

Znak sprawy: IN.271.14.2024

## **ZAŁĄCZNIK NR 1 DO SWZ**

### **OPIS PRZEDMIOTU ZAMÓWIENIA**

**na dostawę i wdrożenie infrastruktury sprzętowej  
oraz oprogramowania dla Gminy Chełmek**

## Spis treści

<b>ROZDZIAŁ I. ZAŁOŻENIA POCZĄTKOWE ORAZ WYMAGANIA OGÓLNE .....</b>	<b>3</b>
I.1 WPROWADZENIE I CEL PROJEKTU .....	3
I.2 AKTY PRAWNE.....	3
I.3 OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA.....	3
I.4 TERMIN REALIZACJI PRZEDMIOTU ZAMÓWIENIA .....	7
I.5 ORGANIZACJA WDROŻENIA .....	7
I.6 PRZYGOTOWANIE DOKUMENTACJI .....	8
I.7 ANALIZA PRZEDWDROŻENIOWA .....	9
I.8 HARMONOGRAM WDROŻENIA .....	10
I.9 DOKUMENTACJA POWYKONAWCZA .....	10
I.10 ODBIÓR DOKUMENTACJI/KOŃCOWY .....	10
I.11 TESTY .....	11
I.12 DODATKOWE ZOBOWIĄZANIA WYKONAWCY .....	11
<b>ROZDZIAŁ II. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA.....</b>	<b>13</b>
II.1 DOSTAWA I WDROŻENIE INFRASTRUKTURY SPRZĘTOWEJ I OPROGRAMOWANIA .....	13
II.2 DOSTAWA I WDROŻENIE URZĄDZENIA UTM – 1 SZT. ....	13
II.3 DOSTAWA I WDROŻENIE MACIERZY DYSKOWEJ WRAZ Z KONFIGURACJĄ FUNKCJI HYPERMIRROR I PODŁĄCZENIEM SERWERÓW – 1 SZT. ....	25
II.4 DOSTAWA I WDROŻENIE SERWERA ZAPASOWEGO – 1 SZT. ....	30
II.5 DOSTAWA I WDROŻENIE SYSTEMU DLP – 1 SZT. ....	41
II.6 DOSTAWA I WDROŻENIE URZĄDZENIA NAS – 1 SZT. ....	48
II.7 DOSTAWA I WDROŻENIE OPROGRAMOWANIA DO WYKONYWANIA KOPII ZAPASOWYCH WEDŁUG POLITYKI I HARMONOGRAMU TWORZENIA KOPII ZAPASOWYCH .....	55
II.8 DOSTAWA I WDROŻENIE ZARZĄDZALNYCH URZĄDZEŃ SIECIOWYCH DO RDZENIA SIECI – 2 SZT.....	62
II.9 DOSTAWA I WDROŻENIE ZARZĄDZALNYCH URZĄDZEŃ SIECIOWYCH DLA PUNKTÓW DOSTĘPOWYCH – 2 SZT.....	66
II.10 DOSTAWA I WDROŻENIE SYSTEMU NAC – 1 SZT. ....	70
II.11 DOSTAWA OPROGRAMOWANIA ANTYWIRUSOWEGO – 1 SZT.....	74
II.12 DOSTAWA I PODŁĄCZENIE ZASILACZA AWARYJNEGO UPS – 1 SZT.....	80
II.13 DOSTAWA I WDROŻENIE OPROGRAMOWANIA SIEM – 1 SZT.....	89
II.14 DOSTAWA I WDROŻENIE DEDYKOWANEGO SERWERA DO OPROGRAMOWANIA SIEM – 1 SZT .....	102
II.15 ZAKUP USŁUG SOC ZAPEWNIAJĄCYCH PREWENCJĘ, DETEKCJĘ I REAKCJĘ NA ZAGROŻENIA CYBERBEZPIECZEŃSTWA – 24 MIESIĄCE .....	108
II.16 SZKOLENIE SPECJALISTYCZNE DLA ADMINISTRATORÓW Z DOSTARCZANYCH PAKIETÓW BEZPIECZEŃSTWA I KONFIGURACJI URZĄDZEŃ I SIECI DLA URZĄDZEŃ UTM – 2 SZT. ....	130
II.17 SZKOLENIE SPECJALISTYCZNE DLA ADMINISTRATORÓW Z ADMINISTRACJI DOSTARCZANYCH SYSTEMÓW OPERACYJNYCH. – 1 SZT. ....	133
<b>ROZDZIAŁ III. GWARANCJA .....</b>	<b>134</b>
III.1 WADY .....	136

## **Rozdział I. Założenia początkowe oraz wymagania ogólne**

### **I.1 Wprowadzenie i cel projektu**

Gmina bierze udział w projekcie „Cyberbezpieczny Samorząd”, którego celem jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego (JST) poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych.

Realizacja projektu poprzez wsparcie grantowe jednostek samorządowych, przyczyni się do:

- wdrożenia lub aktualizacji w JST polityk bezpieczeństwa informacji (SZBI),
- wdrożenia w JST środków zarządzania ryzykiem w cyberbezpieczeństwie,
- wdrożenia w JST mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni,
- podniesienia poziomu wiedzy i kompetencji personelu JST kluczowego z punktu widzenia SZBI wdrożonego w urzędzie,
- przeprowadzenia w JST audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia.

### **I.2 Akty prawne**

Dostarczone rozwiązania teleinformatyczne, ze szczególnym uwzględnieniem dostarczanego i wdrażanego Oprogramowania, muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego. Rozwiązania muszą pozwalać na gromadzenie, przetwarzanie i analizowanie danych i informacji w obszarach objętych wdrożeniem.

### **I.3 Ogólny opis przedmiotu zamówienia**

**Dostawa i wdrożenie infrastruktury sprzętowej oraz oprogramowania dla Gminy Chełmek.**

Przedmiot zamówienia niniejszego postępowania przetargowego obejmuje:

Poz. OPZ	Opis	Ilość sztuk/kpl
Rozdział	Rodzaj zamawianego asortymentu	
II.2	Dostawa i wdrożenie urządzenia UTM	1 szt.
II.3	Dostawa i wdrożenie macierzy dyskowej wraz z konfiguracją funkcji HyperMirror i podłączeniem serwerów	1 szt.
II.4	Dostawa i wdrożenie serwera zapasowego	1 szt.
II.5	Dostawa i wdrożenie systemu DLP	1 szt.
II.6	Dostawa i wdrożenie urządzenia NAS	1szt.
II.7	Dostawa i wdrożenie oprogramowania do wykonywania kopii zapasowych według polityki i harmonogramu tworzenia kopii zapasowych	1 szt.
II.8	Dostawa i wdrożenie zarządzalnych urządzeń sieciowych do rdzenia sieci	2 szt.
II.9	Dostawa i wdrożenie zarządzalnych urządzeń sieciowych dla punktów dostępowych	2 szt.
II.10	Dostawa i wdrożenie systemu NAC	1 szt.

II.11	Dostawa oprogramowania antywirusowego	1 szt.
II.12	Dostawa i podłączenie zasilacza awaryjnego UPS	1 szt.
II.13	Dostawa i wdrożenie oprogramowania SIEM	1 szt.
II.14	Dostawa i wdrożenie dedykowanego serwera do oprogramowania SIEM	1 szt.
II.15	Zakup usług SOC zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa	16 szt.
II.16	Szkolenie specjalistyczne dla administratorów z dostarczanych pakietów bezpieczeństwa i konfiguracji urządzeń i sieci dla urządzeń UTM	2 szt.
II.17	Szkolenie specjalistyczne dla administratorów z administracji dostarczanych systemów operacyjnych.	1 szt.

1. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości do siedziby Zamawiającego.
2. Wszystkie dostarczane:

- Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem Przedmiotu Zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach).
  - Komponenty (rozumiane jako integralna część dostawy i wdrożenia Przedmiotu Zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.
3. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie z zapisami niniejszego SOPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
  4. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami SOPZ oraz Umowy.
  5. Tam, gdzie w opisie przedmiotu zamówienia został wskazany znak towarowy (marka), producent, dostawca, patent, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty dostarczone przez konkretnego Wykonawcę lub nastąpiło wskazanie norm, europejskich ocen technicznych, wspólnych specyfikacji technicznych lub innych odniesień, o których mowa w art. 101 ust. 1 pkt 2 lub ust. 3 ustawy, Zamawiający zgodnie z art. 99 ust. 5 ustawy dopuszcza złożenie oferty równoważnej lub zgodnie z art. 101 ust. 4 ustawy zaoferowanie rozwiązań „równoważnych” w stosunku do wskazanych w opisie przedmiotu zamówienia pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych od założonych w SWZ.
  6. Wykonawca musi dostarczyć wszelkie urządzenia i elementy, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia, elementu i/lub licencji, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt.
  7. Wszelkie dostarczane urządzenia:
    - Muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych. Wszelkie dostarczane urządzenia muszą być wyprodukowane po dniu 1 stycznia 2024r.
    - Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
    - Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
    - Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.

- Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.

#### **I.4 Termin realizacji Przedmiotu Zamówienia**

Termin realizacji pierwszej części Przedmiotu zamówienia do 25 dni kalendarzowych od dnia zawarcia Umowy. Pierwsza część t.j.:

1. Dostawa i wdrożenie macierzy dyskowej wraz z konfiguracją funkcji HyperMirror i podłączeniem serwerów
2. Dostawa i wdrożenie serwera zapasowego

Pozostałe elementy zamówienia zostaną wykonane w terminie do 120 dni od zawarcia umowy zgodnie z ustalonym wcześniej harmonogramem.

Całości Przedmiotu zamówienia wynosi nie więcej niż **120 dni** kalendarzowych od dnia zawarcia Umowy.

#### **I.5 Organizacja wdrożenia**

Założenia podstawowe:

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram wdrożenia, który powinien być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia.
2. Wykonawca w Harmonogramie wdrożenia musi uwzględnić w szczególności podział na zadania takie jak projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji i wdrożeniu i testowaniu).
4. Wykonawca zobowiązany jest do udziału w cyklicznych naradach przeglądu prac przez Zamawiającego. Zamawiający przewiduje częstotliwość narad maksymalnie 1 raz w miesiącu, chyba że, nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań.
5. Wykonawca zobowiązany jest przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
6. W przypadku dostarczania Infrastruktury Serwerowej musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, pochodzić

z oficjalnych kanałów dystrybucji producentów i dostarczona w oryginalnych opakowaniach fabrycznych.

7. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
8. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
9. W ramach wdrożenia Wykonawca przygotowuje informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującą się realizacją Przedmiotu Zamówienia, w ramach której muszą zostać powołane minimum następujące role:
  - a. Kierownik Projektu ze strony Wykonawcy,
  - b. Zespół Wdrożeniowy ze strony Wykonawcy
10. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego.
11. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i interesantów urzędu.

## **I.6 Przygotowanie Dokumentacji**

1. W ramach procesu prac Wykonawca opracuje dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:
  - a) Harmonogram Wdrożenia.
  - b) Dokumentacja Analizy Przedwdrożeniowej (DAP).
  - c) Dokumentacja Powykonawcza.
2. Dokumentacja powyższa będzie zawierać bazowe zapisy opisujące budowane rozwiązania, procesy oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach Przedmiotu zamówienia. Dokumenty te wraz ze Specyfikacją Warunków Zamówienia wraz z załącznikami (dalej zwanych SWZ) będą stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia i DAP warunkuje rozpoczęcie prac Wykonawcy.
4. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z Harmonogramem wdrożenia zostaną opracowane w oparciu o wymagania określone w niniejszym OPZ.



## I.7 Analiza Przedwdrożeńiowa

1. Analiza przedwdrożeńiowa, którą należy rozumieć jako zakres czynności do wykonania przez Wykonawcę mający na celu analizę środowiska biznesowego i informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy Przedwdrożeńiowej Wykonawca przedstawi Zamawiającemu Dokumentację analizy przedwdrożeńiowej (zwana dalej DAP), na podstawie, której będzie realizowany organizacyjnie i technicznie Przedmiot Zamówienia. Dokumentacja Analizy Przedwdrożeńiowej będzie podlegała uzgodnieniu i akceptacji Zamawiającego.
2. Dokumentacja Analizy Przedwdrożeńiowej DAP powinna zawierać w szczególności:

SKŁAD DAP
ZARZĄDCZE
– plan i sposób komunikacji Stron
INFRASTRUKTURA SERWEROWA I SIECIOWA
– podział Przedmiotu Zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty
– analizę wymagań Przedmiotu Zamówienia zawierającą opis sposobu realizacji wymagań, sposób testowania i odbioru
– karty katalogowe urządzeń potwierdzające spełnienie wymagań
– plan dostaw
– opis instalacji i wdrożenia oprogramowania wdrażanego wraz z Infrastrukturą
– Wykonawca określi w Analizie przedwdrożeńiowej systemy, które będą objęte systemem SIEM, centralnym systemem zbierania logów oraz systemem monitorowania infrastruktury informatycznej
– Dla każdego systemu cyberbezpieczeństwa Wykonawca opracuje:
– Architekturę rozwiązania
– Wersje oprogramowania wchodzące w skład Systemu
– Konfigurację Systemu
– Zastosowane licencje/subskrypcje.
– Procedura testowania – scenariusze testowe dla wdrażanych systemów
– harmonogram instruktażu personelu oraz administratorów

## **I.8 Harmonogram wdrożenia**

Wykonawca zobowiązany jest opracować na podstawie SWZ oraz SOPZ szczegółowy harmonogram wdrożenia. Harmonogram należy przedstawić Zamawiającemu w terminie do 14 dni od podpisania Umowy.

## **I.9 Dokumentacja Powykonawcza**

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. Wykonawca wraz z dokumentacją powykonawczą dostarczy propozycję scenariuszy testowych, które będą podlegały akceptacji Zamawiającego.
4. W szczególności dokumentacja ta powinna zawierać następujące elementy:
  - a. Schemat infrastruktury i architekturę rozwiązania wraz z opisem.
  - b. Zasady licencjonowania dostarczonych elementów.
  - c. Konfigurację sprzętową i logiczną elementów infrastruktury dla wdrożonych systemów.
  - d. Procedury uruchamiania, zatrzymywania wdrożonych systemów oraz elementów infrastruktury.
  - e. Procedury konfiguracji kont w dostarczonych systemach.
  - f. Procedury awaryjne umożliwiające dostęp do infrastruktury w przypadku awarii.
  - g. Procedury opisujące standardowe działania administracyjne.
  - h. Procedury odzyskania wdrożonych systemów po awarii.
  - i. Wytyczne (dobre praktyki) dla administratorów.
  - j. Spis dokumentacji zewnętrznej do której odwołuje się Dokumentacja Powykonawcza.

## **I.10 Odbiór Dokumentacji/Końcowy**

1. Odbiór końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy oraz dostarczenia wymaganej zamówieniem Dokumentacji.
2. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej Załącznik nr 9 do SWZ.

## **I.11 Testy**

1. W ramach postępowania zostaną przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji Przedmiotu Zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób lub podmiotów zewnętrznych.
2. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad jest niezbędne, aby dla poszczególnych Komponentów oraz całego Przedmiotu Zamówienia dokonać odbiorów w ramach poszczególnych Etapów i Odbioru końcowego.
3. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. Koszt zewnętrznego audytora będzie kosztem Zamawiającego. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
4. Zamawiający w końcowej fazie wdrożenia oczekuje realizacji przez Wykonawcę testów bezpieczeństwa.
5. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed odbiorem Końcowym Przedmiotu Zamówienia.
6. Zamawiający wymaga, aby Wykonawca przeprowadził testy odbiorcze co najmniej z zakresu:
  - a) Uruchamianie i zatrzymywanie wdrożonych systemów
  - b) Weryfikacja wdrożonych systemów zgodnie ze scenariuszami opisanymi w dokumentacji.
  - c) Weryfikacja poprawności działania procedur.
  - d) Symulację awarii wdrożonych systemów.

## **I.12 Dodatkowe zobowiązania Wykonawcy**

1. Wykonanie Przedmiotu Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
2. Wykonanie w całości Przedmiotu Zamówienia w zakresie określonym w Umowie będącej Załącznikiem nr 9 do SWZ.
3. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającym na każdym etapie realizacji.
4. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.

- 
5. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
  6. Współdziałanie z osobami wskazanymi przez Zamawiającego.

## **Rozdział II. Szczegółowy opis przedmiotu zamówienia**

### **II.1 Dostawa i wdrożenie infrastruktury sprzętowej i oprogramowania**

1. Jeżeli zajdzie potrzeba, wraz z dostarczaną Infrastrukturą, Wykonawca zobowiązany jest dostarczyć niezbędne elementy np. urządzenia i wyposażenie – kable połączeniowe, elementy mocujące, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie dostarczanej infrastruktury. Dostarczona Infrastruktura musi zapewniać bezproblemową pracę po podłączeniu do sieci informatycznej Zamawiającego.
2. Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury oraz oprogramowania w miejscach wskazanych przez Zamawiającego.
3. Wszystkie elementy Infrastruktury serwerowej powinny zostać zamontowane w szafie serwerowej rack, w sposób umożliwiający ich prawidłową wentylację. Jeżeli zajdzie potrzeba wykonawca zobowiązany jest dostarczyć wszelkie niezbędne elementy zapewniające montaż w szafie rack.
4. Szczegóły dotyczące instalacji i uruchomienia Infrastruktury zostaną ustalone w trakcie Analizy Przedwdrożeniowej.

Po zakończonym montażu Wykonawca przekaze Zamawiającemu wszystkie hasła dostępne do kont „super użytkowników” oraz dokumentację do wszystkich oferowanych urządzeń, oprogramowania narzędziowego (systemowego, bazodanowego, wirtualizacyjnego, backupowego itd.) wraz z dokumentami potwierdzającymi nabycie dla Zamawiającego licencji oraz nośnikami danych zawierającymi zainstalowane oprogramowanie (o ile dostarcza je producent). Wykonawca wykona również instruktaże użytkowe dla wskazanych przez Zamawiającego administratorów, z zakresu konfiguracji, obsługi i prawidłowej eksploatacji zainstalowanego Sprzętu.

### **II.2 Dostawa i wdrożenie urządzenia UTM – 1 szt.**

Wykonawca w ramach realizacji Przedmiotu Umowy dokona wdrożenia i uruchomienia systemu w stanie kompletnym.

Osoba realizująca usługi wdrożenia i uruchomienia systemu musi być ekspertem w obszarze związanym z technologią bezpieczeństwa sieci oraz legitymować się ważnym i aktualnym certyfikatem technicznym oferowanym w ramach certyfikacji Producenta oferowanego rozwiązania Next Generation Firewall oraz musi posiadać dostęp do bazy wiedzy tego Producenta.

W ramach wdrożenia Zamawiający wymaga co najmniej następujących czynności:

1. Wykonawca zapewni obecność w miejscu instalacji Urządzeń wykwalifikowanej osoby (inżyniera) podczas wdrożenia i uruchomienia systemu.
2. Wykonawca przeprowadzi analizę infrastruktury sieciowej (optymalizacja zgodna z aktualnymi trendami panującymi w sferze zagrożeń sieciowych i możliwościami systemu)
3. Wykonawca przygotuje środowisko: rejestracja i uruchomienie urządzeń, instalacja licencji, aktualizacja oprogramowania.
4. Wykonawca dokona konfiguracji Urządzeń co najmniej według poniższych wytycznych:
  - a. konfiguracja zarządzania, skomunikowanie z siecią Zamawiającego z wykorzystaniem wskazanych adresów IP dla interfejsów;
  - b. analiza polityki bezpieczeństwa na produkcyjnej zaporze sieciowej i konfiguracja wdrażanego systemu odpowiednich reguł dotyczących:
    - Konfiguracja sieci (interfejsy i routing).
    - Konfiguracja firewalla (w zakres wchodzi również blokowanie ruchu z adresów IP zdefiniowanych/zakwalifikowanych jako botnet, malware, spam, phishing, tor, domen które są uznawane przez CERT jako niebezpieczne. Pełna lista zostanie uzgodniona podczas analizy przedwdrożeniowej)
    - Konfiguracja NAT
    - Konfiguracja VLAN
    - Konfiguracja IPS – zgodnie z wymaganiami klienta.
    - Konfiguracja inspekcji HTTPS wraz z konfiguracją odpowiednich profili (IPS, filtra URL) dla stacji roboczych / serwerów. Jeśli wymagana będzie dodatkowa konfiguracja stacji roboczych/serwerów wykonawca
    - Konfiguracja dodatkowych usług sieciowych tj. DHCP, DNS Proxy.
    - Integracja z AD lub założenie wewnętrznej bazy użytkowników (bez dodawania użytkowników).

- 
- Konfiguracja dostawców Internetu (maksymalnie 2 dostawców).
  - Konfiguracja transparentnej autoryzacji w Active Directory
  - Dodanie do konfiguracji urządzenia wszystkich obiektów sieciowych uruchomionych w ramach sieci zamawiającego (stacje robocze, serwery, telefony IP, itp.) wraz z odpowiadającymi im adresami mac.
  - Konfiguracja systemu logowania dla urządzenia UTM, które umożliwią przechowywanie logów poza urządzeniem oraz ich łatwe przeglądanie, agregowanie poprzez interface graficzny. Wykonawca skonfiguruje odpowiednie rozwiązanie na wskazanej przez zamawiającego maszynie (fizycznej lub wirtualnej)
  - Konfiguracja urządzenia ma zostać dostarczona opisana w kodzie, tj. akceptowane jest przygotowanie odpowiednich skryptów pythona, ansible.
  - Konfiguracja powiadomień na email administratorów w przypadku występowania alarmów / niebezpieczeństw wykrytych przez urządzenie.
  - Konfiguracja SNMP v3 umożliwiające monitorowanie urządzenia liczników wydajnościowych.
- c. Konfiguracja VPN:
- IPSec Site-to-Site (limit 10 tuneli)
  - SSL VPN (na wszystkich wskazanych przez zamawiającego urządzeniach)
  - przekazanie Zamawiającemu wszystkich haseł do systemu.
5. Kopia bezpieczeństwa konfiguracji wdrożonych urządzeń.
  6. Instruktarz obsługi urządzenia z wykorzystaniem GUI.
  7. Przygotowanie i przekazanie zamawiającemu procedury zgłaszania problemów do serwisu.

Minimalne wymagania dla urządzenia:

## ARCHITEKTURA SYSTEMU

1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającą rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności co najmniej Active-Passive, o specyfikacji opisanej poniżej
2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe.
3. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.

1. Metalowa obudowa o wysokości max. 1U przeznaczona do montażu w szafie RACK 19"
2. Podwójne, redundantne, zintegrowane zasilanie.
3. Obsługa nielimitowanej ilości hostów w sieci chronionej.
4. Minimalna liczba i typ interfejsów fizycznych:
  - System realizujący funkcję Firewall musi mieć wbudowanych minimum 8 interfejsów miedzianych Ethernet 2,5 Gbps
  - System realizujący funkcję Firewall musi mieć wbudowane minimum 2 interfejsy optyczne 1Gbit SFP
  - System realizujący funkcję Firewall musi mieć wbudowane minimum 4 interfejsy optyczne 10Gbit SFP+
  - System realizujący funkcję Firewall musi umożliwiać rozbudowę dostępnych interfejsów
  - Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
5. Minimalna liczba nowych połączeń na sekundę: 30 000
6. Minimalna liczba jednoczesnych połączeń: 600 000
7. Minimalna przepustowość Firewall: 10 Gbps
8. Minimalna przepustowość IPS: 5 Gbps
9. Minimalna przepustowość Threat Protection: 1,3 Gbps
10. Minimalna przepustowość IPSec VPN: 2,5 Gbps
11. Minimalna liczba tuneli SSL VPN: 150
12. Minimalna liczba tuneli IPSEC VPN: 1000
13. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania



## PODSTAWOWE FUNKCJE SYSTEMU OCHRONY

### Zarządzanie i utrzymanie

1. Rozwiązanie musi być zarządzane przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH.
2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping
3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego
7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników.
8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.
9. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP
10. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3
11. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie.
12. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)

<b>Zapora sieciowa, konfiguracja sieciowa oraz routing</b>	<ol style="list-style-type: none"> <li>1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.</li> <li>2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia</li> <li>3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.</li> <li>4. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading.</li> <li>5. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection).</li> <li>6. System musi zapewniać ochronę przed skanowaniem portów (portscan blocking).</li> <li>7. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).</li> <li>8. Rozwiązanie musi zapewniać obsługę routingu statycznego.</li> <li>9. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP).</li> <li>10. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP.</li> <li>11. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay.</li> <li>12. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP.</li> <li>13. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łączy.</li> <li>14. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP.</li> <li>15. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe .</li> <li>16. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).</li> </ol>
--	--

	<p>17. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza.</p> <p>18. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).</p> <p>19. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług.</p> <p>20. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.</p> <p>21. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.</p>
<b>Podstawowe kształtowanie pasma oraz limity ilości danych</b>	<p>1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia.</p> <p>2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.</p>
<b>Autoryzacja użytkowników</b>	<p>1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.</p> <p>2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP</p> <p>3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory</p> <p>4. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.</p> <p>5. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal.</p> <p>6. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).</p> <p>7. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.</p>

<b>Samoobsługowy portal dla użytkowników</b>	<ol style="list-style-type: none"> <li>1. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).</li> <li>2. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android</li> <li>3. Rozwiązanie musi umożliwiać zmianę hasła.</li> </ol>
<b>Podstawowe opcje VPN</b>	<p>System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:</p> <ol style="list-style-type: none"> <li>1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)</li> <li>2. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).</li> </ol>
<b>OCHRONA SIECI</b>	
<b>IPS</b>	<ol style="list-style-type: none"> <li>1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur.</li> <li>2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS.</li> <li>3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.</li> <li>4. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur</li> <li>5. System musi generować alerty w przypadku wykrycia ataku.</li> <li>6. System bezpieczeństwa musi posiadać moduł wykrywania typu oprogramowania sieciowego, które jest uruchomione na stacjach roboczych w obrębie chronionej sieci i komunikuje się z siecią Internet. W przypadku kiedy system nie posiada wbudowanego modułu wykrywania typu oprogramowania sieciowego musi być dostarczony zewnętrzny system w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej. Moduł ma nie tylko wykrywać uruchomione oprogramowanie sieciowe, ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu przykładowo poprzez opis wskazanej podatności lub oznaczenie ryzyka związanego z działaniem aplikacji za pomocą skali lub kolorów</li> </ol>

<b>OCHRONA I KONTROLA WEB ORAZ APLIKACJI</b>	
<b>Ochrona i kontrola Web</b>	<ol style="list-style-type: none"> <li>1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.</li> <li>2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.</li> <li>3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym z wykorzystaniem komercyjnego antywirusa.</li> <li>4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów.</li> <li>5. System musi filtrować pliki na podstawie MIME.</li> <li>6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.</li> <li>7. Rozwiązanie musi zawierać przynajmniej 65 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.</li> <li>8. Rozwiązanie musi zapewniać możliwość blokowania i wysyłania treści poprzez HTTP i HTTPS.</li> <li>9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.</li> </ol>
<b>Ochrona i kontrola aplikacji</b>	<ol style="list-style-type: none"> <li>1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji.</li> <li>2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook)</li> <li>3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.</li> </ol>
<b>Kształtowanie pasma dla Web i Aplikacji</b>	<ol style="list-style-type: none"> <li>1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download.</li> <li>2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.</li> <li>3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.</li> </ol>

<b>OCHRONA ANTYWIRUSOWA</b>	
<b>Ochrona i kontrola Email</b>	<ol style="list-style-type: none"><li>1. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy</li><li>2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.</li><li>3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.</li><li>4. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń.</li><li>5. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników.</li><li>6. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL.</li><li>7. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email.</li><li>8. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.</li></ol>
<b>OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY</b>	
<b>On-cloud Sandboxing</b>	<p>Rozwiązaniem musi dawać możliwość rozbudowy o dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności:</p> <ol style="list-style-type: none"><li>1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe</li><li>2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf.</li><li>3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf.</li><li>4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab</li><li>5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows .</li></ol>
<b>LOGOWANIE I RAPORTOWANIE</b>	

1. System musi umożliwiać składowanie oraz archiwizację logów.
2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.
3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
5. Rozwiązanie musi generować raporty w HTML i CSV.
6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog.
7. System musi zapewniać podgląd wykorzystania łącza internetowego.
8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP
9. Rozwiązanie musi oferować możliwość zanonimizowania danych.

**POZOSTAŁE****Certyfikaty**

Urządzenie musi posiadać:

- certyfikat Common Criteria;
- certyfikat ICSSA Labs dla funkcji VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE;

**GWARANCJA I SERWIS**

Wymagania ogólne dla dostarczanych rozwiązań:

- Dostarczone urządzenia muszą być fabrycznie nowe, nieużywane w innych projektach, nie wycofane z produkcji i pochodzić z legalnego, polskiego kanału dystrybucji.
- Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów na teren Polski – ze względów gwarancyjnych niedopuszczalne jest dostarczanie sprzętu z tzw. brokerki,
- Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie zapisanym w specyfikacjach sprzętu,
- Całość dostarczonego sprzętu i oprogramowanie musi być ze sobą kompatybilna i pochodzić od jednego producenta,
- Wykonawca winien w momencie dostawy przedłożyć dokumenty potwierdzające, że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

#### Warunki gwarancji i serwisu:

- Na dostarczany sprzęt musi być udzielona **min. 24-miesięczna gwarancja**; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była wymiana urządzeń zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań,
- Wykonawca lub autoryzowany serwis ma obowiązek przyjmowania zgłoszeń serwisowych w języku polskim przez telefon (od poniedziałku do piątku, w godzinach 8-17), e-mail lub WWW (przez całą dobę),

#### Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiające:

- bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania gwarancji i licencji
- dostęp do dokumentacji sprzętu i oprogramowania,
- dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
- dostęp do pomocy technicznej producenta.
- Zamawiający w momencie odbioru otrzyma:
- licencje obejmujące wszystkie wymagane moduły na okres **min. 24 miesięcy**
- możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji.



### II.3 Dostawa i wdrożenie macierzy dyskowej wraz z konfiguracją funkcji HyperMirror i podłączeniem serwerów – 1 szt.

Zamawiający użytkuje obecnie macierz Huawei OceanStor 2600 V5. Należy dostarczyć drugą macierz umożliwiającą uruchomienie funkcjonalności klastrowania macierzy dyskowych: posiadanej oraz nowo dostarczonej. Kłaster złożony z dwóch macierzy ma na celu wyeliminować pojedynczy punkt awarii w infrastrukturze Zamawiającego. Jako rozwiązanie równoważne Wykonawca może dostarczyć 2 nowe macierze pracujące w trybie klastra odpornego na awarię jednej z macierzy i nieprzerwaną pracę sprawnej macierzy. Wymagania minimalne dla macierzy dyskowej przedstawiono poniżej:

LP	CECHA	OPIS WYMAGAŃ
1)	Obudowa	Obudowa do montażu w szafie rack 19" za pomocą dostarczonych dedykowanych elementów. Oferowana macierz nie może przekroczyć rozmiaru 4U.
2)	Kontrolery dyskowe	Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active-active. Kontrolery nie mogą pracować w trybie active-passive. Macierz nie może posiadać pojedynczego punktu awarii (SPOF), który powodowałby brak dostępu do danych.
3)	CPU	Wymagany min 1 procesor per kontroler min 8 rdzeni każdy. Macierz musi dostarczać sumarycznie min 16 rdzeni.
4)	Wymagana przestrzeń	Fizyczna przestrzeń dyskowa zbudowana za pomocą dysków SSD, SAS. Zainstalowanych min. 24 dysków o pojemności min. 4TB każdy. Wymagana możliwość rozbudowy przestrzeni użytkowej do 500 TB poprzez instalację dysków oraz półek dyskowych. Rozbudowa musi być wykonywana w sposób online, bez przerwy w dostępie do danych.
5)	Zabezpieczenia dyskami SPARE	Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.
6)	Pamięć Cache	Co najmniej 32GB pamięci cache na całą macierz (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii

LP	CECHA	OPIS WYMAGAŃ
		zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin.
7)	Dostępne interfejsy	Razem kontrolery muszą udostępnić do hostów minimum 4 porty 1Gb Eth oraz 4 porty 10Gb Eth SFP+ (wymagane wkładki optyczne). Wymagana możliwość rozbudowy o dodatkowe 8 portów 25Gb Eth SFP+ tylko poprzez instalację dodatkowych kart sieciowych.
8)	Obsługiwane protokoły	Wymagane wsparcie dla FC, iSCSI, NFS, CIFS. Nie dopuszcza się wsparcia dla protokołów plikowych poprzez zastosowanie dodatkowego gateway'a / główki NAS. Protokoły NFS i CIFS muszą być natywnie wspierane przez oferowaną macierz.
9)	Obsługiwane typy zabezpieczenia RAID	Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków bez utraty danych.
10)	Prezentacja dysków logicznych	Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Wymagane dostarczenie w/w funkcjonalność na zainstalowaną przestrzeń dyskową. Max liczba wolumenów blokowych (LUN) obsługiwanych przez macierz nie może być mniejsza niż 2000. Max liczba file system'ów (NAS) obsługiwanych przez macierz nie może być mniejsza niż 500.
11)	Zarządzanie	Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności dysków SSD SAS. Wymagane jest stałe monitorowanie wydajności obiektów takich jak: - cała macierz

LP	CECHA	OPIS WYMAGAŃ
		<ul style="list-style-type: none"> <li>- kontrolery</li> <li>- porty front-end</li> <li>- dyski</li> <li>- LUNy</li> <li>- file systemy</li> <li>- hosty</li> </ul> <p>Pod kątem parametrów takich jak:</p> <ul style="list-style-type: none"> <li>- operacje wejścia/wyjścia IOPS</li> <li>- przepustowość (KB/s lub MB/s)</li> <li>- czas odpowiedzi (latency)</li> <li>- średnie użycie CPU (w %)</li> </ul> <p>Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.</p>
12)	Kopie wewnętrzne macierzy	<p>Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) wolumenów blokowych (LUN) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych lub testów. Snapshoty muszą być wykonywane w technologii ROW (Redirect On Write). Wymagana jest możliwość utworzenia harmonogramu snapshotów. Macierz musi umożliwiać utworzenie min 2000 snapshotów wolumenów blokowych (LUN). Musi być możliwość utworzenia snapshotów których nie można modyfikować ani usunąć przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware.</p> <p>Wymagana również obsługa snapshotów file systemów.</p>

LP	CECHA	OPIS WYMAGAŃ
		<p>Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model macierzy.</p> <p>Wymagana możliwość tworzenia na żądanie kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wymagane możliwość resynchronizacji klona z wolumenem źródłowym (LUN). Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.</p>
13)	Kontrola zasobów plikowych (NAS)	<p>Wymagana możliwość skonfigurowania tzw. quote ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni, z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni.</p> <p>Wymagana możliwość konfiguracji uprawnień użytkowników typu read-only oraz read-write per wystawiony udział NAS.</p> <p>Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania.</p>
14)	Ochrona plików	<p>Wymagana możliwość skonfigurowania funkcjonalności typu WORM, która blokuje pliki przed usunięciem lub modyfikacją. Zabezpieczone pliki mają pozostać tylko do odczytu przez skonfigurowany okres czasu. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.</p>
15)	Tiering	<p>Macierz musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych bez konieczności rekonfiguracji po stronie serwerów korzystających z wolumenów logicznych. Jeżeli funkcjonalność wymaga licencji należy ją dostarczyć wraz z macierzą.</p>
16)	Replikacja danych	<p>Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybach synchroniczna oraz asynchroniczna przy wykorzystaniu portów FC lub IP. Jeżeli funkcjonalność wymaga licencji należy ją dostarczyć wraz z macierzą.</p>

LP	CECHA	OPIS WYMAGAŃ
17)	Klaster macierzowy	Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage Metro Cluster). Macierz musi dostarczać funkcjonalność klastra "wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform oprogramowania i sprzętowych z wykorzystaniem synchronicznej replikacji danych przy wykorzystaniu portów FC lub IP pomiędzy 2 macierzami. Pod użytym pojęciem "wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy (macierz preferowana) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodujących dla danego środowiska brak dostępu do zasobów macierzy preferowanej. Funkcjonalność klastra "wysokiej dostępności" pozwala na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy preferowanej na niepreferowaną w przypadku awarii macierzy preferowanej (tzw. automated failover). Wymagany jest również automatyczny failover z macierzy niepreferowanej na preferowaną. Jeżeli funkcjonalność wymaga licencji należy ją dostarczyć wraz z macierzą.
18)	Priorytety zadań	Macierz musi posiadać możliwość zapewnienia ciągłości biznesu na oczekiwanym poziomie usług (QoS) poprzez definicję polityk QoS w oparciu o maksymalne progi wydajności IOPS i MB/s. Musi istnieć możliwość określenia polityk QoS na poziomie wolumenów. Jeżeli funkcjonalność wymaga licencji należy ją dostarczyć wraz z macierzą.
19)	Wspierane systemy operacyjne	Wsparcie, dla co najmniej Microsoft Server Windows 2016/2019, VMware 7.x/8.x, Linux RedHat 7.x/8.x, CentOS 7.x/8.x
20)	Serwisowalność	Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączenia.

LP	CECHA	OPIS WYMAGAŃ
		<p>Macierz musi umożliwiać zdalne zarządzanie.</p> <p>Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.</p> <p>Wymagana gwarancja na 3 lata w trybie 9x5 NBD onsite.</p>

#### II.4 Dostawa i wdrożenie serwera zapasowego – 1 szt.

Dostawa, instalacja w szafie rack, instalacja hypervizora, konfiguracja do pracy w sieci LAN Zamawiającego, podłączenie redundantne serwera do rdzenia sieci, podłączenie serwera do zasobów macierzy, konfiguracja klastra wirtualnego.

W ramach instalacji serwera wirtualizacji należy:

- zainstalować, skonfigurować oraz zaaktualizować wszystkie instancję maszyn OSS, zakres konfiguracji oraz wymagania dotyczące poszczególnych systemów operacyjnych zostanie przekazana wykonawcy na etapie wdrożenia.
- należy zainstalować, skonfigurować i zabezpieczyć dwa nowe kontrolery domeny, przygotować odpowiednie polityki haseł, konfigurację obiektów Group policy.. Wymagane konfiguracje będą ustalone na etapie wdrożenia z zamawiającym.
- konfiguracja serwerów DNS zintegrowanych z kontrolerami domeny
- konfiguracja serwerów radius wykorzystywanych do autoryzacji użytkowników administracyjnych do urządzeń sieciowych

- W ramach wdrożenia nowej domeny należy prze-migrować użytkowników wraz z profilami, utworzyć grupy, przenieść komputery oraz obecnie używane zasoby.
- dla zasobów urządzeń należy wygenerować certyfikaty SSL w oparciu o wewnętrzne CA lub dostarczyć odpowiednie certyfikaty SSL. Urządzenia sieciowe, serwery, macierze i usługi wewnętrzne mają legitymować się odpowiednimi wygenerowanymi certyfikatami w ramach wdrożenia.
- należy zainstalować, skonfigurować serwer plików, udziały sieciowe. Wszystkie wskazane zasoby zamawiającego należy prze migrować na nowy serwer
- obecnie wykorzystywane zgodnie z wytycznymi zamawiającego przenieść na nową infrastrukturę. Zakres zostanie uzgodniony na etapie wdrożenia z zamawiającym.
- należy zaaktualizować system operacyjny obecnie wykorzystywanego serwera wirtualizacji do najnowszej wersji
- systemy operacyjne należy w uzgodnieniu z zamawiającym przydzielić do odpowiednich usług, tak żeby rozdzielić i nie instalować kilku ról różnego typu na tej samej instancji systemu operacyjnego
- systemy operacyjne zostaną zaadresowane w odpowiednich nowo powstałych vlanach, przygotowanych przez wykonawcę w uzgodnieniu z zamawiającym na etapie wdrożenia w celu segmentacji serwerów oraz stacji roboczych.
- należy dostarczyć rozwiązanie umożliwiające monitoring dostępności wymaganych liczników uzgodnionych w ramach wdrożenia z wykonawcą zasobów (urządzeń sieciowych, systemów operacyjnych) z możliwością wysyłania powiadomień do różnych grup użytkowników w zależności od tego jak istotne jest urządzenie/zdarzenie.
- system monitoringu musi zapewniać:

\*Monitorowania serwerów fizycznych.

- Monitorowania urządzeń sieciowych.
  - Monitorowania stanu połączeń.
  - Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów
  - Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux.
  - Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń.
  - Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu.
  - Grupowanie hostów.
  - Definiowanie planowanych przerw serwisowych dla hostów i usług.
  - Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).
  - Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień, konfiguracje przerw serwisowych).
  - Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).
  - Monitorowanie serwerów za pomocą agentów
- \* Monitorowanie Active Directory.
  - Monitorowanie serwerów plików, udziałów sieciowych.
  - Monitorowanie statusu serwerów Apache.
  - Monitorowanie baz danych (MySQL, Postgres, MSSQL Server)
  - Monitorowanie urządzeń przez następujące protokoły (SNMP, WMI, IPMI)
  - Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW.
  - Monitorowanie poprawności działania DNS.
  - Monitorowanie środowiska VMware.
  - Monitorowanie środowiska Hyper-V.
  - Monitorowanie działania serwera czasu NTP.
  - Monitorowanie offsetu czasu na serwerach.
  - Monitorowanie ping - czasy odpowiedzi, straty pakietów.
  - Monitorowanie zajętości miejsca na poszczególnych partycjach.
- \* Monitorowanie obciążenia dysków.
  - Monitorowanie wykorzystania pamięci RAM.
  - Monitorowanie obciążenia CPU.
  - Monitorowanie logów systemowych Windows.



- Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia.
- Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane.

Dostawca skonfiguruje monitoring dostarczonych elementów oraz wskazanych przez zamawiającego urządzeń, systemów, elementów infrastruktury obecnie wykorzystywanej wskazanej na etapie wdrożenia przez zamawiającego. Zostanie przygotowana przez dostawcę mapa umożliwiająca łatwy przegląd monitorowanej infrastruktury. Mapa będzie zawierać monitorowane urządzenia. Jeśli jedna mapa nie będzie wystarczająca by w czytelny i łatwy do zrozumienia przedstawić infrastrukturę, wtedy należy sporządzić kilka map z odpowiednim podziałem np. maszyny wirtualne, ad, maszyny fizyczne, urządzenia sieciowe itd.

- wykonawca dostarczy oraz skonfiguruje kolektor logów SIEM, rozwiązanie zapewnia zbieranie logów z systemów Linux, Windows oraz urządzeń sieciowych, analizę logów poprzez interface web, detekcję podatności na hostach, system umożliwia weryfikację zgodności z przepisami PCI DSS, NIST 800-53, GDPR, TSC SOC2, and HIPAA, File Integrity Monitoring (FIM) czyli umożliwiać konfigurację monitorowania integralności plików systemowych i aplikacji. Dostawca rozwiązania skonfiguruje kompleksowo system SIEM. Jeśli wymagana jest instalacja agentów na wszystkich stacjach roboczych / serwerach zostanie ona przeprowadzona w ramach wdrożenia. Serwerowe systemy operacyjne zostaną skonfigurowane tak aby wysyłać zdarzenia bezpieczeństwa oraz inne wskazane przez zamawiającego (uzgodnione na etapie wdrożenia) Przełączniki oraz urządzenia sieciowe również wchodzi w zakres wdrożenia. Dostawca przeprowadzi kompleksową konfigurację. Konfiguracja uzgodniona w ramach wdrożenia z zamawiającym.

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami umożliwiającymi wysunięcie i wszystkimi elementami niezbędnymi do zamontowania serwera w szafie).
Procesor	Procesor max. 16 rdzeniowy, osiągający w teście SPECrate®2017_int_base wynik co najmniej 174 punktów. Płyta główna obsługująca procesory od 16 do 128 rdzeni, wymagających mocy 400W i obsługujących do 3TB pamięci RAM.

Zainstalowane procesorów	1
Pamięć operacyjna	Zainstalowanych min. osiem modułów 32 GB DDR5 4800MT/s. Płyta główna z minimum 12 slotami na pamięć, umożliwiającą instalację do minimum 3TB pamięci RAM, obsługująca moduły 4800 MT/s Obsługa zabezpieczeń: Advanced ECC.
Sloty rozszerzeń	Możliwość instalacji 2 kart PCI-Express generacji 5, x16(szybkość slotu – bus width), min. 1 karty pełnej wysokości (full height).
Dysk twardy	Możliwość instalacji do 10 dysków. Zainstalowane min. 2 dyski SSD 240GB pracujące w konfiguracji ze sprzętowym RAID 1.
Interfejsy sieciowe	Zainstalowane dwie karty dwuportowe 10/25Gb SFP28 wraz z 4 modułami SFP+ SR oraz przewodami połączeniowymi.
Karta graficzna	Zintegrowana karta graficzna z pamięcią min. 16 MB, umożliwiającą wyświetlenie obrazu min. 1920 x 1200@60Hz
Porty	Min. 2x USB 3.2 (w tym min. 1 port wewnętrzny i 1 z przodu obudowy), min. 2x USB 3.1 z tyłu obudowy, min. 1 port VGA, port USB dedykowany dla modułu zarządzającego z przodu obudowy. Możliwość rozbudowy/rekonfiguracji o port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express  1x port RJ-45 dedykowany dla interfejsu zdalnego zarządzania
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy max. 1000W, efektywność zasilaczy 94%
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Rozwiązanie sprzętowe, niezależne od

	<p>systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja.</p>
<p>Karta/moduł zarządzający i system zarządzania</p>	<p>Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:</p> <ul style="list-style-type: none"> <li>• monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe</li> <li>• praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP</li> <li>• dostęp do karty zarządzającej poprzez <ul style="list-style-type: none"> <li>- dedykowany port RJ45 z tyłu serwera lub</li> <li>- przez współdzielony port zintegrowanej karty sieciowej serwera</li> </ul> <p>dostęp do karty możliwy</p> <ul style="list-style-type: none"> <li>- z poziomu przeglądarki webowej (GUI)</li> <li>- z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)</li> <li>- z poziomu skryptu (XML/Perl)</li> <li>- poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)</li> </ul> </li> <li>• wbudowane narzędzia diagnostyczne</li> <li>• zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego</li> </ul>

- obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przysyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
- wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
- przysyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
- obsługa zdalnego serwera logowania (remote syslog)
- wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów
- mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii oraz ostatniego startu serwera a także nagrywanie na żądanie
- funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności
- monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
- konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
- zdalna aktualizacja oprogramowania (firmware)
- zarządzanie grupami serwerów, w tym:
  - tworzenie i konfiguracja grup serwerów
  - sterowanie zasilaniem (wł/wył)
  - ograniczenie poboru mocy dla grupy (power capping)
  - aktualizacja oprogramowania (firmware)
  - wspólne wirtualne media dla grupy
- możliwość równoczesnej obsługi przez 6 administratorów
- autentykacja dwuskładnikowa (Kerberos)

	<ul style="list-style-type: none"> <li>wsparcie dla Microsoft Active Directory</li> <li>obsługa SSL i SSH</li> <li>enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli</li> <li>wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API</li> <li>wsparcie dla Integrated Remote Console for Windows clients</li> <li>możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)</li> </ul>
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	<p>Microsoft Windows Server 2022</p> <p>Red Hat Enterprise Linux (RHEL) 8.0</p> <p>SUSE Linux Enterprise Server (SLES) 15</p> <p>VMware ESXi 6.7 U3</p>
Wyposażenie dodatkowe	<p>Napęd USB z 2 nośnikami wymiennymi o pojemności 4TB każdy do tworzenia kopii zapasowej maszyn wirtualnych.</p>
Gwarancja	<p>Minimum 3-letnia gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site z 2-godzinnym czasem reakcji.</p> <p>Przybycie na miejsce w następnym dniu roboczym. Czas reakcji na zdarzenia krytyczne do 2 godzin. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.</p> <p>Możliwość rozszerzenia usługi gwarancyjnej do 5 lat realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy 6 godzin i pozostawieniem uszkodzonych dysków u zamawiającego.</p>
Inne	<p>Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.</p> <p>Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.</p>

Oprogramowanie	<p>Serwerowy System Operacyjny (SSO) spełniające poniższe wymagania minimalne:</p> <p>Dostarczone licencje muszą uprawniać do uruchamiania min. ośmiu maszyn wirtualnych oferowanego systemu operacyjnego dla 1 procesora o 16 rdzeniach. Równoważny system operacyjny musi posiadać następujące, wbudowane cechy:</p> <ol style="list-style-type: none"><li>1. możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,</li><li>2. możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,</li><li>3. możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,</li><li>4. możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,</li><li>5. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,</li><li>6. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,</li><li>7. automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),</li><li>8. wbudowane wsparcie instalacji i pracy na wolumenach, które:<ul style="list-style-type: none"><li>– pozwalają na zmianę rozmiaru w czasie pracy systemu,</li><li>– umożliwiają tworzenie w czasie pracy systemu migawek, dających</li></ul></li></ol>
----------------	--

	<p>użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</p> <ul style="list-style-type: none"><li>– umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,</li><li>– umożliwiają zdefiniowanie list kontroli dostępu (ACL),</li></ul> <p>9. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,</p> <p>10. wbudowane szyfrowanie dysków</p> <p>11. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,</p> <p>12. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,</p> <p>13. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,</p> <p>14. graficzny interfejs użytkownika,</p> <p>15. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,</p> <p>16. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play),</p> <p>17. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,</p> <p>18. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,</p> <p>19. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <ul style="list-style-type: none"><li>– podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,</li><li>– usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udział sieciowy), z możliwością wykorzystania następujących funkcji:<ul style="list-style-type: none"><li>a) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,</li></ul></li></ul>
--	--

	<ul style="list-style-type: none"><li>b) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,</li><li>c) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,</li></ul> <ul style="list-style-type: none"><li>– zdalna dystrybucja oprogramowania na stacje robocze,</li><li>– praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,</li><li>– centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:<ul style="list-style-type: none"><li>a) dystrybucję certyfikatów poprzez http,</li><li>b) konsolidację CA dla wielu lasów domeny,</li><li>c) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,</li></ul></li><li>– szyfrowanie plików i folderów,</li><li>– szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),</li><li>– możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,</li><li>– serwis udostępniania stron WWW,</li><li>– wsparcie dla protokołu IP w wersji 6 (IPv6),</li><li>– wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:<ul style="list-style-type: none"><li>a) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,</li><li>b) obsługi ramek typu jumbo frames dla maszyn wirtualnych,</li><li>c) obsługi 4-KB sektorów dysków,</li></ul></li></ul>
--	--



	<ul style="list-style-type: none"> <li>d) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,</li> <li>e) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),</li> <li>f) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,</li> <li>g) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),</li> <li>h) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,</li> <li>i) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,</li> <li>j) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF</li> </ul>
--	--

## II.5 Dostawa i wdrożenie systemu DLP – 1 szt.

System klasy DLP (Data Leak Prevention) czyli system monitorowania i ochrony poufnych informacji, zapobiegania utracie danych, wyciekom danych. Wymagane jest dostarczenie licencji bezterminowej dla 40 urządzeń końcowych i serwera administracyjnego z wsparciem technicznym na min. 24 miesiące. Oprogramowanie należy wdrożyć oraz przetestować w uzgodnionym zakresie z zamawiającym, biorąc pod uwagę najlepsze praktyki oraz zalecenia producenta. Minimalne wymagania dla systemu DLP:

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11.

2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL oraz AzureSQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
9. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.
13. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
14. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania oraz edycji wyżej wymienionych kategorii.
15. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.

16. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:
  - a. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
  - b. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.
17. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
18. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
  - a. logowanie oraz wylogowanie użytkownika,
  - b. włączenie oraz wyłączenie stacji roboczej,
  - c. blokada oraz odblokowanie stacji roboczej,
  - d. przejście w stan bezczynności stacji roboczej.
19. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
20. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.
21. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
22. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
23. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF oraz XLS.
24. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
25. Serwer musi posiadać możliwość wysyłania alertów, co najmniej za pośrednictwem wiadomości email.

- 
26. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
  27. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
  28. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
  29. Serwer administracyjny musi posiadać domyślnie skonfigurowany serwer SMTP udostępniony przez producenta oprogramowania.
  30. 30. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.
  31. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.
  32. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:
    - a. aplikacje, z której zostały utworzone,
    - b. lokalizację,
    - c. adres URL,
    - d. format pliku,
    - e. zawartość pliku.
  33. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.
  34. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:
    - a. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
    - b. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
    - c. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
    - d. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
    - e. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,

- 
- f. blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
  - g. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:
    - Dropbox,
    - Google Drive,
    - SharePoint,
    - OneDrive Business,
    - OneDrive Personal.
  - h. blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
  - i. blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego,
  - j. blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości oraz wirtualnego drukowania,
  - k. uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikację,
35. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
36. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
37. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
38. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
39. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e-mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.
40. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
41. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.

42. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
43. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
44. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
45. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:
  - a. numery kart kredytowych,
  - b. numer PESEL,
  - c. numer polskiego dowodu osobistego,
  - d. polski numer paszportu,
  - e. wyrażenia regularne,
  - f. określone ciągi znaków,
  - g. numer IBAN.
46. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
47. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition) z wsparciem języka polskiego.
48. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
49. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e-mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy”).
50. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
51. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modułem DLP dostępnym na rozwiązaniu FortiGate.
52. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania klasy SIEM.
53. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do systemu umożliwiającego ochrony poczty, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.
54. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:

- 
- a. audyt i logowanie wiadomości e-mail,
  - b. audyt operacji na plikach Sharepoint Online.
55. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tabeau).
56. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi.
57. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:
- a. Bezpieczeństwo danych:
    - Przegląd informacji o incydentach bezpieczeństwa.
    - Przegląd danych przychodzących.
    - Przegląd danych wychodzących.
    - Podłączane/odłączane urządzenia przenośne.
  - b. Produktywność:
    - Przegląd informacji na temat produktywności użytkowników.
    - Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
    - Trendy.
  - c. Eksploatacja sprzętu:
    - Przegląd informacji na temat eksploatacji sprzętu komputerowego.
    - Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
    - Eksploatacja drukarek.
    - Eksploatacji sieci.
58. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
59. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
60. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt.:
- plików przenoszonych na nośniki USB i inne urządzenia przenośne,
  - plików przesłanych za pomocą wiadomości e-mail,
  - plików przesłanych za pomocą poczty webowej,
  - plików przesłanych do Internetu,
  - plików wysłanych za pomocą komunikatorów,
  - plików przesłanych na dyski chmurowe,

- analiza sposobu korzystania z aplikacji,
- analiza korzystania z Internetu,
- analiza wykorzystania portali do poszukiwania pracy.

61. Konsola aplikacyjna musi umożliwiać możliwość konfiguracji podwójnej autoryzacji

62. Konsola aplikacyjna musi umożliwiać konfigurację dwóch języków dla mechanizmu OCR

## II.6 Dostawa i wdrożenie urządzenia NAS – 1 szt.

Wykonawca dostarczy, zainstaluje w szafie rack, skonfiguruje do pracy sieci Zamawiającego, zintegruje urządzenie z użytkowaną przez Zamawiającego domeną Active Directory. Urządzenie będzie przeznaczone do przechowywania kopii zapasowych systemów Zamawiającego oraz danych/plików użytkowników. Urządzenie wraz z systemem kopii musi zostać tak skonfigurowane, żeby była możliwość bezpośredniego dostępu do urządzenia tylko z sieci zarządzającej (konfiguracja odpowiedniego VLAN dla przestrzeni storage oraz systemu kopii). Urządzenie musi umożliwiać wykonanie kopii zapasowej przy pomocy oprogramowania opisanego w punkcie II.7 SOPZ. oraz zostanie podłączone do rdzenia sieci za pomocą połączeń 10 GB/s SFP+ w celu skrócenia czasu tworzenia oraz odzyskiwania kopii. Urządzenie musi spełniać poniższe wymagania minimalne:

Typ urządzenia	Serwer plików NAS
Obudowa	Rack z dołączonym zestawem przesuwnych szyn montażowych
Procesor	AMD lub Intel
Architektura procesora	64 bit



Procesor liczba rdzeni	Nie mniej niż 8 o taktowaniu nie niższym niż 3,6 GHz
Pamięć RAM	Nie mniej niż 32GB DDR4 lub DDR5
Pamięć RAM liczba slotów	Minimum 4 sloty
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 128 GB
Pamięć Flash	Nie mniej niż 5GB
Liczba zatok na dyski twarde	Minimum 12
Obsługiwane dyski twarde	3.5" SATA oraz 2.5" SATA / SSD SATA
Maksymalna pojemność dysków twardych jakie można stosować	do 20 TB
Możliwość podłączenia modułu rozszerzającego	Tak, do 16 modułów

Porty LAN	Minimum 2 x 1 Gb/s Ethernet, 2 x 10 Gb/s SFP+, 2 x 10 Gb/s Base-T
Diody LED	HDD 1–12, stan urządzenia, LAN
Porty USB	min. 1 gniazdo typu C USB 3.2 Gen2 10 Gb/s min. 1 gniazdo typu A USB 3.2 Gen2 10 Gb/s
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 2U
Dopuszczalna temperatura pracy	od 0 do 40°C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Redundatne min 300 W(x2), 100–240 V
Agregacja łącz	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: ZFS Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+

Możliwość podłączenia karty WLAN na USB	Tak
Łączenie usług z interfejsem	Tak
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	RAID 0,1,5,50,6,60,10, Triple Parity, Triple Mirror Konfiguracja priorytetu odbudowy grup RAID RAID HotSpare i Global HotSpare SSD Trim HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Wykrywanie uszkodzenia i naprawa danych Cache odczytu z wykorzystaniem dysków SSD Cache odczytu i dziennik zapisu z wykorzystaniem dysków SSD Funkcjonalność migawek udziałów oraz LUN, wraz z możliwością ich replikacji na drugie urządzenie
Dyski twarde	Zainstalowanych 10 dysków o pojemności min. 18TB każdy, dyski klasy enterprise, znajdujące się na liście kompatybilności producenta NAS, o

	parametrach: prędkość obrotowa 7200, MTBF min. 2,48 mln gpdzin, cache min. 256MB,
Wbudowana obsługa iSCSI	<p>Obsługa wielu jednostek LUN na Target</p> <p>Obsługa mapowania i maskowania LUN</p> <p>Obsługa SPC-3 Persistent Reservation</p> <p>Obsługa MPIO &amp; MC/S</p> <p>Wykonywanie migawek oraz kopii zapasowej LUN</p>
Obsługa Fiber Channel (FC SAN)	Wsparcie opcjonalnych kart FC / Mapowanie LUN
Zarządzanie prawami dostępu	<p>Przypisanie pojemności dla użytkowników</p> <p>Importowanie listy użytkowników</p> <p>Zarządzanie kontami użytkowników</p> <p>Zarządzanie grupą użytkowników</p> <p>Zarządzanie uprawnieniami dla użytkowników i grup</p> <p>Obsługa zaawansowanych uprawnień dla pod folderów</p>
Obsługa Windows AD	Logowanie użytkowników domenowych poprzez protokoły CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web / Funkcja serwera i klienta LDAP
Funkcje backup	<p>Oprogramowanie do tworzenia kopii bezpieczeństwa plików, opracowane przez producenta urządzenia dla systemów Windows.</p> <p>Backup na zewnętrzne dyski twarde.</p>

Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Dropbox, OneDrive for Business, Google Drive
Darmowe aplikacje na urządzenia mobilne	Monitoring i zarządzanie urządzeniem / Współdzielenie plików / Obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane aplikacje	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer pobierania (Bittorrent/HTTP/HTTPS/FTP)
VPN	VPN client / VPN server Minimum obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail Powiadamianie przez SMS (z wykorzystaniem zewnętrznych usług) DDNS oraz zdalny dostęp w chmurze producenta SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP oraz lokalnych przez USB Monitorowanie zasobów urządzenia Monitorowanie zasobów systemu w czasie rzeczywistym Rejestr zdarzeń Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line

	<p>Aktualizacja oprogramowania</p> <p>Możliwość aktualizacji oprogramowania z powiadomieniem z serwerów producenta</p> <p>Ustawienia systemowe: kopia zapasowa, przywracanie, resetowanie systemu</p>
Wirtualizacja	<p>Możliwość uruchomienia maszyn wirtualnych z systemem Windows, Linux, Unix i Android</p> <p>Import maszyn wirtualnych</p> <p>Klonowanie maszyn wirtualnych</p> <p>Migawki maszyn wirtualnych</p> <p>GPU pass-through dla dodatkowych kart graficznych</p>
Zabezpieczenia	<p>Filtracja IP</p> <p>Ochrona dostępu do sieci z automatycznym blokowaniem połączeń</p> <p>Obsługa HTTPS</p> <p>FTP z SSL/TLS (Explicit)</p> <p>Obsługa SFTP (tylko admin)</p> <p>Szyfrowanie AES 256-bit</p> <p>Import certyfikatu SSL</p>
Gwarancja	<p>Urządzenie NAS: 3 lata gwarancji oraz serwisu realizowanego przez producenta serwera w miejscu instalacji</p> <p>Dyski twarde: 5 lat gwarancji producenta w miejscu instalacji</p>

## **II.7 Dostawa i wdrożenie oprogramowania do wykonywania kopii zapasowych według polityki i harmonogramu tworzenia kopii zapasowych**

W ramach realizacji zadania Wykonawca dostarczy nowe licencje oprogramowania do tworzenia kopii zapasowej wszystkich maszyn wirtualnych działających na hostach Zamawiającego, zainstaluje, skonfiguruje dostarczone oprogramowanie. Wykonawca opracuje politykę backupu 3-2-1 w oparciu o dostarczony sprzęt, oprogramowanie oraz sprzęt Zamawiającego, opracuje harmonogram oraz utworzy zadania backupowe. Wykonawca przeprowadzi testy odtworzeniowe, instruktaż z obsługi wdrożonego systemu tworzenia kopii, opracuje dokumentację powykonawczą.

Wymagane jest dostarczenie licencji bezterminowych z wsparciem technicznym przez okres min. 12 miesięcy (parametr punktowany dodatkowo) dla 4 procesorów serwerów fizycznych Zamawiającego, spełniających poniższe wymagania minimalne:

1. Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
  - a. Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
  - b. Vmware vSphere min. w wersjach v5.5-7.0.3
  - c. Nutanix AHV 5.15, 5.20 (LTS)
  - d. Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012
  - e. Microsoft 365 (Exchange online, One Drive for Business, Sharepoint, Teams)
2. Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
3. Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
  - a. na serwerze Windows lub Linux
  - b. jako maszyna wirtualna VMware
  - c. jako maszyna wirtualna Amazon
  - d. na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
4. Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
5. Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania

6. Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
7. Oprogramowanie ma umożliwiać wdrożenie schematu backupu według zasady 3-2-1
8. Oprogramowanie ma umożliwiać zapewnienie niezmienności kopii chroniąc przed oprogramowaniem ransomware z zastosowaniem niezmiennych kopii zapasowych (worm lub chmura) oraz ze szczeliną powietrzną (rozłączane taśmy, napędy usb lub nas)
9. Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariantcie wieczystym, w którym licencja nie ma terminu ważności
10. W ramach dostawy wymagane jest dostarczenie licencji na ochronę min. 6 gniazd procesorów w hostach Vmware lub Hyper-V
11. Dostarczona wersja oprogramowania i licencji, powinna mieć możliwość rozbudowy ilości chronionych zasobów w przyszłości
12. W ramach dostarczonej licencji wymagane jest zapewnienie wsparcia technicznego producenta, które umożliwia min. dostęp do aktualizacji i poprawek oprogramowania oraz umożliwia kontakt z działem technicznym producenta w zakresie obsługi oferowanego oprogramowania.
13. Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
14. Oprogramowanie musi posiadać funkcje backupu i replikacji:
  - a. Backup maszyn wirtualnych Vmware
  - b. Replikacja maszyn wirtualnych Vmware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
  - c. Backup maszyn wirtualnych Hyper-V
  - d. Replikacja maszyn wirtualnych Hyper-V (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
  - e. Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych



- f. Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
  - g. Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
  - h. Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
  - i. Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych
  - j. Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem
  - k. Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
  - l. Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
15. Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
- a. Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
  - b. Kompresja backupu, w tym konfigurowalny stopień kompresji
  - c. Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
16. Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
- a. Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
  - b. Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
  - c. Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji: Microsoft Exchange 2013, 2016, 2019
  - d. Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
  - e. Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
17. Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V

18. Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
19. Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
20. Oferowany system tworzenia kopii zapasowych musi umożliwiać wysyłanie zaszyfrowanych kopii zapasowych do zasobów chmurowych.
21. Oprogramowanie musi posiadać poniższe funkcje:
  - a. Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
  - b. Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
  - c. Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
  - d. Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
  - e. Microsoft Exchange, MS Active Directory, MS SQL
  - f. Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji VMware i Hyper-V i odwrotnie.
22. Oprogramowanie do backupu musi pozwalać na:
  - a. Tworzenie backupu i replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
  - b. Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
  - c. Backup z pominięciem sieci LAN dzięki opcjom dostępu bezpośredniego w sieciach SAN
  - d. Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
  - e. Wsparcie dla urządzeń oferujących dodatkową deduplikację danych
23. Oprogramowanie musi pozwalać na następujące formy zarządzania:
  - a. Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
  - b. Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej

- c. Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania
- d. wielu harmonogramów dla pojedynczego zadania
- e. Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków, do których będzie robiony eksport.
- f. Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
- g. Oprogramowanie musi umożliwiać integrację z usługą katalogową Active Directory.

W celu skrócenia czasu tworzenia kopii zapasowych z obecnie eksploatowanego serwera Zamawiającego konieczne jest podłączenie serwera do nowego rdzenia sieci LAN.

#### **Instalacja, konfiguracja systemu do tworzenia kopii zapasowej**

Wykonawca dokona konfiguracji dostarczonego systemu kopii bezpieczeństwa, która będzie obejmować:

1. instalację i konfigurację dostarczonego systemu kopii bezpieczeństwa na zasobach Zamawiającego
2. skonfigurowanie przestrzeni dla kopii bezpieczeństwa na dostarczonym serwerze NAS oraz macierzy zapasowej
3. konfigurację miejsc przechowywania, w tym urządzenia NAS, macierzy
4. konfigurację polityki składowania oraz harmonogramów
5. konfigurację zabezpieczeń wewnętrznych, w tym kopii ratunkowej (ang. disaster recovery) systemu kopii bezpieczeństwa
6. instalację i konfigurację dodatkowych maszyn wirtualnych klientów, jeśli są wymagane, w środowisku Zamawiającego
7. konfigurację kopii zapasowych maszyn wirtualnych Zamawiającego dla dwóch repozytoriów
8. instalację niezbędnych agentów dla środowiska bazodanowego Zamawiającego i konfigurację kopii zapasowych baz danych

9. konfigurację automatycznej weryfikacji kopii bezpieczeństwa maszyn wirtualnych Zamawiającego.

10. konfigurację powiadomień i codziennych raportów

Wykonawca opracuje i przedstawi Zamawiającemu dokumentację powykonawczą zawierającą:

1. podstawowe procedury obsługowe
2. opis skonfigurowanych polityk i harmonogramów
3. opis odtworzenia maszyn wirtualnych
4. opis odtworzenia pojedynczego pliku
5. opis odtworzenia bazy danych Zamawiającego
6. opis sposobu aktualizacji systemu

Wykonawca przeprowadzi jednodniowy instruktaż stacjonarny w siedzibie Zamawiającego w czasie do 21 dni kalendarzowych od daty zakończenia wdrożenia dla max. 2 pracowników Zamawiającego, który obejmie co najmniej:

1. podstawową wiedzę dotyczącą systemu
2. dodawania i usuwania z systemu maszyn wirtualnych
3. dodawanie i usuwanie z systemu fizycznych urządzeń
4. zagadnienia dotyczące zmian platform wirtualizacji
5. możliwości dodawania, zmiany i usuwania kolejnych miejsc przechowywania kopii zapasowych
6. procedurę aktualizacji systemu

#### **Opracowanie polityki tworzenia kopii zapasowej (Backup 3-2-1):**

System backup wdrożony zostanie w taki sposób, aby był zgodny z zasadą 3-2-1. Jest to strategia tworzenia kopii zapasowych danych zaprojektowana w celu zapewnienia możliwości szybkiego odzyskania i przywrócenia danych w przypadku incydentu utraty danych. W szczególności ta strategia tworzenia kopii zapasowych musi zapewniać posiadanie trzech niezależnych kopii danych:

- Pierwsza kopia będzie przechowywana lokalnie na macierzy zapasowej,
- Druga kopia będzie przechowywana na serwerze NAS,
- Trzecia kopia danych będzie przechowywana na nośnikach wymiennych Zamawiającego,

Celem wdrożenia strategii tworzenia kopii zapasowych 3-2-1 jest zmniejszenie potencjalnego wpływu „pojedynczego punktu podatności na awarię”. Oznacza to, że jeśli jedno z urządzeń ulegnie awarii i znajdująca się na nim kopia danych zostanie utracona, do dyspozycji są jeszcze pozostałe dwie kopie danych. Wyniesienie nośników wymiennych poza budynek Gminy umożliwia natomiast odzyskanie kluczowych danych Zamawiającego w przypadku awarii dużych rozmiarów bądź fizycznego zniszczenia siedziby Zamawiającego (pożar, wybuch, działania terrorystyczne, klęski żywiołowe).

Kluczowym elementem wdrożenia jest opracowanie polityki backupowej, w której opisane zostaną wszystkie zasady, według których będą tworzone kopie zapasowe z wyszczególnieniem kto je wykonuje, kiedy, gdzie przenoszone będą nośniki danych oraz kto będzie odpowiedzialny za poszczególne etapy wykonywania czynności, kto będzie odpowiedzialny za monitoring i weryfikację tworzonych kopii zapasowych.

Polityka backup oraz uruchomione środowisko backup musi być również zgodne z rekomendacją dotyczącą wykonywania kopii zapasowych opublikowaną przez Ministerstwo Zdrowia, która dostępna jest pod adresem: <https://www.gov.pl/web/baza-wiedzy/tworzenie-zapasowych-kopii-danych>

Wymagany zakres prac do wykonania w ramach zadania Backup 3-2-1:

1. Dostawa macierzy zapasowej przeznaczonej do przechowywania kopii zapasowej systemów produkcyjnych; serwera NAS, niezbędnych licencji oprogramowania do tworzenia kopii zapasowych z wsparciem technicznym oraz dostępem do aktualizacji
2. Montaż macierzy, konfiguracja do pracy w infrastrukturze Zamawiającego, uruchomienie; aktualizacja firmware; konfiguracja, instalacja dostarczanego oprogramowania; konfiguracja maszyny wirtualnej dla systemu backupu; instalacja serwera/konsoli zarządzającej kopiami zapasowymi;
3. Opracowanie polityki backupu 3-2-1 w oparciu o:
  - dostarczony sprzęt, oprogramowanie,
  - sprzęt Zamawiającego
  - przeprowadzoną analizę środowiska Zamawiającego (liczba maszyn wirtualnych, krytyczność systemu, wielkość maszyny wirtualnych czy ilość danych na serwerach fizycznych)

Na podstawie zebranych danych oraz wymagań Zamawiającego, Wykonawca opracuje Harmonogram tworzenia kopii zapasowych z podziałem na maszyny fizyczne/wirtualne; określeniem: częstotliwości tworzenia kopii pełnych, częstotliwości tworzenia kopii przyrostowych, częstotliwości tworzenia kopii na nośnikach wymiennych, częstotliwości weryfikacji poprawności tworzonych kopii zapasowych, częstotliwości i zakresu przeprowadzania testów odtworzeniowych. Na podstawie Harmonogramu Wykonawca skonfiguruje zadania backupowe na dostarczonym oprogramowaniu. Uruchomi tworzenie kopii zapasowych na serwerze backupowym oraz serwerze NAS. Na żądanie

- Zamawiającego Wykonawca skonfiguruje dodatkowo tworzenie kopii zapasowych na wskazanych przez Zamawiającego zasobach dyskowych lub chmurowych.
4. Począwszy od dnia uruchomienia tworzenia kopii zapasowych, Wykonawca będzie zobowiązany do monitorowania pracy systemu backupowego przez min. 7 dni. Nadzór będzie miał na celu potwierdzenie prawidłowości wykonywanych kopii na serwerze oraz nośnikach wymiennych; potwierdzenie tworzenia kopii zgodnie z Harmonogramem.
  5. Po zakończeniu pełnego cyklu tygodniowego tworzenia kopii zapasowych zgodnie z Harmonogramem, Wykonawca odtworzy wszystkie serwery fizyczne/maszyny wirtualne z kopii zapasowych na serwerze backupowym. Testy odtworzeniowe będą przeprowadzone przy udziale administratora Zamawiającego
  6. Po okresie monitorowania, na podstawie potwierdzenia przez Zamawiającego zgodności wykonywanych kopii zgodnie z Harmonogramem oraz na podstawie zakończonych sukcesem testów odtworzeniowych, Wykonawca przeprowadzi instruktaż z zakresu:
    - bieżącej obsługi systemu, podstaw administracji,
    - modyfikacji Harmonogramu i zadań backupowych,
    - czynności sprawdzania prawidłowości wykonywanych kopii zapasowych na serwerze oraz nośnikach wymiennych,
    - procedury i czynności przeprowadzania testów odtworzeniowych,
  7. Wykonawca wykona instruktaż z uruchomienia maszyn wirtualnych z kopii zapasowej.
  8. Ostatnim etapem wdrażania systemu backupu 3-2-1 jest opracowanie dokumentacji powykonawczej, która będzie zawierać opis wszystkich wykonanych prac, niezbędne dane konfiguracyjne, opis polityki backupowej wraz z harmonogramem oraz instrukcjami umożliwiającymi samodzielne użytkowanie, administrowanie wdrożonym środowiskiem przez Zamawiającego.

## **II.8 Dostawa i wdrożenie zarządzalnych urządzeń sieciowych do rdzenia sieci – 2 szt.**

Obecnie używane przez Zamawiającego przełączniki tworzące sieć LAN są przestarzałe, nie ma wydzielonych przełączników do rdzenia sieci, brak możliwości instalacji nowego oprogramowania wewnętrznego. Przedmiotem zadania jest dostawa 2 nowych przełączników umożliwiających utworzenie rdzeń sieci LAN. Wraz z przełącznikami należy dostarczyć wszystkie niezbędne moduły SFP+, przewody połączeniowe umożliwiające uruchomienie nowej sieci LAN oraz podłączenie urządzeń do nowych przełączników. Przełączniki muszą spełniać opisane niżej parametry minimalne:

Element konfiguracji	Wymagania minimalne
Fizyczne	Wysokość w szafie 19” – 1U, głębokość nie większa niż 250mm, możliwość montażu w szafie rack
Techniczne	Minimum 1 port ethernet 10/000BaseT Minimum 24 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Minimum 2 porty SFP28, pozwalające na instalację wkładek 25Gbit. Minimum 1 port konsoli: RJ45
Wydajność	Pojemność matrycy przełączania (capacity L1): minimum 600 Gb/s Wydajność (throughput L1): minimum 300 Gb/s Tablica adresów MAC o wielkości minimum 32k pozycji
Procesor	Min. 1 procesor 650Mhz
Pamięć RAM	Min. 64 MB
Pamięć wbudowana	Min. 16 MB
Stackowanie / MLAG	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) lub możliwość wykonania MLAG (Multichassis Link Aggregation)
Funkcje minimalne	Obsługa ramek Jumbo minimum 9k Routing IPv4 – minimum: statyczny, RIP, OSPF, BFD, VRF, VRRP Routing IPv6 – minimum: statyczny, RIPng, OSPF Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping Obsługa vxlan Obsługa Port isolation Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol Obsługa funkcji Loop Protect Obsługa funkcji Traffic Shaping Obsługa 4094 tagów IEEE 802.1Q oraz minimum 1000 jednoczesnych sieci VLAN z BPDU protection Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie lub MLAG Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping ze wsparciem opcji 82 Obsługa list ACL na bazie informacji z warstw 2/3/4

	<p>modelu OSI</p> <p>Obsługa standardu 802.1p</p> <p>Funkcja mirroringu portów</p> <p>Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) lub CDP Cisco Discovery Protocol</p> <p>Funkcja autoryzacji użytkowników zgodna z 802.1x</p> <p>Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo RADIUS Accounting</p>
Zarządzanie	<p>Zarządzanie poprzez port konsoli (pełne),</p> <p>Musi wspierać możliwość zarządzania przez następujące protokoły:</p> <ul style="list-style-type: none"> <li>• SNMP v.1, 2c i 3,</li> <li>• Telnet, SSH v.2,</li> <li>• http</li> <li>• https</li> <li>• Syslog</li> <li>• NTP</li> </ul> <p>Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej</p>
Zasilanie	<p>Urządzenie musi być wyposażone w dwa redundantne, dedykowane zasilacze</p> <p>Możliwość zasilania PoE</p>
Wyposażenie	<p>Wraz z przełącznikiem należy dostarczyć niezbędne wkładki SFP+, przewody do redundantnego podłączenia wszystkich wskazanych przez Zamawiającego urządzeń do tworzonego rdzenia sieci LAN.</p> <p>Zestaw do montażu w szafie rack</p>
Gwarancja	<p>Min. 24 miesiące gwarancji w miejscu instalacji</p>

### **Zakres wdrożenia przełączników tworzących rdzeń sieci LAN:**

Wykonawca dostarczy nowe urządzenia, przedstawi projekt wdrożenia przełączników do rdzenia sieci LAN Zamawiającego. Na podstawie zaakceptowanego projektu zainstaluje przełączniki w wskazanej szafie rack, skonfiguruje do pracy w sieci LAN Zamawiającego. Wszystkie prace muszą się odbywać poza godzinami



pracy Urzędu, w oknie serwisowym wyznaczonym przez Zamawiającego. Projekt musi obejmować minimum:

- aktualizację oprogramowania układowego przełączników do najnowszej stabilnej wersji
- konfigurację sieci wirtualnych przełącznika na podstawie obecnej infrastruktury
- konfigurację agregacji połączeń do serwerów pomiędzy przełącznikami
- konfigurację agregacji połączeń dla przełączników dostępowych
- konfigurację syslog dla przełączników
- konfigurację protokołu SNMP zgodnie z obecnym systemem monitoringu
- konfigurację użytkowników administracyjnych przełącznika zgodnie z wytycznymi bezpieczeństwa
- uruchomić dostęp poprzez SSH oraz interface www z https. Certyfikaty https należy wygenerować oraz zainstalować na urządzeniach.
- Autoryzacja użytkowników ma się odbywać do konsoli w oparciu o lokalnych użytkowników. Nie możliwy jest dostęp do konsoli bez autoryzacji. Konsola powinna wylogować użytkownika po 5 min nieaktywności. Hasła lokalnych kont mają być szyfrowane, niedopuszczalne jest przechowywanie haseł czystym tekstem.
- Autoryzacja użytkowników SSH oraz www ma odbywać się w oparciu o serwer radius. Wykonawca zainstaluje i skonfiguruje serwery RADIUS (podstawowy oraz zapasowy) wobec których będzie następowała autoryzacja użytkowników przechowywanych w katalogu LDAP
- Konfiguracja NTP – przełączniki mają mieć skonfigurowaną synchronizację czasu w oparciu o serwery ntp 0.pl.pool.ntp.org, 0.pl.pool.ntp.org. Poprawnie zostanie ustawiona strefa czasowa.
- Wykonawca przekaże kopię przełączników do dokumentacji oraz skonfiguruje automatyczną kopię urządzeń sieciowych
- Wszystkie porty na urządzeniach sieciowych zostaną opisane poprzez wykonawcę. Opis
- Wykonawca wyłączy protokoły CDP oraz LLDP na portach dostępowych (np. dla stacji roboczych i telefonów) Natomiast na połączeniach pomiędzy przełącznikami należy zostawić włączone oba protokoły.

- Wykonawca skonfiguruje protokół MSTP w ramach dostarczonych przełączników
- Wykonawca przeprowadzi konfigurację VLANów na przełącznikach wskazanych na etapie wdrożenia przez zamawiającego (wraz z dedykowanym vlanem do zarządzania przełącznikami sieciowymi)
- Wykonawca na urządzeniach zdefiniuje wskazany na etapie wdrożenia serwer DNS oraz domenę wyszukiwania na urządzeniach sieciowych.
- W ramach wdrożenia wykonawca przedstawi możliwe do wdrożenia dodatkowe zabezpieczenia możliwe do wdrożenia w ramach dostarczonych urządzeń i na etapie wdrożenia zamawiający zdecyduje, które zabezpieczenia należy wdrożyć.
- jeśli dostarczone urządzenie dysponuje API umożliwiającym konfigurację urządzeń należy przygotować skrypty odpowiadające konfiguracji (python, ansible) w celu zarządzania zmianą konfiguracji.

## **II.9 Dostawa i wdrożenie zarządzalnych urządzeń sieciowych dla punktów dostępowych – 2 szt.**

Obecnie używane przez Zamawiającego przełączniki tworzące sieć LAN są przestarzałe gdzie nie ma możliwości instalacji nowego oprogramowania wewnętrznego. Przedmiotem zadania jest dostawa 2 nowych przełączników dostępowych. Wraz z przełącznikami należy dostarczyć wszystkie niezbędne moduły SFP+ oraz przewody połączeniowe umożliwiające podłączenie przełączników dostępowych do rdzenia sieci LAN. Przełączniki muszą spełniać opisane niżej parametry minimalne:

Cecha	Wymagania minimalne
Fizyczne	Wysokość w szafie 19” – 1U, głębokość nie większa niż 150mm, możliwość montażu w szafie rack
Techniczne	Minimum 48portów gigabitowych w standardzie 100/1000BaseT Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP), min. 2 porty QSFP+. Dedykowany port konsoli zarządzającej RJ-45
Wydajność	Prędkość matrycy przełączania (capacity L1) : minimum 330Gb/s Wydajność (throughput L1): minimum 160Gb/s

	Tablica adresów MAC o wielkości minimum 32k pozycji
Procesor	Min. 650Mhz
Pamięć RAM	Min. 64MB
Pamięć wbudowana flash	Min. 15MB
Stackowanie / MLAG	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) lub możliwość wykonania MLAG (Multichassis Link Aggregation)
Funkcje minimalne	<p>Obsługa ramek Jumbo minimum 9k</p> <p>Routing IPv4 – minimum: statyczny, RIP, OSPF, BFD, VRF, VRRP</p> <p>Routing IPv6 – minimum: statyczny, RIPng, OSPF</p> <p>Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping</p> <p>Obsługa vxlan</p> <p>Obsługa Port isolation</p> <p>Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol</p> <p>Obsługa funkcji Loop Protect</p> <p>Obsługa funkcji Traffic Shaping</p> <p>Obsługa 4094 tagów IEEE 802.1Q oraz minimum 1000 jednoczesnych sieci VLAN z BPDU protection</p> <p>Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie lub MLAG</p> <p>Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping ze wsparciem opcji 82</p> <p>Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI</p> <p>Obsługa standardu 802.1p</p> <p>Funkcja mirroringu portów</p> <p>Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) lub CDP Cisco Discovery Protocol</p> <p>Funkcja autoryzacji użytkowników zgodna z 802.1x</p> <p>Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo RADIUS Accounting</p>
Zarządzanie	Zarządzanie poprzez port konsoli (pełne),

	<p>Musi wspierać możliwość zarządzania przez następujące protokoły:</p> <ul style="list-style-type: none"> <li>• SNMP v.1, 2c i 3,</li> <li>• Telnet, SSH v.2,</li> <li>• http</li> <li>• https</li> <li>• Syslog</li> <li>• NTP</li> </ul> <p>Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej</p>
Zasilanie	<p>Urządzenie musi być wyposażone w dwa wbudowane zasilacze</p> <p>Możliwość zasilania PoE przez dedykowany port RJ-45</p>
Wyposażenie	<p>Zainstalowane 2 wkładki 10Gb SFP+ SR LC MM</p> <p>Dwa przewody światłowodowe LC-LC min. OM3 o długości min. 5m</p> <p>Zestaw do montażu w szafie rack</p>
Gwarancja	<p>Min. 24 miesiące gwarancji w miejscu instalacji</p>

Projekt i wdrożenie będzie obejmować minimum:

- aktualizacja firmware przełączników do najnowszej stabilnej wersji
- konfiguracja portów do zarządzania (management port)
- wymiana przełączników w szafie rack i podłączenie klientów z demontowanych przełączników
- podłączenie przełączników do rdzenia sieci LAN portami 10Gbit SFP+
- wykonanie testów poprawności działania po przełączeniu produkcyjnym
- uruchomić dostęp poprzez SSH oraz oraz interface www z https. Certyfikaty należy wygenerować
- Autoryzacja użytkowników ma się odbywać do konsoli w oparciu o lokalnych użytkowników. Nie możliwy jest dostęp do konsoli bez autoryzacji. Konsola powinna wylogować użytkownika po 5 min nieaktywności. Hasła lokalnych kont mają być szyfrowane, niedopuszczalne jest przechowywanie haseł czystym tekstem.

- Autoryzacja użytkowników SSH oraz www ma odbywać się w oparciu o serwer radius. Wykonawca zainstaluje i skonfiguruje serwery RADIUS (podstawowy oraz zapasowy) wobec których będzie następowała autoryzacja użytkowników przechowywanych w katalogu LDAP
- Konfiguracja NTP – przełączniki mają mieć skonfigurowaną synchronizację czasu w oparciu o serwery ntp 0.pl.pool.ntp.org, 0.pl.pool.ntp.org. Poprawnie zostanie ustawiona strefa czasowa.
- Wykonawca prześle kopię przełączników do dokumentacji oraz skonfiguruje automatyczną kopię urządzeń sieciowych
- Wszystkie porty na urządzeniach sieciowych zostaną opisane poprzez wykonawcę. Opis
- Wykonawca wyłączy protokoły CDP oraz LLDP na portach dostępowych (np. dla stacji roboczych i telefonów) Natomiast na połączeniach pomiędzy przełącznikami należy zostawić włączone oba protokoły.
- Wykonawca skonfiguruje protokół MSTP w ramach dostarczonych przełączników
- Wykonawca przeprowadzi konfigurację VLANów na przełącznikach wskazanych na etapie wdrożenia przez zamawiającego (wraz z dedykowanym vlanem do zarządzania przełącznikami sieciowymi)
- Wykonawca na urządzeniach zdefiniuje wskazany na etapie wdrożenia serwer DNS oraz domenę wyszukiwania na urządzeniach sieciowych.
- jeśli dostarczone urządzenie dysponuje API umożliwiającym konfigurację urządzeń należy przygotować skrypty odpowiadające konfiguracji (python, ansible) w celu zarządzania zmianą konfiguracji.

## II.10 Dostawa i wdrożenie systemu NAC – 1 szt.

Nowe przełączniki tworzące rdzeń sieci LAN oraz nowe przełączniki dostępowe umożliwiają wdrożenie systemu zabezpieczającego przed nieautoryzowanym dostępem do sieci LAN. Wykonawca dostarczy oraz wdroży system klasy NAC (Network Access Control) zgodnie z zaakceptowanym przez Zamawiającego projektem wdrożenia. Zamawiający wymaga dostarczenia systemu wraz z wsparciem technicznym gwarantującym dostępem do najnowszych wersji i poprawek przez okres min. 24 miesięcy. Zamawiający wymaga wdrożenia oferowanego systemu w taki sposób, aby możliwe było używanie systemu z wymaganą poniżej funkcjonalnością. W ramach wdrożenia Wykonawca musi skonfigurować wszystkie urządzenia Zamawiającego do prawidłowej współpracy z wdrażanym systemem. System kontroli dostępu musi charakteryzować się następującymi cechami:

- Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)
- System musi obsługiwać minimum 120 urządzeń klienckich (w tym gości) w trybie HA – klaster dwóch maszyn wirtualnych pracujących w trybie wysokiej dostępności (redundancja). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia
- Musi posiadać wbudowany serwer Radius
- Musi wspierać RADIUS VSA co najmniej niżej wymienionych producentów, w tym:
  - Cisco Systems
  - D-Link
  - Alcatel-lucent
  - AlliedTelesis
  - HPE Aruba / ProCurve
  - Huawei Networks
  - Fortinet
  - PaloAlto Networks
  - Mikrotik
  - Juniper
  - Netgear
- System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN.

- System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego.
- Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
- Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych
  - Microsoft Active Directory
  - Radius
  - LDAP
  - Google Workspace
  - Azure Active Directory
  - OAuth 2
  - SAML
  - Eduroam
- Musi obsługiwać metody profilowania (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie):
  - DHCP
  - TCP
  - MAC OUI
  - SNMP
- Wspierać min poniższe protokoły:
  - Radius, Radius CoA, web authentication, SAML
  - EAP-FAST (EAP-MSCHAPv2, EAP-TLS)
  - PEAP (EAP-MSCHAPv2, EAP-TLS, EAP-PEAP)
  - EAP-TLS
  - 802.1X
  - NAC
  - Windows machine authentication
  - MAC Auth
  - WPA2-Enterprise
  - OCSP (Online Certificate Status Protocol)

- SNMP (BRIDGE-MIB, Q-BRIDGE-MIB, IF-MIB, IEEE8021-PAE-MIB)
- Funkcja integracji z systemem monitorowania sieci oraz analizy zdarzeń bezpieczeństwa w celu śledzenie ewentualnych niezgodności oraz naruszeń bezpieczeństwa (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie)
- Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:
  - Co najmniej ESXi 7.0
  - Co najmniej Windows 2016 i 2019 z Hyper-V
  - Co najmniej KVM on CentOS 7.7. Ubuntu 18.04, and Ubuntu 20.04
  - Co najmniej Amazon AWS (EC2)
  - Co najmniej Microsoft Azure

Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (150). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.

System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności

- Samodzielna rejestracja klientów gościnnych w oparciu o:
  - Adres e-mail
  - Numer telefonu (wiadomość SMS)
- Logowanie w oparciu o portale społecznościowe (Google, Facebook, Github, LinkedIn)
- Funkcja integracji z systemami trzecimi poprzez API
- Wspieranie rozwiązań mobilnych poprzez skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
- Funkcja personalizacji strony gościnnej

Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.

- System musi wspierać obsługę następujących systemów operacyjnych
  - MS Windows
  - Mac OS X
  - iOS



- Android
- Chromebook
- Ubuntu
- Umożliwienie klientowi samorejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci
- Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
- Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID
- Funkcja dostępu sponsorowanego opartego na rejestracji klienta oraz przesłanie odpowiedniego formularza do administratora systemu celem weryfikacji i zaakceptowania podanego żądania.

Wbudowane mechanizmy natywnej integracji oferowanego systemu NAC z oferowanym systemem SIEM (funkcjonalność opcjonalna, dodatkowo punktowana).

Na dostarczony system NAC należy udzielić Zamawiającemu 24 miesiące gwarancji. Gwarancja musi zapewniać dostęp do poprawek oprogramowania oraz wsparcia technicznego w trybie 24x7x365 na wszystkie elementy systemu. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta lub jego partnera. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego. Zamawiający musi mieć możliwość tworzenia zgłoszeń serwisowych na dedykowanym portalu internetowym oraz poprzez dedykowaną polskojęzyczną infolinię zgłoszeniową.

Do oferowanego rozwiązania musi być dostępna dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.

Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji oferowanego oprogramowania, wymaganych w niemiejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłuższym niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia.

## II.11 Dostawa oprogramowania antywirusowego – 1 szt.

Należy dostarczyć licencje oprogramowania antywirusowego na min. 45 stacji roboczych i serwerów, ze wsparciem technicznym na min. 24 miesiące. Wykonawca zainstaluje oprogramowanie na stacjach roboczych w wskazanych serwerach, skonfiguruje konsolę do zarządzania zgodnie z wymaganiami Zamawiającego.

### Administracja zdalna w chmurze

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, co tygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

## Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
  - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
  - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
  - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
  - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
  - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanym zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
  - tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

- tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
- tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

## Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

#### Dodatkowe wymagania dla ochrony serwerów Windows:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
6. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

#### Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

### **Szyfrowanie**

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

### **Sandbox w chmurze**

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.

7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzewać jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
  - a. Czysty,
  - b. Podejrzany,
  - c. Bardzo podejrzany,
  - d. Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

## **II.12 Dostawa i podłączenie zasilacza awaryjnego UPS – 1 szt.**

W celu zabezpieczenia danych oraz baz danych na serwerach Zamawiającego niezbędne jest podłączenie serwerów do zasilacza awaryjnego, który zagwarantuje ciągłość pracy podczas zaniku prądu w sieci. Zasilacz musi umożliwić pracę infrastruktury kluczowej w głównej szafie rack przez około 30 minut. Zasilacz awaryjny musi spełnić poniższe wymagania minimalne:



Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań minimalnych
1	Moc pozorna	3000 VA
2	Moc rzeczywista	3000 W
3	Topologia (klasyfikacja IEC 62040-3)	Line-interactive z AVR
4	Współczynnik mocy	1
5	Czas przełączenia na baterię	<4 ms
6	Liczba, typ gniazd wyjściowych	8 x IEC C13 (2 grupy gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza 2x2 IEC C13 10A), 1 x IEC C19 16A
7	Typ gniazda wejściowego	IEC C20 16A
8	Czas podtrzymania przy 1 200W obciążenia	Min. 98 min
9	Czas podtrzymania dla 2 500W obciążenia	Min. 40 min

10	Czas podtrzymania przy 3 000W obciążenia z dodatkowym modułem bateryjnym	Min. 36 min
11	Napięcie znamionowe	220/230/240/250 V
12	Tolerancja napięcia prostownika	Od 160V do 294V (regulacja programowa 150-294 V)
13	Częstotliwość znamionowa	50/60 Hz /autodetekcja
14	Tolerancja częstotliwości	47– 70 Hz
15	Kształt napięcia	Sinusoidalny
16	Napięcie znamionowe wyjściowe	Min. 220/230/240 V do wyboru przez użytkownika
17	Zakres zmian napięcia	+6/-10% napięcia nominalnego
18	Częstotliwość wyjściowa	50/60 Hz
19	Współczynnik szczytu	3:1

20	Baterie wymieniane przez użytkownika "na gorąco"	Tak
21	Ochrona przed przeładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
22	Ochrona przed głębokim rozładowaniem	Tak
23	Okresowy automatyczny test baterii	Tak
24	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Na żądanie Zamawiającego należy dostarczyć opis algorytmu nieciągłego ładowania baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis będący materiałem firmowym producenta lub przez niego potwierdzony.
25	Możliwość uruchomienia bez napięcia w sieci "zimny start"	Tak
26	Czas ładowania baterii do poziomu 90%	poniżej 3 godz. do 80% pojemności użytkowej

27	Dodatkowe baterie	Możliwość podłączenia do 4 dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania
28	Interfejsy komunikacyjne	<ul style="list-style-type: none"> <li>• USB</li> </ul>
		<ul style="list-style-type: none"> <li>• RS232 DB-9 żeński (HID)</li> </ul>
		<ul style="list-style-type: none"> <li>• styki przekaźnikowe</li> </ul>
		<ul style="list-style-type: none"> <li>• miniport wyłącznik ON/OFF</li> </ul>
29	Panel sterowania z wyświetlaczem LCD	Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa) dostarczający informacji o: stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe, częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh).
		Poziomy rząd przycisków sterowania

		Poziomy rząd wskaźników stanu: zasilanie z sieć(zielony), trybu bateryjnego (żółty), usterki (czerwony)
		Sygnalizator akustyczny
30	Sygnały akustyczne	<ul style="list-style-type: none"> <li>• Awaria</li> </ul>
		<ul style="list-style-type: none"> <li>• Niski stan naładowania baterii</li> </ul>
		<ul style="list-style-type: none"> <li>• Przeciężenie</li> </ul>
		<ul style="list-style-type: none"> <li>• Serwis</li> </ul>
31	Przyciski sterujące i wskaźniki diodowe LED	<ul style="list-style-type: none"> <li>• Przycisk Escape (anulowanie)</li> </ul>
		<ul style="list-style-type: none"> <li>• Przyciski funkcyjne (przewijanie w górę i w dół)</li> </ul>
		<ul style="list-style-type: none"> <li>• Przycisk Enter (potwierdzający)</li> </ul>
		<ul style="list-style-type: none"> <li>• Przycisk ON/OFF załączenia i wyłączenia</li> </ul>
		<ul style="list-style-type: none"> <li>• LED trybu zasilania z sieć i(kolor zielony)</li> </ul>

		<ul style="list-style-type: none"> <li>• LED trybu baterii (kolor żółty)</li> </ul>
		<ul style="list-style-type: none"> <li>• LED usterki (kolor czerwony)</li> </ul>
32	Dane techniczne karty SNMP	<p>Network Support: Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/</p>
		<p>Tymczasowe hasła: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). Blokowanie konta: Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.</p>
		<p>Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI</p>
		<p>Kamptybilność: SNMP v1/v3 i IP v4/v6</p>
		<p>Interfejs: HTML5</p>
		<p>Adresowanie IP: DHCP/BootP/Manualne</p>
		<p>Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256</p>

		Dostępny port USB (microUSB - port serwisowy)
		Certyfikaty: UL 2900-1, 2900-2-2
33	Dołączone oprogramowanie	<p>Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych:</p> <ul style="list-style-type: none"> <li>- Windows: 7 / 8 / 2008 / Vista / 2003 / XP</li> <li>- Microsoft SCVMM 2012</li> <li>- Linux: Debian GNU Linux: Lenny, SUSE/Novell: SLES 11, OpenSUSE 11.2, Redhat Enterprise Linux: RHEL 5.3, 5.4, 5.5, Fedora core 12 Ubuntu: 10.04</li> <li>- VMWare: vCenter / ESXi 5.1</li> <li>- Citrix XEN 6.0</li> </ul>
34	Standard energetyczny	Min. Energy Star
35	Maksymalna wysokość całkowita zestawu w szafie rack	6U
36	Możliwość montażu bypassu serwisowego	Min. ręcznego

37	Maksymalna głębokość	610 mm
38	Poziom hałasu z odległości 1m dla pracy normalnej	Max. 41 dBA
39	Znaki bezpieczeństwa	Min. CE, Energy Star, IEC/EN 62040-1-1, IEC/EN 62040-2 class B, IEC/EN 62040-3
40	Gwarancja producenta	36 miesięcy dla elektroniki oraz baterii.

**Instalacja, konfiguracja:**

Zamawiający wymaga: dostawy, montażu zasilacza w wskazanej szafie rack, podłączenia, uruchomienia, konfiguracji karty SNMP oraz parametrów pracy zasilaczy wg. zaleceń Zamawiającego. Ponadto Wykonawca podłączy do zasilacza serwery, przełączniki sieci LAN oraz urządzenia wskazane przez Zamawiającego. Wykonawca dostarczy do tego celu wszystkie niezbędne przewody, listwy zasilające itp. Dostawca doda do dostarczanego monitoringu dostarczone urządzenia, w celu ich monitorowania oraz wysyłania powiadomień w przypadku wystąpienia krytycznych zdarzeń. Serwery powinny zostać skonfigurowane w taki sposób, żeby zostały bezpiecznie zamknięte w przypadku braku zasilania w placówce. Jednocześnie do administratorów powinno zostać wysłane powiadomienie o takim zdarzeniu.



## II.13 Dostawa i wdrożenie oprogramowania SIEM – 1 szt.

Zamawiający wymaga dostarczenia i wdrożenia systemu SIEM z gwarancją oraz wsparciem technicznym na okres min. 12 miesięcy.

➤ Wymagania dla Systemu Analizy Logów

- W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
- Rozwiązanie musi zostać dostarczone w postaci maszyn wirtualnej instalowanych w środowisku Vmware lub Windows Hyper-V
- Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach.
- Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.
- Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.
- Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.
- Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.
- Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.
- Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).
- Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.
- Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.
- Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).

- Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.
  - Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).
  - Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów)
  - Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.
  - Rozwiązanie musi umożliwiać tworzenie statycznych raportów.
  - Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF.
  - Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.
  - Rozwiązanie musi umożliwiać tworzenie własnych raportów.
  - Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.
  - Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.
- Wymagania systemowe
- Liczba obsługiwanych zdarzeń na sekundę (EPS): min. 9 000
  - Przechowywanie, zarządzanie logami: min. 2 lata
  - Liczba obsługiwanych urządzeń min. 120
  - Liczba zapisu zdarzeń na dobę: min 9 000 MB
  - System logów musi wspierać hiperwizory: Vmware ESXi oraz Microsoft HyperV

➤ Wymagania dla Systemu SIEM.

W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące incydenty na urządzeniach sieciowych Zamawiającego.

- Rozwiązanie musi w pełni realizować swoją funkcjonalność lokalnie (instalacja on-prem)
- Architektura rozwiązania musi być oparta o fizyczne lub wirtualne sondy monitorujące, których rolą jest odbieranie kopii ruchu sieciowego, generowanie alarmów oraz/lub metadanych o zdarzeniach, przygotowanie przechwyconych plików do dalszej analizy oraz przekazywanie przetworzonych danych do urządzenia administracyjnego.
- Architektura rozwiązania musi być oparta także o fizyczne urządzenie administrujące, którego rolą jest zarządzanie sondami, włącznie z regułami detekcji, sygnaturami i nadzorem stanu, dogłębna analiza odebranych plików, prezentacja wyników detekcji, a także przekazywanie danych do rozwiązań stron trzecich
- Platformy muszą obsługiwać szyfrowanie dysków w standardzie LUKS.
- Rozwiązanie musi wspierać implementację na środowisku wirtualnym takim jak m.in. VMWare, Hyper-V, Proxmox, KVM, OVM, OVF.
- Serwer dedykowany musi obsługiwać do 2 900 zdarzeń na sekundę, musi przechowywać do 5 milionów zdarzeń, musi mieć możliwość detekcji malware, a także musi analizować przy pomocy silnika detekcji shellcode/powershell.
- Licencja na zakup i serwis oprogramowania musi bazować na ilości aktywnie występujących w ruchu sieciowym adresów IP. Ilość adresów, objętych monitorowaniem min. 120.
- Musi posiadać moduły zabezpieczone połączeniem (HTTPS) w przeglądarce
- Konsola rozwiązania musi zawierać informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, sygnatury czasowe.
- Konsola rozwiązania musi szacować poziom ryzyka dla każdego wykrytego zagrożenia oraz musi dawać możliwość tagowania zdarzeń i załączania opisu (notatek).
- Rozwiązanie musi obsługiwać silniki detekcji takie jak Analiza Shellcode i Powershell, tj. detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wywoływania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach.
- Rozwiązanie musi umożliwiać analizowanie całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń.

- 
- Opcjonalny moduł EDR (Endpoint Detection and Response - moduł punktowany dodatkowo).
  - Wykonawca wraz z system SIEM może dostarczyć system klasy Endpoint Detection and Response wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla min. 120 urządzeń wraz z wsparciem technicznym na okres min. 24 miesięcy. Minimalne wymagania dla modułu EDR:
  - Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS umożliwiające bezproblemową współpracę z systemem antywirusowym do ochrony stacji roboczych, użytkowanym przez Zamawiającego.
  - Rozwiązanie musi zawierać centralną konsolę administracyjną umożliwiającą monitorowanie oraz wizualizację zebranych danych z zarządzanych urządzeń.
  - Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej.
  - Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
  - Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
  - Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, nazwę komputera, grupę, użytkownika.
  - Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, rozmiar pliku.
  - Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne lub niebezpieczne.
  - Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.
  - Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania komend zdalnych.
  - Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.

- 
- Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
  - Rozwiązanie musi umożliwiać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
  - Rozwiązanie musi zapewniać integrację z przynajmniej takimi systemami jak: konsola programu antywirusowego, moduł EDR.
  - Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: numer seryjny, informacje o systemie, procesor, pamięć RAM, karty sieciowe).
  - Serwer administracyjny musi posiadać możliwość tworzenia grup komputerów.
  - Rozwiązanie musi zapewniać korzystanie z min. 100 szablonów raportów, przygotowanych przez producenta lub własnych raportów tworzonych przez administratora.
  - Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email oraz do dziennika syslog.
  - Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami.
  - Rozwiązanie musi informować administratora o niezainstalowanych aktualizacjach systemowych.
- Opcjonalny moduł NDR (Network Detection and Response - moduł punktowany dodatkowo).
- Wykonawca wraz z system SIEM może dostarczyć moduł Network Detection and Response wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla min. 120 adresów IP wraz z wsparciem technicznym na okres min. 24 miesięcy. Minimalne wymagania dla modułu NDR:

- Wielowątkowy silnik detekcji umożliwiający obsługę ruchu liczonego w dziesiątkach Gigabitów
- Możliwość obsługi wielu podsieci VLAN
- Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
- Obsługa biblioteki wyrażeń regularnych HyperScan
- Możliwość aktualizacji reguł bez wyłączania/ponownego uruchamiania silnika detekcji
- Obsługa wielowątkowości procesora
- Możliwość analizy kopii ruchu w sieci LAN w czasie rzeczywistym bez ingerencji w ruch sieciowy
- Rejestracja żądań HTTP
- Rejestracja i przechowywanie certyfikatów TLS
- Możliwość wyodrębnienia plików z analizowanego ruchu sieciowego i zapisania ich na dysku do późniejszej analizy
- Możliwość przechwytywania pakietów danych przesyłanych w sieci LAN i zapisywanie ich dla późniejszej analizy offline
- Tworzenie raportów w przypadku wykrycia ruchu opisanego regułami jako ruch niebezpieczny
- Rejestrowanie i dogłębna analiza ruchu szyfrowanego TLS/SSL
- Rejestrowanie wszystkich kluczy wymiany do analizy oraz w celu zapobiegania podmianie
- Rejestrowanie, zapisywanie ruchu HTTP z dowolnego portu do pliku w celu późniejszej analizy
- Możliwość identyfikacji, wyodrębniania i rejestrowania plików w ruchu HTTP
- Rejestracja wszystkich zapytań i odpowiedzi DNS
- Funkcja wykrywania włamań sieciowych
- Funkcja zapobiegania włamaniom sieciowym
- funkcja monitorowania bezpieczeństwa sieci LAN
- Pełne wsparcie dla protokołu IPv6
- Możliwość dekodowania tuneli: IP-IP, IP6-IP4, IP4-IP6, GRE, VXLAN, Geneve, Teredo
- Silnik analizy strumienia danych TCP

- Defragmentacja pakietów w celu poddania ich analizie IPS
  - Możliwość obsługi wielu podsieci VLAN
  - Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
  - Możliwość modyfikacji reguł
  - Możliwość zdefiniowania niebezpiecznych plików przez parametry: wielkość, nazwa, rozszerzenie
  - Możliwość wykrywania złośliwego oprogramowania w oparciu o odcisk palca JA3, JA3S
  - Możliwość wykrywania złośliwego oprogramowania w oparciu o metodę HASSH
  - Obsługa dekodowania pakietów: IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, PPP, PPPoE, Raw, SLL, VLAN, QINQ, MPLS, ERSPAN, VXLAN
  - Dekodowanie warstwy aplikacji: HTTP, HTTP/2, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, ENIP/CIP, DNP3, NFS, NTP, DHCP, TFTP, KRB5, IKEv2, SIP, SNMP, RDP, RFB
  - Możliwość tworzenia raportów zgodnych z standardem JSON, SYSLOG,
  - Możliwość filtrowania alertów z podziałem na wagę/priorytet
  - Możliwość filtrowania alertów dla wybranej reguły z podziałem na wagę/priorytet
  - Wspierane systemy operacyjne: Windows, Linux, FreeBSD, OpenBSD, MacOS, Mac OS X
  - Obsługa przekazywania alertów „dalej” do systemów takich jak: syslog, eve.log, JSON, Unified 2
  - Filtrowanie alertów na poziomie: reguł, hostów, sieci
- Opcjonalny moduł SOAR (moduł punktowany dodatkowo).
- Wykonawca wraz z system SIEM może dostarczyć moduł SOAR wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla min. 120 adresów IP wraz z wsparciem technicznym na okres min. 24 miesięcy. Minimalne wymagania dla modułu SOAR:
  - Możliwość wysyłania powiadomień Push UP o wykrytym incydencie powyżej zdefiniowanego priorytetu wysyłane na urządzenie mobilne z system Android lub iOS.
  - Możliwość wysyłania powiadomień SMS o wykrytym incydencie powyżej określonego priorytetu wysyłane na zdefiniowane numery telefonów.

- Możliwość integracji zewnętrznego systemu z oferowanym systemem SIEM poprzez dedykowane API
- Możliwość zablokowania podejrzanego, potencjalnie niebezpiecznego ruchu sieciowego (LAN, WAN) do danych adresów IP na zarządzanych hostach (serwery, stacje robocze)
- Możliwość obserwacji w czasie rzeczywistym lub wyznaczonych interwałach czasowych określonych plików (np. systemowych) generując alerty, gdy te pliki zostaną zaatakowane lub zmodyfikowane.
- Min. jedna zintegrowana z modułem zarządzania incydentami baza przetworzonych incydentów, znanych zagrożeń, regularnie aktualizowana o nowe incydenty, zagrożenia.
- Możliwość porównania nowo utworzonego incydentu z posiadaną bazą opracowanych incydentów, znanych zagrożeń w wyniku czego administrator otrzymuje listę podobnych incydentów oraz listę incydentów zawierających zmienne obserwacyjne zawarte w nowym incydencie.
- Możliwość przeszukiwania bazy incydentów pod kątem konkretnej zmiennej obserwacyjnej.
- Możliwość klasyfikacji wykrytych zdarzeń na podstawie min. 16 stopniowej skali oraz możliwość modyfikacji poziomów skali wg potrzeb administratora.
- Możliwość klasyfikacji utworzonych incydentów na podstawie kryteriów:
- waga, min. 4 poziomy
- poufność, możliwość nadania incydentowi parametru poufny czyli incydent zawierający dane wrażliwe wymagające szczególnej ochrony
- tagi, możliwość przypisania tagu dla incydentu
- zadanie, możliwość tworzenia zadań w ramach incydentów oraz przypisywania operatora dla zadania
- Możliwość integracji SOAR z usługą katalogową Windows Active Directory.
- Możliwość automatycznego uruchamiania zdefiniowanych działań w odpowiedzi na wykryty incydent, na przykład izolacja hosta, zablokowanie ruchu sieciowego lub zatrzymanie procesu.
- Możliwość integracji z różnymi narzędziami bezpieczeństwa, takimi jak systemy antywirusowe, firewalle, czy też narzędzia do monitorowania ruchu sieciowego.



- Możliwość wykorzystania algorytmów heurystycznych do automatycznego analizowania podejrzanych zachowań lub wzorców w systemie.
- Możliwość dostosowania filtrów, które pomagają w identyfikacji istotnych zdarzeń oraz redukcji fałszywych alarmów, zwiększając ciągłość przepływu pracy.
- Możliwość tworzenia dynamicznych skryptów i reguł reakcji na incydenty, umożliwiających dostosowanie się do zmieniających się warunków i nowych rodzajów zagrożeń.
- Możliwość integracji z platformami chmurowymi oraz możliwość monitorowania i zarządzania SOAR w środowisku chmurowym.
- Możliwość dynamicznego zarządzania dostępem do zasobów w przypadku wykrycia podejrzanego ruchu sieciowego, obejmujące blokowanie dostępu do określonych adresów IP na zarządzanych hostach.
- Możliwość współpracy z systemem IDS i IPS poprzez dedykowane API, umożliwiając wspólne korzystanie z informacji o wykrytych incydentach i zoptymalizowanie działań obronnych.
- Możliwość generowania automatycznych zadań w ramach incydentów.

➤ Oprogramowanie do monitorowania infrastruktury informatycznej

W ramach realizacji zadania Wykonawca dostarczy licencje bezterminowe z wsparciem technicznym na okres min. 24 miesięcy, dokona instalacji, konfiguracji oraz podłączenia wszystkich wymaganych systemów będących celem monitorowania. System musi spełniać poniższe wymagania minimalne:

Użytkownicy	
1	<ul style="list-style-type: none"><li>▪ Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat.</li><li>▪ Zapewnienia równoległego dostępu do systemu dla wielu użytkowników.</li><li>▪ Ograniczania użytkownikom dostępu do wybranych grup hostów.</li></ul>
Monitorowanie	

2	<ul style="list-style-type: none"><li>▪ Monitorowania serwerów fizycznych.</li><li>▪ Monitorowania urządzeń sieciowych.</li><li>▪ Monitorowania stanu połączeń.</li><li>▪ Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów</li><li>▪ Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux.</li><li>▪ Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych.</li><li>▪ Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń.</li><li>▪ Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu.</li><li>▪ Grupowanie hostów.</li><li>▪ Definiowanie planowanych przerw serwisowych dla hostów i usług.</li><li>▪ Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).</li><li>▪ Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych).</li><li>▪ Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).</li><li>▪ Monitorowanie serwerów za pomocą agentów</li><li>▪ Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server.</li><li>▪ Monitorowanie Active Directory.</li><li>▪ Monitorowanie serwerów plików, udziałów sieciowych.</li><li>▪ Monitorowanie statusu serwerów Apache.</li><li>▪ Monitorowanie baz danych:<ul style="list-style-type: none"><li>– ORACLE,</li><li>– MySQL,</li><li>– Postgress.</li><li>– MSSQL Server</li><li>– DB2</li></ul></li><li>▪ Monitorowanie urządzeń przez następujące protokoły:<ul style="list-style-type: none"><li>– SNMP,</li><li>– WMI,</li></ul></li></ul>
---	---

	<ul style="list-style-type: none"> <li>– IPMI.</li> <li>▪ Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW.</li> <li>▪ Monitorowanie poprawności działania DNS.</li> <li>▪ Monitorowanie środowiska VMware.</li> <li>▪ Monitorowanie środowiska Hyper-V.</li> <li>▪ Monitorowanie środowisk Proxmox</li> <li>▪ Monitorowanie działania serwera czasu NTP.</li> <li>▪ Monitorowanie offsetu czasu na serwerach.</li> <li>▪ Monitorowanie ping - czasy odpowiedzi, straty pakietów.</li> <li>▪ Monitorowanie zajętości miejsca na poszczególnych partycjach.</li> <li>▪ Monitorowanie obciążenia dysków.</li> <li>▪ Monitorowanie wykorzystania pamięci RAM.</li> <li>▪ Monitorowanie obciążenia CPU.</li> <li>▪ Monitorowanie logów systemowych Windows.</li> <li>▪ Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia.</li> <li>▪ Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane.</li> <li>▪ Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix.</li> <li>▪ Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence)</li> <li>▪ Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe</li> <li>▪ Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów).</li> <li>▪ Wykrywanie niestabilnie działających usług.</li> <li>▪ Monitorowanie dostępności stron internetowych.</li> <li>▪ Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń).</li> </ul>
	Prezentacja
3	<ul style="list-style-type: none"> <li>▪ Prezentację stanu urządzeń na mapie.</li> <li>▪ Prezentację danych na dashboardach.</li> <li>▪ Elastyczną konfigurację dashboardów, wybór elementów.</li> <li>▪ Wizualizację stanu działania całej infrastruktury na jednym dashboardzie.</li> </ul>

	<ul style="list-style-type: none"> <li>Tworzenie indywidualnych dashboardów przez użytkowników</li> </ul>
Powiadomienia	
4	<ul style="list-style-type: none"> <li>Globalne wyłączenie powiadomień.</li> <li>Powiadamianie użytkownika o problemach przez e-mail.</li> <li>Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie.</li> <li>Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników.</li> <li>Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług</li> </ul>
Konfiguracja	
5	<ul style="list-style-type: none"> <li>Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW</li> <li>Automatyczna konfiguracja i działanie z REST-API</li> <li>Centralne zarządzanie agentami</li> <li>Integracja danych z różnych źródeł danych (JSON, XML, SNMP)</li> </ul>
Monitoring bazy danych systemu HIS	
6	<p>Możliwość monitorowania bazy danych systemu HIS w zakresie co najmniej:</p> <ul style="list-style-type: none"> <li>Instance state</li> <li>Version</li> <li>Jobs</li> <li>Locks</li> <li>Processes</li> <li>Number of active sessions</li> <li>Recovery area</li> <li>Log switch activity</li> <li>General tablespace information</li> <li>Tablespaces performance</li> <li>Long active sessions</li> </ul>

	<ul style="list-style-type: none"> <li>– Undo retention</li> <li>– Checkpoint and online backup state</li> <li>– Custom SQLs</li> <li>– RMAN backup status</li> <li>– RMAN backups</li> <li>– ASM disk groups</li> <li>– Apply and transport lag of Oracle Data-Guard</li> <li>– Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości</li> </ul>
Kolektor logów	
7	<ul style="list-style-type: none"> <li>▪ System posiada własny kolektor logów syslog</li> <li>▪ Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps</li> <li>▪ Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event</li> <li>▪ Klasyfikuje wiadomości bazując zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe.</li> </ul>
Cyberbezpieczeństwo	
8	<ul style="list-style-type: none"> <li>▪ System monitoruje urządzenia klasy UTM minimum w zakresie: <ul style="list-style-type: none"> <li>– wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika</li> <li>– monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany” jest uważany za OK, a status „niezsynchronizowany” CRIT.</li> <li>– monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz” (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda” (1).</li> <li>– monitoruje aktualną liczbę sesji na urządzeniu</li> <li>– monitoruje liczbę dostępnych tuneli IPSec VPN</li> <li>– monitoruje wykrywanie wirusów i szybkość blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika.</li> <li>– monitoruje poziom wykorzystania procesora</li> <li>– Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog</li> <li>System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog.</li> </ul>
Monitoring	
9	<p>W ramach usługi Wykonawca monitoruje co najmniej krytyczne elementy infrastruktury IT:</p> <ul style="list-style-type: none"> <li>Serwer fizyczny – do 4 sztuk</li> <li>maszyna wirtualna Windows / Linux / hosty – do 15 sztuk</li> <li>serwer AD - 2 sztuki</li> <li>Macierze / NASy – do 3 sztuk</li> <li>Przełącznik rdzeniowy – 2 sztuki</li> <li>Przełącznik dostępowy (LAN) – do 6 sztuk</li> <li>Zasilacz awaryjny (UPS) - 2 sztuki</li> <li>Serwer Backupu - 1 sztuka</li> </ul>

## II.14 Dostawa i wdrożenie dedykowanego serwera do oprogramowania SIEM – 1 szt

Dostawa, instalacja w szafie rack, instalacja hypervizora, konfiguracja do pracy w sieci LAN Zamawiającego, podłączenie redundantne serwera do rdzenia sieci.

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami umożliwiającymi wysunięcie i wszystkimi elementami niezbędnymi do zamontowania serwera w szafie).

Procesor	Procesor max. 16 rdzeniowy, osiągający w teście SPECrate®2017_int_base wynik co najmniej 174 punkty. Płyta główna obsługująca procesory od 16 do 128 rdzeni, wymagających mocy 400W i obsługujących do 3TB pamięci RAM.
Liczba procesorów	1
Pamięć operacyjna	Zainstalowanych min. osiem modułów 64 GB DDR5 4800MT/s. Płyta główna z minimum 12 slotami na pamięć, umożliwiającą instalację do minimum 3TB pamięci RAM, obsługująca moduły 4800 MT/s Obsługa zabezpieczeń: Advanced ECC.
Sloty rozszerzeń	Możliwość instalacji 6 kart PCI-Express generacji 5 pełnej wysokości, x16 (szybkość slotu – bus width).
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę min. 8 dysków oraz obsługujący poziomy: RAID 0,1,10,5,50,6,60, nie zajmujący gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.
Dysk twardy	Możliwość instalacji do 20 dysków 3,5”. Zainstalowane min. 3 dyski o pojemności 20TB każdy oraz min. 5 dysków SSD o pojemności min. 3.8 TB każdy.
Urządzenie rozruchowe	Zainstalowana karta rozruchowa, umożliwiającą start hypervizora VMware lub Hyper-V, zainstalowane min. 2 dyski NVMe o pojemności min. 240GB, sprzętowy RAID 1.
Interfejsy sieciowe	Zainstalowane dwie karty sieciowe z dwoma portami 10Gb SFP+ każda, wraz z modułami SFP+. Zainstalowana karta z 4 portami 1Gb BASE-T, karta nie może zajmować slotów PCI-ex.
Karta graficzna	Zintegrowana karta graficzna z pamięcią min. 16 MB, umożliwiającą wyświetlenie obrazu min. 1920 x 1200@60Hz
Porty	Min. 4 porty USB 3.2 wbudowane (w tym min. 1 port wewnętrzny i 1 z przodu obudowy) 1 port VGA

	<p>Możliwość rozbudowy/rekonfiguracji o port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express</p> <p>1x port RJ-45 dedykowany dla interfejsu zdalnego zarządzania</p>
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy maximum 1000W, efektywność zasilaczy 94%
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Zarządzanie i obsługa techniczna	<p>Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej oserwera niezależnie od jego stanu (także podczas startu, restartu OS). Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja.</p>
Karta/moduł zarządzający i system zarządzania	<p>Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:</p> <ul style="list-style-type: none"> <li>• monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe</li> <li>• praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP</li> <li>• dostęp do karty zarządzającej poprzez</li> </ul>



	<ul style="list-style-type: none"><li>- dedykowany port RJ45 z tyłu serwera lub</li><li>- przez współdzielony port zintegrowanej karty sieciowej serwera</li></ul> <p>dostęp do karty możliwy</p> <ul style="list-style-type: none"><li>- z poziomu przeglądarki webowej (GUI)</li><li>- z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SMCLP)</li><li>- z poziomu skryptu (XML/Perl)</li><li>- poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)</li></ul> <ul style="list-style-type: none"><li>• wbudowane narzędzia diagnostyczne</li><li>• zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego</li><li>• obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przysyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie</li><li>• wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników</li><li>• przysyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)</li><li>• obsługa zdalnego serwera logowania (remote syslog)</li><li>• wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów</li></ul>
--	---

	<ul style="list-style-type: none"> <li>• mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie</li> <li>• funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności</li> <li>• monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji</li> <li>• konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)</li> <li>• zdalna aktualizacja oprogramowania (firmware)</li> <li>• zarządzanie grupami serwerów, w tym: <ul style="list-style-type: none"> <li>- tworzenie i konfiguracja grup serwerów</li> <li>- sterowanie zasilaniem (wł/wył)</li> <li>- ograniczenie poboru mocy dla grupy (power capping)</li> <li>- aktualizacja oprogramowania (firmware)</li> <li>- wspólne wirtualne media dla grupy</li> </ul> </li> <li>• możliwość równoczesnej obsługi przez 6 administratorów</li> <li>• autentykacja dwuskładnikowa (Kerberos)</li> <li>• wsparcie dla Microsoft Active Directory</li> <li>• obsługa SSL i SSH</li> <li>• enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli</li> <li>• wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API</li> <li>• wsparcie dla Integrated Remote Console for Windows clients</li> <li>• możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)</li> </ul>
Wsparcie dla systemów	Min. Microsoft Windows Server 2019, 2022 Min. Red Hat Enterprise Linux (RHEL): 8.6, 9.0

operacyjnych i systemów wirtualizacyjnych	Min. SUSE Linux Enterprise Server (SLES) 15 Min. VMware ESXi 7.0 U3, 8.0
Gwarancja	<p>Minimum 3-letnia gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site, z max. 1 godzinnym czasem reakcji przez całą dobę, 7 dni w tygodniu oraz możliwość połączenia ze specjalistą. Wymagany czas rozpoczęcia naprawy do 6 godzin w miejscu instalacji, 7 dni w tygodniu.</p> <p>Usługa wsparcia technicznego musi być świadczona przez autoryzowany serwis producenta oferowanych urządzeń.</p> <p>Możliwość rozszerzenia usługi gwarancyjnej do 5 lat realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy 6 godzin i pozostawieniem uszkodzonych dysków u zamawiającego.</p>
Inne	<p>Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.</p> <p>Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.</p>

## II.15 Zakup usług SOC zapewniających prewencję, detekcję i reakcję na zagrożenia cyberbezpieczeństwa – 16 miesięcy

### 1.1 Słownik pojęć:

Skrót lub Pojęcie	Opis
Best Effort	Stan realizacji usługi, w którym zostały przekroczone ograniczenia SLA ze względu na wystąpienie zwiększonego zapotrzebowania na usługę. W przypadku przekroczenia ograniczeń SLA Wykonawca niezwłocznie poinformuje Zamawiającego o zaistniałej sytuacji.
Cyberbezpieczeństwo	Adekwatny do potrzeb stan ochrony zapewniający możliwość wykrycia oraz reagowania na zdarzenia niepożądane oraz wskazane w dokumentacji systemu zarządzania bezpieczeństwem informacji Zamawiającego.
Cyberprzestrzeń	Przestrzeń, w której następuje wymiana, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikacja między człowiekiem i komputerem.
Czas	Wszystkie wskazania w dokumencie w zakresie czasu dotyczą czasu w aktualnej strefie czasowej przyjętej jako czas urzędowy obowiązujący w Polsce.
Departament	Komórka organizacyjna w strukturach Zamawiającego, odpowiedzialna za bezpieczeństwo informacji.

Bezpieczeństwa	
Dzień roboczy	Od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego.
Incydent Bezpieczeństwa Informacji (Incydent)	Pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
Koordinator Wykonawcy	Osoba z ramienia Wykonawcy odpowiedzialna za podejmowanie decyzji w zakresie realizacji spełniania warunków SLA usługi oraz za kontakt z Zamawiającym. Koordinator może mieć jednego lub wielu zastępców.
Okres przejściowy	Czas, w którym Wykonawca zobowiązany będzie do podjęcia działań, których celem będzie przejęcie wiedzy od Zamawiającego o jego systemie monitoringu, uzgodnienia z Zamawiającym wzoru Miesięcznego Raportu Rozliczenia Usług, ustalenia z Zamawiającym harmonogramu wdrożenia dla pierwszych scenariuszy użycia oraz dopasowanie i uzgodnienie zasad współpracy Zamawiającego z systemami Wykonawcy. Zakończenie okresu przejściowego potwierdzone zostanie Protokołem Odbioru.
Koordinator Zamawiającego	Osoba z ramienia Zamawiającego odpowiedzialna za podejmowanie decyzji w zakresie realizacji usługi. Koordinator może mieć jednego lub wielu zastępców.

Miejsce świadczenia usługi monitorowania cyberbezpieczeństwa	Miejsce świadczenia usługi Monitorowania Cyberbezpieczeństwa przez zespół Wykonawcy spełniające wymagania ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
Pierwsza Linia Wsparcia	<p>Pierwsza Linia Wsparcia SOC – usługa realizująca w szczególności zadania:</p> <ul style="list-style-type: none"> <li>• Identyfikacji zdarzeń;</li> <li>• Analizy i eliminacji najprostszych znanych zdarzeń</li> </ul>
Druga Linia Wsparcia	<p>Druga Linia Wsparcia SOC – usługa realizująca w szczególności zadania:</p> <ul style="list-style-type: none"> <li>• Współpracy w reakcji na zdarzenia skomplikowane i nieznanne;</li> <li>• Tworzenie Scenariuszy Reakcji na powtarzalne zdarzenia;</li> <li>• Nadzór nad poprawnością działania konfiguracji scenariuszy użycia;</li> </ul>
On-call	Dyżur pod telefonem, oczekiwanie w gotowości na zgłoszenie Drugiej Linii Wsparcia, wyłącznie dla Incydentów o priorytecie Poważnym.
CTI/OSINT	Ang. Cyber Threat Intelligence/OpenSource Intelligence - narzędzia dostarczające szczegółowe informacje o technikach hakerskich, zagrożeniach, podatnościach, artefaktach lub umiejętności ich interpretowania i dekodowania oraz czynności pozwalające na pozyskanie informacji z powszechnie dostępnych źródeł umożliwiających powiększenie zakresu wiedzy na temat potencjalnych zagrożeń.
Praca ciągła	Praca systemu w trybie 24/7/365 dni.
PUODO	Prezes Urzędu Ochrony Danych Osobowych – organ właściwy do spraw ochrony danych osobowych na terytorium Polski, utworzony ustawą z 10

	maja 2018 roku o ochronie danych osobowych. Jest również organem nadzorczym w rozumieniu ogólnego rozporządzenia o ochronie danych.
RODO	Ustawa o ochronie danych osobowych z dnia 28 maja 2018 roku uszczegółowiające wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) jest odpowiedzią na wyzwania związane ze zmieniającą się gospodarką danych osobowymi.
SOC	Security Operations Center – centrum operacji bezpieczeństwa, którego zadaniem jest monitorowanie, zapobieganie, wykrywanie, badanie i reagowanie na cyber zagrożenia.
Scenariusz Reakcji	Dokument opisujący wymagane czynności w przypadku wykrycia zdarzenia nieporządnego, składający się z: <ul style="list-style-type: none"> <li>• Zestawu możliwości technicznych wykrycia zdarzenia;</li> <li>• Zdefiniowanych warunków wywołania zdarzenia niepożądanego;</li> <li>• Opisu identyfikacji zdarzeń zależnych;</li> <li>• Instrukcji reakcji na zdarzenie;</li> <li>• Instrukcji uruchomienia działań korekcyjnych;</li> <li>• Instrukcji wykonywania działań informacyjnych;</li> <li>• Ogólnych i szczegółowych ścieżek eskalacyjnych.</li> </ul>
Scenariusz użycia systemu bezpieczeństwa	Dokument opisujący zestaw zadań wymaganych do wykonania w ramach Drugiej Linii Wsparcia, w skład którego wchodzi między innymi:

	<ul style="list-style-type: none"> <li>• Skonfigurowanie jednego lub kilku źródeł zdarzeń;</li> <li>• Przygotowanie Scenariuszy Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia.</li> </ul>
SLA	Zestaw wartości granicznych dla kluczowych wskaźników wydajności, dla których określona realizacja usługi jest wymagany w zakresie jakościowym.
System analizy logów	System umożliwiający zbieranie i analizę logów z urządzeń, sieci i systemów informatycznych
Transfer Wiedzy	Usługa przekazywania kompetencji w zakresie realizacji usług Pierwszej i Drugiej Linii Wsparcia.
Usługa monitorowania Cyberbezpieczeństwa	Zestaw czynności wykonywanych przez Wykonawcę w ramach umowy w celu identyfikacji Incydentów Bezpieczeństwa Informacji.
Zdarzenia niepożądane	Zdarzenie mogące wskazywać na wystąpienie incydentu bezpieczeństwa w środowisku chronionym.
Zdarzenie False-Negative	Wykrycie przez Drugą Linię Wsparcia, zdarzenia nie poprawnie rozpoznanego przy zastosowaniu ustalonych i zaakceptowanych procedur bezpieczeństwa. Realizacja i rozpoznawanie zdarzeń „False-Negative”.
Zdarzenie False-Positive	Wykrycie przez automatyczne systemy zdarzenia, które po analizie zostało uznane jako zdarzenie poprawne. W przypadku notorycznego



	występowania, statystycznie rozumianego jako więcej niż 100 zdarzeń „False - Positive” na 1 incydent bezpieczeństwa w miesiącu, należy uznać regułę automatyczną tworzącą takie zdarzenia jako błędną konfigurację systemu bezpieczeństwa.
Przypadek testowy	Celowe wykonanie pełnego przebiegu zdarzenia od momentu wystąpienia sytuacji niepożądanego do momentu zakończenia przetwarzania fazy analizy incydentu. Gdy jest to możliwe, obejmuje wykonanie odwracalnych kroków reakcji na incydent, sprawdzenie scenariusza end-to-end łącznie z zablokowaniem wskaźników kompromitacji w narzędziach prewencyjnych.

### 1.2 Termin realizacji usługi SOC

1. Świadczenie Usługi SOC rozpoczęte zostanie w terminie określonym na etapie tworzenia planu wdrożenia.
2. Termin, o którym mowa w punkcie 1.2 podpunkt 1 licząc od dnia podpisania umowy do rozpoczęcia świadczenia usługi, traktuje się jako okres przejściowy, w którym Wykonawca zobowiązany będzie do podjęcia działań, których celem będzie dopasowanie i uzgodnienie zasad współpracy. Zakończenie okresu przejściowego potwierdzone zostanie Protokołem Odbioru.
3. Wykonawca do świadczenia usługi będzie wykorzystywał narzędzia dostarczone w niniejszym postępowaniu oraz udostępnione przez Zamawiającego. Dostęp do narzędzi i systemów Zamawiającego musi być zrealizowany za pomocą bezpiecznego połączenia szyfrowanego.

### 1.3 Wymagania dla Usługi SOC (Security Operations Center)

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie Analizy Logów zgodnie z opisanymi poniżej wymaganiami.

### 1.4 Pierwsza i Druga Linia Wsparcia

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie Analizy Logów zgodnie z opisanymi poniżej wymaganiami.

#### Pierwsza Linia Wsparcia

W ramach realizacji zadań Pierwszej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa zgodnie warunkami określonymi w punkcie:  
Ogólne warunki SLA.

Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.

Analizę i eliminację najprostszyc znanych zdarzeń określonych w ramach Scenariusza Reakcji.

Łączenie (korelowanie) zdarzeń i incydentów cyberbezpieczeństwa.

Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszy Reakcji.

Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.

Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive).

Priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa.

Przygotowywanie raportów wykrytych zdarzeń bezpieczeństwa.

#### 1.5 Druga Linia Wsparcia

W ramach realizacji zadań Drugiej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

Dostępność usługi dla Zamawiającego zgodnie z określonymi warunkami SLA (Ogólne warunki SLA).

Analizę zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń poincydentalnych.

Przygotowywanie i realizację Scenariuszy użycia systemu bezpieczeństwa zgodnie z wymaganiami przedstawionymi przez Zamawiającego.

Przygotowanie Scenariuszy Reakcji.

Przygotowanie Miesięcznych raportów z realizacji prac.

## 1.6 Scenariusze

Scenariusz użycia systemu bezpieczeństwa

Zamawiający wymaga przygotowania i wdrożenia możliwych scenariuszy użycia dla zidentyfikowanych przez Zamawiającego ryzyk. Harmonogram wdrożenia zostanie ustalony w okresie przejściowym dla pierwszych scenariuszy użycia, pozostałe scenariusze zostaną przygotowane w uzgodnionym terminie. Każdorazowo Scenariusz użycia musi zostać zaakceptowany przez Zamawiającego. Zamawiający posiada listę przykładowych scenariuszy użycia, które należy przygotować i wdrożyć. Przykładowe scenariusz użycia:

Wykrywanie logowania z pominięciem kanału szyfrowanego

Wykrywanie utworzenia użytkownika (lokalnego i domenowego)

Wykrycie złośliwego oprogramowania na chronionym obiekcie

Minimalny zakres zadań, z których ma być zbudowany Scenariusz użycia systemu bezpieczeństwa zawiera:

Skonfigurowanie jednego lub kilku źródeł zdarzeń,

Stworzenie Scenariusza Reakcji w zakresie czynności wykonywanych przez Pierwszą Linję Wsparcia,

Opisanie szczegółowej ścieżki eskalacji,

Opracowanie scenariusza manualnego lub automatycznego sprawdzania poprawności działania. W przypadku pojawienia się nowych skuteczniejszych technik identyfikacji zagrożeń, Wykonawca ma obowiązek zaktualizować w porozumieniu z Zamawiającym istniejące Scenariusze użycia systemu bezpieczeństwa.

#### Scenariusz Reakcji

Przygotowany przez Wykonawcę oraz zatwierdzony przez Zamawiającego Scenariusz Reakcji określa minimalny zestaw czynności konieczny do udokumentowania oraz wyciągnięcia powtarzalnych wniosków, na podstawie których zostaną podjęte określone czynności. Scenariusz Reakcji składa się z podzadań realizujących funkcje:

Wzbogacenia wiedzy o artefaktach tj. adresy IP, domeny, hash'e plików, nazwy plików, rozpoznawalność wskaźników kompromitacji w celu wyciągania adekwatnych wniosków i podejmowania trafnych decyzji,

Analizy zidentyfikowanego zdarzenia, w tym w szczególności potwierdzenia, że zagrożenie w przypadku uruchomienia w środowisku Zamawiającego może stać się incydem lub jest incydem, jak również rozpoczęcia pobierania lub zabezpieczenia dodatkowych danych z zaatakowanego źródła ataku zasobu na potrzeby realizacji Pierwszej Linii Wsparcia,

Reakcji rozumianej jako ograniczenie możliwości wystąpienia zdarzenia niepożądanego, uruchomienia procesu eskalacyjnego lub innych czynności stosownych do zagrożenia w zakresie uzgodnionym z Zamawiającym,

Informowania i raportowania obejmującego dokumentowanie wykonanych czynności oraz rezultatów przeprowadzonej analizy lub zasadności czynności reakcji.

### 1.7 Raport Poincydentalny

Zamawiający wymaga przygotowania Raportu Poincydentalnego dla incydentów o priorytecie Poważnym i Wysokim nie później niż do 2 dni roboczych od zakończenia realizacji zawierającego informacje:

Unikalny identyfikator zdarzenia

Kiedy incydent wystąpił?

Kiedy incydent został zauważony / wykryty?

Kto lub jaki proces był sprawcą incydentu?

Co się wydarzyło?

Gdzie wydarzenie miało miejsce?

Dlaczego zdarzenie mogło wystąpić?

Jakie czynności zostały przeprowadzone w celu powstrzymania incydentu?

Zalecenia Poincydentalne zawierające informację jakie zabezpieczenia zostały ustanowione lub powinny zostać ustanowione w celu zapobieżenia ponownemu wystąpieniu incydentu.

W przypadku przygotowania zaleceń, dla których konieczne jest wprowadzenie istotnych zmian do systemów bezpieczeństwa lub jakiegokolwiek rekonfiguracji systemów Zamawiającego Koordynator Wykonawcy przedstawi do akceptacji Koordynatorowi Zamawiającego zakres i szczegółową listę zmian. Zwolnione z takiej czynności są Zalecenia Poincydentalne konieczne do powstrzymania zidentyfikowanego Incydentu zagrażającego cyberbezpieczeństwu infrastruktury lub danych Zamawiającego.

## 1.8 Systemy Zamawiającego wymagające monitorowania

Usługa monitorowania, będąca przedmiotem zamówienia, będzie oparta o logi/dane z poniższych systemów Zamawiającego (źródła logów) udostępnionych przez Zamawiającego:

Rodzaj usługi lub urządzenia	Liczba urządzeń / nodów będących źródłami logów
Active Directory (liczba serwerów)	
Windows Server	
Linux Server	
DNS, DHCP	
Systemy bezpieczeństwa np.: serwer systemu antywirusowego, web application firewall, NAC, DLP	
Centralny Firewall / UTM	
Pomocniczy Firewall / UTM	
IPS / IDS	

VPN	
Przełączniki sieci LAN, punkty dostępne WiFi	

Zamawiający na bieżąco będzie aktualizował listę źródeł logów wysyłających nowe dane do Wykonawcy.

### 1.9 Administracja Systemem Analizy Logów:

W ramach realizacji zadań administracji Systemem Analizy Logów Wykonawca będzie odpowiedzialny za:

Informowanie Zamawiającego o awariach Systemu Analizy Logów, mogących uniemożliwić poprawne działanie systemów informacyjnych Zamawiającego i/lub świadczenie usług ujętych w niniejszym dokumencie,

Rekomendowanie zmiany zasobów takich jak: vCPU, vRAM, pamięć masowa.

Optymalizowanie konfiguracji Systemu Analizy Logów w celu nieprzekraczania wartości licencji Systemu posiadanego przez Zamawiającego oraz niezwłocznego zgłaszania sytuacji przekroczenia poziomu utylizacji licencji.

Konfigurację Systemu Analizy Logów w celu gromadzenia i normalizowania logów ze wskazanych systemów Zamawiającego zgodnie z tabelą z punktu: Systemy Zamawiającego wymagające monitorowania

Weryfikację czy System Analizy Logów prawidłowo analizuje logi

Tworzenie wymagań dla systemów Zamawiającego wysyłających logi w zakresie poziomu logowania zdarzeń.

#### 1.10 Testowanie Systemu Analizy Logów:

W ramach realizacji zadań testowania Systemu Analizy Logów Wykonawca będzie odpowiedzialny za:

Przygotowanie i uzyskanie aprobaty Zamawiającego dla scenariuszy testów Systemu Analizy Logów,

Weryfikację wdrożonych scenariuszy użycia oraz implementacji nowych przypadków zgłoszonych przez Zamawiającego,

Weryfikację możliwości wdrożenia przypadków użycia w środowisku Zamawiającego,

Analiza złośliwego oprogramowania:

W ramach realizacji umowy, Zamawiający będzie mógł zlecić Wykonawcy wykonanie analizy złośliwego oprogramowania, nie więcej niż 6 w ciągu roku. Sposób zgłaszania analizy złośliwego oprogramowania zostanie uzgodniony po podpisaniu umowy.

Zakres analizy złośliwego oprogramowania będzie nie mniejszy niż:

Analiza statyczna wskazanej próbki złośliwego oprogramowania,

Analizy dynamiczna w kontrolowanym środowisku pozwalającym na wyłączenie funkcji ukrywania lub wykrywania analizy,

W przypadku wykorzystywania rodziny malware określenia wersji

Każdorazowo po wykonanej analizie złośliwego oprogramowania Wykonawca przekaże drogą mailową raport z wykonanej analizy. Zakres raportu zostanie ustalony po podpisaniu umowy.

Ogólne warunki SLA



Wykonawca zapewni świadczenie Usługi monitorowania zgodnie z określonym poziomem SLA.

Nazwa usługi	Poziom świadczonej usługi																	
<p>Pierwsza Linia Wsparcia</p> <p>Czasy dla pierwszych zdarzeń każdego dnia w wymiarze 30 zdarzeń, pozostałe zadania realizowane będą w trybie „Best Effort”</p>	<p>Dostępność usługi w dni robocze pomiędzy godzinami 8:00 a 17:00.</p> <table><tr><th rowspan="2">Priorytet zdarzenia</th><th colspan="2">Czas od wykrycia przez L1 do</th></tr><tr><th>Podjęcia</th><th>Realizacji</th></tr><tr><td>Poważny</td><td>30 min</td><td>4 h</td></tr><tr><td>Wysoki</td><td>60 min</td><td>8 h</td></tr><tr><td>Średni</td><td>2 h</td><td>12 h</td></tr><tr><td>Niski</td><td>4 h</td><td>24 h</td></tr></table>	Priorytet zdarzenia	Czas od wykrycia przez L1 do		Podjęcia	Realizacji	Poważny	30 min	4 h	Wysoki	60 min	8 h	Średni	2 h	12 h	Niski	4 h	24 h
Priorytet zdarzenia	Czas od wykrycia przez L1 do																	
	Podjęcia	Realizacji																
Poważny	30 min	4 h																
Wysoki	60 min	8 h																
Średni	2 h	12 h																
Niski	4 h	24 h																

<p>Druga Linia Wsparcia</p> <p>Czasy dla pierwszych Incydentów każdego dnia w wymiarze 5 incydentów, pozostałe zadania realizowane w trybie „Best Effort”</p>	<p>Dostępność usługi w dni robocze pomiędzy godzinami 8:00 a 17:00.</p> <table><tr><th rowspan="2">Priorytet incydentu</th><th colspan="2">Czas od eskalacji pierwszej linii wsparcia do</th></tr><tr><th>Podjęcia</th><th>Realizacji</th></tr><tr><td>Poważny</td><td>30 min</td><td>24 h</td></tr><tr><td>Wysoki</td><td>60 min</td><td>2 dni</td></tr><tr><td>Średni</td><td>2 h</td><td>4 dni</td></tr></table>	Priorytet incydentu	Czas od eskalacji pierwszej linii wsparcia do		Podjęcia	Realizacji	Poważny	30 min	24 h	Wysoki	60 min	2 dni	Średni	2 h	4 dni
Priorytet incydentu	Czas od eskalacji pierwszej linii wsparcia do														
	Podjęcia	Realizacji													
Poważny	30 min	24 h													
Wysoki	60 min	2 dni													
Średni	2 h	4 dni													
<p>Analiza złośliwego oprogramowania</p>	<p>Rozpoczęcie analizy w terminie do 2 dni roboczych od przekazania podejrzanej próbki oprogramowania przez Koordynatora Zamawiającego do Koordynatora Wykonawcy oraz potwierdzenia otrzymania próbki przez Koordynatora Wykonawcy.</p>														
<p>Scenariusz użycia systemu bezpieczeństwa</p>	<p>Przygotowanie i wdrożenie scenariusza użycia systemu wraz ze scenariuszami reakcji w terminie do 5 dni roboczych od przekazania informacji od Koordynatora Zamawiającego do Koordynatora</p>														

	Wykonawcy z wyjątkiem scenariuszy ujętych w harmonogramie przygotowanym w okresie przejściowym.
--	---

W uzasadnionych przypadkach Wykonawca ma prawo zwrócenia się do Zamawiającego o zgodę na zawieszenie SLA na usługę Pierwszej i Drugiej Linii Wsparcia na uzgodniony z Zamawiającym okres jednak nie dłuższy niż 14 dni. Wniosek o zawieszenie SLA musi zawierać uzasadnienie. Zamawiający w takim przypadku zobowiązany jest do rozpatrzenia prośby w ciągu 1 dnia roboczego od chwili uzyskania informacji o tym fakcie. W przypadku odmowy Zamawiający jest zobowiązany w ciągu 3 Dni Roboczych do przedstawienia pisemnego uzasadnienia odmowy, wskazując obiektywne czynniki świadczące o bezzasadności wniosku Wykonawcy.

Czas podjęcia Incydentu będzie liczony jako delta czasu pomiędzy odnotowaniem wystąpienia zdarzenia przez pierwszą linię wsparcia a czasem nadania priorytetu.

Czas realizacji Incydentu będzie liczony jako delta czasu pomiędzy podjęciem incydentu a zakończeniem obsługi podsumowanym wydanymi wstępnymi rekomendacjami i/lub raportem, w zależności od przypisanego scenariusza reakcji.

Zamawiający wyróżnia cztery poziomy incydentów: Poważny, Wysoki, Średni, Niski. Domyślnie każdy incydent zarejestrowany, jeżeli nie zostanie to uszczegółowione inaczej ma priorytet Średni.

Minimalny miesięczny czas świadczenia usług analizy zdarzeń to 16 godzin miesięcznie.

Priorytet	Opis
Poważny	Priorytet jest stosowany wyłącznie w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO;

	<p>Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika;</p> <p>Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&amp;C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min);</p> <p>Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanых lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych;</p> <p>Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszonego w ramach inicjatywy Trusted Introducers;</p> <p>Potwierdzona informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową;</p> <p>Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa;</p> <p>Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego;</p> <p>Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności;</p> <p>Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych;</p>
--	---

	<p>Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej;</p> <p>Zgłoszenie incydentu Poważnego skutkuje bezzwłocznym uruchomieniem u Zamawiającego procesu eskalacyjnego KSC lub RODO;</p>
Wysoki	<p>Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym;</p> <p>Ujawnienie zestawionej sesji zwrotnej z C&amp;C, trwającej co najmniej od 30 minut, aktywnie wykorzystywanej przez atakującego (więcej niż 1kb/min);</p> <p>Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w strefie chronionej;</p> <p>Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszony w ramach inicjatywy Trusted Introducers;</p> <p>Potwierdzona Informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową;</p> <p>Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa;</p> <p>Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego;</p>

	<p>Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności;</p> <p>Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, upload na dyski webowe lub przenoszenie przez nieautoryzowane pendrive;</p> <p>Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamывania zabezpieczeń (tzw. grayware);</p> <p>Ujawnienie nieznanego przez VirusTotal lub inne bazy reputacyjne oprogramowania mającego złośliwe funkcje pozwalające operatorowi na uruchomienie nieautoryzowanych skryptów lub kodu;</p> <p>Celowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;</p>
Średni	<p>Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym;</p> <p>Nieautoryzowane dysponowanie uprawnieniami administracyjnymi;</p> <p>Częściowo personalizowany atak na personel zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;</p> <p>Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane</p>

	<p>przez system antywirusowy, ale nie zostało zatrzymane przez inny system bezpieczeństwa;</p> <p>Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome lub nieświadome działanie;</p>
Niski	<p>Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa.</p>

#### 1.11 Transfer wiedzy.

Zamawiający wymaga, aby w każdym półroczu trwania umowy, Wykonawca przeprowadził dla grupy nie większej niż 6 osób wskazanych przez Koordynatora Zamawiającego warsztaty. Łączny wymiar godzin w półroczu wynosi nie więcej niż 4. Spotkanie ma formę Warsztatów prowadzonych w formie zdalnej. Niewykorzystane godziny nie kumulują się i nie przechodzą na kolejne okresy.

Warsztaty swoim zakresem będą obejmować:

Wyjaśnianie zagrożeń płynących z wykrytych i opisanych incydentów

Wyjaśnianie sposobów implementacji zaleceń opisanych w Raportach Miesięcznych

Szczegółowy harmonogram warsztatów oraz lista uczestników zostaną uzgodnione przez Koordynatorów stron.

#### 1.12 Raportowanie i rozliczanie pracy

Miesięczny Raport Rozliczenia Usług

Każdy miesiąc świadczenia Usług podsumowany zostanie Raportem Miesięcznym wg według wzoru przedstawionego przez Wykonawcę. Wykonawca zobowiązany jest przedstawić Raport wraz z listą zaleceń do wykonania przez personel Zamawiającego w terminie 5 Dni Roboczych od dnia zakończenia miesiąca kalendarzowego, w którym była świadczona Usługa.

Zamawiający zastrzega sobie prawo zgłoszenia zastrzeżeń do Raportu, w terminie do 5 Dni roboczych od dnia jego otrzymania i zażądać uzupełnienia lub poprawy Raportu w terminie do 3 dni roboczych. Po uwzględnieniu przez Wykonawcę uwag do Raportu, Zamawiający w terminie kolejnych 3 Dni roboczych zweryfikuje ostateczną treść Raportu.

Dostarczony Raport Miesięczny bez uwag jest potwierdzeniem prawidłowego wykonania Usługi w miesiącu, którego dotyczy.

Raport składa się z sekcji:

Monitorowanie cyberbezpieczeństwa

Data świadczenia usług

Zestawienie obsługiwanych incydentów

Identyfikator incydentu

Nazwa

Klasyfikacja priorytetu Incydentu

Dokładna data i godzina ujawnienia incydentu

Statusy końcowe

Ogólne rekomendacje i zalecenia Zamawiającego w zakresie cyberbezpieczeństwa w nawiązaniu do obsługiwanych Incydentów w celu eliminacji możliwości pojawienia się incydentów w przyszłości.



Analiza złośliwego oprogramowania

Data świadczenia usług

Lista zgłoszonych analiz złośliwego oprogramowania

Liczba analiz przeprowadzonych zgodnie z SLA

### 1.13 Zespół SOC

Dla zapewnienia prawidłowej realizacji usługi SOC Zamawiający stawia minimalny wymóg dla składu zespołu SOC:

Operatorzy I linii SOC – 2 osoby

Operatorzy II linii SOC – 1 osoba

SOC manager – 1 osoba

Zarządzania podatnościami – 1 osoba

Eksperti od bezpieczeństwa urządzeń – 1 osoba

Eksperti od ochrony danych osobowych – 1 osoba

Eksperti od zgodności z NIS2 i KSC – 1 osoba

Wymagania dodatkowe

Cała dokumentacja powinna być dostarczana w edytowalnej postaci elektronicznej, w formacie przetwarzanym przez MS Word, Excel (od wersji 2007) lub PDF.

Zamawiający wymaga zatrudnienia przez Wykonawcę na podstawie umowy o pracę przez cały okres realizacji zamówienia 2 (dwóch) osób, wykonujących usługi w zakresie czynności Pierwszej oraz Drugiej

Linii Wsparcia związanych z obsługą realizacji przedmiotu zamówienia, jeżeli wykonywane przez nich czynności polegają na wykonywaniu pracy w rozumieniu przepisu art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t. j. Dz. U. z 2018 r., poz. 917, z późn. zm.). Zamawiający uzna za spełniony obowiązek zatrudnienia osób wykonujących usługi w zakresie czynności pierwszej linii wsparcia przy realizacji przedmiotu zamówienia na podstawie umowy o pracę w przypadku, gdy Wykonawca skieruje do realizacji zamówienia własnych pracowników (dwóch) lub pracowników zatrudnionych na umowę o pracę. Zamawiający nie będzie ingerować w sposób prowadzenia działalności oraz organizację pracy administracyjno-biurowej Wykonawcy.

Wykonawca zobowiązany zostanie do przestrzegania polityki bezpieczeństwa opisanej w Polityce Bezpieczeństwa Informacji dla dostawców, która stanowi załącznik do umowy. O zmianach polityki mogących mieć wpływ na realizację umowy Wykonawca zostanie bezzwłocznie poinformowany.

## **II.16 Szkolenie specjalistyczne dla administratorów z dostarczanych pakietów bezpieczeństwa i konfiguracji urządzeń i sieci dla urządzeń UTM – 2 szt.**

### **A. Szkolenie techniczne, poświęcone urządzeniom do ochrony styku sieci firmowej z Internetem firmy – voucher na szkolenie ważny przez okres min. 12 miesięcy dla dwóch pracowników zamawiającego**

Szkolenie zakończenie egzaminem oraz certyfikatem, czas trwania min. 3 dni roboczych. Szkolenie musi łączyć teorię oraz zajęcia praktyczne (warsztaty) przy użyciu nowoczesnego sprzętu i oprogramowania. Po zakończeniu szkolenia Zamawiający będzie miał możliwość kontaktu z trenerem w terminie do 14 dni od zakończenia szkolenia. Zakres szkolenia:

1. Zbieranie logów i monitorowanie
  - a. Przedstawienie kategorii zbieranych logów
  - b. Wykresy historyczne i monitorowanie
2. Obiekty
  - a. Typy obiektów oraz ich wykorzystanie
  - b. Obiekty sieciowe i obiekt typu „router”

### 3. Konfiguracja sieci

- a. Tryby pracy urządzenia
- b. Typy interfejsów (Ethernet, modem, bridge, VLAN, GRE/TAP)
- c. Typy routingu oraz ich priorytety

### 4. Translacja adresów sieciowych (NAT)

### 5. Translacja połączeń wychodzących (maskarada)

### 6. Translacja połączeń przychodzących (przekierowanie)

### 7. Translacja dwukierunkowa (jeden do jeden)

### 8. Filtrowanie ruchu sieciowego (Firewall)

### 9. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)

- a. Szczegółowy opis parametrów reguły Firewall
- b. Kolejność przetwarzania reguł Firewall i NAT

### 10. Ochrona aplikacji

- a. Implementacja filtrowania URL dla ruchu http i https
- b. Konfigurowanie skanowania antywirusowego i modułu Breach Fighter
- c. Moduł IPS i stosowanie profili inspekcji

### 11. Użytkownicy i uwierzytelnianie

### 12. Konfiguracja usługi katalogowej

- a. Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)
- b. Rejestracja użytkowników
- c. Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania

### 13. Wirtualne sieci prywatne (VPN)

- a. Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)
- b. Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)
- c. Tunele VTI

### 14. SSL VPN

- a. Zasada działania
- b. Konfiguracja

---

**B. Zaawansowane szkolenie techniczne, poświęcone urządzeniom do ochrony styku sieci firmowej z Internetem firmy – 1 voucher na szkolenie ważny przez okres min. 12 miesięcy dla dwóch pracowników zamawiającego**

Szkolenie zakończenie egzaminem oraz certyfikatem, czas trwania min. 3 dni roboczych. Szkolenie musi łączyć teorię oraz zajęcia praktyczne (warsztaty) przy użyciu nowoczesnego sprzętu i oprogramowania. Po zakończeniu szkolenia Zamawiający będzie miał możliwość kontaktu z trenerem w terminie do 14 dni od zakończenia szkolenia. Zakres szkolenia:

1. Szczegółowe omówienie działania modułu IPS
  - a. Różnice pomiędzy IPS a IDS
  - b. moduł IPS
  - c. Różne tryby analizy
  - d. Profile oparte na protokołach i aplikacjach
2. Infrastruktura klucza publicznego
  - a. Podstawy szyfrowania symetrycznego - i asymetrycznego
  - b. Typy szyfrowania
  - c. Infrastruktura klucza publicznego
  - d. Tworzenie urzędu certyfikacji, certyfikatów serwera i użytkowników
3. SSL Proxy
  - a. Zasada działania
  - b. Konfiguracja SSL Proxy
  - c. Zaawansowana konfiguracja tuneli IPSec VPN
  - d. Szczegółowy opis działania mechanizmu NAT traversal
  - e. Obsługa funkcji DPD (Dead Peer Detection)
  - f. Architektura sieci VPN typu „gwiazda” i „mesh”
  - g. NAT w sieciach IPSec VPN
  - h. Konfiguracja zapasowego - tunelu IPSec VPN
  - i. Konfiguracja tuneli Site-to-Site w oparciu o certyfikaty
  - j. Konfiguracja tuneli dla użytkowników mobilnych (Client-2-Site)
4. GRE i GRE-TAP
  - a. Zasada działania
  - b. Konfiguracja i instalacja
5. Transparentne uwierzytelnianie użytkowników

- a. Zasada działania
  - b. Metoda uwierzytelniania SPNEGO
  - c. Metoda uwierzytelniania oparta na certyfikatach SSL
6. Wysoka dostępność (HA)
- a. Zasada działania
  - b. Kreator umożliwiający tworzenie i konfigurowanie klastra HA
  - c. Konfiguracja interfejsu sieciowego
  - d. Zaawansowana konfiguracja

## **II.17 Szkolenie specjalistyczne dla administratorów z administracji dostarczanych systemów operacyjnych. – 1 szt.**

Wykonawca zapewni przeprowadzenie szkoleń przez certyfikowanego inżyniera producenta oprogramowania w co najmniej poniższym zakresie:

- Identyfikacja zagrożeń występujących w środowisku Windows lub równoważnym wg norm ISO/IEC
- Bezpieczne uwierzytelnianie i ochrona poświadczeń w systemie Windows lub równoważnym (z wykorzystaniem narzędzia MimiKatz)
- Autoryzacja dostępu do zasobów
- Kontrola praw i uprawnień użytkowników
- Infrastruktura Klucza Publicznego
- Uwierzytelnianie dwuskładnikowe w oparciu o karty inteligentne
- Szyfrowanie danych w oparciu o dobre praktyki
- Network Policy Server
- Analiza ruchu sieciowego
- Konfiguracja uprawnień usług systemowych
- Analiza bezpieczeństwa i hardening systemów

- Zarządzanie poprawkami systemowymi i omówienie mechanizmu Windows Update for Business

### Rozdział III. Gwarancja

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją”) na niniejszy przedmiot zamówienia:

**1) Dostawa i wdrożenie Infrastruktury sprzętowej wraz z oprogramowaniem:**

Poz. OPZ	Opis	Gwarancja
Rozdział	Rodzaj zamawianego asortymentu*,**	
II.2	Dostawa i wdrożenie urządzenia UTM*	24 miesiące
II.3	Dostawa i wdrożenie macierzy dyskowej wraz z konfiguracją funkcji HyperMirror i podłączeniem serwerów*,**	36 miesięcy
II.4	Dostawa i wdrożenie serwera zapasowego*,**	36 miesięcy
II.5	Dostawa i wdrożenie systemu DLP	24 miesiące
II.6	Dostawa i wdrożenie urządzenia NAS*,**	36 miesięcy

II.7	Dostawa i wdrożenie oprogramowania do wykonywania kopii zapasowych według polityki i harmonogramu tworzenia kopii zapasowych	12 miesięcy
II.8	Dostawa i wdrożenie zarządzalnych urządzeń sieciowych do rdzenia sieci*	24 miesiące
II.9	Dostawa i wdrożenie zarządzalnych urządzeń sieciowych dla punktów dostępowych*	24 miesiące
II.10	Dostawa i wdrożenie systemu NAC	24 miesiące
II.11	Dostawa oprogramowania antywirusowego	24 miesiące
II.12	Dostawa i podłączenie zasilacza awaryjnego UPS	36 miesięcy
II.13	Dostawa i wdrożenie oprogramowania SIEM	12 miesięcy
II.14	Dostawa i wdrożenie dedykowanego serwera do oprogramowania SIEM*, **	36 miesięcy
II.16	Szkolenie specjalistyczne dla administratorów z dostarczanych pakietów bezpieczeństwa i konfiguracji urządzeń i sieci dla urządzeń UTM	12 miesięcy

II.17	Szkolenie specjalistyczne dla administratorów z administracji dostarczanych systemów operacyjnych.	12 miesięcy
-------	--	-------------

\* W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).

\*\* W przypadku awarii dysków pozostają one własnością Zamawiającego.

2. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem podpisania Protokołu Odbioru Końcowego bez uwag przez Zamawiającego.

### III.1 Wady

1. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia rozumianych jako Awaria lub Błąd lub Usterka zgodnie z definicjami jak poniżej:
  - 1) **Awaria** - Kategoria Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiający jego użytkowanie. Sytuacja, w której dane rozwiązanie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia
  - 2) **Usterka** - Należy przez to rozumieć kategorię Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz OPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
2. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany SZ) przy czym:
  - 1) System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający,
  - 2) za skuteczne przyjęcie zgłoszenia Wady uważa się będzie wprowadzenie przez Zamawiającego wpisu do SZ zawierającego opis zgłaszanej Wady i termin jej zgłoszenia; w razie trudności z dostępem on-line do SZ, zgłoszenia Wady mogą odbywać się także telefonicznie pod ustalonym



numerem telefonu lub pisemnie na formularzu przesyłanym na ustalony adres e-mail, opcjonalnie faksem, których numery i adresy zostaną podane przez Wykonawcę w terminie 15 dni roboczych od dnia podpisania Umowy wraz ze wzorem formularza zgłoszenia Wady.

3. Gwarancja musi zapewniać wymianę uszkodzonego sprzętu, kabli i elementów oraz zapewniać dostęp do aktualizacji oprogramowania, bez wiedzy i wsparcia technicznego producenta.
4. W ramach gwarancji Wykonawca będzie świadczył następujące usługi:
  - 1) Usuwanie Wad w dostarczonym Przedmiocie Zamówienia w przypadku stwierdzenia przez Zamawiającego Wady w jego działaniu, w terminach określonych poniżej:

**Tabela 1. Usługi gwarancji dla Infrastruktury sprzętowej i oprogramowania:**

KWALIFIKACJA A ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE*	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	niezwłocznie, nie później niż 48 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 14 dni od czasu przyjęcia zgłoszenia
USTERKA		nie dotyczy	niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie nie później niż 30 dni od dnia przyjęcia zgłoszenia

\* nie dotyczy sprzętu zastępczego

- 2) dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną,
- 3) czasy naprawy mogą być inne niż wskazane w powyższej tabeli, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 2),

- 4) w przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego,
- 5) Wykonawca w okresie trwania gwarancji, do 5 dnia każdego miesiąca, przedstawi Zamawiającemu raport zawierający co najmniej: numer zgłoszenia, kwalifikację zgłoszenia, godzinę i datę zgłoszenia, temat zgłoszenia, status zgłoszenia, godzinę i datę usunięcia Wady, czas naprawy,

Uwaga:

W przypadku zapisu terminu jako:

- Dzień Roboczy należy rozumieć każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
- Godziny Robocze należy rozumieć godziny:
  - Poniedziałek-Środa:  
**7.30 - 15.30**
  - Czwartek:  
**7.30 - 16.00**
  - Piątek:  
**7.30 - 15.00**

W innych przypadkach należy rozumieć jako dzień kalendarzowy.