remote authentication • Captive Portal • dostęp dla gości • Single Sign-On dla użytkowników bezprzewodowych AP-profile • konfiguracja parametrów radiowych • Rogue AP Detection • Wireless IDS • Putting it all together • WPA Enterprise + autentykacja	

7.3.2.2. Szkolenia autorskie

Wymagane jest zapewnienie szkoleń autorskich dla następujących podsystemów/podobszarów:

Kod / mnemonik	Podsystem / podobszar	Czas trwania [dni]
I_WIFI		
I_WIFI	Sieć bezprzewodowa	2

Zakres szkolenia powinien obejmować funkcje i konfiguracje zastosowane we wdrożonym u Zamawiającego Podsystemie.

7.4. Bezpieczeństwo informacji [I_SEC]

Wymagana jest aktualizacja rozwiązań z zakresu bezpieczeństwa informacji posiadanych przez Zamawiającego pozwalających na dalszą rozbudowę i zapewniające wsparcie producenta do końca roku 2020.

7.4.1. System zdalnego dostępu VPN SSL [I_SEC-VPN_SSL]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	2
Producent	Juniper Networks
Model	Secure Access 4500
Numer katalogowy	SA4500
Numery seryjne	240032012000023, 240032012000032

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Realizacja funkcjonalności spełnianej przez Podsystem obecnie na nowym Podsystemie opisanym w punkcie 7.2.2.

7.4.2. System zdalnego dostępu VPN IPsec/GRE [I_SEC-VPN_GRE]

Obecnie posiadane urządzenia

Produkt	Opis

Ilość sztuk/kompletów produktu	2
Producent	Juniper Networks
Model	SRX650
Numer katalogowy	SRX650-BASE-SRE6-645AP
Numery seryjne	AJ1112AA0152, AJ1112AA0162

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Przedłużenie gwarancji i serwisu producenta do 31.12.2020 r.
2.	Udzielenie Wsparcia technicznego wykonawcy do 31.12.2020 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE.

7.4.3. Zewnętrzne zapory sieciowe [I_SEC-FW_EXT]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	2
Producent	PaloAlto Networks
Model	PA-5050
Numer katalogowy	PAN-PA-5050
Numery seryjne	0009C102218, 0009C102196

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Przedłużenie gwarancji i serwisu producenta do 31.12.2020 r.
2.	Udzielenie Wsparcia technicznego wykonawcy do 31.12.2020 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE.

7.4.4. System filtrowania treści i ochrony ruchu SMTP [I_SEC-CF_MAIL]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	2
Producent	McAfee
Model	Email Security 3400
Numer katalogowy	EMS-3400-BI
Numery seryjne	H045325107, H04532106

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach.
2.	**Wymagania ogólne** System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: • Tryb Gateway. • Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). **Parametry fizyczne systemu antyspamowego** • System musi dysponować minimum 4 portami Gigabit Ethernet RJ-45. • System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1TB. • System musi posiadać wbudowany port konsoli szeregowej. • Zasilanie z sieci 230V/50Hz. **Ogólne funkcje systemu ochrony poczty** Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: • Wsparcie dla co najmniej 20 domen pocztowych. • Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP

(w szczególności powinna być możliwość definiowania reguł all-all).
- Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
- Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
- Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
- Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
- Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
- Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania wiadomości z kwarantanny przez użytkownika.
- Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3.
- Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
- Backup poczty realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
- Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
- Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
- Zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Preention)

Kontrola antywirusowa
W tym zakresie dostarczony system ochrony poczty musi zapewniać:
- Skanowanie antywirusowe wiadomości SMTP.
- Kwarantannę dla zainfekowanych plików.
- Skanowanie załączników skompresowanych.
- Definiowanie komunikatów powiadomień w języku polskim.
- Blokowanie załączników w oparciu o typ pliku.
- Możliwość zdefiniowania nie mniej niż 50 polityk kontroli antywirusowej.
- Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.

Kontrola antyspamowa
System musi zapewniać poniższe funkcje i metody filtrowania spamu:
- Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
- Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
- Szczegółowa kontrola nagłówka wiadomości.
- Analiza Heurystyczna.
- Współpraca z zewnętrznymi serwerami RBL, SURBL.
- Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.
- Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
- Wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF.
- Kontrola w oparciu o Greylisting oraz SPF
- Filtrowanie treści wiadomości i załączników.
- Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
- Możliwość zdefiniowania nie mniej niż 50 polityk kontroli antyspamowej.
- System musi realizować skanowanie antyspamowe z wydajnością min. 70 tyś wiadomości/godzinę
- Ochrona typu outbrake
- Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
- Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości.

Ochrona przed atakami na usługę poczty
System musi zapewniać poniższe funkcje i metody filtrowania:
- Ochrona przed atakami na adres odbiorcy.
- Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
- Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
- Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania
W tym zakresie dostarczony system ochrony poczty musi zapewniać:
- Logowanie do zewnętrznego serwera SYSLOG.
- Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
- Logowanie informacji na temat spamu oraz niedozwolonych załączników.
- Możliwość podglądu logów w czasie rzeczywistym.
- Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
- Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
- Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)
System ochrony poczty musi zapewniać poniższe funkcje:
- Konfigurację HA w każdym z trybów: gateway, transparent.

	• Tryb A-P [Active-Passive] z synchronizacją polityk i wiadomości, gdzie klaster występuje pod jednym adresem IP. • Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. • Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. • Monitorowanie stanu pracy klastra. • System musi być dostarczony w postaci redundantnej (co najmniej dwóch urządzeń). **Aktualizacje sygnatur, dostęp do bazy spamu** W tym zakresie dostarczony system ochrony poczty musi zapewniać • Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. • Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę. **Zarządzanie** System ochrony poczty musi zapewniać poniższe funkcje: • System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. • Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. **Certyfikaty** • VBSpam and VB100 rated lub Common Criteria NDPP, FIPS 140-2 Certified **Serwisy i licencje** W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola Antyspam, URL Filtering, kontrola antywirusowa do dnia 31.12.2020 r. **Gwarancja oraz wsparcie** Gwarancja: System musi być objęty serwisem gwarancyjnym producenta do dnia 31.12.2020 r., polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7

7.4.5. System zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem [I_SEC-SIEM]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	3
Producent	Juniper Networks
Model	STRM 5000
Numer katalogowy	JA-STRM5000-A2-BSE
Numery seryjne	251062012200017, 251062012200020, 251062012200030

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach.
2.	W ramach prac wdrożeniowych niezbędna jest integracja z istniejącymi bazami użytkowników, RADIUS – wykorzystywany w sieci EDUROAM, LDAP wykorzystywany w sieci studenckiej przez portal przechwytujący PaloAlto, tak aby możliwe było wyszukiwanie użytkowników po indeksowanym polu w logach systemowych System ma zapewnić mechanizmy nadzoru nad funkcjonowaniem systemów przetwarzania informacji w zakresie bezpieczeństwa informacji, ciągłości działania, wykrywania awarii, wykrywania anomalii i rozwiązywania problemów. Podstawowymi zadaniami dla systemu SIEM są m.in.: • wykrywanie awarii i innych problemów na podstawie logów i metryk pozyskiwanych z urządzeń i systemów informatycznych. • weryfikacja funkcjonowania zasad bezpieczeństwa i stosowanych środków kontrolnych, • zapewnienie mechanizmów monitorujących pracowników i innych użytkowników infrastruktury teleinformatycznej, • podział obowiązków w zakresie monitorowania i rozliczania użytkowników uprzywilejowanych, • monitorowanie funkcjonowania aplikacji i urządzeń w celu szybszego reagowania na możliwe problemy i awarie,

- zarządzanie wykrywaniem, priorytetyzowaniem i rozwiązywaniem incydentów bezpieczeństwa,
- zbieranie, zapisywania i przechowywanie logów na czas określony przez prawo i regulaminy wewnętrzne. Dane muszą być przechowywane w sposób zapewniający ochronę ich integralności,
- korelacji informacji pochodzących z różnych źródeł w celu wykrycia zaawansowanych zagrożeń i/lub eliminacji fałszywych alarmów.

System musi spełniać następujące wymagania szczegółowe:

Wymagania

1. Wymagania ogólne

1.1. System musi umożliwiać wykorzystanie w innych obszarach niż zarządzanie informacją bezpieczeństwa w oparciu o wspólne dane w szczególności w zakresie monitorowania usług IT, wydajności aplikacji, monitorowania usług.

1.2. System musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności związanych za analizą danych obejmujące:

a) mechanizmy pobierania danych,
b) raporty, dashboardy i formularze,
c) nowe funkcje analityczne,
d) nowe sposoby wizualizacji,
e) mechanizmy powiadamiania, w tym dwukierunkowe inne niż przewidział producent.

Realizacja tych funkcjonalności nie może wymagać konieczności angażowania producenta i nie może naruszać praw autorskich.

1.3. Architektura rozwiązania musi umożliwiać rozdzielenie na osobne serwery funkcji:

a) pobierania danych,
b) przechowywania, wyszukiwania i zarządzania bazą zebranych logów,
c) warstwy analitycznej i interfejsu użytkownika.

1.4. Licencja musi dopuszczać dowolne kształtowanie architektury systemu, w szczególności stosowanie dowolnej liczby komponentów poszczególnych funkcji opisanych w punkcie powyżej. Rozbudowa Platformy SIEM o kolejne elementy przetwarzające, analizujące, zbierające nie może się wiązać, z żadnymi kosztami licencyjnymi.

2. Wymagania funkcjonalne – pozyskiwanie danych

2.1. System musi umożliwiać pobieranie logów/zdarzeń z co najmniej z następujących systemów i aplikacji:

a) Windows 2003/2008/2012 oraz XP/7/8.x/10.
b) Linux każda dystrybucja
c) Urządzanie sieciowe Cisco,Juniper, PaloAlto, F5, Imperva, Meru Networks, McAfee, TrendMicro, PulseSecure, Gemalto, RSA Security, JunosSpace.

Przez pozyskiwanie logów rozumie się:

a) pobranie logów i zapisanie w bazie systemu SIEM,
b) klasyfikacja zdarzeń wg typów (np. zalogowanie użytkownika, nawiązanie połączenia, itp.)
c) normalizację logów, czyli nadanie kontekstów znaczeniowych dla poszczególnych fragmentów logu np. username, source_ip itp.

2.2. Dopuszcza się by zbudowanie obsługi ww. typów logów w ramach wdrożenia. Możliwości oferowane przez rozwiązanie w ramach obsługi tworzonej w trakcie wdrożenia lub używania systemu nie mogą być mniejsze niż dla źródeł obsługiwanych natywnie przez produkt.

2.3. Rozwiązanie musi pozwalać na modyfikację mechanizmów klasyfikacji zdarzeń i normalizacji logów dostarczonych razem z produktem (otwarty kod dostarczonych mechanizmów normalizacji). Aktualizacje oprogramowania nie mogą nadpisywać ww. modyfikacji.

2.4. System SIEM musi umożliwiać pobieranie logów co najmniej następującymi protokołami:

a) syslog UDP/TCP,
b) trap SNMP,
c) logi i informacje przechowywane w bazach danych. Nie mniej niż Oracle, MS SQL, MySQL, PostgreSQL. Musi istnieć możliwość instalacji sterowników do innych typów baz danych w standardzie JDBC lub ODBC (alternatywnie),
d) pliki tekstowe,
e) Windows EventLog,
f) NetFlow v5 i v9, sFlow, jFlow, IPFIX,
g) Pobieranie danych z ww. protokołów musi być możliwe bez wykorzystania agenta dla monitorowanych urządzeń i serwerów.

2.5. System SIEM musi umożliwiać pozyskiwanie danych z nasłuchu sieci. Zbierane informacje muszą obejmować wartości wszystkich nagłówków połączeń do warstwy 4 ISO/OSI, oraz do warstwy 7, dla następujących protokołów:
a) DHCP,
b) DNS,
c) HTTP,
d) IMAP,
e) SIP,
f) SMB,
g) SMTP.

Prowadzenie nasłuch musi być możliwe z dedykowanego serwera, jak również musi być możliwe z agenta zainstalowanego na stacji roboczej lub serwerze.

2.6. Powyższy mechanizm opisany w punkcie 2.5. musi zapewniać funkcjonalność rozszyfrowywania sesji SSL/TLS w celu uzyskania możliwości zapisu informacji wymienionych powyżej również dla ruchu szyfrowanego.
2.7. Powyższy mechanizm opisany w punkcie 2.5 musi zapewniać funkcjonalność wyodrębniania plików będących zawartością danych przesyłanych przez sieć dla co najmniej protokołów SMTP i http.
2.8. Musi istnieć możliwość określenia szczegółowości zbieranych danych w zakresie wybranych protokołów, określonych pól protokołów (np. http_user_agent) oraz opcjonalnie agregację danych.
2.9. System musi umożliwiać stosowanie agentów na monitorowanych serwerach i stacjach roboczych. Agent musi również umożliwiać pobieranie informacji zarówno z systemu, na którym został zainstalowany, jak również z zewnętrznych systemów (np. w celu obsłużenia logów w strefach DMZ lub lokalizacjach zdalnych). Konfiguracja agenta, po podłączeniu do serwera zarządzającego musi odbywać się centralnie.
2.10. Agent musi zapewniać możliwość szyfrowania i uwierzytelnia komunikacji z serwerem centralnym.
2.11. Musi istnieć możliwość ograniczenia przepustowości wykorzystywanej przez agenta do transmisji danych.
2.12. Agent musi mieć możliwość równoważenia obciążenia (wysyłanych danych) pomiędzy kilka serwerów centralnych rozwiązania działających w klastrze lub niezależnie
2.13. Konfiguracja agenta, po podłączeniu do systemu SIEM powinna odbywać się centralnie.
2.14. System musi posiadać możliwość potwierdzania poprawnego dostarczenia danych od agenta do elementów odpowiedzialnych za przechowywanie danych.
2.15. Oprócz źródeł wymienionych wyżej system musi umożliwiać pobierania informacji z wykorzystaniem poniższych mechanizmów:
a) parametry życiowe urządzeń pobierane z wykorzystaniem SNMP v2c/3,
b) dane wydajnościowe Windows Performance Monitor,
c) dowolne dane WMI,
d) wynik działania programów i skryptów uruchamianych na urządzeniu/serwerze lub na podłączonym systemie źródłowym,
e) Zmiany w zawartości plików i kluczy rejestrów.

Pliki tekstowe na zdalnych serwerach poprzez SSH, CIFS i NFS.

2.16. Rozwiązanie musi umożliwiać analizowanie logów wielolinijkowych. Maksymalny wspierany rozmiar pojedynczego logu nie może być mniejszy niż 256kB.

3. Wymagania funkcjonalne – normalizacja danych

3.1. System musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu (np. dodanie nowych pól, zmianę znaczenia lub nazwy istniejących itp.) bez konieczności przeprowadzania ponownego odbudowywania bazy danych. System SIEM musi pozwalać na równoległe używanie różnych sposobów normalizacji logów.

3.2. System musi umożliwiać obsługę logów w formacie XML bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą XML

3.3. System musi umożliwiać obsługę logów w formacie CEF bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą CEF.

3.4. System musi umożliwiać obsługę logów w formacje JSON bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą JSON.

3.5. System musi umożliwiać obsługę logów w formacje CSV bez konieczności tworzenie parserów. Nazwy pól powinny być wierszem nagłówkowym CSV. Musi istnieć możliwość obsługi różnych delimiterów (przecinek, kropka, średnik, tabulator itp.) oraz wartości pól w cudzysłowach.

3.6. System musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość np. „user=jkowalski" powinno tworzyć pole „user" o wartości „jkowalski".

3.7. Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zwarte w zewnętrznych repozytoriach:

a) Katalogi LDAP,
b) Bazy danych,
c) Bazy noSQL
d) Hadoop.
e) Dane geolokalizacyjne.

W celu ograniczenia zajętości przestrzeni dyskowej dane wzbogacające nie mogą być przechowywane razem z logami, a wzbogacanie powinno odbywać w locie w trakcie odczytu danych z źródeł zewnętrznych.

3.8. System musi umożliwiać rozwiązywanie adresów IP do nazw hostów i na odwrót.

3.9. System musi umożliwiać analizę logów różnych językach, w tym co najmniej w języku angielskim i polskim. Znaki w logach źródłowych kodowane przy użyciu różnych stron kodowych muszą być konwertowane do wspólnego kodowania (preferowane UTF8 lub UTF16).

3.10. Licencja nie może ograniczać w żaden sposób liczby podłączonych urządzeń.

4. Wymagania funkcjonalne – wyszukiwanie i przechowywanie danych

4.1. System SIEM musi utrzymywać repozytorium logów z możliwością ich przeglądania w formie rzeczywistej (raw) oraz udostępniać użytkownikowi dane w formie znormalizowanej (z uwzględnieniem znaczenia poszczególnych zmiennych/pól logu). Dostęp do danych w formie rzeczywistej jak i znormalizowanej musi być możliwe w oparciu o te same narzędzia.

4.2. System SIEM musi umożliwiać skalowalność poziomą poprzez dodawanie kolejnych węzłów ww. klastra w celu spełnienia wymagać dot. wydajności lub dostępności (zwiększenie liczby kopii danych). Klastry muszą umożliwiać funkcjonowanie w środowiskach złożonych z wielu lokalizacji, przy czym konfiguracja replikacji danych musi pozwalać na określenie, w której lokalizacji dostępne są kopie zebranych informacji

4.3. System musi samodzielnie zarządzać retencją danych. Wymagana jest obsługa co najmniej dwóch etapów życia danych: WARM i COLD. Z każdym etapem związane jest miejsce przechowywania danych. Migracja danych musi następować automatycznie po określonym czasie (wiek danych) lub osiągnięciu określonej objętości. Musi istnieć możliwość stworzenie różnych schematów retencji dla różnych typów danych. Dane COLD muszą być dostępne w ten sam sposób co dane WARM, w szczególności nie jest dopuszczalne wymaganie jakichkolwiek czynności związanych z odtwarzaniem danych COLD.

4.4. System SIEM musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej CIFS lub NFS lub iSCSI w celu przechowywania danych archiwalnych i danych COLD. Dane COLD powinny być dostępne w systemie w ten

sam sposób jak dane dostępne on-line. Dopuszczalne jest by dane dostępne były z mniejszą wydajnością.

4.5. Przechowywane dane muszą być zabezpieczone przed modyfikacją z wykorzystaniem metod kryptograficznych. Musi być możliwe przechowywanie danych zabezpieczających (skróty/podpisy) poza systemem. Musi być możliwe znakowanie danych czasem.

5. Wymaganie funkcjonalne – narzędzia analityczne danych

5.1. Wyszukiwanie danych musi być możliwe z wykorzystaniem filtrów opartych o dane znormalizowane np. zapytanie o konkretny adres IP występujący jako adres źródłowy połączeń. System musi również pozwalać na wyszukiwanie danych w oparciu o wyrażenia regularne zastosowane wobec całego logu jak również pojedynczych pól.

5.2. System musi analizować zdarzenia w oparciu o znaczniki czasu zawarte w oryginalnych logach jeśli tylko są dostępne. System musi uwzględniać przy prezentacji wyniku możliwość pozyskiwania logów z urządzeń skonfigurowanych w innych strefach czasowych.

5.3. System musi posiadać możliwość tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być tworzone są w wielu formatach – minimum PDF, CSV, JPG.

5.4. Zestaw funkcjonalności analitycznych musi uwzględniać co najmniej następujące funkcje:

a) Statystyki typu suma, średnia, mediana, odchylenie standardowe, najstarszy, najnowszy dla zadanego klucza (np. średni godzinny wolumen danych dla adresu źródłowego),

b) Funkcje wykrywania anomalii danych liczbowych. Rozwiązania musi pozwalać na wykrywanie anomalii dla dowolnych parametrów zawartych w logach, a nie tylko parametrów ruchu sieciowego.

c) Rozwiązanie musi wykrywać rzadkie wystąpienia wartości i zdarzeń w określonym podzbiorze,

d) Budowanie korelacji w oparciu o zdarzenia zawierające jednakowe wartości danych pól.

Badanie zmian wartości danego pola i alarmowanie lub raportowanie w oparciu o zmianę tej wartości (np. wzrost liczby niepoprawnych zalogowań o 50%).

5.5. System SIEM musi umożliwiać alarmowanie i raportowanie o anomaliach statystycznych dla dowolnych parametrów liczbowych zawartych w logach polegając na odchyleniach w stosunku do wartości przewidywanych (zarówno w górę, jak i w dół) z uwzględnieniem sezonowości (np. różnic wynikających z pory dnia, czy dnia tygodnia).

5.6. System SIEM musi pozwalać na akceleracje zapytań i raportów, które wykonywane są często, tak by automatycznie budował agregaty pozwalające na szybkie wykonania raportu obejmującego dowolnie długie okresy czasu. Akceleracja musi być dostępna zarówno dla raportów wbudowanych jak i własnych definiowanych przez użytkownika. Raporty takie powinny być dostępne w czasie nie przekraczającym kilku sekund od ich uruchomienia dla dowolnego okresu czasu.

5.7. System SIEM musi posiadać możliwości wizualizacji danych na raportach i dashboardach z wykorzystaniem:

a) Tabel,

b) Lista zdarzeń,

c) Wykresy (co najmniej: słupkowy, kołowy, liniowy, punktowy, bąbelkowy),

d) Map,

e) Map kolorowanych.

5.8. Musi istnieć możliwość rozbudowy funkcjonalności o wizualizacje dostarczane przez zewnętrzne biblioteki komercyjne lub dostępne na zasadzie otwartego kodu. Musi istnieć możliwość umieszczania takich wizualizacji na standardowych dashboardach systemu.

5.9. Musi istnieć możliwość tworzenie interaktywnych dashboardów zawierających elementy interfejsu użytkownika takie jak np. pola tekstowe, listy wyboru, checkbox itp. pozwalające na parametryzacje wyświetlanych informacji. Musi istnieć możliwość tworzenie ich bez konieczności programowania (z wykorzystaniem narzędzi graficznych).

5.10. Musi istnieć możliwość definiowania akcji typu drill down związanych powiązanych z różnymi typami zdarzeń oraz pól. Dostępne akcje powinny obejmować zewnętrzny URL lub raport/dashboard w samym systemie. Dla zewnętrznych URL musi istnieć możliwość przekazania parametru lub parametrów na podstawie wartości pól,

	których dotyczy akcja drilldown. Musi istnieć możliwość przekazania parametrów metodami GET i POST. 5.11. Musi istnieć możliwość tworzenie na podstawie tego samego zapytania do bazy systemu zarówno alarmów jak i raportów. Musi istnieć możliwość utworzenia panelu dashboardu na podstawie dowolnego raportu. 5.12. Dla warstwy analitycznej, System musi umożliwiać konfigurację klastrów wysokiej dostępności z równoważeniem obciążenia (klastry Active/Active). Musi istnieć możliwość konfiguracji dowolnej liczby węzłów klastra. Równoważenie obciążenia pomiędzy węzły nie może wymagać stosowania zewnętrznego rozwiązania je rozkładającego (tzw. loadbalancer) **6. Wymagania funkcjonalne – analiza zdarzeń bezpieczeństwa** 6.1. System SIEM musi umożliwiać korelację zdarzeń pochodzących z różnych systemów źródłowych na podstawie dowolnych pól i zmiennych logu lub dowolnych innych danych wzbogacających log (dane o tożsamości, geolokalizacja, dane o zasobach) 6.2. System SIEM musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI, jak języka zapytań charakterystycznego dla danego systemu SIEM. 6.3. Musi istnieć możliwość zastosowania bez modyfikacji reguł korelacyjnych dla danych historycznych, w celu wykrycia podobnych zdarzeń w przeszłości. 6.4. System SIEM musi umożliwiać tworzenie reguł korelacyjnych o długim okresie działania (czas pomiędzy najstarszym, a najnowszym zdarzeniem w ramach grupy zdarzeń powiązanych ze sobą). Okres ten nie może być ograniczany żadnymi innymi limitami, poza dostępnością danych w systemie. 6.5. Wynikiem działania reguły korelacyjnej powinno być utworzenie alarmu lub zwiększenie współczynnika ryzyka związanego z obiektem uczestniczącym w zdarzeniu (użytkownik, host, port itp.). 6.6. System musi zawierać mechanizmy zarządzania incydentami obejmujące co najmniej: a) Możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych, b) Możliwość przypisania incydentu do osoby, c) Możliwość zmiany statusu i priorytetu incydentu, d) Możliwość tworzenia komentarzy, e) Możliwość automatycznego i ręcznego modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy. f) Możliwość tworzenia wyjątków stałych i czasowych dla reguł i zdarzeń spełniających określone warunki. Możliwość raportowania wydajności obsługi incydentów. 6.7. System SIEM musi posiadać możliwość automatycznego reagowania na zdarzenie oraz powiadamiania administratorów. Musi istnieć możliwość wysłania email oraz możliwość konfigurowania innych akcji w postaci skryptów, do których może być przekazywana dowolna liczba argumentów na podstawie treści alarmu. 6.8. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o dane geolokalizacyjne np. kraj lub miasto. 6.9. Musi istnieć możliwość prezentacji opisu zasobu w postaci serwera lub stacji roboczej obejmującego: nazwę, istotność, właściciela, funkcję, kontakt do administrator, nawet jeżeli w samym logu występuje wyłączenie adres IP lub MAC tego zasobu. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o te dane. 6.10. System SIEM musi klasyfikować ryzyko związane ze zdarzeń z uwzględnieniem danych priorytetu hosta celu zdarzenia. 6.11. System musi umożliwiać prezentację zdarzeń związanych z użytkownikiem niezależnie od tego z jakiego konta korzystał. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o te dane. 6.12. Musi istnieć możliwość tworzenia list kontrolnych dowolnego typu (użytkownik, adres IP itp.) wykorzystywanych w alarmach i raportach. 6.13. System SIEM musi pozwalać na definiowanie własnych i modyfikację raportów, zapytań i dashboardów dostarczonych przez producenta. 6.14. System musi umożliwiać podejmowanie automatycznych akcji lub alarmowanie. Dostępne akcje muszą obejmować: a) utworzenie incydentu w Systemie, b) wysłanie email,

c) uruchomienie skryptu i przekazanie parametrów wywoławczych,
d) integrację z systemami klasy service-desk,
e) modyfikacja list kontrolnych.

Rozwiązanie musi zawiera API pozwalająca na budowanie nowych akcji w tym przekazanie wybranych pól zdarzenia jako parametrów akcji.

7. Wymagania techniczne i bezpieczeństwa

7.1. Komunikacja użytkownika z systemem SIEM musi odbywać się przy użyciu przeglądarki internetowej (wsparcie dla co najmniej: Internet Explorer, Firefox, Chrome). Nie jest dopuszczalne wymaganie instalacji jakiegokolwiek dedykowanego oprogramowania klienckiego na stacjach roboczych użytkowników w tym wtyczek i środowisk uruchomieniowych w rodzaju Adobe Flash, Java lub Microsoft Silverlight.

Do celów administracyjnych dopuszczalne jest wymaganie zdalnego dostępu do konsoli systemu operacyjnego serwera przy użyciu standardowych narzędzi takich klient SSH lub RDP.

7.2. Rozwiązanie musi umożliwiać komunikację z SIEM za pomocą urządzeń mobilnych Apple IOS i Google Android, i pozwalać na integrację alarmów SIEM z powiadomieniami ww. urządzeń.

7.3. System SIEM musi zostać dostarczony w konfiguracji zapewniającej odporność na awarię w zakresie komponentu przechowującego dane – klaster złożony z co najmniej 2 węzłów. Każdy z węzłów klastra musi spełniać wymagania wydajnościowe określone w p. 7.9 poniżej.

7.4. System SIEM powinien wspierać Role Based Access Control (RBAC) umożliwiając precyzyjne nadawanie uprawnień dla administratorów w zakresie monitorowanego obszaru systemu informatycznego oraz dostępnych operacji w systemie zarządzania. Tożsamość administratorów musi być weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania co najmniej LDAP lub Active Directory.

7.5. System nie może ograniczać liczby równocześnie zalogowanych operatorów/użytkowników.

7.6. System SIEM musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów – login/logoff, uruchamiane zapytania i zmiany konfiguracji systemu.

7.7. Rozwiązanie musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healtcheck).

7.8. Rozwiązanie musi umożliwiać uwierzytelniać i szyfrować połączenia między komponentami systemu.

7.9. Dostarczony system musi umożliwiać analizę wydajną 20.000 EPS-ów, 48.000 Flow/min, 20 GB surowych danych dziennie, 4000 urządzeń.

7.10. Przekroczenie ww. parametrów nie może skutkować żadną utratą danych. System powinien informować o takim przekroczeniu w postaci alarmu i informacji w interfejsie użytkownika.

7.11. Rozwiązanie musi zapewnić możliwość przechowywania danych (dane surowe i metadane) przez okres 1 roku od ich powstania.

7.12. Wraz z systemem należy dostarczyć platformę sprzętową w postaci modularnego systemu serwerowego, którego parametry minimalne określony zostały w poniższej tabeli:

Lp.	Grupa wymagań	Treść wymagania
1	Wymagania dla architektury systemu	System musi być kasetowym systemem serwerowym opartym o: a) Obudowę serwerową przystosowana do montażu w szafie rack 19'' zawierającą gniazda rozszerzenia przewidziane do instalacji serwerów kasetowych jak również modułów przełączająco-zarządzających, zasilaczy oraz wentylatorów; b) Serwery kasetowe przeznaczone do instalacji w obudowie c) Centralny redundantny system przełączania i zarządzania zintegrowany w obudowie serwerowej;

	2	Wymagania dla obudowy serwerów kasetowych	Wymaga się, aby obudowa serwerów kasetowych spełniania następujące wymagania: a) Możliwość instalacji co najmniej 8 serwerów kasetowych. b) Zainstalowane w obudowie co najmniej 4 moduły zasilaczy i co najmniej 8 modułów wentylatorów. Możliwość wymiany „na gorąco” (*hot-swap*) dla wentylatorów oraz zasilaczy. c) Wymagana jest możliwość podwyższenia niezawodności zasilania poprzez pracę zasilaczy w trybach N+1, N+N, Grid; d) Zainstalowane dwa dedykowane sieciowe moduły przełączająco-zarządzające, każdy umożliwiający dołączenie dowolnego serwera kasetowego co najmniej dwoma dedykowanymi wewnętrznymi interfejsami 10GE ze wsparciem dla FCoE (FC over Ethernet). Dołączenie realizowane w ramach obudowy (*backplane*), w sposób nie wymagający użycia kabli e) Maksymalny rozmiar obudowy (*chassis*) nie więcej niż 6 RU (*Rack Unit*);	
	3	Wymagania dla dedykowanego modułu przełączająco-zarzadzającego	Wymaga się, aby każdy z dwóch dedykowanych modułów przełączająco-zarządzających znajdujacych się w obudowie spełniał następujące wymagania: a) Musi posiadać co najmniej 16 wewnętrznych portów 10GB doprowadzonych w ramach obudowy (*backplane)* do gniazd serwerów kasetowych b) Musi posiadać co najmniej 4 zewnętrzne uniwersalne porty 10G w standardzie SFP+ obsługujące następujące wkładki: • Ethernet 1000Base-SX, 1000BaseT, 1000Base-LR • Ethernet 10GE-SR, 10GE Twinax DAC 1,3,5,7,10 metrów • FibreChannel FC 4G SW i FC 8G SW c) Musi posiadać co najmniej jeden zewnętrzny port 40GE w standardzie QSFP+ obsługujący następujące wkładki • Ethernet 4x10GE Twinax DAC 1,3,5,7,10 metrów d) Musi wyprowadzać zewnętrzny dedykowany port zarządzający Ethernet 10/100/1000BaseT e) Musi wyprowadzać zewnętrzny dedykowany port konsoli szeregowej f) Musi posiadać przepustowość nie mniejszą niż 500 Gbps; g) Musi zapewnić wydajność przełączania 375 Mpps h) Musi zapewniać opóźnienie nie większe niż 1 mikrosekunda dla ramek Ethernet przełączanych między serwerami kasetowymi i) Musi umożliwiać bezpośrednie dołączanie zewnętrznych serwerów stelażowych do modułów przełączająco-zarządzających poprzez interfejsy SFP+ oraz QSFP+. j) Musi realizować dostęp serwerów kasetowych do sieci LAN oraz do sieci SAN poprzez konwergetne interfejsy 10GE, w oparciu o protokół FCoE (FibreChannel over Ethernet) zgodnie ze specyfikacją ANSI T11. k) Musi implementować IEEE Data Center Bridging (802.1Qbb PFC, 802.1Qaz Enhanced Transmission Selection) l) Musi realizować następujące funkcje warstwy 2 (*layer 2*): • Obsługa standardu IEEE 802.1Q; • Obsługa 512 wirtualnych sieci LAN (VLAN) i 32 wirtualnych sieci SAN (VSAN); • Obsługa co najmniej 20 000 adresów MAC w tablicy adresów; • Protokół Link Aggregation Control Protocol (LACP): IEEE 802.3ad; • Obsługa ramek Jumbo dla wszystkich portów (ramki o długości do 9216 bajtów); • Protokół IGMP v1, v2, v3 snooping; m) Musi realizować następujące funkcjonalności w zakresie wysokiej dostępności: • Dwa moduły przełączająco-zarządzające muszą umożliwiać klastrowanie a przez to uzyskanie jednego interfejsu do zarządzania całym	

				środowiskiem • Aktualizacja oprogramowania musi odbywać się bez przerw w pracy środowiska (co najmniej jeden moduł przełącznika musi być aktywny w czasie aktualizacji) n) Musi wspierać co najmniej poniższe standardy: • IEEE 802.1p: CoS prioritization • IEEE 802.1Q: VLAN tagging • IEEE 802.3: Ethernet • IEEE 802.3ad: LACP • IEEE 802.3ae: 10 Gigabit Ethernet • IEEE 802.1AB LLDP • SFP+ support • RMON	
		4	Wymagania dla sześciu serwerów kasetowych:	Serwer musi spełniać następujące wymagania: • Musi być oparty o architekturę Intel x86, • Musi posiadać, co najmniej dwa gniazda dla co najmniej 22-rdzeniowych fizycznych procesorów. • Musi posiadać, co najmniej 24gniazd DIMM przeznaczonych do instalacji modułów pamięci DDR4 umożliwiających uzyskanie w maksymalnej konfiguracji 768 GB pamięci. • Musi istnieć możliwość instalacji następujących modułów pamięci: o RDIMM 8 GB 2400 MHz, o RDIMM 16 GB 2400 MHz; o RDIMM 32 GB 2400 MHz o LRDIMM 32 GB 2400 MHz o LRDIMM 64 GB 2400 MHz • Musi umożliwiać instalację dwóch dysków 2.5-in. SFF SAS lub 15mm SATA lub SSD • Musi umożliwiać instalację konwergentnego adaptera sieciowego LAN/SAN zapewniającego: • łączną przepustowość co najmniej 2 x 10Gbps • wirtualizację interfejsów sieciowych z możliwością implementacji co najmniej 256 wirtualnych interfejsów widzianych z poziomu systemu operacyjnego jako niezależne urządzenia PCIe • Musi umożliwiać instalację następujących systemów operacyjnych znajdujących się na oficjalnej liście kompatybilności sprzętu : o Microsoft Windows Server 2012 R2 w wersji Standard i Datacenter, o RedHat Enterprise Linux 6.5 64 bit, o SUSE Linux Enterprise Server 11.3 o Citrix XenServer 6.2 o Solaris 11 10/12 U1 o VMWare vSphere 5.5; • W oferowanej konfiguracji serwery kasetowe muszą być wyposażone w następujące komponenty: o 2 procesory wyposażone w min. 10 rdzeni obliczeniowych każdy, minimum 25MB pamięci cache oraz o katalogowym poborze mocy nie większym niż 90W, umożliwiające osiągnięcie przez serwer w teście SPECint_rate_base2006 wyniku na	

			poziomie min. 850 pkt. o 64 GB pamięci RAM z możliwością rozbudowy do 768GB o Minimum jeden dwuportowy adapter sieciowy 10 GE typu CNA (Converged Network Adapter) z implementacją FCoE i możliwością sprzętowej wirtualizacji interfejsów Ethernet. • Trzy z powyższych serwerów musza być wyposażone w: o 2 karty SD o pojemności 64GB • Trzy z powyższych serwerów muszą być wyposażone w: o Dwa dyski SSD 960GB o Kontroler RAID wyposażony w 2GB FWBC cache i ze wsparciem dla RAID0,RAID1.	
	6	Zarządzanie	Scentralizowane zarządzenie systemem musi spełniać następujące wymagania: a) Centralny system zarządzania obejmujący wszystkie poniżej wymienione funkcjonalności musi być oparty o znajdujące się w obudowie dedykowane moduły przełączająco-zarządzające, bez konieczności instalowania w tym celu jakichkolwiek rozszerzeń sprzętowych systemu; b) Musi mieć możliwość zarządzania zewnętrznymi serwerami stelażowymi dołączonymi do modułów przełączająco-zarządzających w obudowie w dokładnie taki sam sposób jak serwerami kasetowymi w tejże obudowie c) Musi umożliwiać definicję serwera przy pomocy logicznego profilu obejmującego konfigurację serwera w zakresie sieci LAN i SAN. W zakres logicznego profilu serwerowego muszą wchodzić minimum następujące parametry:, adres MAC, adres WWNN/WWPN, sekwencja bootowania systemu, sposób konfiguracji oraz cechy adapterów NIC i HBA, ustawienia BIOS. d) Musi umożliwiać przeniesienie logicznego profilu serwera między dowolną parą serwerów kasetowych oraz stelażowych. e) Musi umożliwiać automatyczne przeniesienie logicznego profilu z uszkodzonego serwera na zdefiniowany wcześniej przez administratora serwer zapasowy f) Musi oferować poprzez graficzny oraz terminalowy interfejs użytkownika następujące funkcjonalności: i. Lista komponentów, z których składają się obudowy serwerowe ii. Wyświetlanie informacji o awariach i zdarzeniach iii. Automatyczne powiadamianie o awarii poprzez email iv. Archiwizacja i odtworzenie konfiguracji v. Zarządzanie z uwzględnieniem podziału roli użytkowników vi. Integracja ze środowiskiem wirtualizacji serwerów vii. Zarządzanie mocą całego środowiska poprzez podgląd maksymalnej i średniej wykorzystanej przez komponenty mocy viii. Zarządzanie chłodzeniem całego środowiska poprzez podgląd temperatur na poszczególnych komponentach środowiska x. Obsługa szablonów definiujących profile serwerowe w tym zapisanie wzorcowej konfiguracji profilu serwerowego, a następnie tworzenie nowych profili z pierwotnie przygotowanego szablonu xii. Konfigurowanie środowiska na podstawie puli wcześniej zdefiniowanych, dzielonych grup adresów LAN i SAN oraz za pomocą szablonów interfejsów LAN i SAN	
	7	Wyprowadzenia zewnętrzne	Z modułów przełączająco-zarządzających znajdujących się w obudowie należy wyprowadzić łącznie: a) 4 interfejsy 10GE-SR dla dołączenia do zewnętrznych sieci LAN b) 4 interfejsy FC 8G dla dołączenia do zewnętrznych sieci SAN	

	8	Poziom świadczenia usług serwisowych	a) Serwis sprzętowy 8x5xNBD dla awarii sprzętu (zgłoszenia przez pięć dni roboczych w tygodniu w czasie ośmiogodzinnego dnia pracy z dostawą części zamiennych w kolejnym dniu roboczym po zakwalifikowaniu usterki) b) Wsparcie dla zgłaszanych problemów z oprogramowaniem i funkcjonowaniem systemu c) Aktualizacja oprogramowania zarządzającego
		Czas świadczenia usług serwisowych	DO 31.12.2020

Dodatkowo należy zapewnić odpowiednie wersje i ilości licencji VMWare.

8. Serwis i wsparcie producenta

8.1. Wraz z Systemem wymagane jest dostarczenie suportu technicznego Producenta ważnego do 31.12.2020, obejmującego następujący zakres: wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

7.4.6. System uwierzytelniania administratorów [I_SEC-ADM_AUTH]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	2 kpl (licencje dla 25 użytkowników)
Producent	RSA EMC
Model	SecurID Appliance 130
Numer katalogowy	RSA-0010500
Numery seryjne	G7GQB5J, 11VQB5J

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach.
2.	1.Dostarczony system zarządzania tożsamością musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych aplikacji instalowanych w środowisku wirtualnym. 2.System uwierzytelniający musi być dostarczony w postaci maszyny wirtualnej zgodnej ze formatem OVF, możliwej do uruchomienia w środowisku VMware ESXi/ESX 3.5/4.0/4.1/5.0/5.5/6.0 3.Dla zapewnienia wysokiej sprawności, skuteczności działania i bezpieczeństw - wszystkie elementy dostarczonego rozwiązania muszą pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. 4.System musi być dostarczony w postaci redundantnej (co najmniej dwóch maszyn wirtualnych) 5.Oferowane rozwiązanie musi stanowić centralny system zarządzania kontami i uwierzytelniania użytkowników. 6.Rozwiązanie musi zapewniać obsługę żądań dwuskładnikowego uwierzytelnienia użytkowników. 7.Wymagane jest aby jeden z czynników wykorzystywanych przez funkcję generującą hasła jednokrotnego użytku był zależny od czasu. 8.Rozwiązanie musi obsługiwać autentykatory sprzętowe tego samego producenta wyposażone w bezpieczną obudowę uniemożliwiającą jej otwarcie i dostęp do elementów wewnętrznych bez ich uszkodzenia oraz w przynajmniej 6 znakowy wyświetlacz LCD i przycisk „budzenia" tokena. Dla systemu musi również istnieć możliwość obsługi tokenów softwareowych tego samego producenta. 9.Dostawa musi obejmować 25 sztuk tokenów programowych spełniających opisane powyżej wymagania. 10.Rozwiązanie musi zapewniać obsługę żądań uwierzytelnienia użytkowników, w których hasło jednorazowe jest

	wysyłane do użytkownika poprzez email lub za pośrednictwem bramki sms. 11.System musi zapewniać obsługę nielimitowanej licencyjnie liczby wirtualnych procesorów, maksymalnie 64GB pamięci operacyjnej, 4 wirtualne interfejsy sieciowe oraz obsługę powierzchni dyskowej - minimum 60 GB. 12.Rozwiązanie musi zapewniać współpracę z posiadanymi przez Zamawiającego bazami użytkowników za pośrednictwem protokołu LDAP/RADIUS. 13.Wymagana jest od systemu możliwość integracji w celu uwierzytelniania użytkowników z systemami firm trzecich za pośrednictwem protokołów RADIUS i LDAP. 14.Rozwiązanie musi pozwalać na uruchomienie lokalnego centrum certyfikacji (CA) obsługującego protokół SCEP. 15.System powinien realizować funkcje serwera uwierzytelniania dla protokołu 802.1x. 16.System musi oferować interfejs samopomocy dla użytkowników końcowych umożliwiający przynajmniej przypomnienie hasła. 17.Dostarczany system musi oferować możliwość tworzenia wielu kont administracyjnych o różnych poziomach uprawnień w celu zapewnienia bezpiecznego rozdzielenia zakresu prac administracyjnych na różne osoby w organizacji. 18.Interfejs administracyjny powinien być dostępny poprzez przeglądarkę internetową po protokole https, bez konieczności instalowania jakiegokolwiek oprogramowania klienckiego na komputerze Administratora. 19.System musi być dostarczony wraz z licencją pozwalającą na obsługę 100 użytkowników oraz wsparcie producenta do dnia 31.12.2020 r.

7.4.7. Szkolenia

7.4.7.1. Szkolenia autoryzowane

Wymagane jest zapewnienie szkoleń autoryzowanych o tematyce:

Tematyka	Liczba osób – pracowników Zamawiającego
I_SEC	
System filtrowania treści i ochrony ruchu SMTP [I_SEC-CF_MAIL] O produkciel • zagrożenia związane z pocztą elektroniczną • główne cechy podsystemu • tryby pracy urządzenia • podstawy protokołów pocztowych Podstawowa konfiguracja urządzenia • konfiguracja połączenia sieciowego • konta administracyjne • logowanie • generowanie raportów • obsługa SNMP Konfiguracja parametrów serwera poczty elektronicznej • "Chronione" domeny pocztowe • potwierdzanie odbiorców • kwarantanna • zarządzanie pocztą użytkowników • aliasy pocztowe • kolejki e-mail Kontrola i inspekcja ruchu pocztowego • reguły Access Control • polityki i profile • reguły dostarczenia • polityki w oparciu o IP • polityki w oparciu o odbiorcę Moduł Antispam • metody antyspamowe używane przez system	3

• antyspam • profile i techniki • tagi X-FEAS • wskazówki konfiguracyjne Monitorowanie sesji • konfiguracja profili sesji • reputacja nadawcy/odbiorcy • sprawdzenie nadawcy • SMTP - limity • manipulacja nagłówkami Skanowanie treści oraz archiwizacja • moduł antywirusowy • profile skanowania treści i załączników • warunki skanowania • archiwizacja i kwarantanna • zarządzanie zarchiwizowaną pocztą • ustawienia użytkownika dot. kwarantanny • raporty z kwarantanny Uwierzytelnienie i zabezpieczenie komunikacji • uwierzytelnienie poprzez SMTP • wsparcie dla PKI • protokół SMTPS • protokół SMTP over Transport Layer Security (TLS) • profil TLS • S/MIME • Identity Based Encryption (IBE) LDAP • profile i zapytania LDAP • weryfikacja odbiorcy i domeny • aliasy pocztowe • routing poczty Diagnostyka i rozwiązywanie problemów • struktura danych • informacje o systemie • błędy sprzętowe • kopia zapasowa • komendy diagnostyczne • analiza logów Tryb transparentny • konfiguracja interfejsów sieciowych • tryb Bridge oraz Router • scenariusze wdrożenia HA • tryb Configuration Share • tryb Active-Passive Mode • konfiguracja klastra • interfejs Heartbeat • monitoring klastra • procedura upgradu Tryb serwera • użytkownicy i grupy użytkowników • globalna oraz osobista książka adresowa • kalendarz	
System uwierzytelniania administratorów	3

7.4.7.2. **Warsztaty autorskie**

Wymagane jest zapewnienie warsztatów o tematyce:

Tematyka	Liczba osób – pracowników Zamawiającego
I_SEC	

System zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem 1. Podstawy a. umiejscowienie Systemu w architekturze przedsiębiorstwa b. zrozumienie zasad działania Systemu c. poznanie interfejsu użytkownika d. zrozumienie podstawowych pojęć (zdarzenie, źródło zdarzeń, itp.) e. poznanie podstaw języka zapytań f. podstawy modelowania danych (ekstrakcje, modele) g. konfiguracja powiadamiania i zlecania zadań (alerty, raporty zlecane) h. umiejętność budowania własnych aplikacji i. zarządzanie bezpieczeństwem w systemie 2. Administracja a. omówienie architektury technicznej systemu b. omówienie procesu przetwarzania danych w systemie c. znajomość konfiguracji indeksowania (tworzenie, obsługa, archiwizacja i parametryzacja indeksów) d. zarządzanie konfiguracją rozproszoną (zastosowanie UF i Deployment Server) e. omówienie typowych problemów administracyjnych i ich rozwiązań 3. Analiza danych a. wprowadzenie do statystyki — pojęcia statystyczne w środowisku b. zrozumienie zastosowania funkcji statystycznych (miary, grupowanie danych) c. zastosowanie Systemu do korelacji danych d. zastosowanie Systemu do prognozowania i analizy trendu („predictive analytics”) e. badanie anomalii	5

7.4.7.3. Szkolenia autorskie

Wymagane jest zapewnienie szkoleń autorskich dla następujących podsystemów/podobszarów:

Kod / mnemonik	Podsystem / podobszar	Czas trwania [dni]
I_SEC		
I_SEC-CF_MAIL	System filtrowania treści i ochrony ruchu SMTP	2
I_SEC-SIEM	System zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem	2
I_SEC-ADM_AUTH	System uwierzytelniania administratorów	1

Zakres szkolenia powinien obejmować funkcje i konfiguracje zastosowane we wdrożonym u Zamawiającego Podsystemie.

7.5. Zintegrowany system łączności [I_UC]

Wymagana jest aktualizacja rozwiązań z zakresu zintegrowanego systemu łączności posiadanych przez Zamawiającego pozwalających na dalszą rozbudowę i zapewniające wsparcie producenta do końca roku 2020.

7.5.1. Bramy głosowe [I_UC-VG]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	2
Producent	Cisco
Model	2951 Integrated Services Router
Numer katalogowy	C2951-VSEC/K9
Numery seryjne	FGL164513RF, FGL164513RE

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Przedłużenie gwarancji i serwisu producenta do 31.12.2020 r.
2.	Udzielenie Wsparcia technicznego wykonawcy do 31.12.2020 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE.

7.6. Środowisko przetwarzania danych [I_CPD]

Wymagana jest aktualizacja rozwiązań z obszaru środowiska przetwarzania danych posiadanych przez Zamawiającego pozwalających na dalszą rozbudowę i zapewniające wsparcie producenta do końca roku 2020.

7.6.1. Obudowy serwerów kasetowych - chassis [I_CPD-BLD_CHASS]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	2
Producent	IBM
Model	BladeCenter H
Numer katalogowy	88524TG
Numery seryjne	88524TGKD3L64A, 88524TGKD4P53Y

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Przedłużenie gwarancji i serwisu producenta do 31.12.2020 r.
2.	Udzielenie Wsparcia technicznego wykonawcy do 31.12.2020 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE.

7.6.2. Serwery kasetowe [I_CPD-BLD_SRV]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	12
Producent	IBM
Model	BladeCenter HS22
Numer katalogowy	7870C6G
Numery seryjne	7870LQU06GBPZ2, 7870LQU06GBPY9, 7870LQU06GBPY6, 7870LQU06GBPY7, 7870LQU06GBPY8, 7870LQU06GBPZ0, 7870LQU06GBPZ1, 7870LQU06GBPZ3, 7870LQU06GBPZ4, 7870LQU06GBPZ5, 7870LQU06GBPZ6, 7870LQU06GBPY5

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Przedłużenie gwarancji i serwisu producenta do 31.12.2020 r.
2.	Udzielenie Wsparcia technicznego wykonawcy do 31.12.2020 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE.
3.	Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach:
4.	**Rozbudowa infrastruktury serwerowej** W związku z rozbudową posiadanej przez Zamawiającego infrastruktury serwerowej oraz aktualnie wykorzystywanym oprogramowaniem zarządzającym, a także w celu zapewnienia dowolności rekonfiguracji sprzętu oraz możliwości centralnego zarządzania Zamawiający wymaga aby oferowane serwery typu blade, miały możliwość instalacji i poprawnego działania w posiadanych przez Zamawiającego obudowach IBM BladeCenter H. Zamawiający posiada wolne miejsca na kolejne serwery w chassie i planuje wykorzystanie serwerów do rozbudowy zasobów pod platformę wirtualizacji Vmware. W związku z czym wymagane jest zachowanie pełnej kompatybilności dostarczanych serwerów z aktualnie posiadaną platformą sprzętową. **Serwer blade 6 kpl** **Parametry minimalne:**

	Typ procesora	min. Intel X5675 6C 3.06GHz
	Liczba procesorów	W każdym serwerze zainstalowane 2 fizyczne procesory
	Pamięć RAM	min 64GB RAM z możliwością rozbudowy do 192GB. min 12 slotów na pamięć w serwerze. Zainstalowane moduły RAM muszą pochodzić od producenta serwera i być oznaczone jego znakiem firmowym.
	Dyski twarde	2 dyski w standardzie SAS lub SATA o pojemności nie mniejszej niż 300GB każdy, typu Hot-Swap
	Interfejsy FC	min. 2 porty w standardzie Fibre Chanel o prędkości każdego portu min 8Gbps współpracujące z zainstalowanym w obudowie blade modułem QLogic(R)8 Gb Intelligent Pass-thru Module for IBM BladeCenter
	Interfejsy sieciowe	min. 2 porty w standardzie 1Gb Ethernet współpracujące z zainstalowanym w obudowie blade przełącznikiem BNT Layer 2/3 Copper Gb Ethernet Switch Module for IBM BladeCenter min. 2 porty w standardzie 10Gb Ethernet współpracujące z zainstalowanym w obudowie blade przełącznikiem BNT Virtual Fabric 10Gb Switch Module for IBM BladeCenter
	Zgodność z systemami operacyjnymi	Każdy serwer oraz zainstalowany w nim osprzęt (adaptery) musi być wspierany przez RedHat Enterprise Linux ES 5 (wersje 32-bitowe i 64-bitowe), Windows Server 2003 i/lub 2008 (wersje 32-bitowe i 64-bitowe) oraz VMware VSphere

Zamawiający w przypadku serwerów blade dopuszcza zaoferowanie urządzeń odnowionych bądź używanych pod warunkiem objęcia ich serwisem na warunkach wymaganych w SIWZ.

Zamawiający wymaga aby oferowane serwery zostały:

a) dostarczone i zamontowane w wskazanym miejscu w obudowach na serwery blade
b) skonfigurowane, zaktualizowane i udostępnione z wykorzystaniem do infrastruktury sieciowej zamawiającego

Zamawiający wymaga dodana oraz skonfigurowania każdego z serwerów do środowiska wirtualizacji opartego na platformie Vmware. W tym celu konieczne jest dostarczenie w odpowiedniej ilości licencji: VS6-EPL-A Academic VMware vSphere 6 Enterprise Plus for 1 processor

7.6.3. Przełączniki Fibre Channel sieci SAN [I_CPD-SW_FC]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	2
Producent	IBM
Model	Express IBM System Storage SAN24B-4
Numer katalogowy	249824E
Numery seryjne	249824E10222HT, 249824E10222LB

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Przedłużenie gwarancji i serwisu producenta do 31.12.2020 r.
2.	Udzielenie Wsparcia technicznego wykonawcy do 31.12.2020 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE.

7.6.4. Macierz dyskowa [I_CPD-DA]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	2
Producent	IBM
Model	Storwize V7000 Disk Control Enclosure Storwize V7000 Disk Expansion Enclosure
Numer katalogowy	2076-124 2076-212
Numery seryjne	78N2BDC, 78N29A9, 78N26NK, 78RF6C1

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o następujących parametrach.
2.	**Należy dostarczyć macierz spełniającą poniższe wymagania. Macierze z punku 7.6.4 oraz 7.6.6 zostaną rozmieszczone odpowiednio w dwóch lokalizacjach z uwzględnieniem konfiguracji replikacji pomiędzy lokalizacjami na potrzeby realizacji środowiska wysokiej dostępności.** **Wymagania wspólne dotyczące macierzy dyskowej:** 1. Macierz musi mieć możliwość zainstalowania w standardowej szafie 19” 2. Macierz musi posiadać dwa redundantne kontrolery pracujące w trybie active-active. wymienialne bez przerywania pracy. 3. Wysokość macierzy oraz półek dyskowych nie może być większa niż 2U (każdy moduł) 4. Pamięć podręczna każdego z kontrolerów musi być nie mniejsza niż 32 GB (64 GB na I/O grupę/ dla dwóch kontrolerów) . 5. Macierz musi mieć co najmniej 4 porty 16Gb Eth oraz musi posiadać możliwość rozbudowy o 8 portów 10 GbE FCoE/iSCSI lub 8 portów 16 Gbit FC 6. Macierz musi posiadać co najmniej 1 dedykowany port do zarządzania w każdym z kontrolerów. 7. Macierz musi wspierać następujące protokoły komunikacji z serwerami: Fibre Channel, iSCSI, FCoE. 8. Macierz powinna wpierać zasilanie z dwóch niezaleznych źródeł prądu 9. Macierz musi obsługiwać dyski 2,5” i 3,5” we właściwych obudowach. Macierz musi obsługiwać dyski 300GB oraz 600 GB 15000 obr/min, 900 GB, 1,2 TB, 1,8 TB 10000 obr/min, dyski 2 TB, 4 TB, 6 TB, 8 TB i 10 TB 7200 rpm oraz, 400 GB, 800 GB, 1,6 TB, 1,92 TB,3,2 TB, 3,84 TB, 7,68 TB i 15,36 TB SAS flash. Macierz musi zapewniać możliwość używania różnych dysków tego samego typu – odpowiednio 2,5” i 3,5” jednocześnie. 10. Macierz musi obsługiwać dyski SSD, NL-SAS oraz SAS w standardzie SAS 12 Gb/s. 11. Macierz musi obsługiwać połączenia do półek dyskowych oraz do dysków w standardzie SAS 12 Gb/s 12. Macierz musi mieć możliwość obsługi do 1005 dysków sumarycznie. 13. Macierz musi obsługiwać poziomy RAID 0,1,5,6,10, distributed. 14. Macierz musi umożliwiać jednoczesne stosowanie półek dyskowych obsługujących dyski 2,5” oraz 3,5”. Półki dyskowe 2,5” muszą umożliwiać instalację co najmniej 24 napędów dyskowych 2,5”. Półki dyskowe 3,5” muszą umożliwiać instalację co najmniej 12 napędów dyskowych 3,5”. **Wymagania co do funkcjonalności**: 1. Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych zarówno wewnętrznych jak i zewnętrznych (zwirtualizowanych) z jednej konsoli administracyjnej. Zarządzanie musi być dostępne poprzez interfejs GUI (WWW) oraz interfejs linii poleceń (Command Line Interface). Dostęp do linii poleceń poprzez połączenie szyfrowane. 2. Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie Macierz się znajduje. Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI 3. Musi istnieć funkcjonalność Cache dla procesu odczytu. 4. Musi istnieć funkcjonalność Mirrored Cache dla procesu zapisu. 5. Musi istnieć możliwość wyłączenia cache dla poszczególnych wolumenów 6. Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych. 7. Macierz musi optymalizować wykorzystanie dysków SSD poprzez automatyczną identyfikację najbardziej obciążonych fragmentów wolumenów w zarządzanych zasobach dyskowych oraz ich automatyczną migracje na dyski SSD. Macierz musi również automatycznie rozpoznawać obciążenie fragmentów

			wolumenów na dyskach SSD i automatycznie migrować z dysków SSD nieobciążone fragmenty wolumenów. Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia danych pomiędzy przynajmniej 3 rodzajami dysków – SSD, Enterprise (15k i 10K) oraz NL-SAS/SATA, jak również przy wykorzystaniu dwóch dowolnych z wyżej wymienionych typów. Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego wolumenu. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla danej konfiguracji.
		8.	Macierz musi umożliwiać automatyczne równoważenie obciążenia w ramach grupy/puli dysków tego samego typu. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla maksymalnej konfiguracji.
		9.	Macierz musi obsługiwać funkcjonalności LUN Masking i LUN mapping.
		10.	Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
		11.	Macierz musi mieć możliwość wykonania kopii danych typu Point-In-Time (PiT) wolumenów. Zasoby źródłowe oraz docelowe kopii PiT mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (, SAS, SSD), jak również na odrębnych, zwirtualizowanych poprzez przedmiotową macierz podsystemach dyskowych. Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować, dla maksymalnej pojemności macierzy i maksymalnej liczby wolumenów.
		12.	Kopie danych typu PIT muszą być tworzone w trybach kopii pełnej (klon) oraz kopii wskaźników (migawka), incremental (kopiowanie tylko bloków zmienionych pomiędzy kolejnymi wykonaniami kopii), multitarget (wiele kopii z jednego źródła), cascaded (kopia z kopii).
		13.	Macierz musi obsługiwać min 255 kopii migawkowych per wolumen, 4096 łącznie w całym systemie.
		14.	Macierz musi obsługiwać grupy spójności wolumenów do celów kopiowania i replikacji.
		15.	Macierz musi posiadać funkcjonalność tworzenia mirrorowanych LUN pomiędzy różnymi zarządzanymi zasobami dyskowymi dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta. Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować, dla maksymalnej pojemności macierzy i maksymalnej liczby wolumenów.
		16.	Macierz musi mieć możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (). Replikacja musi być realizowana przy użyciu interfejsów Fibre Channel.
		17.	Macierz musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych, oraz wewnątrz macierzy, bez zatrzymywania aplikacji korzystającej z tych wolumenów. Wymaga się aby zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogły być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych w szczególności na różnych, zwirtualizowanych przez macierz systemach dyskowych. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla maksymalnej konfiguracji na czas wykonania usługi migracji danych obecnych zasobów.
		18.	Macierz musi posiadać funkcjonalność zarówno zwiększania jak i zmniejszania rozmiaru wolumenów.
		19.	Macierz musi posiadać funkcjonalność zarządzania ilością operacji wejścia-wyjścia wykonywanych na danym wolumenie. Zarządzanie musi być możliwe poprzez określenie maksymalnej ilości operacji I/O na sekundę lub przepustowości określonej w MB/s dla danego wolumenu. Jeżeli funkcjonalność ta wymaga licencji należy ją dostarczyć dla maksymalnej konfiguracji macierzy.
		20.	Macierz musi posiadać funkcjonalnosc kompresji danych online, gdzie dane zapisywane w macierzy są kompresowane w locie i zapisywane na dyskach w postaci skompresowanej, a prz odczycie dane sa również w locie dekompresowane i w takiej postaci przesyłane poza macierz. Operacja kompresji nie może wymagać alokacji innej przestrzeni dyskowej niż ta, która jest niezbędna do zapisania skompresowanych danych. Jeżeli funkcjonalnosc wymaga licencji należy dostarczyć takową dla oferowanej konfiguracji.
		21.	Macierz musi posiadać funkcjonalność migracji danych z innych macierzy dyskowych bez przerywania dostępu danych dla serwerów (import danych). Macierz musi również umożliwiać eksport danych zarządzanych przez tę macierz na inną macierz dyskową. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla maksymalnej konfiguracji.
		22.	Macierz musi umożliwiać stworzenie konfiguracji odpornej na awarię pojedynczej półki dyskowej.
		23.	Macierz musi posiadać możliwość liniowej skalowaności parametrów wydajnościowych zasobów dyskowych oraz ilości obsługiwaych dysków (do co najmniej 1056) poprzez dodanie kolejnej macierzy tego

	samego typu, przy zachowaniu jednolitego i wspólnego zarządzania zasobami dyskowymi. 24. Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu powinny być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych i/lub podłączanych serwerów zależnie od sposobu licencjonowania. 25. Macierz musi być fabrycznie nowa (data produkcji nie późniejsza niż 6 miesięcy przed dostawą), musi pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Polski i być objęta serwisem producenta na terenie RP. Wymagania pojemnościowe dla macierzy 1. Macierz musi zostać wyposażona w następujące dyski : a. 8x1.8TB 2,5” 10krpm b. 2x400GB 2,5” SSD c. 10x6TB NLSAS 7200rpm W ramach dostawy macierzy dyskowych Zamawiający wymaga wykonania nastepujących czynności: 1. Wykonania demontażu starych urządzeń oraz montażu nowych w miejscach wskazanych przez Zamawiającego. 2. Podłączenie macierzy do istniejącej sieci SAN z zachowaniem redundancji połączeń i przepustowości na takim samym poziomie jak dotychczas. 3. Skonfigurowania przełączników, macierzy tak aby była zapewniona zgodna z dotychczasową dostępność do serwerów, a w szczególności hypervisorów vMware i serwera backupu. 4. Wykonania przeniesienia danych na nowe macierze bez ograniczania dostępności do danych produkcyjnych. 5. Wykonania rekonfiguracji infrastruktury w taki sposób aby było możliwe jej przełączenie dla korzystania z nowych zasobów storage’owych. Czas przełączenia nie powinien być dłuższy niż jedna godzina. 6. Wykonanie uzupełnienia konfiguracji dostarczanych macierzy – skonfigurowanie replikacji danych do centrum zapasowego. W przypadku gdy dla wykonania wymienionych zadań konieczne jest uzupełnienie posiadanych przez zamawiającego licencji, oprogramowania, sprzętu Wykonawca zobowiązany jest do ich dostarczenia, zainstalowania i uruchomienia.

7.6.5. **Biblioteka taśmowa [I_CPD-TL]**

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	1
Producent	IBM
Model	TS3200 Tape Library Model L4U Driveless
Numer katalogowy	35734UL
Numery seryjne	78T1521

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Przedłużenie gwarancji i serwisu producenta do 31.12.2020 r.
2.	Udzielenie Wsparcia technicznego wykonawcy do 31.12.2020 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE.

7.6.6. **System zapewnienia ciągłości działania – macierz dyskowa [I_CPD-DR_DA]**

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	1
Producent	IBM
Model	IBM Storwize V7000 Disk Control Enclosure
Numer katalogowy	2076-124
Numery seryjne	78N2A9X

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Dostarczenie, uruchomienie, konfiguracja, integracja z innymi podsystemami Zamawiającego Podsystemu o

	następujących parametrach.
2.	**Należy dostarczyć macierz spełniającą poniższe wymagania. Macierze z punku 7.6.4 oraz 7.6.6 zostaną rozmieszczone odpowiednio w dwóch lokalizacjach z uwzględnieniem konfiguracji replikacji pomiędzy lokalizacjami na potrzeby realizacji środowiska wysokiej dostępności.** **Wymagania wspólne dotyczące macierzy dyskowej:** 15. Macierz musi mieć możliwość zainstalowania w standardowej szafie 19” 16. Macierz musi posiadać dwa redundantne kontrolery pracujące w trybie active-active. wymienialne bez przerywania pracy. 17. Wysokość macierzy oraz półek dyskowych nie może być większa niż 2U (każdy moduł) 18. Pamięć podręczna każdego z kontrolerów musi być nie mniejsza niż 32 GB (64 GB na I/O grupę/ dla dwóch kontrolerów) . 19. Macierz musi mieć co najmniej 4 porty 16Gb Eth oraz musi posiadać możliwość rozbudowy o 8 portów 10 GbE FCoE/iSCSI lub 8 portów 16 Gbit FC 20. Macierz musi posiadać co najmniej 1 dedykowany port do zarządzania w każdym z kontrolerów. 21. Macierz musi wspierać następujące protokoły komunikacji z serwerami: Fibre Channel, iSCSI, FCoE. 22. Macierz powinna wpierać zasilanie z dwóch niezaleznych źródeł prądu 23. Macierz musi obsługiwać dyski 2,5” i 3,5” we właściwych obudowach. Macierz musi obsługiwać dyski 300GB oraz 600 GB 15000 obr/min, 900 GB, 1,2 TB, 1,8 TB 10000 obr/min, dyski 2 TB, 4 TB, 6 TB, 8 TB i 10 TB 7200 rpm oraz, 400 GB, 800 GB, 1,6 TB, 1,92 TB,3,2 TB, 3,84 TB, 7,68 TB i 15,36 TB SAS flash. Macierz musi zapewniać możliwość używania różnych dysków tego samego typu – odpowiednio 2,5” i 3,5” jednocześnie. 24. Macierz musi obsługiwać dyski SSD, NL-SAS oraz SAS w standardzie SAS 12 Gb/s. 25. Macierz musi obsługiwać połączenia do półek dyskowych oraz do dysków w standardzie SAS 12 Gb/s 26. Macierz musi mieć możliwość obsługi do 1005 dysków sumarycznie. 27. Macierz musi obsługiwać poziomy RAID 0,1,5,6,10, distributed. 28. Macierz musi umożliwiać jednoczesne stosowanie półek dyskowych obsługujących dyski 2,5” oraz 3,5”. Półki dyskowe 2,5” muszą umożliwiać instalację co najmniej 24 napędów dyskowych 2,5”. Półki dyskowe 3,5” muszą umożliwiać instalację co najmniej 12 napędów dyskowych 3,5”. **Wymagania co do funkcjonalności**: 26. Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych zarówno wewnętrznych jak i zewnętrznych (zwirtualizowanych) z jednej konsoli administracyjnej. Zarządzanie musi być dostępne poprzez interfejs GUI (WWW) oraz interfejs linii poleceń (Command Line Interface). Dostęp do linii poleceń poprzez połączenie szyfrowane. 27. Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie Macierz się znajduje. Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI 28. Musi istnieć funkcjonalność Cache dla procesu odczytu. 29. Musi istnieć funkcjonalność Mirrored Cache dla procesu zapisu. 30. Musi istnieć możliwość wyłączenia cache dla poszczególnych wolumenów 31. Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych. 32. Macierz musi optymalizować wykorzystanie dysków SSD poprzez automatyczną identyfikację najbardziej obciążonych fragmentów wolumenów w zarządzanych zasobach dyskowych oraz ich automatyczną migracje na dyski SSD. Macierz musi również automatycznie rozpoznawać obciążenie fragmentów wolumenów na dyskach SSD i automatycznie migrować z dysków SSD nieobciążone fragmenty wolumenów. Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia

		danych pomiędzy przynajmniej 3 rodzajami dysków – SSD, Enterprise (15k i 10K) oraz NL-SAS/SATA, jak również przy wykorzystaniu dwóch dowolnych z wyżej wymienionych typów. Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego wolumenu. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla danej konfiguracji.
	33.	Macierz musi umożliwiać automatyczne równoważenie obciążenia w ramach grupy/puli dysków tego samego typu. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla maksymalnej konfiguracji.
	34.	Macierz musi obsługiwać funkcjonalności LUN Masking i LUN mapping.
	35.	Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
	36.	Macierz musi mieć możliwość wykonania kopii danych typu Point-In-Time (PiT) wolumenów. Zasoby źródłowe oraz docelowe kopii PiT mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (, SAS, SSD), jak również na odrębnych, zwirtualizowanych poprzez przedmiotową macierz podsystemach dyskowych. Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować, dla maksymalnej pojemności macierzy i maksymalnej liczby wolumenów.
	37.	Kopie danych typu PIT muszą być tworzone w trybach kopii pełnej (klon) oraz kopii wskaźników (migawka), incremental (kopiowanie tylko bloków zmienionych pomiędzy kolejnymi wykonaniami kopii), multitarget (wiele kopii z jednego źródła), cascaded (kopia z kopii).
	38.	Macierz musi obsługiwać min 255 kopii migawkowych per wolumen, 4096 łącznie w całym systemie.
	39.	Macierz musi obsługiwać grupy spójności wolumenów do celów kopiowania i replikacji.
	40.	Macierz musi posiadać funkcjonalność tworzenia mirrorowanych LUN pomiędzy różnymi zarządzanymi zasobami dyskowymi dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta. Jeżeli funkcjonalność ta wymaga licencji, należy taką licencję zaoferować, dla maksymalnej pojemności macierzy i maksymalnej liczby wolumenów.
	41.	Macierz musi mieć możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (). Replikacja musi być realizowana przy użyciu interfejsów Fibre Channel.
	42.	Macierz musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami macierzy dyskowych, oraz wewnątrz macierzy, bez zatrzymywania aplikacji korzystającej z tych wolumenów. Wymaga się aby zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogły być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych w szczególności na różnych, zwirtualizowanych przez macierz systemach dyskowych. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla maksymalnej konfiguracji na czas wykonania usługi migracji danych obecnych zasobów.
	43.	Macierz musi posiadać funkcjonalność zarówno zwiększania jak i zmniejszania rozmiaru wolumenów.
	44.	Macierz musi posiadać funkcjonalność zarządzania ilością operacji wejścia-wyjścia wykonywanych na danym wolumenie. Zarządzanie musi być możliwe poprzez określenie maksymalnej ilości operacji I/O na sekundę lub przepustowości określonej w MB/s dla danego wolumenu. Jeżeli funkcjonalność ta wymaga licencji należy ją dostarczyć dla maksymalnej konfiguracji macierzy.
	45.	Macierz musi posiadać funkcjonalnosc kompresji danych online, gdzie dane zapisywane w macierzy są kompresowane w locie i zapisywane na dyskach w postaci skompresowanej, a prz odczycie dane sa również w locie dekompresowane i w takiej postaci przesyłane poza macierz. Operacja kompresji nie może wymagać alokacji innej przestrzeni dyskowej niż ta, która jest niezbędna do zapisania skompresowanych danych. Jeżeli funkcjonalnosc wymaga licencji należy dostarczyć takową dla oferowanej konfiguracji.
	46.	Macierz musi posiadać funkcjonalność migracji danych z innych macierzy dyskowych bez przerywania dostępu danych dla serwerów (import danych). Macierz musi również umożliwiać eksport danych zarządzanych przez tę macierz na inną macierz dyskową. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla maksymalnej konfiguracji.
	47.	Macierz musi umożliwiać stworzenie konfiguracji odpornej na awarię pojedynczej półki dyskowej.
	48.	Macierz musi posiadać możliwość liniowej skalowaności parametrów wydajnościowych zasobów dyskowych oraz ilości obsługiwaych dysków (do co najmniej 1056) poprzez dodanie kolejnej macierzy tego samego typu, przy zachowaniu jednolitego i wspólnego zarządzania zasobami dyskowymi.

	49. Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu powinny być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych i/lub podłączanych serwerów zależnie od sposobu licencjonowania. 50. Macierz musi być fabrycznie nowa (data produkcji nie późniejsza niż 6 miesięcy przed dostawą), musi pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Polski i być objęta serwisem producenta na terenie RP. Wymagania pojemnościowe macierzy 1. Macierz musi zostać wyposażona w następujące dyski : a. 14x1.8TB 2,5" 10krpm b. 2x400GB 2,5" SSD c. 10x6TB NLSAS 7200rpm W ramach dostawy macierzy dyskowych Zamawiający wymaga wykonania nastepujących czynności: 1. Wykonania demontażu starych urządzeń oraz montażu nowych w miejscach wskazanych przez Zamawiającego. 2. Podłączenie macierzy do istniejącej sieci SAN z zachowaniem redundancji połączeń i przepustowości na takim samym poziomie jak dotychczas. 3. Skonfigurowania przełączników, macierzy tak aby była zapewniona zgodna z dotychczasową dostępność do serwerów, a w szczególności hypervisorów vMware i serwera backupu. 4. Wykonania przeniesienia danych na nowe macierze bez ograniaczania dostępności do danych produkcyjnych. 5. Wykonania rekonfiguracji infrastruktury w taki sposób aby było możliwe jej przełączenie dla korzystania z nowych zasobów storage'owych. Czas przełączenia nie powinien być dłuższy niż jedna godzina. 6. Wykonanie uzupełnienia konfiguracji dostarczanych macierzy – skonfigurowanie replikacji danych do centrum zapasowego. W przypadku gdy dla wykonania wymienionych zadań konieczne jest uzupełnienie posiadanych przez zamawiającego licencji, oprogramowania, sprzętu Wykonawca zobowiązany jest do ich dostarczenia, zainstalowania i uruchomienia.

7.6.7. System kopii zapasowych - serwer [I_CPD-BKP_SRV]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	1
Producent	IBM
Model	System x3650M3
Numer katalogowy	7945H4G
Numery seryjne	7945H4GKD3L64H

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Przedłużenie gwarancji i serwisu producenta do 31.12.2020 r.
2.	Udzielenie Wsparcia technicznego wykonawcy do 31.12.2020 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE.

7.6.7.1. Szkolenia autorskie

Wymagane jest zapewnienie szkoleń autorskich dla następujących podsystemów/podobszarów:

Kod / mnemonik	Podsystem / podobszar	Czas trwania [dni]
I_CPD		
I_CPD-BLD_	Serwery kasetowe	1
I_CPD-SW_FC	Przełączniki Fibre Channel sieci SAN	0,5
I_CPD-DA	Macierz dyskowa	2
I_CPD-TL	Biblioteka taśmowa	0,5
I_CPD-VRT	Platforma wirtualizacji	1

I_CPD-DR_	System zapewnienia ciągłości działania	1
I_CPD-BKP_	System kopii zapasowych	1

7.7. Zarządzanie infrastrukturą teleinformatyczną [I_MGMT]

Wymagane jest zapewnienie wsparcia producenta dla poniższych podsystemów posiadanych przez Zamawiającego do końca roku 2020.

7.7.1. Wymagania szczegółowe dla stosowanych produktów

7.7.2. Centralny system monitorowania infrastruktury teleinformatycznej [I_MGMT-NMS]

Obecnie posiadane urządzenia

Produkt	Opis
Ilość sztuk/kompletów produktu	1
Producent	Zeoss
Model	CORE
Numer katalogowy	ZENOSSCORE
Numery seryjne	-

Działania Wykonawcy w ramach podsystemu:

Lp.	Wymagania minimalne Zamawiającego
1.	Przedłużenie gwarancji i serwisu producenta do 31.12.2020 r.
2.	Udzielenie Wsparcia technicznego wykonawcy do 31.12.2020 r. – zgodnie z zasadami opisanymi w rozdziale 6. SERWIS, GWARANCJA, WSPARCIE TECHNICZNE.