**Załącznik nr 2 do SWZ**

# OPIS PRZEDMIOTU ZAMÓWIENIA

## 1. Przedmiot Zamówienia:

Przedmiotem zamówienia jest dostawa rozwiązań z zakresu cyberbezpieczeństwa dla środowisk IT i OT spełniających minimalne wymagania określone przez Zamawiającego.

## 2. Miejscem realizacji

Miejscem realizacji przedmiotu zamówienia są obiekty Zamawiającego w Kościerzynie.

## 3. Ogólne warunki realizacji zamówienia

Ogólne warunki realizacji zamówienia:

1. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
2. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
3. Wykonawca zapewni takie opakowanie sprzętu, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
4. Wykonawca ponosi odpowiedzialność za sprzęt i oprogramowanie do momentu podpisania protokołu odbioru.
5. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.
6. Wszystkie prace związane z zakresem prac w środowisku serwerowym oraz sieciowym wykonywane będą na obiektach Zamawiającego w Kościerzynie.
7. Ilekroć w dokumentacji użyto nazwy własnej produktu, producenta lub oprogramowania, należy ją rozumieć jako „lub rozwiązanie równoważne" spełniające wymagania określone przez Zamawiającego.
8. Wszelkie nazwy własne produktów, urządzeń, producentów, systemów, aplikacji, oprogramowania lub technologii wskazane w dokumentacji postępowania należy traktować wyłącznie jako przykładowe, służące określeniu oczekiwanych parametrów technicznych, funkcjonalnych, jakościowych, eksploatacyjnych oraz standardu wykonania. Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych, pod warunkiem, że zapewnią one funkcjonalność, wydajność, kompatybilność, niezawodność oraz parametry nie gorsze niż rozwiązania wskazane w opisie przedmiotu zamówienia. Wykonawca jest zobowiązany wykazać równoważność oferowanego rozwiązania. W każdym przypadku decydujące znaczenie dla oceny oferty mają wymagane funkcjonalności i parametry użytkowe, a nie nazwa handlowa, producent lub marka danego produktu, urządzenia czy oprogramowania. Zamawiający nie ogranicza konkurencji do konkretnych producentów ani dostawców rozwiązań.

# 4. Część 1: Audyty

## 1. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest świadczenie usługi polegającej na opracowaniu, wdrożeniu, przeglądzie oraz aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), opracowaniu, wdrożeniu, przeglądzie oraz aktualizacji Systemu Zarządzania Ciągłością Działania (SZCD), opracowaniu planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla systemów teleinformatycznych, a także przeprowadzeniu audytów w zakresie SZBI, SZCD oraz zgodności z obowiązującymi wymaganiami prawnymi i normatywnymi.

**Przedmiot zamówienia obejmuje realizację następujących zadań:**

1. Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
2. Przeprowadzenie audytów SZBI, SZCD, audytu zgodności z wymaganiami wynikającymi z przepisów dotyczących Krajowych Ram Interoperacyjności (KRI) oraz ustawy o krajowym systemie cyberbezpieczeństwa (uKSC)
3. Opracowanie planów ciągłości działania (BCP) oraz planów odtwarzania po awarii (DRP) dla systemów teleinformatycznych.
4. Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Ciągłością Działania (SZCD).

Wykonawca zobowiązany jest do realizacji przedmiotu zamówienia w sposób zapewniający zgodność z obowiązującymi przepisami prawa, odpowiednimi normami, dobrymi praktykami oraz wymaganiami określonymi w niniejszym Opisie Przedmiotu Zamówienia.

Wszystkie opracowywane dokumenty, procedury, instrukcje, rejestry oraz pozostałe produkty realizacji zamówienia muszą być przygotowane z uwzględnieniem specyfiki działalności Zamawiającego, jego struktury organizacyjnej, realizowanych procesów, wykorzystywanej infrastruktury teleinformatycznej oraz obowiązujących regulacji wewnętrznych. Niedopuszczalne jest przekazanie dokumentacji o charakterze uniwersalnym, niewymagającej dostosowania do rzeczywistych uwarunkowań funkcjonowania Zamawiającego.

W ramach realizacji zamówienia Wykonawca zobowiązany jest do ścisłej współpracy z przedstawicielami Zamawiającego, prowadzenia uzgodnień roboczych oraz uwzględniania uzasadnionych uwag zgłaszanych na etapie realizacji poszczególnych zadań.

Szczegółowy zakres rzeczowy poszczególnych zadań określono w dalszej części niniejszego Opisu Przedmiotu Zamówienia.

## 2. Cel realizacji zamówienia

Celem realizacji zamówienia jest podniesienie poziomu bezpieczeństwa informacji oraz odporności organizacyjnej i technologicznej Zamawiającego poprzez opracowanie, wdrożenie i utrzymanie skutecznych mechanizmów zarządzania bezpieczeństwem informacji oraz ciągłością działania.

Realizacja zamówienia ma zapewnić w szczególności:

1. wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dostosowanego do specyfiki działalności Zamawiającego;
2. wdrożenie Systemu Zarządzania Ciągłością Działania (SZCD) zapewniającego utrzymanie lub szybkie odtworzenie kluczowych procesów w przypadku wystąpienia sytuacji kryzysowych;
3. opracowanie planów ciągłości działania (BCP) oraz planów odtwarzania po awarii (DRP) dla systemów teleinformatycznych wspierających realizację zadań Zamawiającego;
4. ocenę stopnia zgodności funkcjonujących rozwiązań organizacyjnych, technicznych i proceduralnych z obowiązującymi przepisami prawa, wymaganiami norm oraz dobrymi praktykami poprzez przeprowadzenie niezależnych audytów;
5. identyfikację obszarów wymagających doskonalenia oraz opracowanie rekomendacji umożliwiających podniesienie poziomu bezpieczeństwa informacji i ciągłości działania;
6. przygotowanie Zamawiającego do skutecznego utrzymywania, przeglądu i ciągłego doskonalenia wdrożonych systemów zarządzania;
7. zwiększenie odporności organizacji na zagrożenia związane z cyberbezpieczeństwem, awariami infrastruktury, błędami ludzkimi oraz innymi zdarzeniami mogącymi zakłócić realizację procesów biznesowych.

Realizacja zamówienia powinna prowadzić do stworzenia spójnego systemu zarządzania bezpieczeństwem informacji i ciągłością działania, uwzględniającego uwarunkowania organizacyjne, prawne, techniczne oraz procesowe Zamawiającego, a także wspierającego realizację jego celów statutowych i operacyjnych.

## 3. Zakres zamówienia

Zakres zamówienia obejmuje wykonanie kompleksowych usług doradczych, analitycznych, projektowych, wdrożeniowych oraz audytowych, których celem jest opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), Systemu Zarządzania Ciągłością Działania (SZCD), opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP), a także przeprowadzenie audytów zgodności.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do:

1. przeprowadzenia analizy stanu obecnego w zakresie bezpieczeństwa informacji, cyberbezpieczeństwa oraz ciągłości działania;
2. analizy obowiązujących u Zamawiającego dokumentów, regulacji wewnętrznych, procedur oraz rozwiązań organizacyjnych i technicznych mających wpływ na bezpieczeństwo informacji oraz ciągłość działania;
3. opracowania lub aktualizacji dokumentacji wymaganej do funkcjonowania SZBI oraz SZCD;
4. opracowania planów ciągłości działania (BCP) oraz planów odtwarzania po awarii (DRP) dla systemów teleinformatycznych;
5. przeprowadzenia działań wdrożeniowych niezbędnych do uruchomienia opracowanych rozwiązań organizacyjnych;

6. przeprowadzenia przeglądów opracowanej dokumentacji oraz jej aktualizacji w przypadku stwierdzenia konieczności wprowadzenia zmian;
7. przeprowadzenia audytów zgodności zgodnie z zakresem określonym dla poszczególnych zadań;
8. opracowania raportów, rekomendacji oraz dokumentów będących rezultatem realizowanych prac;
9. przekazania Zamawiającemu kompletnej dokumentacji opracowanej w ramach realizacji zamówienia w wersji elektronicznej edytowalnej oraz w formacie PDF.

Zakres rzeczowy poszczególnych zadań obejmuje:

- **Zadanie 1** – opracowanie, wdrożenie, przegląd i aktualizację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI);
- **Zadanie 2** – przeprowadzenie audytów SZBI, SZCD, audytu zgodności z wymaganiami Krajowych Ram Interoperacyjności (KRI), ustawy o krajowym systemie cyberbezpieczeństwa (uKSC) oraz audytów (re)certyfikacyjnych SZBI i SZCD;
- **Zadanie 3** – opracowanie planów ciągłości działania (BCP) oraz planów odtwarzania po awarii (DRP) dla systemów teleinformatycznych;
- **Zadanie 4** – opracowanie, wdrożenie, przegląd i aktualizację Systemu Zarządzania Ciągłością Działania (SZCD).

Szczegółowy opis zakresu oraz wymaganych produktów dla każdego z powyższych zadań został określony w kolejnych rozdziałach niniejszego Opisu Przedmiotu Zamówienia. Opracowanie dokumentacji nastąpi na podstawie informacji, dokumentów oraz danych przekazanych przez Zamawiającego w toku realizacji zamówienia.

## 4. Zadanie 1 – Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

### 4.1. Cel zadania

Celem zadania jest opracowanie, wdrożenie, przegląd oraz aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), dostosowanego do specyfiki działalności Zamawiającego, obowiązujących przepisów prawa oraz dobrych praktyk w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa.

System powinien umożliwiać skuteczne zarządzanie bezpieczeństwem informacji, ograniczanie ryzyka, zapewnienie odpowiedniego poziomu ochrony zasobów informacyjnych oraz wspierać proces ciągłego doskonalenia organizacji.

### 4.2. Zakres prac

W ramach realizacji zadania Wykonawca zobowiązany będzie do wykonania co najmniej następujących czynności:

1. przeprowadzenia analizy stanu obecnego w zakresie organizacji bezpieczeństwa informacji;

2. identyfikacji procesów mających wpływ na bezpieczeństwo informacji;
3. identyfikacji aktywów informacyjnych oraz zasobów wspierających ich przetwarzanie;
4. identyfikacji zagrożeń, podatności oraz ryzyk związanych z bezpieczeństwem informacji;
5. opracowania lub aktualizacji dokumentacji SZBI;
6. dostosowania dokumentacji do struktury organizacyjnej, procesów oraz uwarunkowań technicznych Zamawiającego;
7. przeprowadzenia konsultacji roboczych z przedstawicielami Zamawiającego;
8. przeprowadzenia działań wdrożeniowych o charakterze organizacyjnym i doradczym, obejmujących przedstawienie opracowanych rozwiązań, wsparcie Zamawiającego w ich wdrożeniu oraz udzielanie wyjaśnień dotyczących sposobu ich stosowania;
9. dokonania przeglądu opracowanego Systemu Zarządzania Bezpieczeństwem Informacji;
10. aktualizacji dokumentacji w przypadku stwierdzenia konieczności wprowadzenia zmian wynikających z przeprowadzonych analiz, uzgodnień lub przeglądów.

**4.3. Minimalne wymagania**

W ramach realizacji zadania Wykonawca zapewni, że:

1. opracowana dokumentacja będzie spójna, kompletna oraz wzajemnie powiązana;
2. dokumentacja zostanie dostosowana do rzeczywistych uwarunkowań organizacyjnych i technicznych Zamawiającego;
3. opracowane dokumenty będą posiadały jednolitą strukturę, numerację oraz zasady nadzoru nad dokumentacją;
4. wdrażane rozwiązania będą uwzględniały obowiązujące przepisy prawa oraz wymagania właściwych norm i standardów wskazanych przez Zamawiającego;
5. dokumentacja zostanie przekazana w formatach umożliwiających jej dalszą edycję oraz w formacie PDF;
6. wszystkie opracowania staną się własnością Zamawiającego i będą mogły być przez niego wykorzystywane, aktualizowane oraz rozwijane bez ograniczeń wynikających z praw autorskich Wykonawcy, z zastrzeżeniem przepisów prawa autorskiego.

**4.4. Produkty końcowe**

Rezultatem realizacji zadania będzie w szczególności:

1. opracowany lub zaktualizowany System Zarządzania Bezpieczeństwem Informacji;
2. komplet dokumentacji SZBI wymaganej zakresem realizowanego projektu;
3. dokumentacja potwierdzająca przeprowadzenie działań wdrożeniowych;

4. raport z przeprowadzonego przeglądu SZBI wraz z rekomendacjami dotyczącymi dalszego doskonalenia systemu, jeżeli zostaną zidentyfikowane obszary wymagające poprawy.

### 4.5. Minimalny zakres produktów

W ramach realizacji Zadania 1 Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu kompletny zestaw produktów niezbędnych do funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji, obejmujący co najmniej:

1. dokumentację ustanawiającą zasady funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji;
2. procedury regulujące procesy związane z zarządzaniem bezpieczeństwem informacji;
3. instrukcje określające sposób realizacji wybranych czynności związanych z bezpieczeństwem informacji;
4. rejestry wymagane do prawidłowego funkcjonowania SZBI;
5. formularze, wzory dokumentów oraz szablony wykorzystywane podczas realizacji procesów wynikających z opracowanej dokumentacji;
6. materiały wspomagające wdrożenie opracowanych rozwiązań organizacyjnych;
7. raporty, zestawienia oraz inne opracowania będące rezultatem wykonanych analiz i prac projektowych.

Zakres, liczba oraz szczegółowość opracowanych produktów powinny wynikać z rzeczywistych potrzeb Zamawiającego oraz zapewniać możliwość skutecznego funkcjonowania, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

Opracowane produkty muszą stanowić spójny i wzajemnie powiązany system dokumentacji oraz uwzględniać specyfikę działalności, strukturę organizacyjną, realizowane procesy, wykorzystywane systemy teleinformatyczne oraz obowiązujące u Zamawiającego regulacje wewnętrzne.

## 5. Zadanie 2 – Audyt SZBI, audyt SZCD, audyt zgodności KRI/uKSC oraz audyty (re)certyfikacyjne

### 5.1. Cel zadania

Celem zadania jest niezależna ocena stopnia zgodności funkcjonujących u Zamawiającego rozwiązań organizacyjnych, proceduralnych i technicznych z wymaganiami obowiązujących przepisów prawa, norm, standardów oraz dokumentacji wewnętrznej, a także identyfikacja obszarów wymagających doskonalenia.

### 5.2. Zakres prac

W ramach realizacji zadania Wykonawca zobowiązany będzie do przeprowadzenia:

1. audytu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI);
2. audytu Systemu Zarządzania Ciągłością Działania (SZCD);
3. audytu zgodności z wymaganiami Krajowych Ram Interoperacyjności (KRI);

4. audytu zgodności z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa (uKSC), w zakresie mającym zastosowanie do Zamawiającego;
5. audytu przygotowującego do certyfikacji lub recertyfikacji SZBI i SZCD

Zakres każdego audytu powinien obejmować co najmniej:

1. analizę obowiązującej dokumentacji;
2. Ocena prowadzona jest na podstawie analizy dokumentacji, wywiadów, obserwacji oraz dowodów przedstawionych przez Zamawiającego;
3. wywiady z przedstawicielami Zamawiającego;
4. weryfikację stosowanych zabezpieczeń organizacyjnych i technicznych;
5. ocenę zgodności z wymaganiami określonymi dla danego audytu;
6. identyfikację stwierdzonych niezgodności, spostrzeżeń oraz możliwości doskonalenia.

**5.3. Minimalne wymagania**

Wykonawca zobowiązany jest do:

1. opracowania programu każdego audytu;
2. przeprowadzenia audytów w sposób zapewniający obiektywność i rzetelność oceny;
3. dokumentowania ustaleń audytowych w sposób umożliwiający ich weryfikację;
4. przedstawienia wyników audytu przedstawicielom Zamawiającego;
5. opracowania raportów zawierających opis stanu faktycznego, wyniki oceny, stwierdzone niezgodności, obserwacje oraz rekomendacje działań doskonalących.

**5.4. Produkty końcowe**

Rezultatem realizacji zadania będzie przekazanie Zamawiającemu:

1. programu audytów;
2. raportów z przeprowadzonych audytów;
3. wykazu stwierdzonych niezgodności, obserwacji oraz obszarów wymagających doskonalenia;
4. rekomendacji działań korygujących i doskonalących;
5. podsumowania wyników audytów wraz z oceną stopnia zgodności z wymaganiami objętymi zakresem audytu.

**5.5. Sposób realizacji audytów**

Audyty objęte przedmiotem zamówienia powinny być prowadzone zgodnie z uznanymi zasadami audytowania systemów zarządzania oraz z uwzględnieniem dobrych praktyk w zakresie planowania, prowadzenia, dokumentowania i raportowania audytów.

W przypadku audytów systemów zarządzania Wykonawca zobowiązany jest stosować metodykę zgodną z wymaganiami normy dotyczącej wytycznych audytowania systemów zarządzania oraz uwzględniać wymagania właściwych norm będących przedmiotem audytu.

Proces audytu powinien obejmować w szczególności:

1. przygotowanie programu i planu audytu;
2. analizę dokumentacji oraz innych materiałów przekazanych przez Zamawiającego;
3. przeprowadzenie wywiadów z osobami odpowiedzialnymi za realizację procesów objętych audytem;
4. ocenę funkcjonowania wdrożonych rozwiązań organizacyjnych, proceduralnych oraz technicznych;
5. udokumentowanie ustaleń audytowych;
6. przedstawienie wyników audytu podczas spotkania podsumowującego;
7. przekazanie raportu końcowego zawierającego wyniki oceny, stwierdzone niezgodności, obserwacje oraz rekomendacje działań doskonalących.

Raport z audytu powinien w sposób jednoznaczny wskazywać podstawę dokonanej oceny oraz zawierać uzasadnienie wszystkich stwierdzonych niezgodności i rekomendowanych działań doskonalących.

## 6. Zadanie 3 – Opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla systemów teleinformatycznych

### 6.1. Cel zadania

Celem zadania jest opracowanie planów ciągłości działania (BCP) oraz planów odtwarzania po awarii (DRP), umożliwiających utrzymanie lub możliwie szybkie przywrócenie realizacji kluczowych procesów oraz funkcjonowania systemów teleinformatycznych w przypadku wystąpienia incydentów, awarii lub innych sytuacji zakłócających działalność Zamawiającego.

### 6.2. Zakres prac

W ramach realizacji zadania Wykonawca zobowiązany będzie do:

1. identyfikacji procesów krytycznych realizowanych przez Zamawiającego;
2. identyfikacji systemów teleinformatycznych wspierających realizację procesów krytycznych;
3. określenia zależności pomiędzy procesami biznesowymi, zasobami informacyjnymi oraz infrastrukturą teleinformatyczną;
4. przeprowadzenia analizy wpływu zakłóceń na działalność Zamawiającego;
5. określenia strategii zapewnienia ciągłości działania oraz odtwarzania po awarii;
6. opracowania planów ciągłości działania (BCP);
7. opracowania planów odtwarzania po awarii (DRP);

8. uzgodnienia opracowanych planów z przedstawicielami Zamawiającego.
9. Opracowanie planów BCP i DRP nastąpi na podstawie informacji oraz danych przekazanych przez Zamawiającego dotyczących procesów, systemów teleinformatycznych, zasobów oraz organizacji pracy

**6.3. Minimalne wymagania**

Opracowane plany powinny:

1. uwzględniać strukturę organizacyjną Zamawiającego oraz realizowane procesy;
2. określać role i odpowiedzialności osób uczestniczących w realizacji działań związanych z ciągłością działania i odtwarzaniem po awarii;
3. zawierać procedury postępowania na wypadek wystąpienia zakłóceń;
4. określać sposób komunikacji w sytuacjach kryzysowych;
5. określać zasady uruchamiania, aktualizacji oraz przeglądu opracowanych planów;
6. być dostosowane do rzeczywistych uwarunkowań organizacyjnych i technicznych Zamawiającego.

**6.4. Produkty końcowe**

Rezultatem realizacji zadania będzie przekazanie Zamawiającemu:

1. planów ciągłości działania (BCP);
2. planów odtwarzania po awarii (DRP);
3. dokumentacji opisującej przyjęte założenia oraz strategie zapewnienia ciągłości działania;
4. rekomendacji dotyczących utrzymania oraz doskonalenia opracowanych planów.

**6.5. Minimalny zakres produktów**

W ramach realizacji zadania Wykonawca opracuje dokumentację umożliwiającą skuteczne zarządzanie ciągłością działania oraz odtwarzaniem po awarii, obejmującą co najmniej:

1. plany ciągłości działania dla procesów objętych zakresem projektu;
2. plany odtwarzania po awarii dla systemów teleinformatycznych objętych zakresem projektu;
3. procedury postępowania w sytuacjach zakłócających ciągłość działania;
4. wykaz ról i odpowiedzialności związanych z realizacją działań wynikających z opracowanych planów;
5. wykaz danych niezbędnych do utrzymania aktualności opracowanych planów.

## 6. Zadanie 4 – Opracowanie, wdrożenie, przegląd i aktualizacja Systemu Zarządzania Ciągłością Działania (SZCD)

### 7.1. Cel zadania

Celem zadania jest opracowanie, wdrożenie, przegląd oraz aktualizacja Systemu Zarządzania Ciągłością Działania (SZCD), zapewniającego przygotowanie Zamawiającego do skutecznego reagowania na zdarzenia zakłócające funkcjonowanie organizacji, utrzymania realizacji procesów krytycznych oraz sprawnego odtworzenia działalności po wystąpieniu incydentów, awarii lub sytuacji kryzysowych.

### 7.2. Zakres prac

W ramach realizacji zadania Wykonawca zobowiązany będzie do:

1. przeprowadzenia analizy stanu obecnego w zakresie zarządzania ciągłością działania;
2. identyfikacji procesów krytycznych oraz zasobów niezbędnych do ich realizacji;
3. opracowania lub aktualizacji dokumentacji Systemu Zarządzania Ciągłością Działania;
4. dostosowania dokumentacji do struktury organizacyjnej, procesów oraz uwarunkowań technicznych Zamawiającego;
5. przeprowadzenia konsultacji roboczych z przedstawicielami Zamawiającego;
6. przeprowadzenia działań wdrożeniowych o charakterze organizacyjnym i doradczym, obejmujących przedstawienie opracowanych rozwiązań, wsparcie Zamawiającego w ich wdrożeniu oraz udzielanie wyjaśnień dotyczących sposobu ich stosowania;
7. przeprowadzenia przeglądu funkcjonowania SZCD;
8. aktualizacji dokumentacji w przypadku konieczności wprowadzenia zmian wynikających z przeglądów, analiz lub zmian organizacyjnych.

### 7.3. Minimalne wymagania

Wykonawca zapewni, że:

1. opracowany System Zarządzania Ciągłością Działania będzie dostosowany do specyfiki działalności Zamawiającego;
2. dokumentacja będzie spójna, kompletna i wzajemnie powiązana;
3. opracowane rozwiązania będą uwzględniały obowiązujące przepisy prawa, wymagania właściwych norm oraz dobre praktyki w zakresie ciągłości działania;
4. dokumentacja zostanie przekazana w wersji edytowalnej oraz w formacie PDF;
5. wszystkie opracowania będą mogły być przez Zamawiającego wykorzystywane, rozwijane i aktualizowane bez konieczności uzyskiwania zgody Wykonawcy, z zastrzeżeniem przepisów prawa autorskiego.

### 7.4. Produkty końcowe

Rezultatem realizacji zadania będzie przekazanie Zamawiającemu:

1. opracowanego lub zaktualizowanego Systemu Zarządzania Ciągłością Działania;
2. kompletnej dokumentacji SZCD wymaganej zakresem realizowanego projektu;

3. dokumentacji potwierdzającej przeprowadzenie działań wdrożeniowych;
4. raportu z przeglądu SZCD wraz z rekomendacjami dotyczącymi dalszego doskonalenia systemu.

**7.5. Minimalny zakres produktów**

W ramach realizacji zadania Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu kompletny zestaw produktów niezbędnych do funkcjonowania Systemu Zarządzania Ciągłością Działania, obejmujący co najmniej:

1. dokumentację ustanawiającą zasady funkcjonowania SZCD;
2. procedury regulujące procesy związane z zarządzaniem ciągłością działania;
3. instrukcje wspierające realizację działań związanych z utrzymaniem i odtwarzaniem działalności;
4. rejestry oraz formularze niezbędne do funkcjonowania SZCD;
5. materiały wspomagające wdrożenie opracowanych rozwiązań;
6. raporty oraz inne opracowania będące rezultatem wykonanych analiz i prac projektowych.

Zakres, liczba oraz szczegółowość opracowanych produktów powinny odpowiadać rzeczywistym potrzebom Zamawiającego i zapewniać skuteczne funkcjonowanie oraz ciągłe doskonalenie Systemu Zarządzania Ciągłością Działania.

## 7. Wymagania dotyczące realizacji zamówienia

**8.1. Wymagania ogólne**

1. Wykonawca zobowiązany jest do realizacji przedmiotu zamówienia z należytą starannością, zgodnie z obowiązującymi przepisami prawa, właściwymi normami, dobrymi praktykami oraz postanowieniami zawartej umowy.
2. Wszystkie prace realizowane będą w ścisłej współpracy z przedstawicielami Zamawiającego.
3. Wykonawca zobowiązany jest do uwzględniania uzasadnionych uwag i wniosków zgłaszanych przez Zamawiającego na każdym etapie realizacji zamówienia.
4. Dokumentacja opracowana w ramach realizacji zamówienia musi zostać dostosowana do rzeczywistej struktury organizacyjnej, realizowanych procesów, wykorzystywanych systemów teleinformatycznych oraz uwarunkowań organizacyjnych Zamawiającego.
5. Niedopuszczalne jest przekazywanie dokumentacji o charakterze uniwersalnym, niewymagającej dostosowania do specyfiki działalności Zamawiającego.

**8.2. Współpraca z Zamawiającym**

1. Wykonawca zobowiązany jest do bieżącego uzgadniania z Zamawiającym istotnych zagadnień związanych z realizacją zamówienia.
2. Zamawiający wyznaczy osoby odpowiedzialne za współpracę z Wykonawcą.

3. Wykonawca zobowiązany jest do udziału w spotkaniach roboczych organizowanych w trakcie realizacji zamówienia, w zakresie niezbędnym do prawidłowego wykonania przedmiotu zamówienia.
4. Forma oraz terminy spotkań będą uzgadniane pomiędzy Stronami.

**8.3. Dokumentacja**

1. Wszystkie dokumenty opracowane w ramach realizacji zamówienia muszą stanowić spójny system dokumentacji.
2. Dokumentacja powinna być przygotowana w sposób umożliwiający jej dalszą aktualizację i rozwój przez Zamawiającego.
3. Każdy dokument powinien posiadać co najmniej:
    1. nazwę dokumentu;
    2. numer lub identyfikator;
    3. numer wersji;
    4. datę opracowania lub aktualizacji;
    5. informację o autorze lub wykonawcy;
    6. historię zmian – jeżeli dotyczy.

**8.4. Konsultacje i uzgodnienia**

1. Wykonawca zobowiązany jest do udzielania wyjaśnień dotyczących opracowanej dokumentacji przez cały okres realizacji zamówienia.
2. W przypadku zgłoszenia przez Zamawiającego uwag do przekazanych opracowań, Wykonawca zobowiązany jest do ich analizy oraz wprowadzenia uzasadnionych zmian.
3. Wszelkie uzgodnienia dokonywane pomiędzy Stronami powinny być dokumentowane w sposób umożliwiający odtworzenie przebiegu realizacji zamówienia.

**8.5. Poufność**

1. Wykonawca zobowiązany jest do zachowania poufności wszystkich informacji uzyskanych w związku z realizacją zamówienia.
2. Informacje pozyskane podczas realizacji zamówienia mogą być wykorzystywane wyłącznie w celu wykonania przedmiotu umowy.
3. Obowiązek zachowania poufności obowiązuje również po zakończeniu realizacji zamówienia, zgodnie z obowiązującymi przepisami prawa oraz postanowieniami umowy.

**8.6. Wersje robocze dokumentacji**

1. Wykonawca zobowiązany jest do przekazywania Zamawiającemu wersji roboczych opracowywanej dokumentacji, w zakresie i terminach uzgodnionych pomiędzy Stronami.

2. Celem przekazania wersji roboczych jest umożliwienie Zamawiającemu dokonania oceny zgodności opracowywanej dokumentacji z wymaganiami określonymi w Opisie Przedmiotu Zamówienia oraz zgłoszenia uwag przed przygotowaniem wersji końcowej.
3. Zamawiający ma prawo zgłaszać uwagi i propozycje zmian do przekazanych wersji roboczych, w zakresie zgodności z przedmiotem zamówienia oraz specyfiką funkcjonowania organizacji.
4. Wykonawca zobowiązany jest do analizy zgłoszonych uwag oraz uwzględnienia uwag uzasadnionych, o ile nie pozostają one w sprzeczności z obowiązującymi przepisami prawa, wymaganiami norm lub zasadami wiedzy technicznej.
5. Przekazanie wersji roboczych oraz zgłaszanie uwag nie stanowi odbioru przedmiotu zamówienia ani jego części.
6. Za wersję końcową dokumentacji uznaje się dokumentację przekazaną przez Wykonawcę po uwzględnieniu uzgodnionych zmian i przeznaczoną do odbioru przez Zamawiającego.

## 9. Wymagania dotyczące produktów końcowych

### 9.1. Wymagania ogólne

1. Wszystkie produkty opracowane w ramach realizacji zamówienia muszą być kompletne, spójne, aktualne oraz zgodne z zakresem określonym w Opisie Przedmiotu Zamówienia.
2. Dokumentacja powinna zostać opracowana z uwzględnieniem specyfiki działalności Zamawiającego oraz odzwierciedlać rzeczywisty sposób funkcjonowania organizacji.
3. Niedopuszczalne jest przekazanie dokumentacji zawierającej treści niezwiązane z działalnością Zamawiającego lub wskazujące na wykorzystanie niezmodyfikowanych wzorów opracowanych dla innych podmiotów.
4. Wszystkie wzajemne odwołania pomiędzy dokumentami muszą być zgodne, kompletne i odnosić się wyłącznie do dokumentów przekazanych w ramach realizacji zamówienia lub obowiązujących u Zamawiającego.
5. Dokumentacja nie może zawierać błędów redakcyjnych, merytorycznych ani oczywistych omyłek pisarskich.
6. Wykonawca ponosi odpowiedzialność za jakość oraz zgodność opracowanej dokumentacji z wymaganiami określonymi w Opisie Przedmiotu Zamówienia.
7. Wykonawca nie ponosi odpowiedzialności za skutki wynikające z przekazania przez Zamawiającego niepełnych, nieaktualnych lub niezgodnych ze stanem faktycznym informacji, dokumentów lub danych mających wpływ na realizację przedmiotu zamówienia.

### 9.2. Forma przekazania dokumentacji

1. Dokumentacja zostanie przekazana w wersji elektronicznej.

2. Wszystkie dokumenty tekstowe muszą zostać przekazane w formacie umożliwiającym ich swobodną edycję oraz w formacie PDF.
3. Arkusze, rejestry, zestawienia oraz formularze powinny zostać przekazane w formatach umożliwiających ich dalszą edycję.
4. Diagramy, schematy oraz inne opracowania graficzne powinny zostać przekazane w postaci umożliwiającej ich późniejszą aktualizację lub modyfikację.

**9.3. Wymagania jakościowe**

Wszystkie opracowania przekazywane Zamawiającemu powinny:

1. posiadać jednolitą strukturę i sposób opracowania;
2. stosować jednolite nazewnictwo oraz terminologię;
3. zawierać poprawne oznaczenia wersji oraz dat opracowania;
4. umożliwiać ich dalszą aktualizację bez konieczności ponownego opracowania całej dokumentacji;
5. stanowić spójny system dokumentów wzajemnie się uzupełniających.

**9.4. Prawa do korzystania z dokumentacji**

1. Z chwilą odbioru przedmiotu zamówienia Zamawiający uzyskuje prawo do wykorzystywania, kopiowania, modyfikowania, aktualizowania oraz rozwijania dokumentacji opracowanej w ramach realizacji zamówienia, zgodnie z postanowieniami zawartej umowy.
2. Wykonawca oświadcza, że przekazane opracowania nie naruszają praw osób trzecich oraz mogą być legalnie wykorzystywane przez Zamawiającego.
3. Jeżeli do realizacji zamówienia wykorzystano materiały osób trzecich, Wykonawca zobowiązany jest zapewnić Zamawiającemu prawo do ich dalszego wykorzystywania w zakresie niezbędnym do korzystania z opracowanej dokumentacji.

**10. Założenia realizacji zamówienia**

1. Zamawiający zobowiązuje się do zapewnienia Wykonawcy dostępu do informacji, dokumentów, zasobów oraz osób niezbędnych do prawidłowej realizacji zamówienia.
2. Zamawiający zobowiązuje się do terminowego przekazywania informacji oraz udzielania wyjaśnień niezbędnych do realizacji przedmiotu zamówienia.
3. Wykonawca realizuje przedmiot zamówienia na podstawie informacji, dokumentów oraz danych przekazanych przez Zamawiającego.
4. Zakres realizacji zamówienia nie obejmuje wykonywania zmian konfiguracyjnych w systemach teleinformatycznych, instalacji lub konfiguracji sprzętu i oprogramowania, wykonywania prac administracyjnych ani świadczenia usług serwisowych, chyba że obowiązek taki wynika wprost z umowy.

5. W przypadku ujawnienia w trakcie realizacji zamówienia okoliczności mających istotny wpływ na zakres prac, Strony dokonają stosownych uzgodnień dotyczących dalszego sposobu realizacji zamówienia zgodnie z postanowieniami umowy.

# 5. Część 2: Szkolenia i testy bezpieczeństwa

## 1. Szkolenia podnoszące świadomość w zakresie cyberbezpieczeństwa

### 1.1. Cel zadania

Celem realizacji zadania jest podniesienie poziomu świadomości pracowników Zamawiającego w zakresie bezpieczeństwa informacji, cyberbezpieczeństwa oraz ciągłości działania poprzez przeprowadzenie szkoleń dostosowanych do zakresu obowiązków poszczególnych grup odbiorców.

Szkolenia powinny wspierać budowanie kultury bezpieczeństwa, rozwijanie umiejętności rozpoznawania zagrożeń oraz właściwego reagowania na incydenty bezpieczeństwa, a także zwiększać świadomość obowiązujących przepisów, regulacji wewnętrznych i dobrych praktyk.

### 1.2. Zakres prac

W ramach realizacji zadania Wykonawca zobowiązany będzie do:

1. uzgodnienia z Zamawiającym zakresu merytorycznego poszczególnych szkoleń;
2. opracowania programu szkoleń odpowiadającego zakresowi zamówienia;
3. przygotowania materiałów szkoleniowych;
4. dostosowania treści szkoleniowych do specyfiki działalności Zamawiającego;
5. przeprowadzenia szkoleń dla wskazanych grup uczestników;
6. udzielania uczestnikom wyjaśnień dotyczących omawianych zagadnień;
7. przekazania materiałów szkoleniowych w uzgodnionej formie.

### 1.3. Minimalne wymagania

1. Zakres każdego szkolenia powinien być dostosowany do grupy odbiorców oraz celu szkolenia.
2. Wykonawca może wykorzystywać własne materiały szkoleniowe, pod warunkiem ich aktualności oraz dostosowania do specyfiki działalności Zamawiającego.
3. Zamawiający przekaże informacje niezbędne do właściwego dostosowania treści szkoleniowych.
4. Szkolenia mogą być realizowane w formie stacjonarnej, zdalnej lub hybrydowej, zgodnie z ustaleniami Stron.
5. Harmonogram realizacji szkoleń zostanie uzgodniony pomiędzy Zamawiającym i Wykonawcą.

### 1.4. Wymagania dotyczące realizacji szkoleń

1. Szkolenia powinny mieć charakter praktyczny i uwzględniać przykłady zagrożeń występujących w działalności jednostek sektora publicznego oraz innych organizacji o podobnym profilu.

2. Zakres szkolenia może obejmować prezentację przykładów rzeczywistych incydentów bezpieczeństwa oraz sposobów ograniczania ich skutków.
3. W trakcie szkolenia Wykonawca może wykorzystywać przykłady, materiały demonstracyjne oraz scenariusze edukacyjne wspierające osiągnięcie celu szkolenia.
4. Wykonawca zobowiązany jest do umożliwienia uczestnikom zadawania pytań dotyczących omawianych zagadnień.

### 1.5. Wymagania dotyczące materiałów szkoleniowych

1. Materiały szkoleniowe powinny odpowiadać zakresowi realizowanego szkolenia.
2. Materiały mogą zostać opracowane z wykorzystaniem materiałów własnych Wykonawcy.
3. Materiały powinny zostać dostosowane do specyfiki działalności Zamawiającego w zakresie niezbędnym do realizacji celu szkolenia.
4. Materiały mogą zostać przekazane uczestnikom w formie elektronicznej lub papierowej.

### 1.6. Wymagania dotyczące prowadzących

1. Szkolenia powinny być prowadzone przez osoby posiadające wiedzę oraz doświadczenie odpowiadające tematyce realizowanego szkolenia.
2. W przypadku realizacji szkoleń przez więcej niż jedną osobę Wykonawca zapewni spójność przekazywanych treści.

### 1.7. Rodzaje szkoleń

Zakres zamówienia obejmuje realizację następujących rodzajów szkoleń:

1. podstawowe szkolenia budujące świadomość cyberzagrożeń;
2. szkolenia dla kadry zgodne z obowiązującymi u Zamawiającego zasadami bezpieczeństwa informacji;
3. szkolenia specjalistyczne dla personelu IT oraz kadry kierowniczej;
4. szkolenia powiązane z testami socjotechnicznymi;
5. usługi typu Security Awareness obejmujące symulacje kampanii phishingowych;
6. szkolenia symulacyjne z zakresu zarządzania sytuacjami kryzysowymi;
7. szkolenia przygotowujące do certyfikacji systemów zarządzania.

Szczegółowy zakres merytoryczny każdego rodzaju szkolenia zostanie uzgodniony z Zamawiającym przed rozpoczęciem jego realizacji.

### 1.8. Dokumentowanie realizacji szkoleń

Po zakończeniu szkolenia Wykonawca przekaże Zamawiającemu dokumentację potwierdzającą jego realizację, obejmującą – w zależności od charakteru szkolenia:

1. program szkolenia;

2. materiały szkoleniowe;
3. potwierdzenie przeprowadzenia szkolenia;
4. listę obecności lub inne potwierdzenie uczestnictwa, jeżeli będzie wymagane przez Zamawiającego;
5. krótkie podsumowanie przeprowadzonego szkolenia.

### 1.9. Produkty końcowe

Rezultatem realizacji zadania będzie przekazanie Zamawiającemu:

1. programu szkoleń;
2. materiałów szkoleniowych;
3. dokumentacji potwierdzającej realizację szkoleń;
4. dokumentów potwierdzających uczestnictwo, jeżeli są wymagane;
5. podsumowania przeprowadzonych działań szkoleniowych, jeżeli wynika to z zakresu realizowanego projektu.

### 1.10. Wymagania jakościowe

1. Wszystkie szkolenia powinny zostać przygotowane i przeprowadzone z należytą starannością oraz zgodnie z aktualnym stanem wiedzy w zakresie cyberbezpieczeństwa.
2. Treści szkoleniowe powinny być zgodne z obowiązującymi przepisami prawa oraz uwzględniać aktualne zagrożenia i dobre praktyki.
3. Zakres merytoryczny szkoleń powinien być dostosowany do poziomu wiedzy uczestników oraz charakteru wykonywanych przez nich obowiązków.
4. Wykonawca nie jest zobowiązany do opracowywania odrębnych materiałów szkoleniowych dla każdej grupy uczestników, o ile zastosowane materiały zapewniają realizację celu szkolenia i zostały odpowiednio dostosowane do zakresu tematycznego.

## 2. Podstawowe szkolenia budujące świadomość cyberzagrożeń

### 2.1. Cel

Celem szkolenia jest zwiększenie świadomości pracowników w zakresie najczęściej występujących zagrożeń cyberbezpieczeństwa oraz przekazanie podstawowych zasad bezpiecznego korzystania z systemów teleinformatycznych, poczty elektronicznej, Internetu oraz urządzeń wykorzystywanych do wykonywania obowiązków służbowych.

### 2.2. Zakres

Szkolenie powinno obejmować zagadnienia związane w szczególności z:

1. podstawowymi zasadami bezpieczeństwa informacji;
2. aktualnymi zagrożeniami cyberbezpieczeństwa;
3. phishingiem, smishingiem, vishingiem oraz innymi metodami socjotechnicznymi;

4. bezpiecznym korzystaniem z poczty elektronicznej;
5. bezpiecznym korzystaniem z Internetu;
6. zasadami stosowania haseł oraz mechanizmów uwierzytelniania;
7. bezpiecznym korzystaniem z urządzeń mobilnych oraz nośników danych;
8. zasadami zgłaszania incydentów bezpieczeństwa;
9. odpowiedzialnością pracowników za bezpieczeństwo informacji.

Zakres szkolenia może zostać rozszerzony o zagadnienia wynikające ze specyfiki działalności Zamawiającego.

### 2.3. Minimalne wymagania

1. Program szkolenia powinien zostać dostosowany do charakteru działalności Zamawiającego.
2. Wykonawca może wykorzystywać własne materiały szkoleniowe, odpowiednio dostosowane do zakresu szkolenia.
3. Podczas szkolenia mogą być wykorzystywane przykłady rzeczywistych incydentów bezpieczeństwa, materiały demonstracyjne oraz scenariusze edukacyjne.
4. Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

### 2.4. Produkty końcowe

Po zakończeniu szkolenia Wykonawca przekaże Zamawiającemu:

1. program szkolenia;
2. materiały szkoleniowe;
3. potwierdzenie realizacji szkolenia;
4. dokumentację potwierdzającą uczestnictwo, jeżeli jest wymagana przez Zamawiającego.

## 3. Szkolenia dla kadry zgodne z polityką bezpieczeństwa informacji

### 3.1. Cel

Celem szkolenia jest przygotowanie kadry kierowniczej oraz osób pełniących funkcje związane z zarządzaniem bezpieczeństwem informacji do właściwego wykonywania obowiązków wynikających z funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji oraz obowiązujących u Zamawiającego regulacji wewnętrznych.

### 3.2. Zakres

Szkolenie powinno obejmować zagadnienia związane w szczególności z:

1. rolą kierownictwa w funkcjonowaniu SZBI;
2. odpowiedzialnością kierownictwa za bezpieczeństwo informacji;
3. polityką bezpieczeństwa informacji oraz dokumentacją SZBI obowiązującą u Zamawiającego;

4. zarządzaniem ryzykiem w zakresie bezpieczeństwa informacji;
5. klasyfikacją informacji oraz zasadami ich ochrony;
6. zarządzaniem incydentami bezpieczeństwa;
7. obowiązkami wynikającymi z przepisów prawa oraz regulacji wewnętrznych;
8. nadzorem nad realizacją działań związanych z bezpieczeństwem informacji;
9. rolą kierownictwa w doskonaleniu Systemu Zarządzania Bezpieczeństwem Informacji.

Zakres szkolenia może zostać rozszerzony o zagadnienia wynikające ze specyfiki działalności Zamawiającego.

### 3.3. Minimalne wymagania

1. Program szkolenia powinien uwzględniać strukturę organizacyjną oraz zakres odpowiedzialności kadry kierowniczej Zamawiającego.
2. Wykonawca może wykorzystywać własne materiały szkoleniowe dostosowane do zakresu szkolenia.
3. Podczas szkolenia mogą zostać omówione przykłady praktycznych sytuacji związanych z funkcjonowaniem SZBI oraz podejmowaniem decyzji dotyczących bezpieczeństwa informacji.
4. Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

### 3.4. Produkty końcowe

Po zakończeniu szkolenia Wykonawca przekaże Zamawiającemu:

1. program szkolenia;
2. materiały szkoleniowe;
3. potwierdzenie realizacji szkolenia;
4. dokumentację potwierdzającą uczestnictwo, jeżeli jest wymagana przez Zamawiającego.

## 4. Szkolenia specjalistyczne dla personelu IT oraz kadry zarządzającej

### 4.1. Cel

Celem szkolenia jest podniesienie kompetencji personelu odpowiedzialnego za utrzymanie, rozwój oraz nadzór nad środowiskiem teleinformatycznym w zakresie bezpieczeństwa informacji, cyberbezpieczeństwa oraz ciągłości działania, z uwzględnieniem obowiązujących przepisów prawa, regulacji wewnętrznych oraz dobrych praktyk.

### 4.2. Zakres

Szkolenie powinno obejmować zagadnienia związane w szczególności z:

1. organizacją bezpieczeństwa systemów teleinformatycznych;
2. zarządzaniem podatnościami oraz procesem ich usuwania;
3. monitorowaniem bezpieczeństwa środowiska teleinformatycznego;
4. zarządzaniem incydentami cyberbezpieczeństwa;

5. zarządzaniem kopiami zapasowymi oraz odtwarzaniem danych;
6. zarządzaniem kontami użytkowników oraz uprawnieniami;
7. bezpieczną konfiguracją systemów i usług;
8. bezpieczeństwem sieci teleinformatycznych;
9. bezpieczeństwem stacji roboczych, serwerów oraz urządzeń mobilnych;
10. zarządzaniem zmianą w środowisku teleinformatycznym;
11. wymaganiami wynikającymi z obowiązujących przepisów prawa oraz regulacji wewnętrznych;
12. dobrymi praktykami w zakresie cyberbezpieczeństwa.

Zakres szkolenia może zostać rozszerzony o zagadnienia wynikające ze specyfiki działalności Zamawiającego oraz wykorzystywanych rozwiązań teleinformatycznych.

### 4.3. Minimalne wymagania

1. Program szkolenia powinien zostać dostosowany do zakresu obowiązków uczestników.
2. Wykonawca może wykorzystywać własne materiały szkoleniowe oraz przykłady praktyczne odpowiadające zakresowi szkolenia.
3. W trakcie szkolenia mogą zostać wykorzystane przykłady rzeczywistych incydentów bezpieczeństwa, scenariusze zagrożeń oraz wyniki analiz podatności, o ile nie naruszają obowiązujących przepisów ani zobowiązań dotyczących poufności.
4. Szkolenie nie obejmuje prowadzenia warsztatów administracyjnych, konfiguracji urządzeń ani wykonywania prac wdrożeniowych w środowisku teleinformatycznym Zamawiającego.
5. Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

### 4.4. Produkty końcowe

Po zakończeniu szkolenia Wykonawca przekaże Zamawiającemu:

1. program szkolenia;
2. materiały szkoleniowe;
3. potwierdzenie realizacji szkolenia;
4. dokumentację potwierdzającą uczestnictwo, jeżeli jest wymagana przez Zamawiającego.

## 5. Szkolenia powiązane z testami socjotechnicznymi

### 5.1. Cel

Celem szkolenia jest zwiększenie świadomości uczestników w zakresie zagrożeń wynikających z ataków socjotechnicznych oraz omówienie najczęściej stosowanych metod manipulacji wykorzystywanych przez cyberprzestępców. Szkolenie powinno umożliwić uczestnikom rozpoznawanie prób wyłudzenia informacji oraz właściwe reagowanie na tego rodzaju zagrożenia.

### 5.2. Zakres

Szkolenie powinno obejmować zagadnienia związane w szczególności z:

1. metodami prowadzenia ataków socjotechnicznych;
2. phishingiem, spear phishingiem, smishingiem, vishingiem oraz innymi formami wyłudzania informacji;
3. analizą najczęściej popełnianych błędów przez użytkowników;
4. rozpoznawaniem podejrzanych wiadomości, stron internetowych oraz prób kontaktu;
5. zasadami bezpiecznego postępowania w przypadku podejrzenia próby oszustwa;
6. omówieniem wyników przeprowadzonych testów socjotechnicznych, jeżeli były realizowane w ramach projektu;
7. rekomendowanymi działaniami ograniczającymi ryzyko skutecznego przeprowadzenia ataków socjotechnicznych.

Zakres szkolenia może zostać rozszerzony o zagadnienia wynikające ze specyfiki działalności Zamawiającego.

### 5.3. Minimalne wymagania

1. Zakres szkolenia powinien być dostosowany do wyników przeprowadzonych testów socjotechnicznych, jeżeli takie testy były wykonywane.
2. W przypadku braku realizacji testów socjotechnicznych szkolenie może zostać przeprowadzone z wykorzystaniem przykładowych scenariuszy edukacyjnych przygotowanych przez Wykonawcę.
3. Wykonawca może wykorzystywać własne materiały szkoleniowe, przykłady oraz scenariusze symulacyjne.
4. Omówienie wyników testów powinno odbywać się z poszanowaniem prywatności uczestników oraz bez wskazywania danych umożliwiających identyfikację konkretnych osób, chyba że Zamawiający postanowi inaczej.
5. Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

### 5.4. Produkty końcowe

Po zakończeniu szkolenia Wykonawca przekaże Zamawiającemu:

1. program szkolenia;
2. materiały szkoleniowe;
3. potwierdzenie realizacji szkolenia;
4. dokumentację potwierdzającą uczestnictwo, jeżeli jest wymagana przez Zamawiającego;
5. podsumowanie najważniejszych wniosków wynikających z przeprowadzonych testów socjotechnicznych, jeżeli były one objęte zakresem realizowanego projektu.

## 6. Usługi typu Security Awareness (symulacje phishingu)

### 6.1. Cel

Celem realizacji zadania jest zwiększenie świadomości użytkowników w zakresie rozpoznawania wiadomości phishingowych oraz innych zagrożeń wykorzystujących techniki socjotechniczne, a także ocena poziomu przygotowania użytkowników do identyfikowania prób wyłudzenia informacji.

### 6.2. Zakres

W ramach realizacji zadania Wykonawca zobowiązany będzie do:

1. uzgodnienia z Zamawiającym zakresu oraz scenariusza realizowanych działań;
2. przygotowania scenariuszy symulacji odpowiadających charakterowi działalności Zamawiającego;
3. przeprowadzenia uzgodnionych symulacji phishingowych;
4. analizy wyników przeprowadzonych działań;
5. opracowania rekomendacji dotyczących podnoszenia świadomości użytkowników;
6. przedstawienia wyników Zamawiającemu.

### 6.3. Minimalne wymagania

1. Symulacje powinny być realizowane w sposób niepowodujący zakłóceń w funkcjonowaniu systemów teleinformatycznych Zamawiającego.
2. Zakres oraz harmonogram realizacji symulacji powinny zostać uzgodnione z Zamawiającym przed rozpoczęciem działań.
3. Wykonawca samodzielnie dobiera narzędzia wykorzystywane do realizacji symulacji.
4. Symulacje powinny mieć charakter edukacyjny i służyć podnoszeniu świadomości użytkowników.
5. Wyniki symulacji powinny być prezentowane w formie zbiorczej, chyba że Zamawiający uzgodni z Wykonawcą inny sposób prezentacji wyników.
6. Realizacja symulacji nie obejmuje pozyskiwania rzeczywistych haseł użytkowników ani wykonywania działań mogących naruszać poufność przetwarzanych informacji.

### 6.4. Produkty końcowe

Po zakończeniu realizacji zadania Wykonawca przekaże Zamawiającemu:

1. opis zastosowanego scenariusza symulacji;
2. zbiorcze wyniki przeprowadzonych działań;
3. analizę uzyskanych rezultatów;
4. rekomendacje dotyczące dalszych działań zwiększających świadomość użytkowników;
5. raport podsumowujący realizację zadania.

## 7. Szkolenia symulacyjne z zarządzania kryzysowego

### 7.1. Cel

Celem realizacji zadania jest przygotowanie kadry kierowniczej oraz osób odpowiedzialnych za bezpieczeństwo informacji i ciągłość działania do właściwego reagowania na sytuacje kryzysowe mogące zakłócić funkcjonowanie Zamawiającego.

Szkolenie ma na celu rozwijanie umiejętności podejmowania decyzji, współpracy oraz koordynacji działań w przypadku wystąpienia incydentów bezpieczeństwa lub innych zdarzeń wpływających na ciągłość działania organizacji.

### 7.2. Zakres

W ramach realizacji zadania Wykonawca zobowiązany będzie do:

1. przygotowania scenariusza ćwiczenia dostosowanego do specyfiki działalności Zamawiającego;
2. uzgodnienia scenariusza z Zamawiającym;
3. przeprowadzenia ćwiczenia symulacyjnego;
4. moderowania przebiegu ćwiczenia;
5. omówienia przebiegu ćwiczenia oraz przedstawienia wniosków;
6. opracowania rekomendacji dotyczących doskonalenia organizacji w zakresie reagowania na sytuacje kryzysowe.

### 7.3. Minimalne wymagania

1. Ćwiczenia powinny mieć charakter warsztatowy i opierać się na przygotowanych scenariuszach zdarzeń.
2. Scenariusz ćwiczenia powinien uwzględniać charakter działalności Zamawiającego oraz zakres realizowanego projektu.
3. Ćwiczenia nie obejmują przeprowadzania rzeczywistych działań operacyjnych, wyłączania systemów teleinformatycznych ani ingerencji w środowisko produkcyjne Zamawiającego.
4. Wykonawca może wykorzystywać własne scenariusze ćwiczeń, odpowiednio dostosowane do specyfiki działalności Zamawiającego.
5. Ćwiczenia mogą być realizowane w formie stacjonarnej lub zdalnej.

### 7.4. Produkty końcowe

Po zakończeniu realizacji zadania Wykonawca przekaże Zamawiającemu:

1. scenariusz przeprowadzonego ćwiczenia;
2. podsumowanie przebiegu ćwiczenia;
3. wnioski oraz rekomendacje dotyczące doskonalenia organizacji w zakresie zarządzania sytuacjami kryzysowymi;
4. potwierdzenie realizacji szkolenia.

## 8. Szkolenia przygotowujące do certyfikacji

### 8.1. Cel

Celem realizacji zadania jest przygotowanie przedstawicieli Zamawiającego do procesu certyfikacji lub re-certyfikacji systemów zarządzania poprzez przekazanie wiedzy dotyczącej wymagań właściwych norm, zasad prowadzenia audytów certyfikacyjnych oraz sposobu przygotowania organizacji do procesu oceny zgodności.

Realizacja szkolenia ma wspierać właściwe przygotowanie uczestników do udziału w procesie certyfikacji oraz zwiększyć świadomość obowiązków wynikających z funkcjonowania systemów zarządzania.

### 8.2. Zakres

W ramach realizacji zadania Wykonawca zobowiązany będzie do:

1. przedstawienia zasad funkcjonowania procesu certyfikacji;
2. omówienia wymagań właściwych norm objętych zakresem projektu;
3. omówienia przebiegu audytu certyfikacyjnego lub recertyfikacyjnego;
4. przedstawienia zasad przygotowania organizacji do procesu certyfikacji;
5. omówienia najczęściej występujących niezgodności identyfikowanych podczas audytów;
6. przedstawienia dobrych praktyk wspierających utrzymanie zgodności systemów zarządzania.

Zakres szkolenia może zostać rozszerzony o zagadnienia wynikające ze specyfiki działalności Zamawiającego.

### 8.3. Minimalne wymagania

1. Zakres szkolenia powinien odpowiadać systemom zarządzania objętym zakresem realizowanego projektu.
2. Wykonawca może wykorzystywać własne materiały szkoleniowe, odpowiednio dostosowane do zakresu szkolenia.
3. Szkolenie powinno uwzględniać praktyczne aspekty przygotowania organizacji do procesu certyfikacji.
4. Szkolenie nie obejmuje świadczenia usług jednostki certyfikującej ani gwarancji uzyskania certyfikatu.
5. Szkolenie może być realizowane w formie stacjonarnej, zdalnej lub hybrydowej.

### 8.4. Produkty końcowe

Po zakończeniu realizacji zadania Wykonawca przekaże Zamawiającemu:

1. program szkolenia;
2. materiały szkoleniowe;
3. potwierdzenie realizacji szkolenia;

4. dokumentację potwierdzającą uczestnictwo, jeżeli jest wymagana przez Zamawiającego;
5. zestaw rekomendacji wspierających przygotowanie organizacji do procesu certyfikacji.

## 9. Postanowienia wspólne dotyczące realizacji szkoleń

### 9.1. Organizacja szkoleń

1. Szczegółowy harmonogram realizacji szkoleń zostanie uzgodniony pomiędzy Zamawiającym a Wykonawcą przed rozpoczęciem realizacji zadania.
2. Zamawiający zobowiązany jest do wskazania grup uczestników oraz wyznaczenia terminów realizacji szkoleń z odpowiednim wyprzedzeniem.
3. Szkolenia mogą być realizowane w formie stacjonarnej, zdalnej lub hybrydowej, zgodnie z ustaleniami Stron.
4. Za zapewnienie sal szkoleniowych, sprzętu multimedialnego oraz organizację uczestnictwa pracowników odpowiada Zamawiający, o ile Strony nie uzgodnią inaczej.
5. Dopuszcza się realizację szkoleń dla kilku grup uczestników jednocześnie, jeżeli zakres merytoryczny szkolenia jest tożsamy.

### 9.2. Materiały szkoleniowe

1. Wykonawca może wykorzystywać własne materiały szkoleniowe, prezentacje, scenariusze ćwiczeń oraz przykłady edukacyjne, pod warunkiem ich dostosowania do zakresu realizowanego projektu.
2. Materiały szkoleniowe powinny być aktualne, zgodne z obowiązującymi przepisami prawa oraz uwzględniać dobre praktyki w zakresie cyberbezpieczeństwa.
3. Materiały mogą zostać przekazane Zamawiającemu w postaci elektronicznej lub papierowej.

### 9.3. Prowadzący szkolenia

1. Szkolenia prowadzone będą przez osoby posiadające wiedzę oraz doświadczenie odpowiednie do zakresu realizowanego szkolenia.
2. Wykonawca może realizować szkolenia z udziałem więcej niż jednego prowadzącego.
3. Zmiana osoby prowadzącej szkolenie nie wymaga zgody Zamawiającego, pod warunkiem zapewnienia osoby posiadającej kwalifikacje nie niższe niż osoba zastępowana.

### 9.4. Zakres odpowiedzialności Wykonawcy

1. Wykonawca odpowiada za przygotowanie i przeprowadzenie szkoleń zgodnie z zakresem określonym w Opisie Przedmiotu Zamówienia.
2. Wykonawca nie ponosi odpowiedzialności za nieobecność uczestników, brak zapewnienia odpowiednich warunków organizacyjnych przez Zamawiającego ani za niewdrożenie przez Zamawiającego zaleceń przedstawionych podczas szkolenia.
3. Zakres realizacji zamówienia nie obejmuje opracowywania indywidualnych programów szkoleniowych dla poszczególnych uczestników, świadczenia usług doradczych wykraczających

poza zakres szkolenia ani prowadzenia konsultacji po zakończeniu szkolenia, chyba że umowa stanowi inaczej.

### 9.5. Dokumentowanie realizacji

1. Po zakończeniu każdego szkolenia Wykonawca przekaże dokumentację potwierdzającą jego realizację w zakresie wynikającym z Opisu Przedmiotu Zamówienia.
2. Dokumentacja może obejmować w szczególności:
    1. program szkolenia;
    2. materiały szkoleniowe;
    3. potwierdzenie przeprowadzenia szkolenia;
    4. listę obecności lub inne potwierdzenie uczestnictwa, jeżeli jest wymagane;
    5. podsumowanie przeprowadzonego szkolenia.

## 10. Postanowienia końcowe

1. Szczegółowy zakres merytoryczny poszczególnych szkoleń może zostać doprecyzowany z Zamawiającym przed ich realizacją, z zastrzeżeniem, że nie będzie prowadził do zmiany zakresu przedmiotu zamówienia.
2. W przypadku konieczności aktualizacji treści szkoleniowych wynikającej ze zmiany przepisów prawa, norm lub wytycznych obowiązujących w okresie realizacji zamówienia, Wykonawca uwzględni te zmiany w zakresie niezbędnym do prawidłowej realizacji szkolenia.

## 11. Testy bezpieczeństwa

1. Cel zadania:
2. Celem realizacji zadania jest ocena poziomu bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego poprzez identyfikację podatności, błędów konfiguracyjnych oraz innych słabości mogących mieć wpływ na bezpieczeństwo przetwarzanych informacji.
3. Realizacja zadania ma umożliwić identyfikację potencjalnych zagrożeń oraz opracowanie rekomendacji ograniczających poziom ryzyka związanego z eksploatacją infrastruktury teleinformatycznej.

### 11.1. Zakres prac

1. W ramach realizacji zadania Wykonawca zobowiązany będzie do:
2. uzgodnienia zakresu badania z Zamawiającym;
3. identyfikacji zasobów objętych badaniem;
4. identyfikacji aktywnych urządzeń oraz usług sieciowych;
5. identyfikacji otwartych portów oraz wykorzystywanych protokołów komunikacyjnych;
6. identyfikacji znanych podatności bezpieczeństwa;
7. identyfikacji wybranych błędów konfiguracyjnych mających wpływ na bezpieczeństwo;

8. oceny poziomu ryzyka związanego ze zidentyfikowanymi podatnościami;
9. opracowania rekomendacji dotyczących ograniczenia wykrytych ryzyk.

### 11.2. Minimalne wymagania

1. Przed rozpoczęciem realizacji zadania Wykonawca uzgodni z Zamawiającym zakres testów, listę systemów, urządzeń oraz usług objętych badaniem.
2. Testy bezpieczeństwa powinny być prowadzone w sposób niepowodujący celowego zakłócenia pracy środowiska teleinformatycznego Zamawiającego.
3. Zakres badania powinien zostać dostosowany do charakteru infrastruktury teleinformatycznej oraz uzgodnionego zakresu prac.
4. Wykonawca samodzielnie dobiera metodykę badania oraz narzędzia wykorzystywane podczas realizacji testów, z uwzględnieniem celu oraz zakresu zamówienia.
5. Badanie wykonywane jest na podstawie informacji oraz dostępu do zasobów zapewnionych przez Zamawiającego.
6. W przypadku stwierdzenia okoliczności mogących mieć wpływ na bezpieczeństwo realizacji testów Wykonawca niezwłocznie poinformuje o tym Zamawiającego oraz uzgodni dalszy sposób prowadzenia prac.

### 11.3. Ograniczenia zakresu badania

1. Testy bezpieczeństwa obejmują wyłącznie zasoby uzgodnione z Zamawiającym przed rozpoczęciem realizacji zadania.
2. Badanie polega na identyfikacji podatności, analizie konfiguracji oraz ocenie poziomu bezpieczeństwa infrastruktury teleinformatycznej i nie obejmuje działań prowadzących do świadomego wykorzystania wykrytych podatności lub ingerencji w środowisko produkcyjne. Zakres zadania nie obejmuje wykonywania zmian konfiguracyjnych, instalacji aktualizacji, usuwania wykrytych podatności ani świadczenia usług administracyjnych, chyba że obowiązek taki wynika wprost z odrębnej umowy.
3. Wykonawca nie ponosi odpowiedzialności za podatności lub nieprawidłowości występujące w systemach, urządzeniach lub usługach nieobjętych zakresem uzgodnionego badania.
4. Wykonawca nie ponosi odpowiedzialności za skutki wynikające z przekazania niepełnych lub nieaktualnych informacji dotyczących infrastruktury objętej badaniem.
5. Rozszerzenie zakresu testów poza zakres uzgodniony przed rozpoczęciem realizacji zadania wymaga uzgodnienia pomiędzy Stronami.

### 11.4. Raportowanie wyników

1. Po zakończeniu testów bezpieczeństwa Wykonawca opracuje raport zawierający wyniki przeprowadzonego badania.
2. Raport powinien zawierać co najmniej:
3. opis zakresu przeprowadzonych testów;
4. opis zastosowanej metodyki badania;
5. zestawienie zasobów objętych badaniem;

6. wykaz zidentyfikowanych podatności oraz nieprawidłowości;
7. ocenę poziomu ryzyka dla poszczególnych podatności lub grup podatności;
8. opis potencjalnego wpływu wykrytych podatności na bezpieczeństwo infrastruktury teleinformatycznej;
9. rekomendacje działań mających na celu ograniczenie lub usunięcie zidentyfikowanych ryzyk;
10. podsumowanie wyników badania.
11. Rekomendacje powinny uwzględniać możliwości organizacyjne i techniczne Zamawiającego oraz wskazywać zalecane kierunki działań naprawczych.
12. Raport może zawierać informacje pomocnicze, w szczególności zestawienia wykrytych usług sieciowych, otwartych portów, wersji oprogramowania, wyników analizy konfiguracji oraz inne dane uzyskane w trakcie realizacji badania.
13. Raport zostanie przekazany Zamawiającemu w postaci elektronicznej.

### 11.5. Produkty końcowe

1. Po zakończeniu realizacji zadania Wykonawca przekaże Zamawiającemu:
2. raport z przeprowadzonych testów bezpieczeństwa;
3. wykaz zidentyfikowanych podatności i nieprawidłowości;
4. ocenę poziomu ryzyka dla zidentyfikowanych podatności;
5. rekomendacje działań naprawczych oraz zwiększających poziom bezpieczeństwa;
6. podsumowanie przeprowadzonych prac.

### 11.6. Wymagania jakościowe

1. Testy bezpieczeństwa powinny zostać przeprowadzone zgodnie z aktualnym stanem wiedzy technicznej oraz z wykorzystaniem powszechnie stosowanych metod identyfikacji podatności.
2. Wykonawca dobiera metodykę oraz narzędzia badawcze odpowiednio do zakresu i celu realizowanego zadania.
3. Wszystkie ustalenia zawarte w raporcie powinny być możliwe do uzasadnienia na podstawie wyników przeprowadzonego badania.
4. W przypadku wykrycia podatności o wysokim lub krytycznym poziomie ryzyka Wykonawca niezwłocznie poinformuje o tym Zamawiającego, bez konieczności oczekiwania na przekazanie raportu końcowego.
5. Przekazanie raportu końcowego nie obejmuje obowiązku usuwania wykrytych podatności, wykonywania zmian konfiguracyjnych ani ponownego przeprowadzania testów po wdrożeniu działań naprawczych, chyba że zakres zamówienia lub odrębna umowa stanowią inaczej.
6. W przypadku potrzeby weryfikacji skuteczności wdrożonych działań naprawczych może zostać przeprowadzone ponowne badanie, jeżeli zostało przewidziane w zakresie zamówienia lub zostanie zlecone przez Zamawiającego jako odrębna usługa.

**11.7. Wymagania końcowe:**

W celu przeprowadzenia testów bezpieczeństwa infrastruktury teleinformatycznej Wykonawca wykorzysta specjalistyczne narzędzia klasy Network Discovery oraz Vulnerability Assessment, umożliwiające identyfikację aktywnych urządzeń, analizę świadczonych usług sieciowych oraz wykrywanie podatności bezpieczeństwa. Narzędzia te muszą zapewniać możliwość identyfikacji aktywnych hostów, skanowania portów TCP i UDP, identyfikacji uruchomionych usług i ich wersji, określenia wykorzystywanych systemów operacyjnych oraz wykrywania nieautoryzowanych usług sieciowych. W zakresie analizy podatności narzędzia muszą umożliwiać automatyczne wykrywanie znanych podatności bezpieczeństwa, błędów konfiguracji, brakujących aktualizacji bezpieczeństwa oraz innych podatności mogących wpływać na poufność, integralność i dostępność systemów teleinformatycznych. Wykorzystane rozwiązania powinny bazować na aktualizowanej bazie podatności, obejmującej między innymi identyfikatory CVE, oraz umożliwiać ocenę poziomu ryzyka zgodnie z powszechnie stosowaną metodyką CVSS. Wyniki przeprowadzonych testów muszą zostać przedstawione w formie raportu zawierającego wykryte podatności, ocenę poziomu ryzyka, opis ich wpływu na bezpieczeństwo środowiska teleinformatycznego oraz rekomendacje działań naprawczych. Proces testów bezpieczeństwa obejmuje identyfikację infrastruktury teleinformatycznej, analizę dostępnych usług sieciowych, wykonanie testów podatności oraz opracowanie raportu końcowego z wynikami badań i zaleceniami dotyczącymi podniesienia poziomu bezpieczeństwa. Dopuszcza się wykorzystanie dowolnych narzędzi spełniających powyższe wymagania funkcjonalne, w tym rozwiązań równoważnych pod względem funkcjonalności do narzędzi klasy Nmap oraz OpenVAS (Greenbone Vulnerability Management).

# 6. Część 3: Dostawa, konfiguracja i wdrożenie rozwiązań z zakresu cyberbezpieczeństwa dla środowisk IT i OT

## 6.1. Usługa i system do zarządzanego skanowania podatności i zarządzania ryzykiem

**Zakres: IT/OT**

1. **Wymagania minimalne i model usługi:**

Okres subskrypcji: Licencje na system oraz świadczenie usługi muszą zostać zapewnione na okres 3 lat (**36 miesięcy**).

Rozpoczęcie świadczenia: Bieg usługi rozpoczyna się w dniu złożenia zamówienia lub w innym terminie określonym przez Zamawiającego.

Model dostarczania: Usługa typu Managed Service (SaaS), w ramach której Dostawca zapewnia technologię zarządzania ekspozycją oraz dedykowany zespół ekspertów odpowiedzialnych za monitorowanie, analizę i priorytetyzację podatności oraz ekspozycji.

Lokalizacja danych: Przetwarzanie i przechowywanie danych musi odbywać się na terenie Unii Europejskiej (zgodność z RODO).

Wsparcie ekspertów: Dostawca musi zapewnić dostęp do zespołu analityków w trybie 24/7/365 w języku angielskim.

- Zakres operacyjny usługi: Usługa musi obejmować co najmniej:
- bieżące monitorowanie i analizę wykrytych podatności oraz ekspozycji,
- priorytetyzację ryzyka na podstawie kontekstu zagrożeń i krytyczności zasobów,
- dostarczanie zaleceń naprawczych (remediacji),
- eskalację krytycznych ekspozycji do zespołu Zamawiającego poprzez mechanizmy powiadomień.

2. **Zarządzanie Powierzchnią Ataku (Attack Surface Management)**

Usługa musi zapewniać pełną widoczność infrastruktury Zamawiającego poprzez:

Zewnętrzne zarządzanie powierzchnią ataku (EASM): Ciągłe monitorowanie i identyfikację zasobów wystawionych na działanie publicznej sieci Internet (np. serwery WWW, bramy VPN, publiczne API, serwery pocztowe).

Wewnętrzne zarządzanie powierzchnią ataku (IASM): Identyfikację i ocenę podatności systemów oraz usług funkcjonujących wewnątrz sieci Zamawiającego, z perspektywy potencjalnego napastnika.

Wykrywanie nieznanych i nieautoryzowanych zasobów (Shadow IT): Automatyczne odnajdywanie oraz raportowanie zasobów nieudokumentowanych lub wdrożonych poza formalnym procesem IT, w tym usług i systemów mogących stanowić niekontrolowaną ekspozycję bezpieczeństwa.

3. **Zaawansowana Technologia Skanowania i Priorytetyzacja**

Automatyzacja i elastyczność: System musi realizować regularne, zautomatyzowane skany, a eksperci muszą mieć możliwość uruchomienia dodatkowych skanów w przypadku pojawienia się podatności krytycznych lub aktywnie wykorzystywanych w środowisku zagrożeń.

Wykorzystanie technologii zarządzania ekspozycją: Rozwiązanie musi bazować na uznanej technologii zarządzania ekspozycją (klasy Tenable), zintegrowanej natywnie z usługą zarządzaną Dostawcy.

Priorytetyzacja oparta na AI: Usługa musi wykorzystywać mechanizmy analityczne oparte na sztucznej inteligencji do oceny prawdopodobieństwa wykorzystania danej podatności oraz priorytetyzacji ryzyka. Priorytetyzacja musi wykraczać poza standardową punktację CVSS, uwzględniając kontekst zagrożeń oraz charakter zasobu.

4. **Współpraca z Zespołem Analityków i Remediacja**

Konsultacje eksperckie: Dostawca musi zapewnić regularne sesje konsultacyjne z analitykami w celu omówienia wyników, trendów ryzyka oraz postępów w zabezpieczaniu środowiska Zamawiającego, realizowane co najmniej raz w miesiącu (w formie zdalnej).

Wytyczne naprawcze: Każda zidentyfikowana istotna podatność lub ekspozycja musi zostać opatrzona konkretnymi instrukcjami technicznymi dotyczącymi jej usunięcia lub ograniczenia ryzyka, obejmującymi co najmniej:

- rekomendowaną akcję naprawczą (np. aktualizacja, zmiana konfiguracji, obejście tymczasowe),
- priorytet realizacji oraz uzasadnienie,
- identyfikację zasobu/systemu, którego dotyczy problem,

- odniesienie do identyfikatorów podatności (np. CVE), jeżeli są dostępne.

Natywna integracja w ekosystemie: Usługa powinna umożliwiać natywną wymianę informacji o ryzyku z pozostałymi modułami bezpieczeństwa w ramach jednego ekosystemu, w celu wsparcia korelacji incydentów oraz priorytetyzacji działań ochronnych.

5. **Raportowanie i Powiadomienia**

- Raporty podatności i ekspozycji: System musi zapewniać dostęp do raportów prezentujących cyfrowy ślad organizacji, wykryte ekspozycje oraz zestawienia podatności wraz z priorytetami ryzyka.
- Powiadomienia o zagrożeniach: System musi generować alerty dla zespołu Zamawiającego w przypadku wykrycia krytycznych ekspozycji lub podatności o wysokim ryzyku wykorzystania, w tym poprzez mechanizmy powiadomień dostępne w konsoli oraz kanały komunikacji zdefiniowane przez Zamawiającego.

6. **Wdrożenie**

Wykonawca przeprowadzi kompleksowe wdrożenie oprogramowania, obejmujące jego instalację, konfigurację, uruchomienie oraz dostosowanie do środowiska Zamawiającego. Wdrożenie zostanie wykonane z należytą starannością, zgodnie z aktualną wiedzą techniczną, zaleceniami producenta oraz najlepszymi praktykami branżowymi.

## 6.2. Usługa MDR

**Zakres: IT/OT**

| **OGÓLNE** | |
|---|---|
| 1 | Dostawa subskrypcji usługi MDR w wariancie rozszerzonym, świadczonej 24/7/365 przez wyspecjalizowany zespół ekspertów producenta. |
| 2 | Wariant rozszerzony obejmuje pełen zakres wariantu podstawowego, rozszerzony o: zdalne reagowanie na incydenty z pełną neutralizacją zagrożeń, umowę o poziomie usługi (SLA) z mechanizmem rekompensat, gwarancję oraz rozszerzony zakres dochodzeń. |
| 3 | Dostawa licencji subskrypcyjnych na oprogramowanie agenta lub sensora. Licencja **XDR** zawarta w każdej subskrypcji MDR.<br><br>Wymagania dotyczące licencji XDR:<br><br>• Oprogramowanie powinno zapewniać kompleksową ochronę antywirusową stacji roboczych i serwerów, obejmującą wykrywanie, blokowanie oraz usuwanie złośliwego oprogramowania, w tym wirusów, trojanów, spyware, malware, ransomware oraz innych zagrożeń.<br>• Rozwiązanie powinno działać w czasie rzeczywistym i automatycznie analizować uruchamiane pliki, procesy, skrypty oraz pobierane lub otwierane obiekty pod kątem złośliwej aktywności. |

- Oprogramowanie powinno wykorzystywać mechanizmy ochrony nowej generacji, w tym analizę behawioralną, uczenie maszynowe oraz mechanizmy wykrywania podejrzanych działań, a nie wyłącznie klasyczne sygnatury wirusów.
- System powinien umożliwiać automatyczną reakcję na wykryte zagrożenie, w tym zablokowanie pliku, zakończenie procesu, objęcie pliku kwarantanną oraz powiadomienie administratora.
- Rozwiązanie powinno posiadać centralną konsolę zarządzającą umożliwiającą konfigurację polityk bezpieczeństwa, monitorowanie stanu ochrony, analizę alertów oraz raportowanie incydentów dla wszystkich chronionych urządzeń.
- Oprogramowanie powinno zapewniać regularne i automatyczne aktualizacje mechanizmów ochrony, baz reputacyjnych, komponentów detekcyjnych oraz polityk bezpieczeństwa bez konieczności ręcznej instalacji na każdym stanowisku.
- Rozwiązanie powinno umożliwiać centralne monitorowanie stanu bezpieczeństwa infrastruktury informatycznej, w tym stacji roboczych, serwerów oraz innych zintegrowanych źródeł danych bezpieczeństwa, wraz z prezentacją alertów i zdarzeń w jednej konsoli administracyjnej.
- System powinien zapewniać gromadzenie, korelację i analizę zdarzeń bezpieczeństwa pochodzących z chronionej infrastruktury IT, umożliwiając wykrywanie podejrzanych aktywności, anomalii, prób naruszenia bezpieczeństwa oraz incydentów wymagających reakcji administratora.
- Rozwiązanie powinno umożliwiać prowadzenie inwentaryzacji aktywów teleinformatycznych objętych ochroną, w szczególności stacji roboczych i serwerów, wraz z informacją o ich statusie, przypisaniu do grup, stanie agenta ochronnego, ostatniej aktywności oraz zdarzeniach bezpieczeństwa.
- umożliwia analizę incydentów bezpieczeństwa oraz zabezpieczanie materiału dowodowego w postaci telemetrii, logów i artefaktów z chronionych systemów. Rozwiązanie pozwala wykrywać, analizować i dokumentować podejrzane aktywności na stacjach roboczych, serwerach, sieci, poczcie, chmurze oraz usługach zintegrowanych.
- menedżera logów: centralne gromadzenie logów oraz telemetrii z punktów końcowych, serwerów, urządzeń sieciowych, zapór sieciowych, poczty elektronicznej, środowisk chmurowych oraz innych zintegrowanych źródeł
- normalizację i korelację zdarzeń bezpieczeństwa z wielu źródeł w celu identyfikacji incydentów i anomalii
- przechowywanie danych umożliwiające analizę bieżącą oraz retrospektywną;
- analiza wpływu po incydencie bezpieczeństwa
- zaawansowane wyszukiwanie zdarzeń i artefaktów bezpieczeństwa
- automatyczne wykrywanie zagrożeń, wskaźników kompromitacji (IOC) oraz nietypowych zachowań
- analizę przyczyn źródłowych oraz rekonstrukcję przebiegu incydentu
- generowanie raportów i zestawień dotyczących zdarzeń bezpieczeństwa oraz aktywności użytkowników i systemów
- integrację z rozwiązaniami producentów trzecich w celu rozszerzenia zakresu monitorowania

| | |
|---|---|
| 4 | Licencja serwerowa musi obejmować zaawansowaną ochronę urządzeń klasy serwer z funkcjonalnością XDR, w tym ochronę przed exploitami, ransomware, zaawansowane mechanizmy behawioralne oraz pełne możliwości rozszerzonego wykrywania i reagowania. |
| 5 | Stacje robocze (licencjonowane per User): **21** szt. |
| 6 | Serwery (licencjonowane per Server):**10** szt. |
| 7 | Okres subskrypcji: **36** miesięcy, liczony od dnia aktywacji usługi. |
| 8 | Agent XDR — funkcje ochrony, wykrywania zagrożeń oraz reagowania na incydenty. |
| 9 | Sensor XDR — wyłącznie funkcje wykrywania zagrożeń oraz reagowania na incydenty. |
| 10 | Decyzja o wyborze wariantu oprogramowania dla poszczególnych urządzeń należy do Zamawiającego. |
| 11 | Oprogramowanie kompatybilne ze stacjami roboczymi i serwerami (fizycznymi oraz wirtualnymi). |
| 12 | Funkcja zdalnego reagowania na incydenty, SLA, gwarancja, rozszerzone dochodzenia wymagają instalacji pełnego agenta XDR |
| 13 | Limit chmurowego repozytorium danych dla stacji roboczych (per User): do 20 MB dziennie, retencja 90 dni. |
| 14 | Limit chmurowego repozytorium danych dla serwerów (per Server): do 40 MB dziennie, retencja 90 dni. |
| 15 | Limit zapytań do repozytorium danych minimum: 500 zapytań dziennie. |
| 16 | Usługa świadczona przez dedykowany zespół ekspertów w modelu SOC, wspomaganym przez AI i uczenie maszynowe. |
| 17 | Producent dysponuje co najmniej 5 globalnymi centrami operacji bezpieczeństwa. |
| 18 | Zespół liczy co najmniej 100 ekspertów ds. wykrywania zagrożeń i reagowania na incydenty. |
| 19 | Usługa świadczona 24/7/365. |

| | |
|---|---|
| 20 | Ciągłe monitorowanie środowiska: komputery, serwery, sieci, chmura, poczta elektroniczna, kopie zapasowe. |
| 21 | Analiza ekspercka łączona z uczeniem maszynowym — identyfikacja, agregacja i priorytetyzacja zdarzeń bezpieczeństwa. |
| 22 | Automatyczne grupowanie zdarzeń o wysokim poziomie istotności w sprawy podlegające przeglądowi analityków. |
| 23 | Analitycy przeprowadzają dochodzenia w celu potwierdzenia zagrożeń i podjęcia działań reagowania. |
| 24 | Dochodzenia obejmują również sprawy z innych kompatybilnych produktów, na które Zamawiający posiada licencję. |
| 25 | Proaktywne wyszukiwanie zagrożeń prowadzone przez analityków, wykrywające zagrożenia omijające mechanizmy detekcji. |
| 26 | Wyszukiwanie oparte na threat intelligence oraz wskaźnikach kompromitacji (IoC). |
| 27 | Stałe badania producenta nad nowymi grupami zagrożeń i technikami ataków. |
| 28 | Wykrycie złośliwej aktywności skutkuje utworzeniem sprawy i dochodzeniem. |
| 29 | Pełna neutralizacja ataków — powstrzymywanie, zakłócanie oraz całkowite wyeliminowanie obecności atakującego ze środowiska Zamawiającego. |
| 30 | Działania reagowania: zdalne zapytania diagnostyczne, izolacja urządzeń, terminowanie procesów, blokowanie IP, usuwanie złośliwych artefaktów. |
| 31 | Średni czas reagowania na zagrożenie nie przekracza 40 minut. |
| 32 | W przypadku potwierdzonej kompromitacji lub nieautoryzowanego dostępu (interaktywni atakujący, szyfrowanie/niszczenie danych, eksfiltracja) usługa musi obejmować pełne zdalne reagowanie na incydent. |
| 33 | Przydzielenie dedykowanego koordynatora reagowania na incydent na czas jego trwania. |
| 34 | Wstępna analiza i dochodzenie w celu określenia zakresu i wpływu incydentu. |
| 35 | Analiza dodatkowych źródeł danych udostępnionych przez Zamawiającego. |

| | |
|---|---|
| 36 | Działania neutralizujące złośliwy dostęp i zapobiegające dalszym szkodom. |
| 37 | Wytyczne naprawcze w sytuacjach wymagających działań po stronie Zamawiającego. |
| 38 | Bieżące raportowanie statusu incydentu i śledzenie realizacji zadań. |
| 39 | Proaktywne rekomendacje zapobiegające ponownemu wystąpieniu incydentu. |
| 40 | Zdalne reagowanie dostępne wyłącznie na urządzeniach, które przed wystąpieniem incydentu były zintegrowane z usługą. |
| 41 | Tryb „Współpraca” — brak działań reagowania bez pisemnej zgody Zamawiającego; opcja automatycznego przejścia do trybu „Autoryzacja” przy braku kontaktu. |
| 42 | Tryb „Autoryzacja” — zespół samodzielnie podejmuje działania powstrzymywania i pełnej neutralizacji; informuje Zamawiającego; eskalacja tylko gdy nie może działać samodzielnie. |
| 43 | Tryb „Tylko powiadomienie” — ograniczone dochodzenie, powiadomienia bez działań; przy podejrzeniu incydentu prośba o zmianę trybu. |
| 44 | Cel: czas utworzenia sprawy — do 5 minut od wykrycia zdarzenia. |
| 45 | Cel: czas pierwszego działania reagowania — do 30 minut od utworzenia sprawy. |
| **UMOWA O POZIOMIE USŁUGI — SLA** | |
| 46 | Czas reakcji dla spraw o wysokim/krytycznym poziomie istotności: maks. 60 minut dla co najmniej 90% spraw, mierzony miesięcznie. |
| 47 | Początek pomiaru SLA: od 1. dnia 4. miesiąca |
| 48 | Rekompensata przy więcej niż 3 przekroczeniach w 12 mies.: 5% opłaty za poprzedni okres lub 5 000 USD – niższa kwota. |
| 49 | Rekompensata zaliczana na poczet kolejnego okresu subskrypcji. |
| 50 | Wniosek o rekompensatę w ciągu 30 dni kalendarzowych z dowodami (logi/raporty). Maks. 3 wnioski rocznie. |
| 51 | Wyłączenia SLA: siła wyższa, ataki infrastrukturalne, okna serwisowe, naruszenie umowy przez Zamawiającego. |

| | |
|---|---|
| **GWARANCJA, KONTROLA, AKTUALIZACJE** | |
| 52 | Gwarancja na usługę MDR. Warunek: agent XDR wdrożony na wszystkich licencjonowanych urządzeniach. |
| 53 | Kontrola konfiguracji i ustawień urządzeń końcowych (dla urządzeń z pełnym agentem XDR). |
| 54 | Kontrola wykonywana przy wdrożeniu oraz okresowo w trakcie subskrypcji. |
| 55 | Wynik kontroli: punktowa ocena stanu zabezpieczeń (skala 0–100). |
| 56 | Powiadomienie o konfiguracjach obniżających bezpieczeństwo wraz z krokami naprawczymi. |
| 57 | Stałe aktualizacje reguł wykrywania zagrożeń oraz integracji technologicznych. |
| **PANEL ZARZĄDZANIA USŁUGĄ** | |
| 58 | Podsumowanie ostatnio wykrytych i zbadanych zagrożeń. |
| 59 | Baner powiadomień wymagających działania w przypadku incydentów. |
| 60 | Sekcja spraw — przegląd szczegółów powiadomień. |
| 61 | Podsumowanie stanu zabezpieczeń konta z oceną punktową (skala 0–100). |
| 62 | Wykres obsady analityków w poszczególnych godzinach doby |
| 63 | Metryki: nakład pracy w godzinach, liczba sesji wyszukiwania zagrożeń, nowe detekcje, klasyfikacja wg MITRE ATT&CK, nowe/zmodyfikowane reguły detekcji. |
| 64 | Oś czasu łącznego nakładu pracy zespołów (w osobogodzinach). |
| 65 | Podsumowanie spraw: łączna liczba, statystyki eskalacji, wskaźnik złośliwości. |
| 66 | Graficzna prezentacja przepływu danych od źródła do detekcji. |
| 67 | Sekcja ostatnich zapytań i ostatnich spraw. |
| 68 | Sekcja historii raportów (tygodniowe i miesięczne). |

| | |
|---|---|
| **RAPORTOWANIE I KOMUNIKACJA** | |
| 69 | Raporty tygodniowe i miesięczne: dochodzenia, zagrożenia, stan bezpieczeństwa. |
| 70 | Comiesięczne spotkania informacyjne dot. zagrożeń i najlepszych praktyk bezpieczeństwa. |
| 71 | Powiadomienia o problemach ze stanem zabezpieczeń lub błędach konfiguracyjnych. |
| 72 | Bieżące raportowanie statusu incydentu w trakcie zdalnego reagowania. |
| 73 | Możliwość konfiguracji preferencji komunikacyjnych (e-mail, telefon, portal). |
| 74 | Bezpośredni kontakt telefoniczny z zespołem usługowym 24/7/365 w celu przeglądu spraw i incydentów. |
| **KOMPATYBILNOŚĆ Z PRODUKTAMI FIRM TRZECICH** | |
| 75 | Możliwość integracji z produktami bezpieczeństwa firm trzecich — przyjmowanie telemetrii z zewnętrznych systemów. |
| **WDROŻENIE USŁUGI** | |
| 76 | Zebranie danych kontaktowych Zamawiającego. |
| 77 | Ustalenie preferencji komunikacyjnych. |
| 78 | Wybór trybu reagowania na zagrożenia. |
| 79 | Przeprowadzenie kontroli stanu zabezpieczeń na urządzeniach z pełnym agentem XDR. |
| 80 | Wdrożenie oprogramowania na co najmniej 80% licencjonowanych urządzeń. |
| 81 | Dla objęcia gwarancją: agent XDR wdrożony na 100% licencjonowanych urządzeń. |
| **OGRANICZENIA USŁUGI** | |
| 82 | Usługa świadczona zdalnie. Działania wymagające fizycznej obecności poza zakresem. |
| 83 | Wykonawca nie gwarantuje wykrycia, zapobieżenia ani zneutralizowania wszystkich incydentów. |

| | |
|---|---|
| 84 | Wykonawca może modyfikować i aktualizować usługę bez istotnego obniżenia funkcjonalności. |
| 85 | Wykonawca może zmieniać listę wspieranych systemów firm trzecich. |
| 86 | Wykonawca nie odpowiada za incydenty sprzed daty rozpoczęcia subskrypcji. |
| 87 | Poza zakresem: obecność na miejscu, wsparcie procesów sądowych i e-Discovery, współpraca z organami ścigania — leżą po stronie Zamawiającego. |

Wykonawca i Zamawiający zobowiązują się do ścisłej, sprawnej i terminowej współpracy, opartej na bieżącej wymianie informacji oraz wzajemnym uwzględnianiu uzasadnionych rekomendacji.

Zamawiający wyznaczy osobę lub osoby posiadające odpowiednią wiedzę techniczną i uprawnienia decyzyjne, zapewni prawidłowe funkcjonowanie wymaganych systemów i integracji oraz będzie terminowo reagował na zgłoszenia, zagrożenia i zalecenia Wykonawcy. W szczególności Zamawiający będzie wdrażał rekomendacje wynikające z kontroli bezpieczeństwa, udostępniał niezbędne dane oraz podejmował działania naprawcze w systemach, do których Wykonawca nie ma zdalnego dostępu.

### 6.2.1. Wykaz integracji z usługą MDR

Usługa MDR powinna mieć integrację z systemami firm trzecich co najmniej z wskazanymi poniżej:

| | | |
|---|---|---|
| 1 | Kopie zapasowe i odzyskiwanie danych | Acronis |
| 2 | Kopie zapasowe i odzyskiwanie danych | Rubrik |
| 3 | Kopie zapasowe i odzyskiwanie danych | Veeam Backup & Replication |
| 4 | Ochrona poczty elektronicznej | Mimecast Email Security 1.0 |
| 5 | Ochrona poczty elektronicznej | Mimecast Email Security 2.0 |

| | | |
|---|---|---|
| 6 | Ochrona poczty elektronicznej | Proofpoint Targeted Attack Protection |
| 7 | Ochrona poczty elektronicznej | Trend Micro Email Security |
| 8 | Ochrona urządzeń końcowych | Broadcom Symantec Endpoint Security |
| 9 | Ochrona urządzeń końcowych | CrowdStrike Falcon |
| 10 | Ochrona urządzeń końcowych | CylanceOPTICS |
| 11 | Ochrona urządzeń końcowych | Jamf Protect |
| 12 | Ochrona urządzeń końcowych | SentinelOne Singularity Endpoint |
| 13 | Ochrona urządzeń końcowych | Trend Micro Vision One |
| 14 | Zapory sieciowe (Firewall) | Barracuda |
| 15 | Zapory sieciowe (Firewall) | Check Point Quantum Firewall |
| 16 | Zapory sieciowe (Firewall) | Cisco Firepower |
| 17 | Zapory sieciowe (Firewall) | Cisco Meraki (API) |

| | | |
|---|---|---|
| 18 | Zapory sieciowe (Firewall) | Cisco Meraki (Log collector) |
| 19 | Zapory sieciowe (Firewall) | F5 BIG-IP ASM |
| 20 | Zapory sieciowe (Firewall) | Forcepoint |
| 21 | Zapory sieciowe (Firewall) | Fortinet FortiGate |
| 22 | Zapory sieciowe (Firewall) | Fortinet FortiAnalyzer (API) |
| 23 | Zapory sieciowe (Firewall) | Fortinet FortiAnalyzer (Log collector) |
| 24 | Zapory sieciowe (Firewall) | Palo Alto PAN-OS |
| 25 | Zapory sieciowe (Firewall) | SonicWall SonicOS |
| 26 | Zapory sieciowe (Firewall) | Ubiquiti UniFi |
| 27 | Zapory sieciowe (Firewall) | WatchGuard Firebox |
| 28 | Tożsamość i dostęp | Auth0 |
| 29 | Tożsamość i dostęp | Cisco Duo |
| 30 | Tożsamość i dostęp | Cisco ISE |
| 31 | Tożsamość i dostęp | ManageEngine AD Audit Plus |

| | | |
|---|---|---|
| 32 | Tożsamość i dostęp | Okta |
| 33 | Sieć | Aryaka |
| 34 | Sieć | Armis |
| 35 | Sieć | Cisco Umbrella |
| 36 | Sieć | Darktrace Detect |
| 37 | Sieć | Secutec |
| 38 | Sieć | Thinkst Canary |
| 39 | Sieć | Vectra AI |
| 40 | Sieć | Zscaler ZIA |
| 41 | Produktywność i współpraca | Google Workspace |
| 42 | Produktywność i współpraca | Microsoft 365 Management Activity |
| 43 | Produktywność i współpraca | Microsoft 365 Response Actions |
| 44 | Produktywność i współpraca | MS Graph Security API (Legacy) |
| 45 | Produktywność i współpraca | MS Graph Security API V2 |
| 46 | Chmura publiczna | AppOmni |
| 47 | Chmura publiczna | Orca Security |

| | | |
|---|---|---|
| 48 | Chmura publiczna | Trend Micro Cloud App Security |

## 6.3. System zabezpieczenia poczty e-mail oraz edukacji użytkowników

**Zakres: IT/OT**

1. **Wymagania Ogólne i Licencjonowanie**
    a. Okres subskrypcji: Licencje na system muszą zostać dostarczone na okres 3 lat (**36 miesięcy**).
    b. Rozpoczęcie subskrypcji: Bieg licencji rozpoczyna się w dniu złożenia zamówienia lub w innym terminie wskazanym przez Zamawiającego.
    c. Model dostarczania: System musi być rozwiązaniem typu Cloud-native (SaaS), zarządzanym z poziomu jednej, centralnej konsoli administracyjnej.
    d. Lokalizacja danych: Hosting danych oraz logów musi odbywać się na terenie UE (zgodność z RODO).
    e. Wsparcie techniczne: Producent zapewnia wsparcie 24/7/365 (telefon + portal zgłoszeniowy).
2. **Architektura i Integracja (ochrona poczty)**
    a. Kompatybilność: System musi wspierać:
        i. Microsoft Exchange Online / Microsoft 365,
        ii. Microsoft Exchange 2003 lub nowszy,
        iii. Google Workspace Gmail.
    b. Metody wdrażania (co najmniej):
        i. tryb bramy pocztowej oparty o zmianę trasowania (np. rekordy MX),
        ii. integracja z Microsoft 365 poprzez API umożliwiająca realizację integracji reguł przepływu poczty (Mailflow Rules) oraz pracę bezpośrednio na skrzynkach w modelu chmurowym.
    c. Integracja reguł przepływu (Microsoft 365 API): System musi umożliwiać tworzenie połączenia i wykorzystanie API do automatycznej konfiguracji reguł przepływu poczty w środowisku Microsoft 365.
    d. Ochrona przed manipulacją konfiguracją integracji: System musi wykrywać i alarmować o nieautoryzowanych lub nieoczekiwanych zmianach konfiguracji po stronie integracji (np. reguł przepływu poczty w Microsoft 365).
3. **Ochrona przed Zagrożeniami**
    a. Wielowarstwowa detekcja: System musi zapewniać detekcję zagrożeń w treści i załącznikach, w tym mechanizmy oparte o modele uczenia maszynowego do wykrywania zagrożeń także bez polegania wyłącznie na sygnaturach.
    b. Ochrona linków:
        i. przepisanie adresów URL w wiadomościach,
        ii. weryfikacja adresu docelowego w momencie kliknięcia oraz reakcja zgodnie z polityką bezpieczeństwa.

c. Wycofywanie wiadomości po dostarczeniu: System musi mieć funkcję „na żądanie" umożliwiającą usunięcie lub wycofanie wiadomości z dostarczonych skrzynek, jeśli później zostanie potwierdzone zagrożenie.
d. Chmurowe środowisko analizy plików (Sandbox): System musi posiadać chmurowe środowisko do detonacji podejrzanych plików i generowania raportu analizy.

**4. Ciągłość Biznesowa**

a. Kolejkowanie poczty: W przypadku niedostępności serwera docelowego system musi automatycznie kolejkować pocztę i ponawiać próby dostarczenia przez okres minimum 5 dni.
b. Awaryjna skrzynka odbiorcza: System musi zapewniać portalowy dostęp użytkowników do wiadomości zatrzymanych w kolejce (co najmniej odczyt; dopuszczalnie również odpowiedź) w trakcie awarii podstawowej usługi pocztowej.

**5. Ochrona Danych i Szyfrowanie (DLP w kanale e-mail)**

a. Skanowanie treści i załączników: System musi automatycznie analizować treść wiadomości i załączniki pod kątem danych wrażliwych.
b. Predefiniowane klasy danych / wykrywanie danych wrażliwych: System musi umożliwiać wykrywanie w poczcie m.in. PII, danych finansowych, informacji zdrowotnych oraz innych danych poufnych; polityki muszą wspierać co najmniej scenariusze dla grup i użytkowników indywidualnych.
c. Zaawansowane reguły: Możliwość budowy reguł w oparciu o słowa kluczowe oraz wyrażenia regularne i atrybuty wiadomości (np. nagłówki, źródło, rozmiar).
d. Akcje po dopasowaniu polityki: System musi umożliwiać działania typu blokowanie albo szyfrowanie wiadomości po wykryciu dopasowania do reguł ochrony danych.
e. Szyfrowanie:
    i. wymuszane szyfrowanie transmisji TLS,
    ii. możliwość stosowania podpisu cyfrowego S/MIME,
    iii. szyfrowanie portalowe obejmujące całą wiadomość lub same załączniki,
    iv. opcjonalny portal do odczytu/odpowiedzi na zaszyfrowane wiadomości (jeśli przewidziane licencyjnie w oferowanym rozwiązaniu).

**6. Moduł Symulacji Ataków i Edukacji Użytkowników (Security Awareness Training)**

a. Typy kampanii (co najmniej):
    i. symulacje phishingowe,
    ii. symulacje wyłudzania poświadczeń,
    iii. symulacje z wykorzystaniem załączników,
    iv. kampanie szkoleniowe.
b. Szkolenia naprawcze po „niezdanym teście": System musi umożliwiać przypisanie szkolenia użytkownikom, którzy nie zaliczyli symulacji (np. kliknęli link, otworzyli załącznik lub wprowadzili poświadczenia), wraz z mechanizmem przypomnień.
c. Raportowanie skuteczności i ryzyka:
    i. raporty statusu szkoleń (zapisani / nieukończone),
    ii. eksport raportów do CSV.
d. Bezpośrednie dostarczanie kampanii (Direct Delivery) – Microsoft 365: System powinien wspierać tryb „Direct Delivery" w środowisku Microsoft 365, ograniczający potrzebę ręcznego utrzymywania list dozwolonych domen/URL/IP dla testów.
e. Obsługa Google Workspace: System musi wspierać integrację z Google Workspace na potrzeby dostarczalności kampanii (wymagana konfiguracja wyjątków/allowlist po stronie Google Workspace zgodnie z dokumentacją producenta).

7. **Administracja i Portal Użytkownika**
    a. Zunifikowana konsola: Administracja ochroną poczty oraz kampaniami edukacyjnymi z jednego panelu zarządzania.
    b. Portal użytkownika: Użytkownicy końcowi muszą mieć możliwość:
        i. podglądu działań kampanii i przypisanych szkoleń,
        ii. wglądu w elementy samoobsługowe związane z pocztą (np. operacje na kwarantannie/allowlist/blocklist – jeśli przewidziane w oferowanym rozwiązaniu).
8. **Wdrożenie**

Wykonawca przeprowadzi kompleksowe wdrożenie oprogramowania, obejmujące jego instalację, konfigurację, uruchomienie oraz dostosowanie do środowiska Zamawiającego. Wdrożenie zostanie wykonane z należytą starannością, zgodnie z aktualną wiedzą techniczną, zaleceniami producenta oraz najlepszymi praktykami branżowymi.

# 6.4. Zapora sieciowa – typ 1

## Ilość sztuk: 1 sztuka

**Zakres: IT**

**Wymagania minimalne:**

1. System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania.
2. Rozwiązanie powinno być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2.
3. Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca)
4. Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie HA Active-Passive lub Active-Active.
5. System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej.
6. Rozwiązanie powinno być wyposażone w wysokowydajny wielordzeniowy procesor x86 (CPU)
7. Rozwiązanie musi być wyposażone w co najmniej jeden dysk służący m.in. do przechowywania logów i raportów bezpośrednio na urządzeniu.
8. Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy.
9. Urządzenie w metalowej obudowie o wysokości 1U z możliwością montażu w szafie rack 19" (uchwyty montażowe jako opcjonalne wyposażenie).
10. Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB).
11. Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie.
12. Wbudowany port USB umożliwiający podłączenie pamięci flash i przeprowadzenie konfiguracji w trybie Zero Touch.
13. Możliwość rozbudowy o dodatkowe moduły interfejsów sieciowych.

**Parametry:**

1. Pamięć operacyjna RAM nie mniej niż (GB): 8
2. Przestrzeń do przechowywania logów i raportów nie mniej niż (GB) 64

3. Liczba fizycznych interfejsów 1000BASE-T nie mniej niż: 4
4. Liczba fizycznych interfejsów 2.5GBASE-T nie mniej niż: 2
5. Liczba fizycznych interfejsów 10GBASE-X nie mniej niż: 2
6. Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q nie mniej niż: 128

**Wydajność:**

1. Wydajność Firewall nie mniej niż (Gbps): 19.1
2. Wydajność Firewall IMIX nie mniej niż (Gbps): 10.5
3. Wydajność IPS nie mniej niż (Gbps): 5.85
4. Wydajność FW+IPS+AV nie mniej niż (Gbps): 4.75
5. Wydajność NGFW nie mniej niż (Gbps): 5.1
6. Liczba równoczesnych połączeń nie mniejsza niż: 6550000
7. Liczba nowych połączeń na sekundę nie mniejsza niż: 105000
8. Wydajność IPsec VPN nie mniej niż (Gbps): 6.6
9. Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Gbps): 1.7
10. Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż: 18400
11. Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: 1500
12. Liczba równoczesnych tuneli IPsec VPN nie mniejsza niż: 2500

**Zarządzanie:**

1. Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym.
2. Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA).
3. Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN.
4. Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter.
5. Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.
6. Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administratora, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów.
7. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
8. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności.
9. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
10. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.

11. Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).
12. System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.
13. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm).
14. System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog).
15. Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej.
16. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS).
17. Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta.
18. System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednika).
19. System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia.
20. System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta, przy czym w podstawowej wersji utrzymywany i udostępniany jest on bezpłatnie i nie wymaga zakupu osobnych subskrypcji.
21. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP, via email jak i dodatkowo do centralnego systemu zarządzania w chmurze.
22. Rozwiązanie powinno oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.
23. Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.
24. Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.
25. Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu licencyjnego a synchronizacja subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.
26. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego. Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI.
27. Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć.
28. Rozwiązanie powinno oferować mechanizm szyfrowania danych takich jak loginy, hasła, klucze które przechowywane są w konfiguracji urządzenia. Dane powinny być zabezpieczone

dedykowanym kluczem szyfrującym tworzonym na podstawie bezpiecznie składowanego poza urządzeniem hasła.

29. Rozwiązanie powinno zapewniać możliwość zmiany nazw interfejsów sieciowych.

**Zapora sieciowa:**

1. Wymagane jest, aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection.
2. System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6.
3. Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas.
4. System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.
5. System powinien pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania).
6. System powinien pozwalać na grupowanie reguł zapory. Wymagana jest funkcjonalność automatycznego wiązania nowotworzonych reguł do właściwych grup na podstawie kryteriów opisujących grupę.
7. Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.
8. System ochrony powinien zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN.
9. Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.
10. System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
11. Rozwiązanie powinno oferować narzędzie do symulowanego testu reguł zapory w oparciu o zadane przez administratora kryteria takie jak IP, strefa zapory, użytkownik, dzień, godzina.
12. System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.

**Trasowanie ruchu:**

1. Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing.
2. Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.
3. Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów.
4. Rozwiązanie powinno umożliwiać rozkładanie ruchu w oparciu o wagi interfejsów WAN.
5. Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast.
6. Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).
7. Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).
8. Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.

**Translacja adresów i portów:**

1. Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT.
2. Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT

3. Rozwiązanie powinno pozwalać na automatyczne tworzenie reguł NAT typu loopback czy reflexive rule.

**Kształtowanie pasma i jakość usług:**

1. System powinien zapewniać możliwość elastycznego kształtowania pasma dla sieci, użytkowników i aplikacji.
2. Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.
3. System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
4. Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6.
5. Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet (od 1 Business Critical do 7 Best Effort).

**Podstawowa ochrona przed atakami DoS i DDoS:**

- System powinien zapewniać ochronę przed atakami DoS czy DDoS.

**Pozostałe:**

1. Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.
2. Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).
3. System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.
4. System powinien oferować wsparcie dla IEEE 802.1Q VLAN z możliwością konfiguracji niezależnych puli DHCP.
5. Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
6. System powinien oferować wsparcie dla usług Dynamic DNS
7. Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).
8. Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo).
9. Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.

**Uwierzytelnianie i obsługa użytkowników:**

1. Wymagane uwierzytelniaine użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta.
2. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników.
3. System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.
4. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.
5. System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm).
6. Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server.

7. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.
8. Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci.
9. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania.
10. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS.
11. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android.
12. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu.

**Koncentrator VPN:**

1. System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.
2. System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519).
3. System musi obsługiwać połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN.
4. Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN.
5. Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback.
6. Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego.
7. Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth.
8. Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.
9. Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.
10. Urządzenie musi obsługiwać połączenia L2TP over IPsec.
11. Połączenia VPN terminowane muszą być dedykowanej strefie zapory sieciowej.

**Logowanie i raportowanie:**

1. System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym.
2. System powinien umożliwiać składowanie oraz archiwizację logów.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów.
5. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa
6. System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.
7. System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących.
8. Rozwiązanie powinno umożliwiać wysyłanie raportów via email.
9. Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV.

10. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.
11. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.
12. System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.
13. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.
14. System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.

**Intrusion Prevention System i Advanced Threat Protection (IPS, ATP)**

1. Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 4500 sygnatur.
2. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.
3. Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS.
4. Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.
5. System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.

**Ochrona przed Malware i kontrola web:**

1. Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP.
2. Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania.
3. Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej.
4. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.
5. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.
6. Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek.
7. Rozwiązanie musi przeprowadzać emulację skryptów Java.
8. Rozwiązanie powinno przeprowadzać w trybie rzeczywistym weryfikować bazę zagrożeń producenta.
9. Rozwiązanie powinno umożliwiać blokowanie potencjalnie niechcianych aplikacji.
10. System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur.

**Inspekcja ruchu SSL/TLS:**

1. Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów.
2. Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2.
3. Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP.
4. Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443).
5. Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web.

6. Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen.

**Filtr Web:**

1. Rozwiązanie powinno zawierać przynajmniej 70 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron.
2. Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy.
3. Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól.
4. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowania treści komunikatu w tym dodania logo organizacji.
5. Rozwiązanie powinno umożliwiać filtrowanie stron web analizując ich zawartość wykorzystując tzw. Content Filtering na bazie haseł kluczowych.
6. Rozwiązanie powinno oferować ochronę przed Pharmingiem.

**Ochrona i kontrola aplikacji:**

1. Rozwiązanie powinno oferować bazę danych opisująca co najmniej 2700 aplikacji.
2. Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.
3. Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji.
4. Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów.
5. Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp.
6. Rozwiązanie powinno oferować funkcje CASB (Cloud Access Security Broker) celem monitorowania i regulowania dostępu do aplikacji chmurowych wykorzystywanych przez użytkowników.
7. Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN.

**Ochrona przed nieznanymi zagrożeniami:**

1. Rozwiązanie klasy Sandbox do ochrony przez zagrożeniami typu Zero-Day.
2. Rozwiązanie oferujące statyczną i dynamiczną analizę kodu przesyłanego w ramach ruchu web czy email.
3. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll.
4. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf.
5. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf.
6. Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.
7. System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows
8. System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu.
9. System zapewniający analizę struktury kodu w tym analizę przeprowadzaną przez mechanizmy głębokiego uczenia maszynowego.

10. System zapewniający ochronę przed exploitami i złośliwym kodem ransomware.
11. System badający reputację pliku w zewnętrznych bazach takich jak np.Virustotal.
12. System powinien oferować szczegółowe raporty dowodzące przeprowadzanie analizy dla w/w mechanizmów.

**Gwarancja i wsparcie producenta:**

• Gwarancja sprzętowa producenta z procedurą RMA oraz wymianą wyprzedzającą (wysyłka sprzętu zastępczego przed odesłaniem uszkodzonego) na okres 36 miesięcy.

• Bezpłatne aktualizacje bezpieczeństwa i poprawki w okresie obowiązywania subskrypcji.

• Bezpłatne aktualizacje funkcjonalne oraz nowe wersje oprogramowania w okresie obowiązywania subskrypcji.

**Wdrożenie:**

Wykonawca przeprowadzi kompleksowe wdrożenie sprzętu, obejmujące jego dostawę, instalację, konfigurację i uruchomienie. Wszystkie prace zostaną wykonane z należytą starannością, zgodnie z aktualną wiedzą techniczną, zaleceniami producenta oraz najlepszymi praktykami branżowymi.

## 6.5. Zapora sieciowa – typ 2

### Ilość sztuk: 2 sztuki

**Zakres: OT**

**Wymagania minimalne:**

1. System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania.
2. Rozwiązanie powinno być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2.
3. Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca)
4. Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie HA Active-Passive lub Active-Active.
5. System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej.
6. Rozwiązanie powinno być wyposażone w wysokowydajny wielordzeniowy procesor x86 (CPU)
7. Urządzenie w metalowej obudowie typu desktop z możliwością montażu w szafie rack 19" przy użyciu opcjonalnego zestawu montażowego.
8. Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB).
9. Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie.
10. Wbudowany port USB umożliwiający podłączenie pamięci flash i przeprowadzenie konfiguracji w trybie Zero Touch.

**Parametry:**

1. Pamięć operacyjna RAM nie mniej niż (GB): 4
2. Przestrzeń do przechowywania logów i raportów nie mniej niż (GB): 16 GB

3. Liczba fizycznych interfejsów 2.5GBASE-T nie mniej niż: 4
4. Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q nie mniej niż: 128

**Wydajność:**

1. Wydajność Firewall nie mniej niż (Gbps): 9.9
2. Wydajność Firewall IMIX nie mniej niż (Gbps): 6.5
3. Wydajność IPS nie mniej niż (Gbps): 2
4. Wydajność FW+IPS+AV nie mniej niż (Gbps): 2
5. Wydajność NGFW nie mniej niż (Gbps): 2
6. Liczba równoczesnych połączeń nie mniejsza niż: 1600000
7. Liczba nowych połączeń na sekundę nie mniejsza niż: 40500
8. Wydajność IPsec VPN nie mniej niż (Gbps): 6
9. Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Gbps): 0.6
10. Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż: 8100
11. Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: 500
12. Liczba równoczesnych tuneli IPsec VPN nie mniejsza niż: 500

**Zarządzanie:**

1. Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym.
2. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA).
3. Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN.
4. Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter.
5. Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.
6. Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administratora, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów.
7. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
8. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności.
9. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.
10. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.

11. Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).
12. System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.
13. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm).
14. System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog).
15. Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej.
16. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS).
17. Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta.
18. System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednika).
19. System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia.
20. System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta, przy czym w podstawowej wersji utrzymywany i udostępniany jest on bezpłatnie i nie wymaga zakupu osobnych subskrypcji.
21. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP, via email jak i dodatkowo do centralnego systemu zarządzania w chmurze.
22. Rozwiązanie powinno oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.
23. Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.
24. Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.
25. Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu licencyjnego a synchronizacja subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.
26. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego. Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI.
27. Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć.
28. Rozwiązanie powinno oferować mechanizm szyfrowania danych takich jak loginy, hasła, klucze które przechowywane są w konfiguracji urządzenia. Dane powinny być zabezpieczone

dedykowanym kluczem szyfrującym tworzonym na podstawie bezpiecznie składowanego poza urządzeniem hasła.

29. Rozwiązanie powinno zapewniać możliwość zmiany nazw interfejsów sieciowych.

**Zapora sieciowa:**

1. Wymagane jest, aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection.
2. System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6.
3. Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas.
4. System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.
5. System powinien pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania).
6. System powinien pozwalać na grupowanie reguł zapory. Wymagana jest funkcjonalność automatycznego wiązania nowotworzonych reguł do właściwych grup na podstawie kryteriów opisujących grupę.
7. Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.
8. System ochrony powinien zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN.
9. Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.
10. System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).
11. Rozwiązanie powinno oferować narzędzie do symulowanego testu reguł zapory w oparciu o zadane przez administratora kryteria takie jak IP, strefa zapory, użytkownik, dzień, godzina.
12. System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.

**Trasowanie ruchu:**

1. Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing.
2. Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.
3. Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów.
4. Rozwiązanie powinno umożliwiać rozkładanie ruchu w oparciu o wagi interfejsów WAN.
5. Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast.
6. Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).
7. Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).
8. Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.

**Translacja adresów i portów:**

1. Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT.

2. Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT
3. Rozwiązanie powinno pozwalać na automatyczne tworzenie reguł NAT typu loopback czy reflexive rule.

**Kształtowanie pasma i jakość usług:**

1. System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji.
2. Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.
3. System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
4. Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6.
5. Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet (od 1 Business Critical do 7 Best Effort).

**Podstawowa ochrona przed atakami DoS i DDoS:**

- System powinien zapewniać ochronę przed atakami DoS czy DDoS.

**Pozostałe:**

1. Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.
2. Rozwiązanie powinno oferować możliwość tworzenia wielu mostów oraz mostów zbudowanych z wielu portów.
3. System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.
4. System powinien oferować wsparcie dla IEEE 802.1Q VLAN z możliwością konfiguracji niezależnych puli DHCP.
5. Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).
6. System powinien oferować wsparcie dla usług Dynamic DNS.
7. Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).
8. Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo).
9. Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.

**Uwierzytelnianie i obsługa użytkowników:**

1. Wymagane uwierzytelnianie użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta.
2. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników.
3. System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.
4. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.
5. System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm).

6. Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server.
7. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.
8. Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci.
9. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania.
10. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS.
11. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android.
12. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu.

**Koncentrator VPN:**

1. System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.
2. System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519).
3. System musi obsługiwać połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN.
4. Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN.
5. Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback.
6. Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego.
7. Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth.
8. Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN.
9. Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.
10. Urządzenie musi obsługiwać połączenia L2TP over IPsec.
11. Połączenia VPN terminowane muszą być dedykowanej strefie zapory sieciowej.

**Logowanie i raportowanie:**

1. System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym.
2. System powinien umożliwiać składowanie oraz archiwizację logów.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów.
5. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa
6. System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.
7. System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących.
8. Rozwiązanie powinno umożliwiać wysyłanie raportów via email.
9. Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV.

10. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.
11. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.
12. System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.
13. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.
14. System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.

**Intrusion Prevention System i Advanced Threat Protection (IPS, ATP):**

1. Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 4700 sygnatur.
2. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.
3. Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS.
4. Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.
5. System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.

**Ochrona przed Malware i kontrola web:**

1. Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP.
2. Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania.
3. Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej.
4. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.
5. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.
6. Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek.
7. Rozwiązanie musi przeprowadzać emulację skryptów Java.
8. Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta.
9. Rozwiązanie powinno umożliwiać blokowanie potencjalnie niechcianych aplikacji.
10. System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates)

**Inspekcja ruchu SSL/TLS:**

1. Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów.
2. Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2.
3. Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP.
4. Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443).
5. Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web.

6. Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen.

**Filtr Web:**

1. Rozwiązanie powinno zawierać przynajmniej 70 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron.
2. Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy.
3. Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól.
4. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowanie treści komunikatu w tym dodania logo organizacji.
5. Rozwiązanie powinno umożliwiać filtrowanie stron web analzując ich zawartość na bazie haseł kluczowych.
6. Rozwiązanie powinno oferować ochronę przed Pharmingiem.

**Ochrona i kontrola aplikacji:**

1. Rozwiązanie powinno oferować bazę danych opisująca co najmniej 2500 aplikacji.
2. Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.
3. Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji.
4. Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów.
5. Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp.
6. Rozwiązanie powinno oferować funkcje CASB (Cloud Access Security Broker) celem monitorowania i regulowania dostępu do aplikacji chmurowych wykorzystywanych przez użytkowników.
7. Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN.

**Ochrona przed nieznanymi zagrożeniami:**

1. Rozwiązanie klasy Sandbox do ochrony przez zagrożeniami typu Zero-Day.
2. Rozwiązanie oferujące statyczną i dynamiczną analizę kodu przesyłanego w ramach ruchu web czy email.
3. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll.
4. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf.
5. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf.
6. Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.
7. System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows
8. System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu.
9. System zapewniający analizę struktury kodu w tym analizę przeprowadzaną przez mechanizmy głębokiego uczenia maszynowego.

10. System zapewniający ochronę przed exploitami i złośliwym kodem ransomware.
11. System badający reputację pliku w zewnętrznych bazach takich jak np.Virustotal.
12. System powinien oferować szczegółowe raporty dowodzące przeprowadzanie analizy dla w/w mechanizmów.

**Gwarancja i wsparcie producenta:**

- Gwarancja sprzętowa producenta z procedurą RMA oraz wymianą wyprzedzającą (wysyłka sprzętu zastępczego przed odesłaniem uszkodzonego) na okres 36 miesięcy.
- Bezpłatne aktualizacje bezpieczeństwa i poprawki w okresie obowiązywania subskrypcji.
- Bezpłatne aktualizacje funkcjonalne oraz nowe wersje oprogramowania w okresie obowiązywania subskrypcji.

**Wdrożenie:**

Wykonawca przeprowadzi kompleksowe wdrożenie sprzętu, obejmujące jego dostawę, instalację, konfigurację i uruchomienie. Wszystkie prace zostaną wykonane z należytą starannością, zgodnie z aktualną wiedzą techniczną, zaleceniami producenta oraz najlepszymi praktykami branżowymi.

## 6.6. System do inwentaryzacji aktywów teleinformatycznych i monitorowania infrastruktury informatycznej

**Zakres: IT/OT**

**Podstawowa funkcjonalność systemu:**

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 200 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.

10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
    a. VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
    b. Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
    a. serwera RADIUS dla infrastruktury sieciowej,
    b. serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
    c. serwera SYSLOG,
    d. serwera TACACS+,
    e. serwera Monitoringu,
    f. serwera DHCP,
    g. serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
    h. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).

24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.

47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
    a. Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
    b. Czy włączony jest firewall
    c. Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
    d. Czy jest włączone szyfrowanie dysku systemowego
    e. Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
    f. Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
    g. Czy w systemie są uruchomione procesy wskazane przez administratora
    h. Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
    i. Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
        i. Wartości klucza rejestru
        ii. Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.

62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
    a. Microsoft Windows
    b. Mac OS
    c. iOS
    d. Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

**Mechanizmy uwierzytelniania**

1. 1.System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. 2.System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
    a. MAC,
    b. PAP/ASCII,
    c. CHAP,
    d. SNMP,
    e. 802.1X.
3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
    a. Tożsamość/Urządzenie końcowe,
    b. Grupa tożsamości/urządzeń końcowych,
    c. Parametry urządzeń końcowych, min: system operacyjny, wersja,
    d. Atrybuty Active Directory,
    e. Jednostka organizacyjna tożsamości/urządzeń końcowych,
    f. Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
    g. Grupy urządzeń sieciowych,
    h. Porty urządzeń sieciowych,
    i. Grupy portów urządzeń sieciowych,
    j. Jednostka organizacyjna portów,
    k. Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
    l. Data, czas ważności polityki,
    m. Wewnętrzny Captive Portal,

**Metoda autoryzacji.**

8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących

producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.

9. System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

**Obsługa serwerów certyfikatów CA**

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
    a. możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
    b. możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
    c. Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
    d. usługę OCSP (Online Certificate Status Protocol).

**Obsługa serwerów DHCP**

1. System musi posiadać funkcję zintegrowanego serwera DHCP.

2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
    a. Uruchamianie usługi dla wybranych podsieci,
    b. Przypisanie ustalonego adresu IP dla adresu MAC.
    c. Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
    d. Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
    e. Możliwość określania braku dostępu dla wybranych adresów MAC,
    f. Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
    g. Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
    h. Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
    i. Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
    j. Dokonywanie zmian bez konieczności wyłączania usług.

**Obsługa serwerów TACACS+**

1. System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:
2. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
3. System musi umożliwiać tworzenia haseł administratorom.
4. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
5. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
6. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
7. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
8. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
9. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

**Raportowanie i monitoring:**

**System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:**

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.

9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.

**Raport zdarzeń Microsoft Active Directory, minimum:**

- Logowania, wylogowania z system w tym błędne logowania
- Logowania do sieci 802.1X

**Alarmy**

**System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:**

1. wiadomości e-mail,
2. Syslog,
3. notyfikacji systemowych.

**Alarmy mogą być generowane w sytuacjach, min:**

1. Ilości obsługiwanych transakcji RADIUS,
2. Opóźnienie obsługi transkacji RADIUS,
3. Statusu krytycznego modułów.

**System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:**

1. badanie łączności IP za pomocą ping, traceroute, tcpdump protokołów RADIUS, TACACS+,
2. wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
3. nazwy użytkownika,
4. adresu MAC,
5. statusu uwierzytelnienia (udana lub nieudana),
6. powodu, jeżeli uwierzytelnienie nieudane,
7. zakresu czasowego, co do dnia, godziny i minuty,
8. wykonanie zdalnego polecenia na urządzeniu sieciowym.

**Wdrożenie:**

Wykonawca przeprowadzi kompleksowe wdrożenie oprogramowania, obejmujące jego instalację, konfigurację, uruchomienie oraz dostosowanie do środowiska Zamawiającego. Wdrożenie zostanie wykonane z należytą starannością, zgodnie z aktualną wiedzą techniczną, zaleceniami producenta oraz najlepszymi praktykami branżowymi.

**Licencja wsparcia technicznego producenta oprogramowania:**

1. Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 36 miesięczną licencję na wsparcie producenta oprogramowania. Licencja ta powinna obejmować minimum:
2. Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC
3. Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
4. Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
5. Dostęp do dokumentacji i instrukcji na stronie internetowej.
6. Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

# 6.7. Macierz dyskowa (NAS)

## Ilość sztuk: 1 sztuka

**Zakres: IT**

| **Specyfikacja sprzętowa** | |
|---|---|
| **Procesor** | Procesor 64 bit x86 o takowaniu nie mniejszym niż 2.2 GHz |
| **Procesor liczba rdzeni** | Nie mniej niż 4 |
| **Pamięć RAM** | Nie mniej niż 8GB |
| **Pamieć RAM liczba slotów** | Minimum 2 sloty |
| **Pamięć RAM - możliwość rozszerzenia** | Nie mniej niż do 64GB |
| **Pamięć Flash** | Nie mniej niż 5 GB |
| **Liczba zatok na dyski** | Minimum 8 zatok 3,5" |
| **Obsugiwane dyski twarde** | 3.5" SATA oraz 2.5" SATA oraz 2.5" SATA SSD |
| **Możliwość stosowania dysków twardych o pojemnościach** | do 22TB |
| **Możliwość podłączenia modułu rozszerzającego** | Tak, co najmniej 2 |
| **Porty LAN 2,5 GbE** | Minimum 2 RJ-45 |
| **Diody LED** | Minimum Status, LAN, HDD, |
| **Porty USB** | Minimum 3 x typu A USB 3.2 Gen 2 10 Gb/s<br>Minimum 1 x typu C USB 3.2 Gen 1 5 Gb/s |
| **Port PCiE** | Tak, minimum 2xGen 3x4 |
| **Przyciski** | Reset, Zasilanie |
| **Typ obudowy** | Tower |
| **Dopuszczalna temperatura pracy** | od 0 do 40˚C |

| | |
|---|---|
| **Wilgotność względna podczas pracy** | 5-95% R.H. |
| **Zasilanie** | Max. 250 W |
| **Specyfikacja oprogramowania** | |
| **Obsługa dwóch systemów operacyjnych** | Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS |
| **Agregacja łączy** | Tak |
| **Obsługiwane systemy plików** | Dyski wewnętrzne: EXT4<br>Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT |
| **Możliwość podłączenia karty WLAN na USB** | Tak |
| **Szyfrowanie udziałów** | Tak, min AES 256 |
| **Szyfrowanie dysków zewnętrznych** | Tak |
| **Zarządzanie dyskami** | Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD,<br>Obsługa Hot Spare per grupa RAID oraz global hot spare<br>Rozszerzanie pojemności Online RAID<br>Migracja poziomów Online RAID<br>HDD S.M.A.R.T.<br>Skanowanie uszkodzonych bloków<br>Przywracanie macierzy RAID<br>Obsługa map bitowych<br>Pula pamięci masowej<br>Obsługa migawek<br>Obsługa replikacji migawek |
| **Wbudowana obsługa iSCSI** | Multi-LUNs na Target<br>Obsługa LUN Mapping & Masking<br>Obsługa SPC-3 Persistent Reservation<br>Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN |
| **Zarządzanie prawami dostępu** | Ograniczenie dostępnej pojemności dysku dla użytkownika<br>Importowanie listy użytkowników<br>Zarządzanie kontami użytkowników<br>Zarządzanie grupą użytkowników<br>Zarządzanie współdzieleniem w sieci<br>Tworzenie użytkowników za pomocą makr<br>Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL |
| **Obsługa Windows AD** | Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web<br>Funkcja serwera LDAP |
| **Funkcje backup** | Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde, |
| **Współpraca z zewnętrznymi dostawcami usług chmury** | Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box |
| **Darmowe aplikacje na urządzenia mobilne** | Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer<br>Dostępne na systemy iOS oraz Android |

| | |
|---|---|
| **Minimum obsługiwane serwery** | Serwer plików<br>Serwer FTP<br>Serwer WEB<br>Serwer kopii zapasowych<br>Serwer multimediów UPnP<br>Serwer pobierania (Bittorrent / HTTP / FTP)<br>Serwer Monitoringu |
| **VPN** | VPN client / VPN server<br>Obsługa PPTP, OpenVPN |
| **Administracja systemu** | Połączenia HTTP/HTTPS<br>Powiadamianie przez e-mail (uwierzytelnianie SMTP)<br>Powiadamianie przez SMS<br>Ustawienia inteligentnego chłodzenia<br>DDNS oraz zdalny dostęp w chmurze<br>SNMP (v2 & v3)<br>Obsługa UPS z zarządzaniem SNMP (USB)<br>Obsługa sieciowej jednostki UPS<br>Monitor zasobów<br>Kosz sieciowy dla CIFS/SMB oraz AFP<br>Monitor zasobów systemu w czasie rzeczywistym<br>Rejestr zdarzeń<br>System plików dziennika<br>Całkowity rejestr systemowy (poziom pliku)<br>Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line<br>Aktualizacja oprogramowania automatyczna<br>Możliwość aktualizacji oprogramowania ręcznie<br>Ustawienia systemu: Kopia, Przywracanie, Resetowanie |
| **Wirtualizacja** | Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.<br>Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5<br>Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych. |
| **Konteneryzacja** | Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker |
| **Zabezpieczenia** | Filtracja IP<br>Ochrona dostępu do sieci z automatycznym blokowaniem<br>Połączenie HTTPS<br>FTP z SSL/TLS (Explicit)<br>Obsługa SFTP (tylko admin)<br>Szyfrowanie AES 256-bit<br>Szyfrowana zdalna replikacja (Rsync poprzez SSH)<br>Import certyfikatu SSL<br>Powiadomienia o zdarzeniach za pośrednictwem Email i SMS |

| | |
|---|---|
| **Możliwość instalacji dodatkowego oprogramowania** | Tak, sklep z aplikacjami; możliwość instalacji z paczek |
| **Gwarancja** | 3 lata |

## 6.8. System typu Centralny menedżer haseł

**Zakres: IT**

System do zarządzania hasłami powinien być kompleksową platformą, która zapewnia bezpieczne przechowywanie, zarządzanie i udostępnianie danych uwierzytelniających dla użytkowników w organizacji. Powinien oferować zaawansowane funkcje szyfrowania, szerokie możliwości integracji, wsparcie dla systemów SIEM i API, a także opcje hostingu lokalnego i chmurowego.

**Kluczowe funkcje i możliwości:**

Przechowywanie i zarządzanie hasłami:

1. System powinien zapewniać centralne, szyfrowane repozytorium do przechowywania haseł, danych logowania i informacji wrażliwych, z zastosowaniem szyfrowania AES-256 bit.
2. System powinien posiadać wbudowane narzędzie do generowania silnych (tzw. generator haseł), losowych haseł w celu zminimalizowania ryzyka ponownego użycia danych uwierzytelniających.
3. System powinien umożliwiać bezpieczne przechowywanie kluczy dostępu, takich jak klucze FIDO2, do uwierzytelniania bez hasła.
4. System powinien pozwalać na import danych z innych narzędzi do przechowywania haseł co najmniej w formacie plików JSON, CSV, XML, TXT.

**Szyfrowanie i bezpieczeństwo:**

1. Wszystkie dane powinny być szyfrowane AES-256 bit, z szyfrowaniem odbywającym się po stronie klienta przed przesłaniem danych.
2. System powinien stosować model bezpieczeństwa zero-knowledge, zapewniając, że dostawca nie ma dostępu do danych użytkowników.
3. System do bezpiecznego przechowywania kluczy szyfrujących z haseł użytkowników powinien wykorzystywać tzw. funkcję Key Derivation Function (KDF) z wykorzystaniem algorytmów Argon2 lub PBKDF2.
4. System powinien stosować unikalny klucz do szyfrowania danych w sejfie, który nie jest przesyłany ani przechowywany przez dostawcę.
5. System powinien wspierać uwierzytelnianie wieloskładnikowe z wykorzystaniem takich metod jak TOTP, U2F i klucze sprzętowe FIDO2.
6. System powinien umożliwiać uwierzytelnianie biometryczne na obsługiwanych urządzeniach.

**Kompatybilność z wieloma platformami:**

1. System powinien posiadać aplikację kliencką systemów Windows, macOS i Linux.
2. System powinien oferować aplikację kliencką dla urządzeń iOS i Android.
3. System powinien integrować się z przeglądarkami Chrome, Firefox, Safari i Edge, umożliwiając automatyczne wypełnianie formularzy i bezpieczne logowanie.

**Single Sign-On (SSO):**

- System powinien obsługiwać różne protokoły SSO, w tym SAML 2.0 i OpenID Connect, do integracji z systemami zarządzania tożsamością i dostępem.

**Udostępnianie i Współpraca:**

1. System powinien umożliwiać bezpieczne udostępnianie elementów sejfu lub całych sejfów innym użytkownikom lub zespołom.
2. Powinien oferować funkcje zarządzania użytkownikami i dostępem w ramach organizacji, z centralnym zarządzaniem uprawnieniami i konfiguracją.
3. Powinien umożliwiać tworzenie kolekcji do grupowania elementów sejfu w ramach organizacji, z możliwością zarządzania dostępem do różnych zasobów.
4. Powinien oferować możliwość tworzenia, edytowania i usuwania kolekcji w ramach organizacji.
5. System powinien umożliwiać przesyłanie tekstów lub plików w sposób zaszyfrowany, z możliwością nadania polityki dostępu do wiadomości wraz z możliwością zabezpieczenie wiadomości hasłem i możliwością ustawienia dostępu tymczasowego (na określony polityką czas).

**Synchronizacja i zarządzanie:**

1. Powinien automatycznie synchronizować dane sejfu między różnymi urządzeniami użytkowników, zapewniając dostęp do aktualnych informacji.
2. Powinien umożliwiać tworzenie i zarządzanie grupami użytkowników w ramach organizacji, co ułatwia zarządzanie dostępem i uprawnieniami.
3. Powinien umożliwiać ustalanie polityk bezpieczeństwa i zarządzania, w tym wymogów dotyczących haseł, uwierzytelniania i zarządzania dostępem.

**Compliance i Raportowanie:**

1. System powinien dostarczać szczegółowe dzienniki działań użytkowników i zmian w systemie.
2. Powinien generować raporty dotyczące siły haseł, naruszeń i ocen bezpieczeństwa.
3. Narzędzie powinno zapewnić możliwość sprawdzenia czy dane hasło jest oznaczone na liście skompromitowanych haseł.
4. Narzędzie powinno zapewnić weryfikację haseł pod kątem siły hasła.

**Synchronizacja i Integracja:**

1. Powinien integrować się z usługami katalogowymi w celu zarządzania użytkownikami.
2. Powinien wspierać SCIM w celu zarządzania użytkownikami i synchronizacji.
3. Powinien ułatwiać integrację z systemami korporacyjnymi i aplikacjami zewnętrznymi.

**Integracja z SIEM:**

- Powinien obsługiwać integrację z systemami SIEM w celu centralnego zarządzania zdarzeniami bezpieczeństwa, umożliwiając analizę w czasie rzeczywistym i powiadamianie.

**Integracja API:**

1. System powinien oferować dobrze udokumentowane API do integracji z innymi systemami, umożliwiając automatyzację zarządzania użytkownikami, dostępem do sejfu i zarządzaniem grupami.

2. Dostęp do interfejs API powinno wspierać autoryzację i autentykację użytkowników za pomocą minimum OAuth 2.0.

**Hosting Lokalny i Open Source:**

1. System powinien oferować opcję hostingu lokalnego, co pozwala organizacjom na pełną kontrolę nad środowiskiem wdrożeniowym.
2. Powinien umożliwiać wdrożenia lokalne w postaci gotowego kontenera dostarczanego przez producenta oprogramowania, upraszczając proces instalacji i zarządzania. Dokumentacja i wsparcie dla wdrożeń lokalnych powinny być ogólnodostępne.
3. Organizacje powinny być odpowiedzialne za zarządzanie aktualizacjami, łatkami bezpieczeństwa i utrzymaniem lokalnej instancji, z regularnymi aktualizacjami i dokumentacją dostarczaną w celu wsparcia tych działań.
4. System powinien posiadać wbudowaną bazę danych MSSQL Express z możliwością migracji do zewnętrznej bazy danych MSSQL.
5. Opcjonalnie producent oferowanego oprogramowania do zarządzania hasłami powinien mieć dostępną formę dostarczania usługi w chmurze (SaaS) z lokalizacją centrum danych na terenie Unii Europejskiej, w celu przyszłej możliwej migracji środowiska.

**Elastyczność Modelu Wdrożenia i Licencjonowania**

1. System powinien zapewniać pełną elastyczność licencjonowania, umożliwiając organizacji płynne przejście pomiędzy modelem hostingu lokalnego (on-premises) a modelem chmury publicznej (SaaS) dostawcy.
2. Struktura licencji powinna być jednolita, co oznacza, że ten sam typ subskrypcji powinien uprawniać do korzystania zarówno z wersji on-premises, jak i chmurowej, bez konieczności zmiany typu licencji podczas migracji.
3. Migracja danych pomiędzy środowiskami (on-premises do chmury lub odwrotnie) powinna być wspierana przez producenta i możliwa do przeprowadzenia przy użyciu dostarczonych narzędzi eksportu/importu sejfu organizacji, minimalizując zakłócenia w dostępie do usługi.
4. Licencja powinien umożliwiać organizacji zachowanie pełnej kontroli nad danymi i kluczami szyfrującymi, niezależnie od wybranego modelu hostingu, rygorystycznie przestrzegając modelu zero-knowledge.

**Hosting w Chmurze Producenta (SaaS)**

1. Dostawca powinien oferować usługę w modelu SaaS (Software-as-a-Service) z gwarancją lokalizacji centrum danych na terenie Unii Europejskiej, w celu zapewnienia zgodności z wymogami RODO (GDPR).
2. W modelu SaaS, producent oprogramowania jest w pełni odpowiedzialny za zarządzanie infrastrukturą, skalowalność, wysoką dostępność (SLA), aktualizacje oraz wdrażanie łatek bezpieczeństwa, zwalniając organizację z obowiązków utrzymaniowych.
3. Usługa chmurowa powinien rygorystycznie przestrzegać modelu bezpieczeństwa zero-knowledge, zapewniając, że dostawca w żadnym momencie nie ma dostępu do odszyfrowanych danych (w tym haseł i kluczy) przechowywanych w sejfach użytkowników.
4. Dostawca usługi chmurowej powinien regularnie poddawać swoją infrastrukturę i oprogramowanie niezależnym audytom bezpieczeństwa (np. SOC 2 Typ 2, ISO 27001) i udostępniać raporty z tych audytów klientom korporacyjnym w celu weryfikacji zgodności.
5. Dostępna powinien być szczegółowa, publiczna dokumentacja dotycząca zarządzania organizacją w modelu chmurowym oraz procedur migracji.

**Wymagania dla Rozwiązań Open Source**:

1. System powinien być dostępny jako oprogramowanie open-source, umożliwiając organizacjom przeglądanie, modyfikowanie i wniesienie wkładu w kod źródłowy.
2. Powinien określać wymagania sprzętowe i programowe dla samodzielnego hostowania, w tym obsługę konteneryzacji.
3. Powinien zachęcać do wkładu społeczności w ulepszanie oprogramowania poprzez wnoszenie kodu, zgłaszanie problemów i udział w dyskusjach.

**Wdrożenie:**

Wykonawca przeprowadzi kompleksowe wdrożenie oprogramowania, obejmujące jego instalację, konfigurację, uruchomienie oraz dostosowanie do środowiska Zamawiającego. Wdrożenie zostanie wykonane z należytą starannością, zgodnie z aktualną wiedzą techniczną, zaleceniami producenta oraz najlepszymi praktykami branżowymi.

# 6.9. System typu MFA z wykorzystaniem sprzętowych kluczy bezpieczeństwa

**Zakres: IT**

**Wymagania ogólne**

Zamawiający wymaga dostarczenia systemu wieloskładnikowego uwierzytelniania (MFA) wykorzystującego sprzętowe klucze (**25 sztuk**) bezpieczeństwa zgodne z otwartymi standardami uwierzytelniania. Rozwiązanie ma zapewniać silne uwierzytelnianie użytkowników podczas dostępu do systemów teleinformatycznych, aplikacji oraz usług lokalnych i chmurowych, skutecznie ograniczając ryzyko przejęcia tożsamości użytkowników oraz ataków phishingowych.

System powinien umożliwiać stosowanie sprzętowych kluczy bezpieczeństwa jako drugiego składnika uwierzytelniania lub jako mechanizmu logowania bezhasłowego, zgodnie z możliwościami integrowanych systemów.

**Minimalne wymagania funkcjonalne**

Oferowany system musi zapewniać co najmniej:

1. uwierzytelnianie wieloskładnikowe (MFA) z wykorzystaniem sprzętowych kluczy bezpieczeństwa;
2. ochronę przed atakami phishingowymi poprzez wykorzystanie kryptografii asymetrycznej zgodnej ze standardami FIDO2/WebAuthn;
3. obsługę standardów FIDO2, WebAuthn, FIDO U2F, PIV (Smart Card), OTP, OATH-TOTP, OATH-HOTP, Challenge-Response oraz statycznego hasła;
4. możliwość wykorzystania sprzętowych kluczy jako drugiego składnika uwierzytelniania oraz do uwierzytelniania bezhasłowego (Passwordless Authentication);
5. obowiązkowe potwierdzenie obecności użytkownika poprzez fizyczną interakcję z urządzeniem podczas procesu uwierzytelniania;
6. współpracę z systemami Microsoft Windows, macOS, Linux, ChromeOS, Android oraz iOS;
7. współpracę z najpopularniejszymi przeglądarkami internetowymi, w szczególności Chrome, Microsoft Edge, Firefox, Safari oraz Opera;

8. kompatybilność z usługami wykorzystującymi standardy FIDO2/WebAuthn, w tym rozwiązaniami klasy Microsoft 365, Google Workspace, Bitwarden oraz innymi systemami wspierającymi wskazane standardy;
9. obsługę interfejsów USB-A lub USB-C oraz NFC;
10. obsługę biblioteki PKCS#11;
11. obsługę algorytmów kryptograficznych RSA 2048, RSA 4096 (OpenPGP), ECC P-256 oraz ECC P-384;
12. możliwość bezpiecznego przechowywania poświadczeń OTP na urządzeniu;
13. brak konieczności instalacji dodatkowych sterowników do obsługiwanych systemów operacyjnych;
14. brak konieczności stosowania baterii oraz połączenia z Internetem do działania urządzenia;
15. konstrukcję nieposiadającą pamięci masowej przeznaczonej do przechowywania plików użytkownika;
16. brak wykorzystania technologii Bluetooth;
17. jednolitą, trwałą konstrukcję odporną na uszkodzenia mechaniczne, o stopniu ochrony minimum IP68;
18. możliwość trwałego oznakowania urządzenia (np. numerem identyfikacyjnym lub logo);
19. konstrukcję utrudniającą ingerencję w urządzenie bez pozostawienia śladów naruszenia;
20. brak wykorzystania biometrii jako mechanizmu uwierzytelniania;
21. niewielkie wymiary umożliwiające codzienne użytkowanie oraz wyposażenie w otwór umożliwiający przypięcie do breloka lub identyfikatora;
22. gwarancję producenta na okres co najmniej 12 miesięcy oraz możliwość objęcia urządzeń usługą wymiany z pozostawieniem uszkodzonego urządzenia u Zamawiającego.

**Wdrożenie:**

Wykonawca przeprowadzi kompleksowe wdrożenie sprzętu, obejmujące jego dostawę, instalację, konfigurację i uruchomienie. Wszystkie prace zostaną wykonane z należytą starannością, zgodnie z aktualną wiedzą techniczną, zaleceniami producenta oraz najlepszymi praktykami branżowymi.

## 6.10. Oprogramowanie do zarządzania tożsamością i dostępem

**Zakres: IT**

**Zakres rozwiązania**

Rozwiązanie musi być dostarczane w modelu subskrypcyjnym jako usługa chmurowa (SaaS) i służyć do wykrywania, oceny oraz reagowania na zagrożenia związane z tożsamościami w środowisku Organizacji. Ochroną objęte są:

- **Co najmniej: 21** tożsamości użytkowników,
- **Co najmniej: 10** serwerów.

**Zakres tożsamości objętych ochroną**

Rozwiązanie musi obejmować ochroną:

- tożsamości ludzkie (pracownicy, goście oraz podmioty zewnętrzne),
- tożsamości maszynowe (NHI), w tym:
    - aplikacje,
    - Service Principals,
    - konta usługowe,
    - maszyny,
    - pozostałe tożsamości wykorzystywane do uwierzytelniania i autoryzacji dostępu do zasobów oraz komunikacji pomiędzy systemami.

**Redukcja powierzchni ataku na tożsamości**

Rozwiązanie musi zapewniać:

- ciągłe wykonywanie co najmniej 50 kontroli bezpieczeństwa tożsamości wykraczających poza podstawową higienę bezpieczeństwa;
- ciągłe skanowanie środowiska dostawcy tożsamości w chmurze w celu wykrywania błędów konfiguracji oraz luk bezpieczeństwa związanych z tożsamością;
- priorytetyzację wykrytych zagrożeń wymagających natychmiastowej reakcji;
- identyfikację ryzyk obejmujących co najmniej:
    - luki w politykach dostępu warunkowego,
    - konta osierocone,
    - konta o nadmiernych uprawnieniach,
    - aplikacje podwyższonego ryzyka.

**Ograniczanie ryzyka wycieku lub kradzieży poświadczeń**

Rozwiązanie musi zapewniać:

- ochronę przed technikami **Credential Access** zgodnie z taksonomią MITRE ATT&CK, obejmującą pełne (100%) pokrycie tej kategorii;
- wykrywanie ujawnionych poświadczeń w wyciekach danych;
- wykrywanie nietypowej aktywności użytkowników, w tym:
    - nietypowych wzorców logowania,
    - wykorzystania skradzionych poświadczeń;
- ciągłe monitorowanie wycieków poświadczeń wraz z weryfikacją aktualności odnalezionych rekordów;
- zapewnienie prywatności danych poświadczeń poprzez:
    - nieprzechowywanie haseł w postaci jawnej,
    - nieprzechowywanie skrótów (hashy) haseł,
    - niepozyskiwanie haseł od dostawców tożsamości,
    - stosowanie własnych mechanizmów skrótowania,
    - możliwość oceny unikalności haseł bez przechowywania ich rzeczywistej wartości;
- monitorowanie źródeł wycieków obejmujących co najmniej:
    - serwisy działające w Dark Web,
    - sieć TOR,
    - publiczne i ukryte kanały komunikatorów,
    - logi złośliwego oprogramowania typu Stealer.

**Funkcje wykrywania i reagowania na zagrożenia tożsamości**

Rozwiązanie musi zapewniać:

- scentralizowany katalog wszystkich tożsamości występujących w środowisku Organizacji;
- pulpit prezentujący co najmniej:
    - liczbę monitorowanych tożsamości,
    - grup,
    - urządzeń,
    - aplikacji;
- ciągłą ocenę stanu bezpieczeństwa tożsamości wraz z rekomendacjami działań naprawczych;
- ocenę poziomu ryzyka z prezentacją trendów w czasie oraz możliwością eksportu wykresów;
- widok ustaleń umożliwiający:
    - sortowanie według poziomu ryzyka,
    - prezentację statusu,
    - kategorii,
    - poziomu ryzyka,
    - danych wspierających proces triage;
- analitykę zachowań użytkowników wykrywającą:
    - wykorzystanie skradzionych poświadczeń,
    - zagrożenia wewnętrzne,
    - nietypową aktywność użytkowników;
- zaawansowane wykrywanie zagrożeń tożsamości poprzez identyfikację działań odpowiadających technikom przeciwnika na wczesnym etapie łańcucha ataku;
- działania reagowania obejmujące co najmniej:
    - wymuszenie zmiany hasła,
    - blokadę kont wykazujących podejrzane zachowanie,
    - inne działania neutralizujące zagrożenie.

**Dane wywiadowcze z Dark Web**

Rozwiązanie musi prezentować co najmniej następujące metryki:

- liczbę aktywnych, unikalnych źródeł wycieków,
- liczbę aktywnych wycieków zawierających hasła jawne,
- liczbę aktywnych wycieków zawierających hasła zahaszowane,
- liczbę aktywnych, unikalnych adresów e-mail,
- liczbę aktywnych kont administracyjnych,
- liczbę aktywnych, unikalnych haseł.

Dodatkowo rozwiązanie musi umożliwiać:

- filtrowanie danych dotyczących użytkowników oraz rekordów wycieków,
- prezentację statusu wycieku,
- podgląd szczegółów wycieku,
- podejmowanie działań reagowania.

**Integracja**

Rozwiązanie musi zapewniać:

- integrację z dostawcą tożsamości w chmurze z wykorzystaniem powszechnie stosowanych protokołów uwierzytelniania i autoryzacji;
- zarządzanie:

  - tożsamościami,
  - grupami,
  - dostępem opartym o role (RBAC),
  - dostępem uprzywilejowanym,
  - politykami dostępu warunkowego;
- jeden, zunifikowany interfejs administracyjny służący do wykrywania oraz neutralizacji zagrożeń tożsamości;
- możliwość rozszerzenia funkcjonalności IAM o:
  - ocenę higieny tożsamości,
  - ocenę stanu bezpieczeństwa,
  - monitorowanie Dark Web,
  - zaawansowane wykrywanie zagrożeń.

**Licencjonowanie**

Rozwiązanie musi zapewniać:

- model subskrypcyjny rozliczany według liczby użytkowników i serwerów:
  - **21 użytkowników**
  - **10 serwerów**
- licencję/subskrypcję na okres: **36 miesięcy**.

**Wdrożenie:**

Wykonawca przeprowadzi kompleksowe wdrożenie oprogramowania, obejmujące jego instalację, konfigurację, uruchomienie oraz dostosowanie do środowiska Zamawiającego. Wdrożenie zostanie wykonane z należytą starannością, zgodnie z aktualną wiedzą techniczną, zaleceniami producenta oraz najlepszymi praktykami branżowymi.

# 6.11. Urządzenie typu UPS

## Ilość sztuk: 2 sztuki

**Zakres: OT**

| Charakterystyka podstawowa | Parametry wymagane |
|---|---|
| **Technologia wykonania UPS** | Line-interactive |
| **Moc pozorna (VA)** | 1000 |
| **Moc rzeczywista (W)** | 1000 |
| **Kształt fali na wyjściu(praca na baterii)** | Pełna fala sinusoidalna |
| **Kompatybilność z zasilaczami z aktywnym PFC** | Wymagana |
| **Automatyczna regulacja napięcia (mechanizm AVR)** | Wymagany |
| **Podwyższanie napięcia(przy zaniżonym napięciu z sieci)** | Dwustopniowe |
| **Obniżanie napięcia(przy zawyżonym napięciu z sieci)** | Jednostopniowe |

| | |
|---|---|
| **Ochrona przed przeciążeniem** | Wymagana(minimum bezpiecznik i wewnętrzny ogranicznik prądu) |
| **Filtr EMI/RFI** | Wymagany |
| **Ochrona dla urządzeń telekomunikacyjnych** | minimum 1 port RJ45 wejście/wyjście |
| **Układ przeciwprzepięciowy (Dżule)** | Wymagany, minimum 2400 |
| **Charakterystyka wejścia/wyjścia** | |
| **Nominalne napięcie wejściowe (V)** | 220 ; 230 ; 240 |
| **Obsługiwany zakres napięcia wejściowego (V)** | 160 ~ 286 |
| **Częstotliwość wejściowa(Hz)** | 50+/-3 ; 60+/-3 |
| **Wykrywanie częstotliwości wejściowej** | Wymagane automatyczne |
| **Napięcie przy pracy na baterii (V)** | 220+/-5% ; 230+/-5% ; 240+/-5% |
| **Częstotliwość przy pracy baterii (Hz)** | 50+/-1% ; 60+/-1% |
| **Charakterystyka gniazd** | |
| **Rodzaj złącza wejściowego** | IEC C14 |
| **Całkowita ilość gniazd** | minimum 10 |
| **Rodzaj gniazd** | IEC C13 |
| **Ilość gniazd chronionych (bateria oraz przepięcie)** | minimum 10 |
| **Rozróżnienie gniazd na krytyczne i nie krytyczne** | Wymagane, minimum 2 gniazda krytyczne |
| **Charakterystyka baterii** | |
| **Typowy czas przełączenia na baterie (ms)** | nie więcej niż 4 |
| **Czas pracy na baterii przy połowie obciążenia** | minimum 20 minut |
| **Typowy czas ponownego ładowania baterii (h)** | 3 |
| **Możliwość uruchomienia UPS przy pracy na baterii** | Wymagana |
| **Możliwość wymiany baterii przez użytkownika** | Wymagana |
| **Funkcja Hot-Swap** | Wymagana |
| **Zarządzanie** | |
| **Sygnalizacja** | Wymagane alarmy dźwiękowe oraz wyświetlacz LCD |

| | |
|---|---|
| **Alarmy dźwiękowe** | minimum Tryb baterii , Niski poziom baterii , Przeciążenie , Przeładowanie , Przegrzanie |
| **Konfiguracja wybranych parametrów** | Przez wyświetlacz LCD, minimum ustawienia alarmów, wejście/wyjście, ustawienia baterii |
| **Port komunikacyjny USB** | Wymagany |
| **Port wyłącznika awaryjnego EPO** | Wymagany |
| **Dołączone oprogramowanie do zarządzania** | Wymagane, obsługa platform Windows, Linux, VmWare |
| **Zarządzanie przez sieć** | Wymagana możliwość rozbudowy o zarządzanie HTTP/SNMP, np. poprzez doinstalowanie karty zarządzającej |
| **Cechy fizyczne** | |
| **Obudowa** | Wymagana możliwość instalacji w szafie RACK lub ustawienia jako Tower |
| **Konstrukcja obudowy** | Metalowa |
| **Szyny/uchwyty rack** | Wymagane |
| **Rozmiary (szer. x wys. x dł.) (mm)** | Nie większe niż 561x276x531 |
| **Waga** | maksiumum 30 kg |
| **Dane środowiskowe** | |
| **Temperatura robocza (°C)** | 0 ~ 40 |
| **Względna wilgotność robocza (bez kondensacji) (%)** | 0 ~ 95 |
| **Wysokość robocza (stopy/metry)** | 0-3000 metrów |
| **Technologia oszczędzania energii** | Wymagana |
| **Certyfikaty** | |
| **Certyfikat Energy Star** | Wymagany |
| **Pozostałe wymagane certyfikaty** | CE |
| **Gwarancja** | |
| **Na urządzenie** | minimum 2 lata |
| **Na baterie** | minimum 2 lata |

# 6.12. Serwer pod rozwiązania bezpieczeństwa

## Ilość sztuk: 1 sztuka

**Zakres: IT**

| Lp. | Nazwa parametru, elementu lub cechy | Wymagane minimalne parametry techniczne |
|---|---|---|
| | 1 | 2 |
| **Typ 1 - 1 sztuka** | | W ofercie wymagane jest podanie modelu, symbolu oraz producenta |
| **1.** | **Obudowa** | Obudowa Rack o wysokości max. 2U z możliwością zainstalowania min. 12 dysków 3.5" SAS/SATA oraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Szyny wyposażone w organizer (ramię) do kabli.<br><br>Możliwość zainstalowana karty umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| **2.** | **Płyta główna** | Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **3.** | **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych. |
| **4.** | **Procesor** | Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 199 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla jednego procesora. Dla oferowanego serwera. |
| **5.** | **RAM** | Min. 64GB DDR5 RDIMM 6400MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 4TB pamięci RAM. |
| **6.** | **Zabezpieczenia pamięci RAM** | Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection |
| **7.** | **Gniazda PCIe** | Min. trzy sloty PCIe x16 generacji 5 |
| **8.** | **Interfejsy sieciowe/FC/SAS** | Karta czteroportowa 1GbE Base-T, nie zajmująca slotów PCIe. |
| **9.** | **Kontroler dysków** | Zainstalowany sprzętowy kontroler dysków umożliwiający obsługę poziomów RAID: 0/1/10. |
| **10.** | **Dyski twarde** | Zainstalowane dwa dyski hot-plug SSD SATA 6Gbps o pojemności min. 960GB w RAID 1. |
| **11.** | **Wbudowane porty** | min. port USB 2.0 oraz 2 x USB 3.1, port VGA. |
| **12.** | **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **13.** | **Wentylatory** | Redundantne |
| **14.** | **Zasilacze** | Min. dwa zasilacze Hot-Plug min. 800W klasy Titanium. |

| | | |
|---|---|---|
| **15.** | **System operacyjny/dodatkowe licencje** | • Windows Server 2025 Standard<br>• 25 Windows Server 2025/2022 User CALs<br><br>Dostarczona licencja musi zapewnić pełne pokrycie rdzeni procesora oferowanego serwera. Dostarczona licencja musi umożliwiać uruchomienie na serwerze fizycznym min. 2 maszyn wirtualnych z Windows Server 2025 Standard. |
| **16.** | **Bezpieczeństwo** | Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.<br><br>Możliwość wyłączenia w BIOS funkcji przycisku zasilania.<br><br>BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła<br><br>Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą<br><br>Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.<br><br>Możliwość integracji z RSA SecurID<br><br>Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. |
| **17.** | **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:<br><br>• zdalny dostęp do graficznego interfejsu Web karty zarządzającej<br>• szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika<br>• możliwość podmontowania zdalnych wirtualnych napędów<br>• wirtualną konsolę z dostępem do myszy, klawiatury<br>• wsparcie dla IPv6<br>• wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH<br>• możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.<br>• możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer<br>• integracja z Active Directory<br>• możliwość obsługi przez ośmiu administratorów jednocześnie<br>• Wsparcie dla automatycznej rejestracji DNS<br>• wsparcie dla LLDP<br>• wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej<br>• możliwość podłączenia lokalnego za pomocą interfejsu USB-C na froncie serwera, który pozwala na bezpośredni dostęp interfejsu karty zarządzającej (zarówno UI w przeglądarce, jak i konsolę RACADM czy API Redfish) bez potrzeby połączenia sieciowego<br>• Monitorowanie zużycia dysków SSD<br>• Automatyczne zgłaszanie alertów do centrum serwisowego producenta<br>• Automatyczne update firmware dla wszystkich komponentów serwera |

| | | |
|---|---|---|
| | | • Możliwość przywrócenia poprzednich wersji firmware<br>• Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON<br>• Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych<br>• Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.<br>• Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera<br>• Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów.<br>• komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.<br>• kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania<br>• Automatyczne odświeżanie certyfikatów SSL<br>• możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej<br>• możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień<br>• możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera<br>• możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer<br>• możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych serwerów<br>• Musi oferować wbudowany dziennik cyklu życia sprzętu, który rejestruje szczegółowe zdarzenia dotyczące konfiguracji, integracji fizycznych i operacji serwera, powiązane bezpośrednio z tożsamością użytkownika inicjującego zmiany, umożliwiając pełną audytowalność od momentu produkcji do użytkowania.<br><br>Do oferty należy dołączyć oświadczenie producenta serwera potwierdzające spełnienie powyższych wymagań. |
| **18.** | **Oprogramowanie do zarządzania** | Zainstalowane oprogramowanie producenta serwera do zarządzania, spełniające poniższe wymagania:<br><br>• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych<br>• integracja z Active Directory<br>• Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta<br>• Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish<br>• Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram |

| | | |
|---|---|---|
| | | • Szczegółowy opis wykrytych systemów oraz ich komponentów<br>• Możliwość eksportu raportu do CSV, HTML, XLS, PDF<br>• Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.<br>• Grupowanie urządzeń w oparciu o kryteria użytkownika<br>• Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji<br>• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach<br>• Szybki podgląd stanu środowiska<br>• Podsumowanie stanu dla każdego urządzenia<br>• Szczegółowy status urządzenia/elementu/komponentu<br>• Generowanie alertów przy zmianie stanu urządzenia.<br>• Filtry raportów umożliwiające podgląd najważniejszych zdarzeń<br>• Integracja z service desk producenta dostarczonej platformy sprzętowej<br>• Możliwość przejęcia zdalnego pulpitu<br>• Możliwość podmontowania wirtualnego napędu<br>• Kreator umożliwiający dostosowanie akcji dla wybranych alertów<br>• Możliwość importu plików MIB<br>• Przesyłanie alertów „as-is” do innych konsol firm trzecich<br>• Możliwość definiowania ról administratorów<br>• Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów<br>• Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)<br>• Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta<br>• Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów<br>• Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.<br>• Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.<br>• Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile<br>• Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.<br>• Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.<br>• Zdalne uruchamianie diagnostyki serwera.<br>• Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.<br><br>Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| **19.** | **Normy Środowiskowe** | Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami rozporządzenia nr |

| | | |
|---|---|---|
| | | 1272/2008WE. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - ***Wykonawca złoży dokument potwierdzający spełnianie*** **wymogu.**<br><br>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych **w postaci oświadczenia producenta serwera.** |
| **20.** | **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.<br>Serwer musi posiadać deklaracja CE.<br>Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej.<br><br>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2022, Microsoft Windows 2025. |
| **21.** | **Warunki gwarancji** | Zamawiający wymaga min. 36 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w dni robocze, od 8-16, następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.<br><br>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.<br><br>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.<br><br>Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. |
| **22.** | **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim.<br>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

# 6.13. Sprzęt Sieciowy

**Zakres: IT/OT**

## 6.13.1. Przełącznik dostępowy typ 1

**Ilość sztuk: 4 sztuki – <u>sprzęt, który zapewni Zamawiający, wyłączony z zakresu dostaw Wykonawcy</u>**

**Wymagania ogólne**

- Urządzenie musi być dedykowanym przełącznikiem sieciowym klasy Enterprise.
- W zależności od wariantu musi umożliwiać montaż w szafie Rack 19” lub poza szafą Rack.
- Urządzenie musi być fabrycznie nowe, nieużywane oraz pochodzić z autoryzowanego kanału dystrybucji na rynek UE.

**Parametry sprzętowe**

- Jeden wewnętrzny zasilacz 230 V AC.
- Wbudowany port USB umożliwiający podłączenie pamięci Flash.
- Pamięć RAM minimum 1 GB.
- Pamięć Flash minimum 1 GB.
- Obsługa minimum 16 000 adresów MAC.
- Obsługa ramek Jumbo o wielkości minimum 9216 bajtów.

**Interfejsy**

- Wariant 10-portowy: minimum 8 portów 1GbE RJ45, 2 porty uplink RJ45 oraz 2 porty SFP.
- Wszystkie porty dostępne od frontu urządzenia.

**Funkcje sieciowe**

- Obsługa VLAN IEEE 802.1Q oraz QinQ.
- Obsługa LLDP i LLDP-MED.
- Obsługa DHCP Server.
- Obsługa IGMP Snooping v1/v2/v3.
- Obsługa minimum 1000 grup multicast.
- Obsługa statycznego routingu IPv4 i IPv6.
- Obsługa MSTP oraz RSTP.
- Obsługa GVRP lub rozwiązania równoważnego.

**Stackowanie**

- Tworzenie stosu minimum 4 urządzeń.
- Zarządzanie stosem pod jednym adresem IP.
- Obsługa Link Aggregation pomiędzy członkami stosu.
- Stos widoczny jako jedno urządzenie logiczne.
- Obsługa ISSU umożliwiająca aktualizację bez przerywania pracy.

**Bezpieczeństwo**

- IEEE 802.1X z dynamicznym przydziałem VLAN i ACL.
- Uwierzytelnianie MAC oraz Captive Portal.
- Zarządzanie poprzez HTTPS, SSHv2 oraz SNMP.
- Obsługa DHCP Snooping, ARP Protection/Dynamic ARP Inspection, IP Source Guard, Port Security, Voice VLAN.
- Filtrowanie ruchu na podstawie MAC, IPv4, IPv6 oraz TCP/UDP.

**Zarządzanie**

- Możliwość lokalnego i zdalnego port mirroring.
- Edycja konfiguracji offline.
- Dedykowany port konsoli RS-232.
- Obsługa skryptów Bash oraz Python.
- Pełna obsługa REST API.

**Dokumentacja i gwarancja**

- Dokumentacja w języku polskim lub angielskim.
- Deklaracja zgodności CE.
- Gwarancja producenta typu Limited Lifetime.
- Rozszerzone wsparcie minimum 3 lata z wymianą sprzętu w trybie 9x5 oraz dostępem do aktualizacji oprogramowania.

### 6.13.2. Przełącznik dostępowy typ 2

## Ilość sztuk: 3 sztuki – <u>sprzęt, który zapewni Zamawiający, wyłączony z zakresu dostaw Wykonawcy</u>

**Wymagania ogólne**

- Urządzenie musi być dedykowanym przełącznikiem sieciowym klasy Enterprise.
- Urządzenie musi być przystosowane do montażu w szafie Rack 19”.
- Wraz z urządzeniem należy dostarczyć niezbędne akcesoria montażowe.
- Urządzenie musi być fabrycznie nowe, nieużywane oraz pochodzić z autoryzowanego kanału dystrybucji na rynek UE.

**Parametry sprzętowe**

- Jeden wewnętrzny zasilacz 230 V AC.
- Wbudowany port USB umożliwiający podłączenie pamięci Flash.
- Konstrukcja bezwiatrakowa, chłodzenie pasywne.
- Pamięć RAM minimum 1 GB.
- Pamięć Flash minimum 1 GB.
- Obsługa minimum 16 000 adresów MAC.
- Obsługa ramek Jumbo o wielkości minimum 9216 bajtów.
- Matryca przełączająca o wydajności minimum 92 Gbps.

**Interfejsy**

- Minimum 24 porty gigabitowe w standardzie 100/1000Base-T.
- Minimum 2 porty typu COMBO 1Gb SFP/RJ45.
- Minimum 2 porty typu SFP+ 1G/10G do wykorzystania jako porty uplink lub stacking.
- Wszystkie porty muszą być dostępne od frontu urządzenia.

**Funkcje sieciowe**

- Obsługa VLAN IEEE 802.1Q oraz QinQ.
- Obsługa minimum 4000 sieci VLAN jednocześnie.
- Obsługa LLDP i LLDP-MED.
- Obsługa DHCP Server.
- Obsługa IGMP Snooping v1/v2/v3.
- Obsługa minimum 1000 grup multicast.
- Obsługa statycznego routingu IPv4 i IPv6.
- Obsługa minimum 64 tras dla routingu IPv4.
- Obsługa minimum 32 tras dla routingu IPv6.
- Obsługa MSTP oraz RSTP.
- Obsługa minimum 64 instancji MSTP lub osobnej instancji STP dla każdego VLAN.
- Obsługa GVRP lub rozwiązania równoważnego.

**Stackowanie**

- Tworzenie stosu minimum 4 urządzeń.
- Zarządzanie stosem pod jednym adresem IP.
- Magistrala stackująca o wydajności minimum 40 Gb/s.
- Obsługa Link Aggregation zgodnie z IEEE 802.3ad dla portów należących do różnych jednostek w stosie.
- Stos widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning Tree.
- Obsługa ISSU umożliwiająca aktualizację przełączników w stosie bez przerywania pracy całego stosu.
- Jeżeli realizacja funkcji stackowania wymaga dodatkowych interfejsów lub modułów, muszą zostać dostarczone w ramach zamówienia.

**Bezpieczeństwo**

- Minimum 4 poziomy dostępu administracyjnego poprzez konsolę.
- IEEE 802.1X z możliwością dynamicznego przydziału VLAN oraz dynamicznego przypisania list ACL.
- Uwierzytelnianie urządzeń na porcie w oparciu o adres MAC.
- Uwierzytelnianie użytkowników poprzez wbudowany Captive Portal.
- Zarządzanie poprzez HTTPS, SSHv2 oraz SNMP z wykorzystaniem IPv4 i IPv6.
- Obsługa DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, Port Security, Voice VLAN oraz Private VLAN lub rozwiązania równoważnego.
- Filtrowanie ruchu na podstawie adresów MAC, IPv4, IPv6 oraz portów TCP/UDP.

**Zarządzanie**

- Możliwość lokalnego i zdalnego port mirroring.
- Możliwość przesyłania kopiowanego ruchu do urządzenia monitorującego przez określony VLAN.
- Edycja pliku konfiguracyjnego offline w postaci tekstowej.
- Wbudowany port USB do przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów.
- Dedykowany port konsoli zgodny ze standardem RS-232.
- Obsługa skryptów Bash oraz Python.
- Pełna obsługa REST API dla funkcji przełącznika.

**Dokumentacja i gwarancja**

- Dokumentacja w języku polskim lub angielskim.
- Dokumenty potwierdzające zgodność z wymaganymi normami bezpieczeństwa, w tym CE, lub oświadczenie, że deklaracja nie jest wymagana.
- Gwarancja producenta typu Limited Lifetime, zapewniająca wymianę urządzenia w okresie do 5 lat od zakończenia sprzedaży danego modelu.
- Rozszerzone wsparcie minimum 3 lata dla sprzętu i oprogramowania.
- Wymiana uszkodzonego elementu w trybie 9x5 wraz ze wsparciem technicznym i dostępem do najnowszych wersji oprogramowania.

### 6.13.3. Przełącznik dostępowy typ 3

**Ilość sztuk: 3 sztuki – <u>sprzęt, który zapewni Zamawiający, wyłączony z zakresu dostaw Wykonawcy</u>**

**Wymagania ogólne**

- Urządzenie musi być dedykowanym przełącznikiem sieciowym klasy Enterprise.
- Urządzenie musi być przystosowane do montażu w szafie Rack 19”.
- Wraz z urządzeniem należy dostarczyć niezbędne akcesoria montażowe.
- Urządzenie musi być fabrycznie nowe, nieużywane oraz pochodzić z autoryzowanego kanału dystrybucji na rynek UE.

**Parametry sprzętowe**

- Jeden wewnętrzny zasilacz 230 V AC.
- Wbudowany port USB umożliwiający podłączenie pamięci Flash.
- Konstrukcja bezwiatrakowa, chłodzenie pasywne.
- Pamięć RAM minimum 1 GB.
- Pamięć Flash minimum 1 GB.
- Obsługa minimum 16 000 adresów MAC.
- Obsługa ramek Jumbo o wielkości minimum 9216 bajtów.
- Matryca przełączająca o wydajności minimum 92 Gbps.

**Interfejsy**

- Minimum 24 porty gigabitowe w standardzie 100/1000Base-T.
- Minimum 2 porty typu COMBO 1Gb SFP/RJ45.
- Minimum 2 porty typu SFP+ 1G/10G do wykorzystania jako porty uplink lub stacking.
- Wszystkie porty muszą być dostępne od frontu urządzenia.

**Funkcje sieciowe**

- Obsługa VLAN IEEE 802.1Q oraz QinQ.
- Obsługa minimum 4000 sieci VLAN jednocześnie.
- Obsługa LLDP i LLDP-MED.
- Obsługa DHCP Server.
- Obsługa IGMP Snooping v1, v2 i v3.
- Obsługa minimum 1000 grup multicast.
- Obsługa statycznego routingu IPv4.
- Obsługa statycznego routingu IPv6.
- Obsługa minimum 64 tras dla routingu IPv4.
- Obsługa minimum 32 tras dla routingu IPv6.
- Obsługa protokołów RSTP oraz MSTP.
- Obsługa minimum 64 instancji MSTP lub osobnej instancji STP dla każdego VLAN.
- Obsługa GVRP lub rozwiązania równoważnego.

**Stackowanie**

- Możliwość tworzenia stosu obejmującego minimum 4 urządzenia.
- Zarządzanie stosem z wykorzystaniem jednego adresu IP.
- Magistrala stackująca o wydajności minimum 40 Gb/s.
- Obsługa Link Aggregation zgodnie z IEEE 802.3ad pomiędzy urządzeniami należącymi do stosu.
- Stos przełączników musi być widoczny jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning Tree.
- Obsługa funkcji ISSU umożliwiającej aktualizację oprogramowania przełączników w stosie bez przerywania pracy całego stosu.
- Jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów lub interfejsów, muszą one zostać dostarczone w ramach zamówienia.

**Bezpieczeństwo**

- Minimum cztery poziomy dostępu administracyjnego.
- Obsługa uwierzytelniania IEEE 802.1X z możliwością dynamicznego przydziału VLAN oraz list ACL.
- Możliwość uwierzytelniania urządzeń na podstawie adresu MAC.
- Możliwość uwierzytelniania użytkowników z wykorzystaniem wbudowanego Captive Portal.
- Zarządzanie poprzez HTTPS, SNMP oraz SSHv2 z wykorzystaniem IPv4 i IPv6.
- Obsługa mechanizmów DHCP Snooping.
- Obsługa mechanizmu Dynamic ARP Inspection.
- Obsługa mechanizmu IP Source Guard.
- Obsługa Port Security.
- Obsługa Voice VLAN.

- Obsługa Private VLAN lub rozwiązania równoważnego.
- Filtrowanie ruchu na podstawie adresów MAC, IPv4, IPv6 oraz portów TCP/UDP.

**Zarządzanie**

- Możliwość lokalnego i zdalnego port mirroring.
- Możliwość przesyłania kopiowanego ruchu do urządzenia monitorującego poprzez dedykowany VLAN.
- Możliwość edycji pliku konfiguracyjnego w trybie offline.
- Wbudowany port USB umożliwiający przechowywanie obrazów systemu, plików konfiguracyjnych oraz certyfikatów.
- Dedykowany port konsoli zgodny ze standardem RS-232.
- Obsługa skryptów Bash.
- Obsługa skryptów Python.
- Pełna obsługa REST API umożliwiająca zarządzanie wszystkimi funkcjami przełącznika.

**Dokumentacja i gwarancja**

- Dokumentacja techniczna w języku polskim lub angielskim.
- Dokumenty potwierdzające zgodność z wymaganymi normami bezpieczeństwa, w tym CE, lub równoważne.
- Gwarancja producenta typu Limited Lifetime.
- Rozszerzone wsparcie serwisowe minimum 3 lata.
- Wymiana uszkodzonego urządzenia w trybie 9x5 wraz ze wsparciem technicznym.
- Dostęp do aktualizacji oprogramowania przez cały okres wsparcia.

### 6.13.4. Punkt dostępowy

**Ilość sztuk: 6 sztuk – <u>sprzęt, który zapewni Zamawiający, wyłączony z zakresu dostaw Wykonawcy</u>**

**Wymagania ogólne**

- Urządzenie musi być przeznaczone do montażu wewnątrz budynków.
- Urządzenie musi posiadać dwa niezależne moduły radiowe pracujące jednocześnie w pasmach 2,4 GHz oraz 5 GHz.
- Urządzenie musi umożliwiać zdalne zarządzanie.
- Urządzenie musi współpracować z centralnym kontrolerem sieci bezprzewodowej.
- Urządzenie musi umożliwiać pracę autonomiczną bez wykorzystania kontrolera.
- Zmiana trybu pracy pomiędzy trybem autonomicznym a zarządzanym centralnie musi odbywać się z poziomu interfejsu graficznego, bez konieczności instalowania nowego oprogramowania.
- Urządzenie musi umożliwiać tworzenie klastra obejmującego minimum 255 punktów dostępowych.

**Parametry radiowe**

- Obsługa standardów IEEE 802.11a/b/g/n/ac/ax.
- Obsługa technologii OFDM oraz OFDMA.
- Obsługa modulacji BPSK, QPSK, CCK, 16-QAM, 64-QAM, 256-QAM oraz 1024-QAM.
- Obsługa kanałów 20 MHz, 40 MHz oraz 80 MHz.

- Obsługa technologii DFS dla pasma 5 GHz.
- Obsługa agregacji ramek A-MPDU oraz A-MSDU.
- Obsługa technologii STBC.
- Obsługa technologii LDPC.
- Obsługa technologii Tx Beamforming.
- Możliwość konfiguracji mocy nadawczej dla każdego modułu radiowego.
- Wbudowane anteny pracujące w konfiguracji minimum 2×2:2 dla pasma 2,4 GHz oraz 5 GHz o zysku nie mniejszym niż 3 dBi.

**Interfejsy**

- Minimum dwa porty Ethernet 10/100/1000Base-T.
- Obsługa zasilania PoE zgodnie ze standardem IEEE 802.3af.
- Możliwość zasilania z dedykowanego zasilacza.
- Port USB.
- Przycisk przywracania ustawień fabrycznych.
- Diody LED umożliwiające sygnalizację stanu urządzenia oraz lokalizację punktu dostępowego.

**Funkcje sieci bezprzewodowej**

- Automatyczne zarządzanie kanałami radiowymi.
- Automatyczna regulacja mocy nadawczej.
- Monitorowanie środowiska radiowego.
- Automatyczne równoważenie obciążenia pomiędzy punktami dostępowymi.
- Automatyczne kierowanie klientów do pasma 5 GHz.
- Wykrywanie zakłóceń radiowych.
- Wykrywanie obszarów bez pokrycia sygnałem.
- Możliwość rozłączania klientów niespełniających zdefiniowanych parametrów jakości sygnału.
- Możliwość automatycznego przenoszenia klientów pomiędzy punktami dostępowymi w celu zapewnienia optymalnych parametrów transmisji.
- Obsługa minimum 16 identyfikatorów SSID na urządzenie.
- Możliwość definiowania parametrów radiowych niezależnie dla każdego SSID.
- Możliwość definiowania harmonogramów emisji poszczególnych sieci SSID.
- Obsługa roamingu zgodnego ze standardami IEEE 802.11r, 802.11k oraz 802.11v.

**Zarządzanie**

- Zarządzanie poprzez interfejs WWW z wykorzystaniem protokołu HTTPS.
- Możliwość pełnej konfiguracji urządzenia z poziomu przeglądarki internetowej.
- Możliwość centralnego zarządzania przez kontroler WLAN.
- Możliwość pracy jako urządzenie autonomiczne.
- Możliwość konfiguracji klastra urządzeń.
- Możliwość lokalizacji urządzenia z wykorzystaniem diod LED.

**Bezpieczeństwo**

- Obsługa bezpiecznego zarządzania poprzez HTTPS.
- Możliwość integracji z centralnym systemem zarządzania politykami bezpieczeństwa.
- Obsługa mechanizmów zapewniających bezpieczny roaming użytkowników.
- Możliwość konfiguracji odrębnych parametrów bezpieczeństwa dla każdej sieci SSID.

**Warunki środowiskowe**

- Temperatura pracy od 0°C do +45°C.
- Wilgotność pracy od 5% do 95% bez kondensacji.
- Zgodność z wymaganiami CE.
- Zgodność z normami EN 60601-1-1 oraz EN 60601-1-2.

**Wyposażenie**

- Urządzenie musi zostać dostarczone z kompletem elementów montażowych umożliwiających instalację na ścianie lub suficie.

**Dokumentacja i gwarancja**

- Dokumentacja techniczna w języku polskim lub angielskim.
- Gwarancja producenta minimum 2 lata.
- Rozszerzone wsparcie serwisowe obejmujące wymianę uszkodzonego urządzenia w trybie 9x5 Next Business Day.
- Dostęp do aktualizacji oprogramowania przez cały okres obowiązywania wsparcia serwisowego.

## 6.13.5. System do zarządzania siecią

**System do zarządzania siecią (NMS - Network Management System)**

1. System musi zapewnić możliwość zarządzania siecią przewodową (LAN) i bezprzewodową (WLAN).
2. System musi pochodzić od tego samego producenta co urządzania LAN i WLAN.
3. System musi zapewnić możliwość zarządzania urządzeniami sieciowymi (LAN i WLAN) w ilościach ujętych w ramach postępowania oraz możliwość dalszej rozbudowy za pomocą licencji typu pojemnościowego. Minimalna pojemność systemu nie może być mniejsza niż:
    a. 50 przełączników sieciowych
    b. 150 punktów dostępowych
4. System musi być dostępny w formie maszyny wirtualnej możliwej do uruchomienia na platformach VMWare ESXi, Microsoft Hyper-V i Linux-KVM
5. System powinien mieć możliwość rozszerzenia funkcjonalności za pomocą opcjonalnej licencji, tak aby był w stanie wspierać mechanizmy wysokiej dostępności (praca w trybie High Availability)
6. System musi posiadać zintegrowany moduł kontroli dostępu (Network Access Control) z różnymi możliwościami uwierzytelniania, takimi jak 802.1x, MAC i uwierzytelnianie oparte na certyfikatach.
7. System powinien posiadać wbudowany serwer RADIUS i funkcje Captive Portal
8. System musi obsługiwać zewnętrzne serwery RADIUS i LDAP z możliwością przypisywania ról oraz możliwość integracji z usługami Active Directory.
9. System musi obsługiwać ujednoliconą konfigurację zasad bezpieczeństwa dla uwierzytelniania urządzeń i użytkowników.
10. System powinien posiadać wbudowaną lokalną bazę danych zapewniającą obsługę dla urządzeń firmowych / należących do organizacji, kont użytkowników dla pracowników oraz gości.

11. Obsługa system musi być możliwa poprzez interfejs graficzny z wykorzystaniem przeglądarki WWW oraz skalowanie interfejsu umożliwiające wykorzystanie przeglądarek w urządzeniach mobilnych.
12. System musi zapewnić ujednolicony widok topologii sieci zarówno dla punktów dostępowych jak i przełączników, widok sąsiednich elementów sieci oraz ich połączeń i trybu w jakim obecnie pracują.
13. System musi wspierać geolokalizację zapewniając odwzorowanie topologii sieci bazując na koordynatach GPS lub podanym adresie fizycznym.
14. System musi zapewnić lokalizowanie użytkowników w infrastrukturze sieciowej tj. miejsce podłączenia switch/port oraz informacje nt. usługi L2 tj.: VLAN, usługa SPB, VxLAN, GRE Tunel. Weryfikowanie lokalizacji po adresie, nazwie sieciowej użytkownika, IP oraz MAC.
15. System powinien umożliwiać konfigurację przełączników sieciowych za pomocą predefiniowanych w systemie szablonów konfiguracji.
16. System musi posiadać narzędzia do automatycznego wykrywania urządzeń sieciowych instalowanych w sieci wraz z ich automatyczna konfiguracją tj. autoprovisioning. Nie dopuszcza się systemów NMS które wymagają fizycznego dostępu administratorów do przekazania przełącznikowi konfiguracji inicjalnej.
17. System musi posiadać możliwość granularnego definiowania poziomu dostępu dla administratorów, w tym możliwość tworzenia własnych ról z elastycznym wyborem uprawnień dla odczytu i/lub zapisu dla poszczególnych elementów systemu zarządzania oraz możliwość uwierzytelniania administratorów w oparciu o zewnętrzną bazę.
18. System musi obsługiwać uwierzytelnianie dwuskładnikowe dla dostępu administratora.
19. System musi zapewnić monitorowanie wydajności sieci i wskaźników KPI w czasie rzeczywistym za pomocą konfigurowalnego pulpitu z wizualnymi widżetami.
20. System powinien zapewniać możliwość tworzenia kopii zapasowych i przywracania konfiguracji urządzeń sieciowych.
21. System powinien obsługiwać zautomatyzowaną aktualizację oprogramowania sprzętowego urządzeń sieciowych w całej sieci.
22. Obsługa monitoringu przez SNMP v2/v3
23. System musi zapewnić wsparcie dla konfiguracji:
    a. sFlow
    b. protokołu mDNS
    c. multicast (m.in. PIM) w całej sieci
    d. interfejsów VLAN w sieci przewodowej i bezprzewodowej
    e. polityk QoS
    f. pakietów SIP
    g. VXLAN
24. System umożliwia konfigurację urządzeń poprzez terminal CLI bezpośrednio ze strony internetowej systemu zarządzania
25. System musi zapewniać wsparcie dla REST API, umożliwiające integrację z urządzeniami innych producentów.
26. System musi zapewnić obsługę priorytetyzacji ruchu dla dostępu gościnnego.
27. System musi zapewnić możliwość uwierzytelniania użytkowników typu BYOD oraz typu gość w ilości min. 10 dla każdego typu, za pomocą wbudowanego captive portal, bez konieczności stosowania jakichkolwiek dodatkowych urządzeń/oprogramowania.

28. System musi zapewniać obsługę dostępu gościnnego poprzez
    a. Samodzielną rejestrację klientów w oparciu o adres email, numer telefonu (wiadomość SMS)
    b. Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)
    c. Logowanie w oparciu o konta w mediach społecznościowych (min. Facebook, Google).
29. Zamawiający wymaga, aby system zarządzania posiadał minimum 3-letni serwis tj. dostęp do najnowszych wersji oprogramowania, obsługę zgłoszeń serwisowych, pomoc w konfiguracji oraz analizie błędów.

# 6.14. System kopii zapasowych

**Zakres: IT/OT**

| Lp. | Nazwa parametru, elementu lub cechy | Wymagane parametry techniczne |
|---|---|---|
| | **1** | **2** |
| **TYP** | | **W ofercie wymagane jest podanie nazwy oprogramowania.** |
| **1.** | **Licencja** | • W ramach dostawy należy dostarczyć taką ilość licencji, aby umożliwiały ochronę min. 20 maszyn wirtualnych.<br>• W ramach dostarczonych licencji musi być możliwość ochrony zarówno maszyn wirtualnych, jak i maszyn fizycznych oraz stacji roboczych.<br>• Dostarczone licencje mają upoważniać do użytkowania dostarczonego oprogramowania na czas nieokreślony.<br>• W ramach dostarczonej licencji ma być zapewnione/wykupione min. 3-letnie wsparcie producenta upoważniające do m.in.:<br>  ○ aktualizacji oprogramowania do najnowszych wersji bez uiszczania dodatkowych opłat,<br>  ○ zgłaszania problemów z oprogramowaniem. |
| **Zamawiający wymaga spełnienia przez oprogramowanie minimalnych wymagań w zakresie funkcjonalności określonych poniżej:** | | |
| **2.** | **Wymagania ogólne** | • Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner Peer Insights: i spełniać minimalne wymaganie : - minimalna liczba referencji 500, - minimalna ocena z referencji 4,6.<br>• Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x, 8.x i 9.0 oraz Microsoft Hyper-V 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne dla powyższych platform wirtualizacyjnych, chyba, że wyszczególniono inaczej<br>• Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.8.x - 7.3, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.5 lub nowszy, Proxmox VE 8.2, 8.3, 8.4 lub 9.0 oraz Scale Computing HyperCore 9.4.32.218226 – 9.5.x.<br>• Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data |

| | | |
|---|---|---|
| | | Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |
| **3.** | **W zakresie funkcjonalności** | • System backupowy musi mieć możliwość wdrożenia wszystkich komponentów (np. serwer backupowy, serwer pośredniczący, repozytorium) na platformach Windows oraz Linux<br>• System backupowy musi mieć mieć możliwość wdrożenia w oparciu o tzw. appliance zgodny z wytycznymi bezpieczeństwa DISA (Defense Information Systems Agency)<br>• Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej<br>• Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków<br>• Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.<br>• Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć wiele wirtualnych puli pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej 20 pamięci masowych w pojedyńczej puli.<br>• Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta.<br>• Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage, IBM Cloud Storage, 11:11 Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.<br>• Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.<br>• Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania do backupu oraz odtwarzania obrazu maszyny wirtualnej<br>• Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)<br>• Oprogramowanie musi umożliwiać tworzenie logicznie odseparowanych środowisk dla różnych organizacji/działów. Dodatkowo system musi wspierać kontrolę dostępu w oparciu o role (RBAC) - predefiniowane lub własne<br>• Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API<br>• Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji<br>• Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji |

| | | |
|---|---|---|
| | | • Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania<br>• Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej<br>• Oprogramowanie musi umożliwiać integracje z różnymi dostarczycielami tożsamości (IdP - Identity Providers) z wykorzystaniem protokołu SAML (np. Entra ID, Okta)<br>• Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora, reset zablokowanego konta)<br>• Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)<br>• Oprogramowanie musi posiadać integracje z systemami typu SIEM<br>• Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej oraz analizy istniejącej instalacji systemu backupowego. Powinna istnieć możliwość wyłączenia tej opcji.<br>• Oprogramowanie musi pozwalać na wydawanie komend głosowych asystentowi AI |
| **4.** | **W zakresie RPO** | • Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.<br>• Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna co najmniej dla platformy VMware i Hyper-V<br>• Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.<br>• Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.<br>• Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).<br>• Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)<br>• Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.<br>• Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 - 2025 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.<br>• Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.<br>• Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. |

| | | |
|---|---|---|
| | | Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.<br>• Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere lub dowolnego systemu operacyjnego Windows Server 2016-2025 (z innych platfrom - fizycznych, wirtualnych, chmurowych). Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.<br>• Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik<br>• Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) |
| **5.** | **W zakresie RTO** | • Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.<br>• Dodatkowo dla środowiska vSphere, Hyper-V, Nutanix AHV i MS Azure powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)<br>• Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w platformę. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami<br>• Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny, zarówno fizycznej jak i wirtualnej<br>• Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.<br>• Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków<br>• Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.<br>• Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików<br>• Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.<br>• Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell |

| | | |
|---|---|---|
| | | • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM<br>• Oprogramowanie musi wspierać bezagentowy backup, spójny aplikacyjnie (tzw. Application Consistent) dla maszyn wirtualnych z platfrom vSphere, Hyper-V, Nutanix AHV, Proxmox.<br>• Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej (Minimum dla Active Directory, MS Exchange, MS SQL, MS Sharepoint, Oracle i PostgreSQL).<br>• Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects oraz pozwalać na odtworzenie haseł.<br>• Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications, Conditional Access Policies, Intune Policies oraz logi audytowe i sign-in.<br>• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.<br>• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.<br>• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.<br>• Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.<br>• Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.<br>• Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.<br>• Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji<br>• Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN<br>• Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle<br>• Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI<br>• Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2<br>• Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |

| | | |
|---|---|---|
| **6.** | **W zakresie ograniczenia ryzyka** | • Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)<br>• Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych<br>• Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem<br>• Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.<br>• Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backpowych<br>• Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware<br>• Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania<br>• Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków<br>• Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise<br>• Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.<br>• Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR/XSIAM, CrowdStrike Falcon LogScale, Microsoft Sentinel. |
| **7.** | **Środowiska Fizyczne** | • Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego<br>• Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych<br>• Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Rocky Linux, AlmaLinux<br>• Rozwiązanie musi wspierać system operacyjny macOS<br>• Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix<br>• Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)<br>• Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster |

| | | |
|---|---|---|
| | | • Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów<br>• Rozwiązanie musi wspierać backup podłączonych dysków USB<br>• Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym<br>• Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)<br>• Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone<br>• Rozwiązanie musi wspierać kontrolę pasma sieciowego<br>• Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych<br>• Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN<br>• Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft<br>• Rozwiązanie musi wspierać technologię BitLocker<br>• Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania<br>• Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange, Microsoft Active Directory, Microsoft Sharepoint, Microsoft SQL, Oracle, PostgreSQL oraz MongoDB<br>• Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych<br>• Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.<br>• Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform<br>• Rozwiązanie musi wspierać szyfrowanie<br>• Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne<br>• Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego<br>• Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej<br>• Rozwiązanie musi wspierać tworzenie wielu zadań backupowych. |

# 6.15. Wdrożenie serwera i sprzętu sieciowego

**Zakres: IT/OT**

Wszystkie dostarczone urządzenia zostaną podłączone i skonfigurowane zgodnie z aktualną wiedzą techniczną i zaleceniami producenta oraz przez osobę odpowiednio wykwalifikowaną. Prace wdrożeniowe będą obejmowały instalację i konfigurację urządzeń oraz oprogramowania.

Minimalny zakres:

- fizyczny montaż urządzeń w miejscu wskazanym przez Zamawiającego
- podłączenie urządzeń do istniejącej instalacji prądowej
- podłączenie nowych urządzeń do sieci LAN Zamawiającego
- instalacja i konfiguracja serwera
- instalacja i konfiguracja NAS
- instalacja i konfiguracja przełączników LAN
- konfiguracja bezprzewodowych punktów dostępowych AP i ustalonych sieci WiFi
- instalacja i konfiguracja systemu zarządzania siecią w zakresie integracji z dostarczanymi urządzeniami
- segmentacja sieci – wykreowanie na dostarczanych urządzeniach uzgodnionych podsieci VLAN, przepuszczenie ich pomiędzy przełącznikami i doprowadzenie do urządzenia pełniącego rolę bramy w danej lokalizacji, zdalne wsparcie w procesie readresacji urządzeń końcowych i zmiany przypisania portów przełączników do nowych sieci, zdalne wsparcie przy konfiguracji nowych sieci na urządzeniach pełniących rolę bramy
- konfiguracja i uruchomienie wirtualizacji na dostarczonym serwerze
- skonfigurowanie 3 maszyn wirtualnych zgodnie z wytycznymi Zamawiającego które zostaną podane na etapie wdrożenia
- instalacja i konfiguracja systemu kopii zapasowych
- konfiguracja polityk wykonywania kopii zapasowych
- wykonanie weryfikacji prawidłowego działania dostarczonych urządzeń oraz oprogramowania

**Wyłączenia dotyczące montażu:**

- bez fizycznego montażu bezprzewodowych punktów dostępowych AP

**Wyłączenia dotyczące konfiguracji:**

- bez konfiguracji/rekonfiguracji obecnych urządzeń Zamawiającego
- w kontekście segmentacji sieci - bez readresacji IP urządzeń końcowych Zamawiającego i rekonfiguracji portów końcowych na przełącznikach (obie czynności muszą być zsynchronizowane)

Dostarczenie wszelkich komponentów potrzebnych do zamontowania dostarczonych urządzeń oraz do połączenia urządzeń do infrastruktury pasywnej (np. przewody krosowe).

Wykonawca po zainstalowaniu wszystkich dostarczonych urządzeń opracuje dokumentację techniczną powykonawczą zawierającą opis montażu, instalacji i konfiguracji zainstalowanych komponentów.

# 6.16. System GRC

**Zakres: IT/OT**

System GRC w oferowanym zakresie powinien stanowić narzędzie wspierające kompleksowe zarządzanie ryzykiem, w tym ryzykiem operacyjnym, ryzykiem IT oraz ryzykiem związanym z bezpieczeństwem informacji. System powinien umożliwiać rejestrowanie ryzyk, prowadzenie procesu ich analizy i oceny, zarządzanie parametrami ryzyka, definiowanie mechanizmów kontrolnych oraz planowanie działań związanych z postępowaniem z ryzykiem.

System powinien co najmniej umożliwiać:

1. Rejestrowanie, edytowanie i przechowywanie informacji o zidentyfikowanych ryzykach.
2. Prowadzenie centralnego rejestru obejmującego wszystkie zarejestrowane w systemie ryzyka.
3. Bezpośrednie przechodzenie z rejestru ryzyk do szczegółowych informacji dotyczących wybranego ryzyka.
4. Opisywanie ryzyka za pomocą konfigurowalnego zestawu parametrów uzupełnianych na poszczególnych etapach jego obsługi.
5. Prowadzenie procesu analizy i oceny ryzyka z uwzględnieniem co najmniej prawdopodobieństwa wystąpienia, wpływu oraz wynikającego z nich poziomu istotności ryzyka.
6. Klasyfikowanie i grupowanie ryzyk według określonych kryteriów, w szczególności typu ryzyka, właściciela, procesu oraz jednostki organizacyjnej.
7. Przypisywanie ryzyka do właściciela, procesu, jednostki organizacyjnej oraz innych właściwych obiektów wykorzystywanych w procesie zarządzania ryzykiem.
8. Obsługę cyklu życia ryzyka za pomocą konfigurowalnego przepływu pracy.
9. Nadawanie użytkownikom odpowiednich uprawnień do tworzenia, przeglądania, analizowania, edytowania i procesowania rekordów ryzyka.
10. Tworzenie i prowadzenie rekordów dotyczących ryzyk, procesów, mechanizmów kontrolnych oraz działań.
11. Definiowanie mechanizmów kontrolnych stosowanych w celu ograniczenia danego ryzyka.
12. Powiązywanie ryzyka z jednym lub wieloma mechanizmami kontrolnymi.
13. Tworzenie nowych mechanizmów kontrolnych bezpośrednio w ramach obsługi ryzyka lub wybieranie ich spośród mechanizmów już istniejących w systemie.
14. Tworzenie i przypisywanie do ryzyk działań związanych z postępowaniem z ryzykiem.
15. Tworzenie nowych działań bezpośrednio w ramach obsługi ryzyka lub wybieranie ich spośród działań już istniejących w systemie.
16. Prezentowanie powiązań pomiędzy ryzykiem, procesem, mechanizmami kontrolnymi i działaniami.
17. Filtrowanie danych w rejestrze ryzyk według wybranych kryteriów.
18. Sortowanie danych prezentowanych w rejestrze ryzyk według wartości dostępnych w poszczególnych kolumnach.
19. Zawężanie zakresu prezentowanych informacji przy wykorzystaniu zestawu dostępnych filtrów.
20. Eksportowanie danych z rejestru ryzyk do powszechnie stosowanych formatów plików, w tym XLS, PDF, CSV lub RTF.
21. Prezentowanie ryzyk na macierzy ryzyka, uwzględniającej ich prawdopodobieństwo oraz wpływ.
22. Prezentowanie macierzy ryzyka w postaci liczbowej lub graficznej.

23. Filtrowanie danych prezentowanych na macierzy ryzyka, w szczególności według typu ryzyka, właściciela ryzyka, procesu lub jednostki organizacyjnej.
24. Eksportowanie macierzy ryzyka do pliku PDF.
25. Prezentowanie panelu operacyjnego zawierającego graficzne raporty i zestawienia dotyczące ryzyk.
26. Prezentowanie ryzyk w podziale co najmniej według ich typu, rankingu, sposobu odpowiedzi na ryzyko, właściciela oraz przedziału czasowego przewidywanej materializacji.
27. Monitorowanie statusu ryzyka oraz informacji dotyczących powiązanych mechanizmów kontrolnych i działań.
28. Raportowanie informacji o zarejestrowanych ryzykach, ich istotności, właścicielach, statusach oraz sposobach postępowania z ryzykiem.

**Wdrożenie:**

Wykonawca przeprowadzi kompleksowe wdrożenie oprogramowania, obejmujące jego wstępną konfigurację. Wdrożenie zostanie wykonane z należytą starannością, zgodnie z aktualną wiedzą techniczną, zaleceniami producenta oraz najlepszymi praktykami branżowymi.

Signed by / Podpisano przez:

Robert Tomasz Fennig

Date / Data: 2026-07-17 10:19