

ZAŁĄCZNIK NR 6 DO SWZ
OPIS PRZEDMIOTU ZAMÓWIENIA

Dokument wspólny dla dwóch części zamówienia

**„Podniesienie odporności cybernetycznej Zakładu Wodociągów i
Kanalizacji Sp. z o.o. w Tczewie w ramach projektu Cyberbezpieczne Wodociągi”**

Zamawiający	Zakład Wodociągów i Kanalizacji Sp. z o.o. w Tczewie, ul. Czatkowska 8, 83-110 Tczew, NIP 5930103234
Numer postępowania	ZP/032/2026
Źródło finansowania	Krajowy Plan Odbudowy i Zwiększania Odporności, Inwestycja C3.1.1 „Cyberbezpieczeństwo – CyberPL”, projekt grantowy „Cyberbezpieczne Wodociągi”
Liczba części	2

Wstęp i status OPZ

Niniejszy Opis Przedmiotu Zamówienia stanowi integralną część Specyfikacji Warunków Zamówienia. Przedmiot zamówienia opisano zgodnie z art. 99 ust. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, z uwzględnieniem wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty.

Zamówienie zostało podzielone na dwie części. Wykonawca może złożyć ofertę na jedną albo obie części – zgodnie z zasadami określonymi w SWZ. Postanowienia wspólne niniejszego OPZ stosuje się do każdej części odpowiednio do jej przedmiotu. Wymagania szczególne właściwe dla danej części uzupełniają postanowienia wspólne.

Jeżeli określone wymaganie ze względu na charakter świadczenia nie ma zastosowania do danej części, nie nakłada ono na Wykonawcę obowiązku niezwiązanego z przedmiotem tej części. W razie dostrzeżenia rozbieżności pomiędzy OPZ, pozostałymi postanowieniami SWZ albo projektowanymi postanowieniami umowy Wykonawca powinien wystąpić o wyjaśnienie dokumentów zamówienia przed upływem terminu składania ofert.

Zakres części zamówienia

Część	Zakres	Kod/y CPV
I	ZASILANIE AWARYJNE I MOBILNY AGREGAT PRĄDOTWÓRCZY	CPV główny: 31154000-0, CPV dodatkowy: 31431000-6, 31122000-7
II	SYSTEMY CYBERBEZPIECZEŃSTWA I INFRASTRUKTURA SERWEROWA	CPV główny: 48730000-4 CPV dodatkowy: 48820000-2, 48731000-1, 48620000-0, 72263000-6, 72268000-1, 72611000-6, 72253200-5

Cel i charakter zamówienia

Celem zamówienia jest podniesienie poziomu bezpieczeństwa i odporności infrastruktury informatycznej oraz środowiska IT/OT Zamawiającego, zapewnienie ciągłości działania procesów wodociągowo-kanalizacyjnych, uporządkowanie zarządzania bezpieczeństwem informacji, rozwój kompetencji personelu oraz dostarczenie rozwiązań, usług i dokumentacji wskazanych dla poszczególnych części.

W zależności od części realizacja obejmuje usługi analityczne, dokumentacyjne, audytowe i szkoleniowe, testy bezpieczeństwa, dostawy urządzeń i oprogramowania, instalację, konfigurację, uruchomienie, integrację, testy odbiorowe, przekazanie dokumentacji oraz transfer wiedzy. Obowiązek wykonania konkretnego świadczenia powstaje wyłącznie wtedy, gdy wynika z tabeli lub opisu właściwego dla danej części, SWZ albo projektowanych postanowień umowy.

Wspólne wymagania dotyczące realizacji

- **Dostawa i logistyka:** w częściach obejmujących sprzęt lub oprogramowanie Wykonawca zapewni dostawę, rozładunek, wniesienie, zabezpieczenie transportowe oraz przekazanie do lokalizacji wskazanej przez Zamawiającego.
- **Wdrożenie i integracja:** jeżeli dana część obejmuje wdrożenie, Wykonawca przeprowadzi instalację, konfigurację, uruchomienie, integrację i testy, z zachowaniem kompatybilności oraz ciągłości działania środowiska Zamawiającego.
- **Usługi i audyty:** prace zostaną wykonane zgodnie z zakresem, metodyką, produktami i kryteriami odbioru określonymi dla danej części, z wykorzystaniem podejścia opartego na ryzyku i dowodach.
- **Szkolenia i transfer wiedzy:** Wykonawca zapewni program, materiały, prowadzących, organizację zajęć, potwierdzenie udziału albo ukończenia oraz dokumentację wymaganą dla właściwej części.
- **Dokumentacja:** dokumenty zostaną przekazane w języku polskim, w formatach i liczbie egzemplarzy wskazanych dla danej części; dokumenty tworzone w ramach zamówienia należy przekazać również w formacie edytowalnym, jeżeli wynika to z charakteru dokumentu.
- **Zgodność:** Wykonawca zrealizuje zamówienie zgodnie z prawem, wymaganiami SWZ i umowy, właściwymi normami i dobrymi praktykami oraz aktualnymi instrukcjami producentów – w zakresie mającym zastosowanie do danej części.

Ciągłość działania i bezpieczeństwo prac

Infrastruktura Zamawiającego wspiera procesy realizowane w trybie ciągłym. Wykonawca zorganizuje prace tak, aby ograniczyć ryzyko przerw, utraty danych, pogorszenia bezpieczeństwa lub zakłócenia procesów technologicznych. Prace ingerujące w systemy produkcyjne, SCADA, OT/ICS, SUW, urządzenia sieciowe albo mechanizmy bezpieczeństwa mogą być wykonywane wyłącznie po uzgodnieniu terminu, zakresu, sposobu zabezpieczenia i planu wycofania zmiany z Zamawiającym.

Wykonawca zapewni adekwatne kopie bezpieczeństwa konfiguracji, procedury odtworzeniowe, kontrolę dostępu, rejestrowanie czynności i ochronę informacji uzyskanych w związku z realizacją zamówienia, jeżeli obowiązki te są związane z wykonywanym zakresem.

Bezpieczna konfiguracja i zarządzanie dostępem

W zakresie mającym zastosowanie do danej części Wykonawca zapewni bezpieczny sposób wykonywania prac w środowisku Zamawiającego, zgodny z zasadą minimalnych uprawnień i wymaganiami ochrony informacji.

- Dostęp personelu Wykonawcy do systemów, sieci, danych lub miejsc o ograniczonym dostępie może nastąpić wyłącznie po uprzednim uzgodnieniu z Zamawiającym, w zakresie i czasie

niezbędnym do wykonania prac. Wykonawca zapewni objęcie osób uzyskujących dostęp obowiązkiem poufności oraz prowadzenie wykazu tych osób i udzielonych imostępów.

- Dostęp administracyjny lub zdalny będzie realizowany z użyciem indywidualnych kont, kanałów szyfrowanych oraz uwierzytelniania wieloskładnikowego, jeżeli jest ono obsługiwane przez dane rozwiązanie, a czynności administracyjne będą rejestrowane w zakresie technicznie dostępnym.
- Na dzień odbioru oprogramowanie i urządzenia muszą posiadać stabilne, wspierane wersje oprogramowania oraz dostępne aktualizacje bezpieczeństwa, chyba że Zamawiający uprzednio zaakceptuje udokumentowane odstępstwo. Konta, hasła i ustawienia domyślne muszą zostać zmienione albo wyłączone, a konta administracyjne, klucze, certyfikaty i dane dostępowe niezbędne do eksploatacji należy bezpiecznie przekazać Zamawiającemu.
- Po zakończeniu prac Wykonawca usunie lub zwróci wszystkie przyznane mu dostępy, wyłączy konta tymczasowe i unieważni zbędne klucze lub certyfikaty oraz przekaże Zamawiającemu pisemne potwierdzenie wykonania tych czynności. Niedopuszczalne jest pozostawienie nieudokumentowanych kont, mechanizmów dostępu zdalnego lub innych ukrytych możliwości dostępu.

Zarządzanie projektem i harmonogram

Wykonawca wyznaczy osobę odpowiedzialną za koordynację realizacji i komunikację z Zamawiającym. Szczegółowy harmonogram, kamienie milowe, okna serwisowe i procedury odbiorowe zostaną uzgodnione w terminie określonym w SWZ lub umowie, a w Części II – w Dokumentacji Analizy Przedwdrożeniowej (DAP).

Terminy realizacji zamówienia dla poszczególnych części:

Część I – do 45 dni od dnia zawarcia umowy, nie później jednak niż do dnia 30.12.2026 r.;

Część II – Faza Wdrożeniowa (dostawy, wdrożenie i odbiór) – do 45 dni od dnia zawarcia umowy, nie później jednak niż do dnia 30.12.2026 r.; Usługi Ciągłe (m.in. kopie zapasowe w chmurze, MDR, SOC) – przez okresy określone w niniejszym OPZ, liczone od dnia wskazanego w Protokole Uruchomienia Usługi.

Odpowiedzialność za kompletność rozwiązania i cena

Wykonawca uwzględni wszystkie elementy, licencje, akcesoria, materiały, prace i koszty, które zostały wyraźnie wskazane w dokumentach zamówienia albo są obiektywnie niezbędne do wykonania opisanego zakresu zgodnie z jego przeznaczeniem i możliwe do ustalenia przez profesjonalnego wykonawcę na podstawie dokumentów zamówienia. Postanowienia tego nie należy interpretować jako obowiązku wykonania świadczeń nieopisanych lub niemożliwych do racjonalnego przewidzenia.

Cena oferty dla danej części, rozumiana zgodnie z art. 7 pkt 1 Pzp, obejmuje wszystkie koszty wykonania tej części, w szczególności koszty licencji, dostaw, transportu, ubezpieczenia, wniesienia, instalacji, konfiguracji,

integracji, testów, dokumentacji, szkoleń, gwarancji, serwisu i wsparcia – w zakresie wymaganym dla danej części.

Wymagania ogólne dotyczące sprzętu i oprogramowania

Poniższe wymagania stosuje się wyłącznie do części i elementów obejmujących dostawę sprzętu, urządzeń, licencji lub oprogramowania, z uwzględnieniem wymagań szczególnych zawartych w tabelach poszczególnych części.

- Sprzęt i oprogramowanie muszą pochodzić z legalnego źródła, być zgodnie z prawem wprowadzone do obrotu lub udostępnione do używania na terytorium Rzeczypospolitej Polskiej i Unii Europejskiej oraz nie mogą być obciążone prawami osób trzecich uniemożliwiającymi korzystanie zgodne z umową.
- Urządzenia muszą być fabrycznie nowe, nieużywane, kompletne i dostarczone w oryginalnych opakowaniach producenta. Niedopuszczalne są urządzenia odnawiane (refurbished), z demontażu lub ekspozycji, chyba że OPZ danej części wyraźnie stanowi inaczej.
- Na dzień dostawy oferowane urządzenia nie mogą mieć ogłoszonego przez producenta końca sprzedaży ani końca wsparcia, który uniemożliwi zapewnienie wymaganej gwarancji, serwisu, aktualizacji i utrzymania w okresach wskazanych w SWZ lub umowie.
- Licencje muszą być legalne, ważne, niewykorzystane w sposób ograniczający prawa Zamawiającego i wystawione albo skutecznie przeniesione na Zamawiającego zgodnie z modelem licencjonowania. Wykonawca przekaże dokumenty potwierdzające uprawnienia licencyjne.
- Sprzęt będzie objęty gwarancją obowiązującą na terytorium Rzeczypospolitej Polskiej, przez okres i na warunkach wskazanych w tabeli właściwej części oraz projektowanych postanowieniach umowy.
- Jeżeli dla danego urządzenia wymagano serwisu producenta, autoryzowanego serwisu albo obsługi On-Site, świadczenie musi być dostępne niezależnie od sytuacji prawnej lub ekonomicznej Wykonawcy przez cały wymagany okres.
- Korzystanie z dostarczonych produktów zgodnie z ich przeznaczeniem i umową nie może naruszać praw własności intelektualnej ani praw majątkowych osób trzecich.
- Wykonawca dostarczy komplet akcesoriów, przewodów, elementów montażowych, modułów, nośników, kluczy, kont, dokumentacji i innych składników wskazanych w OPZ lub obiektywnie niezbędnych do uruchomienia oraz eksploatacji wymaganego rozwiązania.
- Dostawy będą realizowane do lokalizacji Zamawiającego w dni robocze, w godzinach 8:00–15:00, po uprzednim uzgodnieniu terminu, chyba że SWZ lub umowa określają inne zasady dla danej części.

Rozwiązania równoważne i zasady ich oceny

Jeżeli w OPZ występuje odniesienie do znaku towarowego, patentu, pochodzenia, źródła lub szczególnego procesu charakteryzującego produkty albo usługi konkretnego wykonawcy, odniesieniu temu należy przypisać wyrazy „lub równoważny”, na zasadach określonych w art. 99 ust. 5 i 6 Pzp. Jeżeli OPZ odwołuje się do norm, ocen technicznych, specyfikacji technicznych lub systemów referencji technicznych, odniesieniu towarzyszą wyrazy „lub równoważne”, zgodnie z art. 101 ust. 4–6 Pzp.

Rozwiązanie równoważne musi w równoważnym stopniu spełniać wszystkie wymagania związane z przedmiotem danej części. Równoważność nie oznacza obowiązku identyczności technicznej, lecz osiągnięcie co najmniej takiego samego poziomu funkcjonalności, wydajności, bezpieczeństwa, interoperacyjności, trwałości i jakości jak rozwiązanie opisane wymaganiami minimalnymi.

Kryteria równoważności

- spełnienie wszystkich minimalnych parametrów technicznych i funkcjonalnych wskazanych w tabeli właściwej części;
- osiągnięcie co najmniej wymaganej wydajności, pojemności, przepustowości, dokładności, dostępności albo skuteczności;
- zgodność i interoperacyjność z elementami istniejącego środowiska Zamawiającego wskazanymi w OPZ, bez ograniczenia funkcjonalności lub bezpieczeństwa;
- zapewnienie co najmniej równoważnego poziomu cyberbezpieczeństwa, kontroli dostępu, rejestrowania zdarzeń, aktualizacji i odporności;
- zapewnienie wymaganego modelu licencjonowania, okresu gwarancji, wsparcia, serwisu, aktualizacji i cyklu życia produktu;
- dla urządzeń – zachowanie nie gorszych parametrów elektrycznych, mechanicznych, środowiskowych, eksploatacyjnych, energetycznych i akustycznych, odpowiednio do wymagań tabeli;
- dla usług, audytów i testów – zachowanie co najmniej równoważnego zakresu, metodyki, produktów prac, kwalifikacji zespołu i kryteriów odbioru;
- dla szkoleń – zachowanie co najmniej równoważnego zakresu merytorycznego, liczby i formy zajęć, materiałów, ćwiczeń, sposobu weryfikacji wiedzy oraz wartości dokumentu potwierdzającego ukończenie, jeżeli są wymagane.

Przedmiotowe środki dowodowe dotyczące równoważności

W przypadku zaoferowania rozwiązania równoważnego Wykonawca składa wraz z ofertą, jako przedmiotowe środki dowodowe w rozumieniu art. 106 i art. 107 ust. 1 Pzp:

- wykaz oferowanych rozwiązań równoważnych, ze wskazaniem elementu OPZ, którego dotyczą;
- porównanie wymagania po wymaganiu, wykazujące spełnienie każdego właściwego kryterium równoważności;
- karty katalogowe producenta, specyfikacje techniczne, deklaracje producenta, certyfikaty, raporty z badań, dokumentację licencyjną albo inne odpowiednie dokumenty potwierdzające parametry i funkcjonalności, na które powołuje się Wykonawca.

Zamawiający akceptuje równoważne przedmiotowe środki dowodowe, jeżeli potwierdzają spełnienie wymagań. Zamawiający przewiduje możliwość wezwania do złożenia lub uzupełnienia przedmiotowych środków dowodowych na zasadach art. 107 ust. 2 Pzp, z zastrzeżeniem przypadków określonych w art. 107 ust. 3 Pzp.

Poza dokumentami dotyczącymi rozwiązania równoważnego dokumenty producenta są składane na etapie realizacji umowy, najpóźniej wraz z dostawą i przed odbiorem właściwej części, chyba że SWZ lub tabela danej części wyraźnie wskazuje konkretny dokument jako przedmiotowy środek dowodowy wymagany wraz z ofertą.

Dostępność, wymagania środowiskowe i DNSH

W zakresie, w jakim przedmiot zamówienia jest przeznaczony do użytku osób fizycznych, w tym pracowników Zamawiającego, wymagania dotyczące interfejsów, platform szkoleniowych, materiałów elektronicznych i dokumentacji należy realizować z uwzględnieniem wymagań dostępności i projektowania dla wszystkich użytkowników, stosownie do art. 100 Pzp i charakteru danego świadczenia.

Każda część zamówienia podlega ogólnej zasadzie „nie czyni poważnych szkód” dla środowiska (DNSH), odpowiednio do jej przedmiotu i sposobu realizacji. Szczegółowe wymagania techniczne, obowiązki dotyczące opakowań, ZSEiE, odpadów eksploatacyjnych oraz dokumentowania zgodności określają pkt 3.7 SWZ, OPZ właściwy dla danej części, Załącznik nr 5 do SWZ i projektowane postanowienia umowy.

Zgodność z zakresem przedsięwzięcia grantowego

Przedmiot każdej części zamówienia musi pozostawać w bezpośrednim i możliwym do wykazania związku z podniesieniem poziomu cyberbezpieczeństwa systemów teleinformatycznych IT lub OT wykorzystywanych przez Zamawiającego przy realizacji zbiorowego zaopatrzenia w wodę oraz z zakresem rzeczowym zatwierdzonego wniosku o przyznanie grantu i umowy o powierzenie grantu. Wykonawca nie jest uprawniony do samodzielnej zamiany produktów, usług lub rezultatów na elementy o innym zasadniczym przeznaczeniu.

- Sprzęt serwerowy, pamięci masowe, systemy operacyjne, licencje i usługi wdrożeniowe objęte zamówieniem mogą być wykorzystywane w ramach Projektu wyłącznie w zakresie, w jakim są niezbędne do wdrożenia, utrzymania lub poprawy rozwiązań cyberbezpieczeństwa. Nie mogą zostać przeznaczone zasadniczo do obsługi systemów dziedzicznych, w szczególności SCADA lub HMI.
- Dostawa lub modernizacja urządzeń dziedzicznych OT/ICS/IIoT, w szczególności sterowników, mierników, sensorów, wodomierzy, modułów telemetrycznych lub systemów zdalnego odczytu, a także systemów CCTV, nie może być wykonana w miejsce produktów cyberbezpieczeństwa opisanych w OPZ. Integracja rozwiązań bezpieczeństwa z takimi urządzeniami albo systemami jest dopuszczalna wyłącznie w zakresie wymaganym w OPZ.
- Systemy zasilania awaryjnego i gwarantowanego z Części I, w tym urządzenia UPS, akumulatory i mobilny agregat prądotwórczy, muszą służyć zapewnieniu ciągłości działania wskazanych przez Zamawiającego systemów teleinformatycznych IT/OT, systemów komunikacji między nimi lub rozwiązań cyberbezpieczeństwa. W dokumentacji odbiorowej Wykonawca wskaże zasilane urządzenia lub obwody, parametry podtrzymania, sposób przyłączenia oraz wyniki prób funkcjonalnych. Urządzenia te nie są przeznaczone do regularnego ani podstawowego zasilania procesów technologicznych.
- W odniesieniu do licencji, subskrypcji, gwarancji, serwisu i wsparcia o charakterze okresowym Wykonawca wskaże w dokumentach dostawy lub protokole odbioru datę rozpoczęcia i zakończenia świadczenia, jednostkę rozliczeniową oraz zakres świadczenia, w sposób umożliwiający przyporządkowanie kosztu do okresu kwalifikowalności określonego w umowie o powierzenie grantu.

Dokumentacja, odbiór i prawa do rezultatów

- Odbiór każdej części nastąpi na podstawie kryteriów, produktów prac, testów i dokumentów wskazanych w OPZ, SWZ oraz umowie.
- Dokumentacja techniczna, powykonawcza, administracyjna, audytowa, szkoleniowa i licencyjna zostanie przekazana w zakresie właściwym dla danej części.
- Wykonawca usunie stwierdzone w toku odbioru wady, braki i niezgodności w terminie określonym w umowie.
- Podpisanie protokołu odbioru nie ogranicza uprawnień Zamawiającego wynikających z gwarancji, rękojmi, odpowiedzialności kontraktowej ani zobowiązań dotyczących wsparcia i serwisu.
- Prawa do korzystania, modyfikowania i dalszego wykorzystywania dokumentacji oraz innych rezultatów niematerialnych zostaną zapewnione w zakresie określonym w projektowanych postanowieniach umowy.

Dokumentowanie rezultatów i identyfikowalność

Dokumentacja odbiorowa musi zapewniać Zamawiającemu możliwość wykazania wykonania zakresu zamówienia, powiązania wydatku z przedsięwzięciem grantowym oraz osiągnięcia właściwych produktów i wskaźników. Wykonawca przekaże, odpowiednio do charakteru danej części:

- dla dostaw — zestawienie dostarczonych urządzeń i oprogramowania obejmujące co najmniej producenta, nazwę i model, numer seryjny lub inny unikalny identyfikator, ilość, miejsce instalacji, datę dostawy i uruchomienia, okres gwarancji lub wsparcia oraz identyfikatory i okresy licencji lub subskrypcji;
- protokoły dostawy, instalacji, konfiguracji, uruchomienia i testów — odpowiednio do zakresu części — wraz z wynikami testów, wykazem stwierdzonych niezgodności i potwierdzeniem ich usunięcia;
- dla usług dokumentacyjnych, wdrożeniowych i testowych — raport albo inny produkt wskazany w OPZ, zawierający opis zakresu i metodyki, daty wykonania, skład zespołu realizującego, wykonane czynności oraz osiągnięte rezultaty;
- dla szkoleń — program lub agendę, wymiar godzin, listę uczestników i potwierdzenie udziału, opis sposobu weryfikacji nabycia kompetencji oraz imienne zaświadczenia, świadectwa lub certyfikaty potwierdzające ukończenie szkolenia i zakres nabytych kompetencji, z zachowaniem przepisów o ochronie danych osobowych;
- dla audytów — raport z określeniem zakresu, zastosowanej metodyki, wykorzystanych dowodów, ustaleń i zaleceń, protokół odbioru oraz dokumenty potwierdzające spełnienie przez audytora wymagań kwalifikacyjnych wynikających z przepisów prawa lub SWZ, jeżeli są wymagane;
- na żądanie Zamawiającego — dodatkowe wyjaśnienia, zestawienia i kopie dokumentów niezbędne do rozliczenia przedsięwzięcia, pomiaru wskaźników lub przeprowadzenia kontroli, z zachowaniem ochrony informacji prawnie chronionych i tajemnicy przedsiębiorstwa w zakresie dopuszczonym przez prawo.

Każdy dokument odbiorowy powinien umożliwiać identyfikację postępowania, właściwej części zamówienia, umowy oraz przedsięwzięcia grantowego „Cyberbezpieczne Wodociągi”.

Uzasadnienie wybranych wymagań

Wymagania określone w OPZ mają charakter funkcjonalny, techniczny i organizacyjny oraz wynikają z potrzeby zapewnienia ciągłości działania, bezpieczeństwa, trwałości i możliwości utrzymania infrastruktury Zamawiającego. Zamawiający dopuszcza rozwiązania równoważne na zasadach wskazanych powyżej.

Wymóg dostawy urządzeń nieobjętych statusem końca sprzedaży lub końca wsparcia służy zapewnieniu dostępności aktualizacji, części zamiennych, serwisu i wsparcia przez wymagany okres. Wymóg gwarancji producenta lub autoryzowanego serwisu, w tym obsługi On-Site tam, gdzie została wskazana, służy

ograniczeniu przestojów i ryzyka braku możliwości wykonania naprawy. Wymagania te nie mają na celu uprzywilejowania wykonawcy ani producenta i powinny być interpretowane zgodnie z zasadami uczciwej konkurencji, równego traktowania, przejrzystości i proporcjonalności określonymi w art. 16 Pzp.

CZĘŚĆ I – ZASILANIE AWARYJNE I MOBILNY AGREGAT PRĄDOTWÓRCZY

Zakres części

- urządzenia UPS do produktów i rozwiązań z zakresu bezpieczeństwa;
- akumulatory do urządzeń UPS;
- mobilny agregat prądotwórczy wraz z przyczepą-platformą i wyposażeniem.

1. Akumulatory do urządzeń typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa - 1 komplet

Wymagania ogólne	Zamawiający wymaga dostarczenia: 18 szt. przemysłowych akumulatorów AGM, bezobsługowych, szczelnych, przeznaczonych do pracy w systemach zasilania awaryjnego UPS.
Wymagania szczegółowe	1. Napięcie znamionowe: 12 V. 2. Pojemność znamionowa przy rozładowaniu 20-godzinnym w temperaturze 20°C: minimum 7,2 Ah. 3. Pojemność znamionowa przy rozładowaniu 10-godzinnym w temperaturze 20°C: minimum 6,0 Ah. 4. Akumulator musi być przystosowany do pracy buforowej oraz do współpracy z układem ładowania UPS. 5.
Wymiary	1. Długość: maksymalnie 152 mm 2. Szerokość: maksymalnie 66 mm 3. Wysokość z terminalami: maksymalnie 102 mm 4. Waga: maksymalnie 2,8 kg
Typ końcówki	FASTON – Quickfit 6,35
Zakres temperatur pracy	1. Przechowywanie: -15°C do +40°C 2. Ładowanie: -0°C do +40°C 3. Rozładowywanie: -15°C do +50°C
Przechowywanie	Utrata pojemności na miesiąc przy 20°C: 3%
Materiał obudowy	Obudowa szczelna, odporna na warunki eksploatacji przewidziane dla akumulatorów AGM.
Napięcie ładowania	1. Przy 20 C podczas pracy buforowej (V)/blok: 13,5–13,8 V 2. Przy 20 C podczas pracy cyklicznej (V)/blok: 14,4–15,0 V
Prąd ładowania	1. Limit prądu ładowania - praca cykliczna: nie więcej niż 2.8A
Maksymalny rozładowania prąd	1 sekunda: nie mniej niż 105 A lub 5 sekund: nie mniej niż 130 A
Impedancja	Mierzone przy 1 kHz (mΩ): nie więcej niż 24
Gwarancja	Min. 12 miesięcy

2. Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa – 1 komplet

Wymagania ogólne	Zamawiający wymaga dostarczenia: 4 szt. urządzeń UPS do podtrzymania zasilania awaryjnego.
Typ obudowy	RACK, do montażu w szafie RACK
Wejściowe zasilania parametry	• Złącze wejściowe: C14 • Zakres częstotliwości wejściowych: 45-55 Hz (system 50 Hz), 55-65 Hz (system 60 Hz) • Napięcie znamionowe wejściowe: Domyślnie 230 V (220/230/240 V) • Zakres napięcia wejściowego: 184–276 V • Częstotliwość znamionowa: 50–60 Hz
Wyjściowe zasilania parametry	• Napięcie znamionowe wyjściowe: Domyślnie 230 V (220/230/240 V) • Wyjściowy współczynnik mocy: nie mniejszy niż 0,7 • Zakres napięcia wyjściowego: 230 V nie więcej niż (+6%/-10%) • Kształt fali na wyjściu: Sinusoida • Gniazda: C13 • Wartość znamionowa VA: nie mniejsza niż 1400 VA • Zakres napięcia: 230 V • Moc: nie mniejsza niż 1050 W
Specyfikacja baterii	1. Zarządzanie akumulatorem: ABM lub metoda ładowania stałym napięciem (wybór przez użytkownika), automatyczny test baterii, ochrona przed głębokim rozładowaniem 2. Parametry znamionowe akumulatora: 12 V / 9 Ah 3. Wymiana akumulatorów: Możliwość wymiany przez użytkownika 4. Rodzaj akumulatora: Kwasowo-olowiowe, bezobsługowe (wymienialny)
Komunikacja	1. Łączność: Port USB (HID) 2. Port szeregowy: (RS232) Mini-terminal zacisków do zdalnego włączania/wyłączania i zdalnego wyłączania zasilania. 3. Interfejs Ethernet: karta rozszerzeń, obsługująca SNMP i kompatybilna z producentem urządzenia. 4. Interfejs użytkownika: Wyświetlacz LCD, Serwer WWW
Dodatkowe informacje	Długość/głębokość produktu: maksymalna 450 mm Zgodność: EN 62040-1 IEC lub równoważny, EN 62040-2 Automatyczne wyłączanie: Wymagane Sprawność przy maks. Obciążeniu: >96
Specyfikacja rozszerzeń karty	1. Obsługiwane protokoły: Fast ETHERNET, 10/100 Mbps, autonegotiation, HTTP 1.1, SNMP V1, SNMP V3, NTP, TFTP, SMTP, BOOTP/DHCP IPv6 Telnet, CLI, SSH, ARP 2. Wspierane MIB: MIB II, Standard IETF UPS MIB (RFC 1628)
Gwarancja	12 miesięcy SLA: Wykonawca potwierdzi przyjęcie zgłoszenia awarii krytycznej w ciągu 24 godzin, rozpocznie działania diagnostyczne w ciągu 72 godzin, zapewni naprawę gwarancyjną w czasie nie większym niż 21 dni.

3. Mobilny agregat prądotwórczy

Cecha / Funkcjonalność	Minimalne parametry wymagane przez Zamawiającego
Wymagania ogólne	1. Agregat fabrycznie nowy, rok produkcji min. 2026 r. 2. Wyprodukowany w UE. 3. Moc (zgodnie z ISO 8528): - Praca nominalna P.R.P. – nie mniej niż 44 kVA, 35 kW. - Praca awaryjna L.T.P. – nie mniej niż 48 kVA, 35 kW. 4. Napięcie: 230/400 V, 50 Hz. 5. Prąd znamionowy min. 60 A. 6. Klasa regulacji G3. 7. Emisja spalin: Stage 5. 8. Agregat mobilny. 9. Stopień ochrony prądnicy: IP23. 10. Wymiary zewnętrzne maksymalne 2500 × 1200 × 1600 (długość × szerokość × wysokość) mm. 11. Podgrzewacz płynu chłodzącego w czasie czuwania grzejący do temperatury silnika nastawianej ze sterownika. 12. Zintegrowany prostownik baterii rozruchowych. 13. Samoczynny start po podaniu sygnału startu. 14. 4 polowy wyłącznik główny prądnicy zabezpieczający prądnicę przed przeciążeniem/zwarcie. 15. Dodatkowo piąte pole zabezpieczone przekaźnikiem różnicowym prądu. 16. Wyłącznik awaryjny. 17. Pomiar poziomu paliwa w % z odczytem na wyświetlaczu sterownika. 18. Zbiornik paliwa zintegrowany z ramą pozwalający na min. 16 h pracy z obciążeniem 70% bez uzupełniania paliwa. 19. Wersja w obudowie wyciszonej, odpornej na warunki atmosferyczne. 20. Agregat zamontowany na przyczepie. 21. Urządzenie wyposażone w fabryczny panel gniazd sterowniczych do komunikacji z SZR, wtyk zasilania potrzeb własnych. Gniazda zamontowane na zewnątrz agregatu. IP65. 22. Na agregacie zamontowany we wnęce fabryczny panel gniazd IP67 z zabezpieczeniami: - 3 szt. 16 A 230 V, - 1 szt. 16 A 400 V,

	- 1 szt. 32 A 400 V, - 1 szt. 63 A 400 V. 23. Wszystkie ruchome elementy silnika w agregacie oraz kolektor wydechowy - powinny zawierać metalowe elementy ochronne uniemożliwiające ich przypadkowe dotknięcie. 24. Agregat gotowy do pracy, zalany płynami eksploatacyjnymi i olejem napędowym w minimum 10% pojemności zbiornika paliwa, tak aby można było przeprowadzić testy w dniu dostawy agregatu. 25. Pompa spustowa oleju silnikowego umożliwiająca w łatwy i szybki sposób na wymianę oleju silnikowego. 26. Obudowa wyposażona w centralne zawiesie agregatu.
Dane ogólne silnika zespołu prądotwórczego	1. Nominalna prędkość obrotowa: ok. 1500 obr/min. 2. Silnik wysokoprężny, 4-cylindrowy, rzędowy z doładowaniem. 3. Moc znamionowa silnika min. 38 kW. 4. Spełniający normę emisji spalin Stage V. 5. Instalacja 12 V DC. 6. Zużycie paliwa maks. 11,0 l/h przy 100% obciążenia. 7. Układ zasilania paliwem: elektronicznie sterowany wtrysk bezpośredni Common Rail. 8. Regulator obrotów silnika - elektroniczny. 9. Silnik wyposażony w czujniki podłączone do sterownika: - pomiaru chwilowego ciśnienia oleju, - pomiaru chwilowej temperatury płynu chłodzącego, - chwilowego spalania, - całkowitego zużycia paliwa, - dziennego zużycia paliwa. 10. Układ oczyszczania spalin: katalizator utleniający DOC oraz filtr cząstek stałych DPF. Nie jest dopuszczany AdBlue. 11. Serwis fabryczny silnika musi znajdować się na terenie Polski.
Dane ogólne prądnicy zespołu prądotwórczego	1. Konstrukcja: bezszczotkowa, synchroniczna, samowzbudna 4 biegunowa 2. Wyprodukowana na terenie UE. 3. Stopień ochrony co najmniej IP23. 4. Miedziane uzwojenie.

	5. Stabilizacja napięcia: +/- 0,5%. 6. Klasa izolacji: H. 7. Elektroniczny regulator napięcia. 8. Norma obciążenia G3 – zgodna z ISO 8528-5:2020
Dane ogólne panelu sterowania	1. Sterownik Agregatu ma być wyposażony w fabryczny moduł ModbusTCP RS485, oraz moduł SNMP. Moduły mają być zainstalowane, aktywne i skonfigurowane. 2. Sprawdzenie poziomu paliwa. 3. Sprawdzenie napięć jedno i trójfazowych na każdej z faz. 4. Licznik motogodzin – dzienny, miesięczny, całkowity. 5. Pomiar i sprawdzenie napięcia akumulatora 6. Przegląd historii alarmów. 7. Licznik udanych i nieudanych uruchomień. 8. Sprawdzenie generowanej mocy pozornej (kVA), czynnej (kW) i biernej (kVAr) oraz współczynnika mocy. 9. Zabezpieczenie przed zbyt wysoką temperaturą płynu chłodzącego. 10. Zabezpieczenie przed zbyt niskim ciśnieniem oleju. 11. Zabezpieczenie przed brakiem ładowania z alternatora. 12. Zabezpieczenie przed nadobrotami silnika. 13. Zabezpieczenie przed zbyt niskimi obrotami silnika. 14. Informacja o pracy ze zbyt małym obciążeniem agregatu. 15. Zabezpieczenie przed zbyt niskimi i wysokimi napięciami. 16. Zabezpieczenie i informacja przed zbyt niską i wysoką częstotliwością [Hz]. 17. Zabezpieczenie przed zwarcie. 18. Zabezpieczenie i informacja o asymetrii międzyfazowej. 19. Zabezpieczenie i informacja przed przeciążeniem. 20. Sterownik musi posiadać funkcję „zdalny start” 21. Sterownik z możliwością podpięcia zdalnego monitoringu, realizowany po sieci GSM oraz LAN 22. Sterownik umożliwiający lokalizację GPS 23. Programowalne alarmy, wejścia i wyjścia umożliwiające dalszą rozbudowę sterownika.
Jednoosiowa przyczepa dedykowana do montażu,	1- Oś hamowna 1 x 1800 kg 2 - Urządzenie najazdowe z hamulcem ręcznym postojowym

użytkowania i przewozu agregatu	3- wymiary platformy maksymalnie 2500 x 1200 mm 4 - zaczep kulowy 5 - 2 podpory rurowe z przodu 6 - 2 podpory kątowe z tyłu 7 - podłoga ze sklejki wodoodpornej antypoślizgowej grubości w przedziale - 10 - 15 mm 8 - masa całkowita ok. 1800 kg 9 - ładowność ok. 1400kg 10 - Homologacja specjalna – agregat elektryczny 11 - Przyczepa musi posiadać homologację europejską 12 - Koło manewrowe z przodu wzmocnione ok. 300 kg. 13 - Kliny pod koła – 2 szt. 14 - Koła z oponami wielosezonowymi
Gwarancja:	AGREGAT 1. Wymagana gwarancja fabryczna producenta agregatu. 2. Gwarancja na agregat – minimum 24 miesiące, lub 1000 motogodzin w zależności co nastąpi pierwsze. 3. Po odbiorach należy przedstawić certyfikat potwierdzający rozpoczęcie fabrycznej gwarancji na agregat prądotwórczy. 4. Aby gwarancja została zachowana przyjęto następujące kryteria: - pierwszy przegląd po 50 motogodzinach pracy lub po roku - kolejne przeglądy co rok lub co każde 500 przepracowanych motogodzin agregatu. PRZYCZEPA Gwarancja na przyczepę 24 miesiące.
SLA:	Wykonawca potwierdzi przyjęcie zgłoszenia awarii krytycznej w ciągu 4 godzin, rozpocznie działania diagnostyczne w ciągu 6 godzin i przywróci sprawność albo zapewni rozwiązanie zastępcze w ciągu 24 godzin. Dla pozostałych wad potwierdzi zgłoszenie w 1 dzień roboczy, rozpocznie działania w 2 dni robocze i usunie wadę w 5 dni roboczych, chyba że Zamawiający zaakceptuje inny termin z uwagi na obiektywną dostępność części.
WARUNKI REALIZACJI ZAMÓWIENIA	1. Wykonawca, który nie jest producentem agregatu winien przedstawić dokument że jest dystrybutorem danej marki agregatu.

	2. Wykonawca jeżeli nie jest serwisem fabrycznym danego producenta agregatu winien przedstawić dokument, kto jest uprawniony do wykonywania serwisów przedłużających gwarancję agregatu. 3. Wymagane jest aby producent agregatu dla pełnego wsparcia zamawiającego posiadał w Polsce co najmniej 15 lat własny oddział, serwis, oraz magazyn części zamiennych i materiałów eksploatacyjnych. 4. Miejsce serwisowania w ramach udzielonej gwarancji będzie się odbywać we wskazanej jednostce zamawiającego. 5. Płyny eksploatacyjne silnika na dzień odbioru agregatu winny być napełnione wg normy. 6. Zgłoszenie wad i awarii przedmiotu zamówienia będzie dokonywane telefonicznie i pisemnie (e-mailem) przez osoby upoważnione przez Zamawiającego. 7. Dostarczony sprzęt powinien być fabrycznie nowy i nie nosić śladów użytkowania, w pełni sprawny oraz odpowiadać standardom jakościowym i technicznym wynikającym z funkcji i przeznaczenia, zgodnie ze specyfikacją istotnych warunków zamówienia oraz powinien być wolny od wad prawnych i fizycznych. 8. W przypadku stwierdzenia podczas odbioru: • widocznych wad, • niezgodności dostawy pod względem wymaganych parametrów, braku wymaganych dokumentów technicznych, Wykonawca zobowiązany jest do wymiany towaru na wolny od wad, uzupełnienia braków towaru lub wymiany dostarczonego towaru na zgodny z Umową, najpóźniej w ciągu 14 dni roboczych. 9. Stan formalny- prawny: • w pełni udokumentowane legalne pochodzenie, • urządzenie w 100% przygotowane do pracy, kompletna, sprawna technicznie zgodnie z przeznaczeniem użytkowania, wymagana gwarancja na ww. towar - minimum 24 miesiące, od daty otrzymania towaru przez Zamawiającego. 10. Bieg terminu gwarancji liczony będzie od daty dostawy w miejsce docelowe wskazane w niniejszym OPZ z zastrzeżeniem, że dostarczony towar jest wolny od nieprawidłowości. W przypadku ich stwierdzenia termin gwarancji rozpoczyna obowiązywać od dnia usunięcia wskazanych nieprawidłowości. 11. Wykonawca przeprowadzi szkolenie w siedzibie Zamawiającego- miejsce dostawy z zakresu obsługi oraz funkcjonalności agregatu i przyczepy wraz z akcesoriami oraz wykorzystania ich parametrów technicznych. 12. Dostarczony sprzęt musi być wyposażony w dokumenty gwarancyjne, certyfikaty CE, fabryczną instrukcję obsługi w języku polskim, książkę serwisową oraz dokumenty umożliwiające rejestrację przyczepy i poruszanie się po drogach publicznych. 13. Wykonawca zobowiązany jest na własny koszt i
--	--

	ryzyko dostarczyć przedmiot zamówienia do miejsca wskazanego przez Zamawiającego. 14. Wykonawca zawiadomi Zamawiającego o planowanym terminie dostawy z wyprzedzeniem min. 2 dni roboczych. 15. Rozliczenie za wykonanie przedmiotu umowy odbędzie jednorazowo fakturą wystawioną po dokonaniu odbioru. 16. Dostarczone dokumenty oraz przedmiot zamówienia zostaną poddane sprawdzeniu przez Zamawiającego. 17. Termin wykonania dostawy: zgodny z terminem dostawy określonym w umowie - jednak nie dłuższy niż 45 dni od dnia zawarcia umowy i nie później niż do dnia 30.12.2026 r. 18. Zakończenie dostawy oraz gotowość do odbioru końcowego będą stwierdzone przez Wykonawcę pisemnie lub mailowo. 19. Cena zaoferowana w ofercie powinna uwzględnić wszystkie koszty związane z dostawą przedmiotu zamówienia, w tym koszty transportu oraz rozładunek.
--	--

CZĘŚĆ II – SYSTEMY CYBERBEZPIECZEŃSTWA I INFRASTRUKTURA SERWEROWA

1. S13. Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa – typ I – 2 sztuki

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
	2 sztuki	W ofercie wymagane jest podanie modelu, symbolu oraz producenta
1.	Obudowa	Obudowa Rack o wysokości max. 2U z możliwością zainstalowania min. 16 dysków 2.5" SAS/SATA oraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Szyny wyposażone w organizator (ramię) do kabli.
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 jednoprocessorowych.
4.	Procesor	Zainstalowany jeden procesor min. 32-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 375 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla jednego procesora. Dla oferowanego serwera.
5.	RAM	Min. 128GB 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. cztery sloty PCIe x16 generacji 5
8.	Interfejsy sieciowe/FC/SAS	1 x karta dwuportowa 10/25Gb SFP28, nie zajmująca slotów PCIe. 2 x wkładka 10GbE SFP+ SR
9.	Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10. Obsługa dysków SATA/SAS.
10.	Dyski twarde	Zainstalowane dwa dyski hot-plug SSD SATA 6Gbps o pojemności min. 960GB z możliwością spięcia w RAID 1. Zainstalowane dwa dyski hot-plug SSD SATA 6Gbps o pojemności min. 3.84TB z możliwością spięcia w RAID 1.

11.	Wbudowane porty	min. port USB 2.0 oraz 2 x USB 3.1, port VGA.
12.	Video	Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1920x1200
13.	Wentylatory	Redundantne
14.	Zasilacze	Min. dwa zasilacze Hot-Plug min. 1100W klasy Titanium.
15.	Bezpieczeństwo	Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. Możliwość integracji z RSA SecurID 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.
16.	Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiającą:

		• zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez ośmiu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • 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 • Monitorowanie zużycia dysków SSD • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. • Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • Automatyczne odświeżanie certyfikatów SSL • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielokrotnego przy logowaniu do karty zarządzającej • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych serwerów • 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. Do oferty należy dołączyć oświadczenie producenta serwera potwierdzające spełnienie powyższych wymagań.
17.	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. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera.
18.	Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. 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.

		Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
19.	Warunki gwarancji	Zamawiający wymaga min. 36 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następny dzień roboczy od zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 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. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.



20.	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
21.	Dodatkowe wymaganie dotyczące serwera	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera

		▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Informacje o poziomie redukcji danych • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Dostarczane w ramach postępowania urządzenia (serwer Typ-1, serwer Typ-2) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
--	--	---

		Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android.
22.		- Możliwość zainstalowania 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.
23.	Oprogramowanie do zarządzania	Zainstalowane oprogramowanie producenta serwera do zarządzania, spełniające poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB

		• Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • 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. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modułarnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
--	--	---

2. S13. Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa – typ II – 1 sztuka

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
-----	-------------------------------------	---

	1	2
	1 sztuka	W ofercie wymagane jest podanie modelu, symbolu oraz producenta
1.	Obudowa	Obudowa Rack o wysokości max. 2U z możliwością zainstalowania min. 16 dysków 2.5" 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.
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 jednoprocessorowych.
4.	Procesor	Zainstalowany jeden procesor min. 32-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 375 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla jednego procesora. Dla oferowanego serwera.
5.	RAM	Min. 128GB 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.	Zabezpieczeni a pamięci RAM	Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection
7.	Gniazda PCIe	Min. cztery sloty PCIe x16 generacji 5
8.	Interfejsy sieciowe/FC/S AS	1 x karta dwuportowa 10/25Gb SFP28, nie zajmująca slotów PCIe. 2 x wkładka 10GbE SFP+ SR
9.	Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10.

		Obsługa dysków SATA/SAS.
10.	Dyski twarde	Zainstalowane dwa dyski hot-plug SSD SATA 6Gbps o pojemności min. 960GB z możliwością spięcia w RAID 1.
11.	Wbudowane porty	min. port USB 2.0 oraz 2 x USB 3.1, port VGA.
12.	Video	Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1920x1200
13.	Wentylatory	Redundantne
14.	Zasilacze	Min. dwa zasilacze Hot-Plug min. 1100W klasy Titanium.
15.	Bezpieczeństwo	Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. Możliwość integracji z RSA SecurID 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.
16.	Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez ośmiu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • 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 • Monitorowanie zużycia dysków SSD • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. • Możliwość wykrywania odchyłań konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • Automatyczne odświeżanie certyfikatów SSL • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z

		możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych serwerów • 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. Do oferty należy dołączyć oświadczenie producenta serwera potwierdzające spełnienie powyższych wymagań.
17.	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. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera.
18.	Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. 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.

		Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
19.	Warunki gwarancji	Zamawiający wymaga min. 36 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następny dzień roboczy od zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 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. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z

		oficjalnego kanału dystrybucyjnego producenta.
20.	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
21.	Dodatkowe wymaganie dotyczące serwera	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów

		▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Informacje o poziomie redukcji danych • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Dostarczane w ramach postępowania urządzenia (serwer Typ-1, serwer Typ-2) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
--	--	---

		Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android.
22.		- Możliwość zainstalowania 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.
23.	Oprogramowanie do zarządzania	Zainstalowane oprogramowanie producenta serwera do zarządzania, spełniające poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu

		• Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • 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. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modułarnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
--	--	---

3. Licencje systemu operacyjnego – 8 sztuk

O46. System wirtualizacyjny dedykowany do systemów, na których zostanie zainstalowanych produkt z zakresu cyberbezpieczeństwa / O47. System operacyjny i (również rozbudowa licencji do już istniejącego systemu), na których zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa oraz S35. Stacja robocza fizyczna lub wirtualna z rolą stacji przesiadkowej (Stacja robocza wirtualna z rolą stacji przesiadkowej)

Konsolidacja pozycji – pozycja dotyczy dostawy licencji – systemu operacyjnego, który umożliwia wykorzystanie systemu wirtualizacyjnego, wirtualnych maszyn oraz wirtualnej stacji roboczej.

Ilość – 8 sztuk.

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
1.	Oprogramowanie	MS Windows Server 2025 Standard - 16 Core lub równoważne (opis równoważności w pkt. 2).
Zamawiający wymaga spełnienia przez oprogramowanie równoważne minimalnych wymagań w zakresie funkcjonalności określonych poniżej:		



2.	Funkcjonalności i kryteria	Oprogramowanie równoważne musi spełnić poniższe kryteria: Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. Licencja ma umożliwiać uruchomienie min. dwóch maszyn wirtualnych systemu SSO. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,
----	-----------------------------------	---



	u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) połączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII.możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),
--	--

		x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
--	--	---

4. O47. Licencje dostępne (również rozbudowa licencji do już istniejącego systemu), na których zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa – 30 sztuk

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
1.	Oprogramowanie	MS Windows Server 2025 RDS CAL per User lub równoważne.
Zamawiający wymaga spełnienia przez oprogramowanie równoważne minimalnych wymagań w zakresie funkcjonalności określonych poniżej:		
2.	Funkcjonalności i kryteria	Oprogramowanie równoważne musi spełnić poniższe kryteria: Licencja oprogramowania musi uprawniać użytkownika do wykorzystywania za pośrednictwem terminali w których posiadaniu jest Zamawiający funkcji

		Serwerowych Systemów Operacyjnych w trybie zdalnego pulpitu.
		Licencja musi uprawniać do wykorzystywania w trybie zdalnego pulpitu najnowszej dostępnej w dniu składania oferty wersji Serwerowego Systemu Operacyjnego danego producenta z bezterminową licencją użytkowania w podmiotach leczniczych.
		Licencje muszą być bezterminowe.

5. O47. Licencje dostępne (również rozbudowa licencji do już istniejącego systemu), na których zainstalowany będzie system lub wdrożone rozwiązanie z zakresu cyberbezpieczeństwa – 20 sztuk

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
1.	Oprogramowanie	MS Windows Server 2025 CAL per User lub równoważne (opis równoważności w pkt. 2).
Zamawiający wymaga spełnienia przez oprogramowanie równoważne minimalnych wymagań w zakresie funkcjonalności określonych poniżej:		
2.	Funkcjonalności i kryteria	Oprogramowanie równoważne musi spełnić poniższe kryteria: Licencja oprogramowania musi uprawniać użytkownika do korzystania za pośrednictwem urządzeń z usług i zasobów Serwerowych Systemów Operacyjnych dostarczonych w ramach tego postępowania.

		Nie wymaga się aby licencje dostępowe uprawniały użytkowników do wykorzystywania funkcji Serwerowych Systemów Operacyjnych w trybie zdalnego pulpitu.
		Licencje muszą być bezterminowe.

6. S13. Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa - serwer typu NAS – 1 sztuka

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
1 sztuka		W ofercie wymagane jest podanie modelu, symbolu oraz producenta
24.	Obudowa	Typu tower, max. wymiary 170x240x240mm
25.	Procesor	Procesor klasy x86 4 rdzenie/8 wątków, o taktowaniu bazowym min. 2,1 GHz
26.	Szyfrowanie	Sprzętowy mechanizm szyfrowania
27.	RAM	Min. 32 GB pamięci DDR4
28.	Dyski	5 x dysk o pojemności min. 4TB 2 x dysk m.2 o pojemności 400GB
29.	Rozbudowa	Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap.

30.	Porty zewnętrzne	2 port USB 3.2 1. generacji
31.	Porty sieciowe	2 porty 2.5GbE 1 port 10GbE RJ-45
32.	Dodatkowa funkcjonalność	Gniazdo rozszerzeń PCIe, min. 1x gniazdo x2 gen. 3
33.	Chłodzenie	Wentylator min. 2 szt.
34.	Obsługiwane typy macierzy RAID	Min. JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
35.	Zarządzanie pamięcią masową	- Maksymalny rozmiar pojedynczego wolumenu: 108 TB - Minimalna liczba wewnętrznych wolumenów: 32
36.	Obsługiwane protokoły	SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPS, FTP, SNMP, LDAP, CalDAV
37.	Konto i folder współdzielony	- Minimalna liczba kont użytkowników: 1024 - Minimalna liczba grup użytkowników: 256 - Minimalna liczba folderów współdzielonych: 256
38.	Usługi plików	- Protokół plików: SMB, AFP, NFS, FTP, WebDAV, Rsync - Minimalna liczba połączeń SMB (oparta na FSCT): 40 - Uwierzytelnianie NFS Kerberos
39.	Gwarancja	- min. 3 lata z czasem reakcji następny dzień roboczy (NBD) - Pozostawienie uszkodzonych dysków u Zamawiającego (KYD)

7. S14. Serwer do wykonywania kopii zapasowych (w tym z usługą/licencją deduplikacji) wraz z O16. Oprogramowanie do wykonywania kopii zapasowych (w tym deduplikacji) – serwer typu NAS – 1 sztuka

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
1 sztuka		W ofercie wymagane jest podanie modelu i producenta urządzenia.
40.	Wymagania ogólne	Wymagane jest dostarczenie rozwiązania z wbudowanym systemem/oprogramowaniem do realizacji i zarządzania kopiami zapasowymi.
41.	Obudowa	Desktop
42.	Procesor	Procesor osiągający w teście CPU Benchmarks, w kategorii CPU Mark wynik co najmniej 3250 pkt. według wyników opublikowanych na stronie.
43.	Pamięć	Min. 16GB Pamięć musi być w 100% kompatybilna z wymogami producenta. Listę zgodności sprzętowej producent musi prezentować na swojej stronie internetowej.
44.	Pamięć masowa	Min. 2 dyski SSD 400GB każdy; Min. 4 dyski 8 TB każdy; Dyski muszą być w 100% kompatybilne z wymogami producenta;

		Listę zgodności sprzętowej producent musi prezentować na swojej stronie internetowej.
45.	Zabezpieceni e przed awarią dysków	Minimalna obsługa systemów RAID 1, 5 Obsługa systemu plików Btrfs
46.	Interfejsy	Oddzielny port zarządzający: min. 1 port 1GbE RJ-45 Przesył danych: min. 1 port 10GbE RJ-45
47.	Właściwości systemu/oprog ramowania	Wymagane jest, aby system: 1. posiadał konsolę zarządzającą; 2. realizował kopię zapasową, przywracał, deduplikował, 3. replikował i zarządzał kopiami danych; 4. był chroniony przed nieautoryzowanym dostępem do interfejsu za pomocą oddzielnego interfejsu zarządzającego; 5. posiadał dostęp do interfejsu minimum z poziomu protokołu https z konfigurowalną obsługą podwójnej autoryzacji MFA; 6. posiadał wbudowany, konfigurowalny firewall; 7. realizował kopie zapasowe i przywracanie dla: • systemów PC z systemem Windows i Mac, • bezagentowa kopia systemów maszyn wirtualnych VMware/Hyper-V, • serwerów Windows/Linux, • kopii danych bazodanowych: Oracle i Microsoft SQL. 8. posiadał możliwość tworzenia planów kopii zapasowych; 9. posiadał wbudowany, konfigurowalny firewall; 10. posiadał funkcję szyfrowania kopii; 11. posiadał możliwość sdzyfrowanej transmisji przesyłu danych; 12. posiadał funkcjonalność blokowego przesyłania pakietów danych dla zoptymalizowania wydajności tworzenia kopii; 13. posiadał funkcjonalność WORM (Write-Once-Read-Many); 14. posiadał własny system wirtualizacji, w którym można szybko uruchomić kopie zwirtualizowanej maszyny; 15. posiadał możliwość realizacji testowego odzyskiwania po awarii w środowisku „piaskownicy” 16. posiadał możliwość odzyskiwania granularnego plików lub całego urządzenia; 17. posiadał możliwość monitorowania stanu całego w czasie rzeczywistym; posiadał możliwość zarządzania kopiami zapasowymi innych serwerów backupowych tej samej technologii producenta;

48.	Gwarancja	36 miesięcy
-----	-----------	-------------

Pakiet uzupełniających się rozwiązań: Oprogramowanie do wykonywania kopii zapasowych (w tym deduplikacji)

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
1 sztuka		W ofercie wymagane jest podanie nazwy oprogramowania.
1.	Wymagania ogólne	System kopii zapasowych musi stanowić rozwiązanie typu appliance oparte o system NAS do ochrony danych środowiska IT, zapewniające centralne zarządzanie procesami backupu oraz odtwarzania danych z poziomu jednego interfejsu webowego. Oprogramowanie musi być kompatybilne z posiadanymi przez Zamawiającego urządzeniami firmy Synology.
2.	Wymagania	Minimalne wymagane funkcje oprogramowania do backupu: oprogramowanie musi być w pełni zgodne z oferowanym urządzeniem, kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal, kopia zapasowa maszyn wirtualnych (VMware, Hyper-V) kopia zapasowa serwerów fizycznych (Windows, Linux) obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania,

		obsługa wielu wersji i retencji, możliwość wyzwalania kopii zapasowej według harmonogramu, obsługa klastra przełączania awaryjnego Microsoft Hyper-V, centralne zarządzanie, konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań, portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora, kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace.
3.	Gwarancja	36 miesięcy

8. S21. Network Attached Storage (NAS) – jednostka rozszerzająca - 2 sztuki

1.	Wymagania ogólne	Przedmiotem zamówienia jest dostawa fabrycznie nowych jednostek rozszerzających pamięć masową do serwerów NAS, umożliwiających rozbudowę przestrzeni dyskowej o dodatkowe zatoki na dyski twarde oraz współpracującej z systemem zarządzania posiadanymi urządzeniami Synology RS1219+ oraz RS819 przez Zamawiającego. Dodatkowo urządzenia muszą zostać wyposażone w kompatybilne dyski SATA, umieszczone na liście zgodności producenta. Dyski muszą być pojemności 8TB w ilości 8 szt. po 4
----	-------------------------	---



		na każde urządzenie.
2.	Obudowa i konstrukcja	Urządzenie przeznaczone do montażu w szafie teleinformatycznej Rack 19". Wysokość maksymalnie 1U. Konstrukcja umożliwiającą montaż w szafach 19" dwu- i czterosłupowych. Głębokość urządzenia nie większa niż 330 mm.
3.	Pamięć masowa	Minimum 4 zatoki na dyski. Obsługa dysków: SATA HDD 3,5", SATA HDD 2,5", SATA SSD 2,5". Obsługa wymiany dysków podczas pracy (Hot Swap). Zarządzanie macierzami RAID z poziomu systemu operacyjnego urządzenia nadrzędnego.
4.	Interfejsy	Min. 1 port eSATA do połączenia z jednostką główną. Dostarczony przewód połączeniowy eSATA.
5.	Zarządzanie	Pełna integracja z systemem zarządzania urządzeniami posiadanych przez Zamawiającego. Zarządzanie urządzeniem bez konieczności instalowania dodatkowego

		oprogramowania. Obsługa automatycznej hibernacji dysków.
6.	Zasilanie	Zasilanie 100–240 V AC, 50/60 Hz. Automatyczna synchronizacja stanu zasilania z urządzeniem nadrzędnym. Maksymalny pobór mocy nie większy niż 25 W podczas pracy.
7.	Warunki środowiskowe	Temperatura pracy: minimum od 5°C do 35°C. Wilgotność pracy: minimum 8–80% RH.
8.	Certyfikaty	Urządzenie musi posiadać deklarację zgodności CE
9.	Gwarancja	- Min. 36 miesięcy gwarancji producenta. - Urządzenie musi pochodzić z oficjalnego kanału dystrybucyjnego producenta. - Serwis gwarancyjny realizowany na terenie Polski.

9. S16. Macierz dyskowa wraz z dodatkowymi dyskami – 1 komplet

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
	1 sztuka	W ofercie wymagane jest podanie modelu, symbolu oraz producenta



1.	Procesor	O Architekturze x86 64-bit, posiadający co najmniej 6 rdzeni, 12 wątków, o taktowaniu min. 2,2GHz, osiągający wynik min. 7640 pkt. w teście wielowątkowym PassMark CPU Mark
2.	Obudowa	RACK, w zestawie szyny teleskopowe do instalacji urządzenia w szafie RACK.
3.	Pamięć RAM	8 GB DDR4 ECC RAM
4.	Ilość obsługiwanych dysków	12 dysków 3,5" /2,5" SATA III 6Gb/s 2 dyski M.2 NVMe (możliwość uzyskania poprzez dołożenie karty rozszerzeń tego samego producenta co NAS).
5.	Ilość zainstalowanych dysków	8 dysków o pojemności min. 8TB znajdujące się na liście zgodności serwera NAS; możliwość aktualizacji firmware dysków z poziomu serwera NAS, 2 dyski M.2 NVMe o pojemności min. 800GB znajdujące się na liście zgodności serwera NAS; możliwość aktualizacji firmware dysków z poziomu serwera NAS
6.	Interfejsy sieciowe	4 x Gigabit (10/100/1000), 2 x 10GbE SFP+
7.	Porty	2 x USB 3.2 Gen 1, 2 x Infiniband
8.	Gniazda PCIe	2 x Gen3 x8 slots (x8 link)

9.	Wskaźniki LED	Status, LAN, HDD1 -12
10.	Obsługa RAID	Basic, JBOD, RAID F1,0,1,5,6,10 + Hot Spare 1,5,6,10
11.	Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
12.	Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych, kluczem AES-256bitów.
13.	Licencja na Kamery IP	W zestawie licencja na dwie kamery z możliwością rozszerzenia do 75. Funkcja CMS.
14.	Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP, WebDAV, CalDAV, SFTP.
15.	Usługi	Wsparcie dla High Availability Serwer VPN Serwer pocztowy dla kilku domen Stacja monitoringu Windows ACL Integracja z Windows ADS Firewall z kontrolą ruchu

		Serwer WWW Serwer plików Manager plików przez WWW Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie Antyvirus Klient VPN Usługa DDNS Oprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware
16.	Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów.
17.	Język GUI	Polski
18.	System plików	Dyski wewnętrzne Btrfs, EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT4, EXT3, HFS+, exFAT.
19.	Zasilanie	Zasilanie redundantne min. 500W
20.	Chłodzenie	FAN x 4
21.	Bezpieczeństwo	Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zaporą sieciową, szyfrowanie folderu



		współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.
22.	Oprogramowanie	Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych Wymaga się zapewnienia aplikacji do realizacji chmury prywatnej, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI, a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Ww. usługa musi umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ww. usługa musi umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. Usługa musi być dostępna bez dodatkowych opłat, co najmniej w okresie gwarancji na urządzenie. Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync Obsługa minimum 256 migawek na folder współdzielony i minimum 4096

		migawek na cały system. Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 16 jednoczesnych połączeń
23.	Akcesoria	2 wkładka SFP+ 10GbE MM
24.	Certyfikaty	CE
25.	Gwarancja	- min. 3 lat z czasem reakcji następny dzień roboczy (NBD) - Pozostawienie uszkodzonych dysków u Zamawiającego (KYD)

Dodatkowe dyski do dostarczenia – do montażu samodzielnego przez Zamawiającego w macierzy do rozbudowy:

- 4 sztuki dysków – SSD 1.92TB 2.5 SAS 24Gb/s DWPD

10. S27. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X (switch) – typ I – 2 sztuki

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
	TYP	W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
1.	Wymagania ogólne	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack.

2.	Wymagane parametry fizyczne	Wymagane parametry fizyczne a) możliwość montażu w szafie 19" b) jeden wewnętrzny zasilacz 230V AC c) port USB umożliwiający podłączenie zewnętrznej pamięci flash
3.	Wymagana konfiguracja portów	Przełącznik musi posiadać minimum: • 48 portów gigabitowych w standardzie 100/1000BaseT • 2 porty 1G typu COMBO SFP/RJ45 • 2 porty 1G/10G SFP+ pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
4.	Przełącznik	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a) Zarządzanie stosem poprzez jeden adres IP b) Do min. 8 jednostek w stosie c) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie d) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree UWAGA: Przełącznik powinien wspierać tzw. in-service software upgrade (ISSU) czyli aktualizację przełączników w stosie bez przerywania pracy całego stosu przełączników
5.	Matryca przełączająca	Matryca przełączająca o wydajności min. 140 Gbps
6.	Przepustowość	Przepustowość minimalna 104 Mpps
7.		Obsługa min 16 000 adresów MAC
8.		Wbudowana pamięć RAM min. 1 GB
9.		Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB
10.		Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling

		(QinQ)
11.		Obsługa ramek jumbo o wielkości min. 9 216 bajtów
12.		Obsługa protokołu MVRP lub równoważny
13.		Wsparcie dla protokołów: • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 16 instancji protokołu MSTP lub zastosowanie osobnej instancji STP dla każdego VLANu.
14.		Obsługa min. 256 tras dla routingu IPv4
15.		Obsługa min. 32 tras dla routingu IPv6
16.		Obsługa protokołów routingu minimum: • IPv4: minimum: statyczny • IPv6: minimum: statyczny
17.		Obsługa protokołów LLDP i LLDP-MED
18.		Przełącznik musi posiadać funkcjonalność DHCP Server
19.		Obsługa ruchu multicast: • IGMP Snooping v1, v2 i v3 • Obsługa 1000 grup multicast
20.		Obsługa mechanizmu DHCP snooping
21.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a) min. 4 poziomy dostęp administracyjny poprzez konsolę b) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL c) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www d) zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6 e) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP

		f) obsługa mechanizmów Port Security, IP Source Filtering, port mirroring, voice vlan g) Możliwość uwierzytelnia użytkowników przez wbudowany w przełącznik CaptivePortal – nie dopuszcza się rozwiązań z uwierzytelnieniem na zewnętrznym Captive Portal.
22.	Wymagane opcje zarządzania	a) możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN, b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC), c) urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych, d) dedykowany port konsoli zgodny ze standardem RS-232, e) Obsługa skryptów BASH oraz Python f) Możliwość zarządzania przełącznikiem przez Rest API – konieczność obsługi wszystkich funkcji przełącznika.
23.		Wraz z urządzeniami muszą zostać dostarczone: a) pełna dokumentacja w języku polskim lub angielskim, b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.
24.		Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
25.		Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.
26.		Przełącznik powinien być objęty co najmniej ograniczoną dożywotnią gwarancją producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni od momentu otrzymania niesprawnego urządzenia przesyła przełącznik spełniający minimalne parametry techniczne wskazane w niniejszym dokumencie.

		Dodatkowo: zamawiający wymaga, aby przełącznik posiadał roczny serwis gwarancyjny na sprzęt. Wymiana uszkodzonego elementu w trybie 9x5xNBD, wraz z dostępem do najnowszych wersji oprogramowania.
--	--	--

11. S27. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X (switch) – typ II – POE – 2 sztuki

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
	TYP	W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
1.	Wymagania ogólne	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack.
2.	Wymagane parametry fizyczne	Wymagane parametry fizyczne d) możliwość montażu w szafie 19" e) jeden wewnętrzny zasilacz 230V AC f) zasilacz powinien zapewnić budżet mocy PoE minimum: 350 W g) port USB umożliwiający podłączenie zewnętrznej pamięci flash
3.	Wymagana konfiguracja portów	Przełącznik musi posiadać minimum: • 48 portów gigabitowych w standardzie 100/1000BaseT ze wsparciem dla standardu 802.3at (PoE+) • 2 porty 1G typu COMBO SFP/RJ45 • 2 porty 1G/10G SFP+ pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
4.	Przełącznik	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: e) Zarządzanie stosem poprzez jeden adres IP f) Do min. 8 jednostek w stosie g) Magistrała stakująca o wydajności 40 Gb/s

		h) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie i) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree j) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów statkujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. UWAGA: Przełącznik powinien wspierać tzw. in-service software upgrade (ISSU) czyli aktualizację przełączników w stosie bez przerwania pracy całego stosu przełączników
5.	Funkcje PoE	Wymagane inteligentne funkcje dla POE • Perpetual PoE – podtrzymywanie zasilania dla krytycznych urządzeń podczas restartu przełącznika (np. kamery IP) • Fast POE - po przywróceniu zasilania przełącznik zaczyna dostarczać moc do punktów końcowych bez czekania na pełne załadowanie systemu operacyjnego przełącznika, co przyspiesza uruchomienie podłączonego urządzenia.
6.	Matryca przełączająca	Matryca przełączająca o wydajności min. 140 Gbps
7.	Przepustowość	Przepustowość minimalna 104 Mpps
8.		Obsługa min 16 000 adresów MAC
9.		Wbudowana pamięć RAM min. 1 GB
10.		Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB
11.		Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
12.		Obsługa ramek jumbo o wielkości min. 9 216 bajtów
13.		Obsługa protokołu MVRP lub równoważny

14.		Wsparcie dla protokołów: • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 16 instancji protokołu MSTP lub zastosowanie osobnej instancji STP dla każdego VLANu.
15.		Obsługa min. 256 tras dla routingu IPv4
16.		Obsługa min. 32 tras dla routingu IPv6
17.		Obsługa protokołów routingu minimum: • IPv4: minimum: statyczny • IPv6: minimum: statyczny
18.		Obsługa protokołów LLDP i LLDP-MED
19.		Przełącznik musi posiadać funkcjonalność DHCP Server
20.		Obsługa ruchu multicast: • IGMP Snooping v1, v2 i v3 • Obsługa 1000 grup multicast
21.		Obsługa mechanizmu DHCP snooping
22.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: h) min. 4 poziomy dostępu administracyjnego poprzez konsolę i) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL j) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www k) zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6 l) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP m) obsługa mechanizmów Port Security, IP Source Filtering n) Możliwość uwierzytelnienia użytkowników przez wbudowany w przełącznik CaptivePortal – nie dopuszcza się rozwiązań z uwierzytelnieniem na zewnętrznym Captive Portal.
23.	Wymagane opcje zarządzania	g) możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim

		ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN, h) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC), i) urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych, j) dedykowany port konsoli zgodny ze standardem RS-232, k) Obsługa skryptów BASH oraz Python l) Możliwość zarządzania przełącznikiem przez Rest API – konieczność obsługi wszystkich funkcji przełącznika.
24.		Wraz z urządzeniami muszą zostać dostarczone: c) pełna dokumentacja w języku polskim lub angielskim, d) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.
25.		Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
26.		Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.
27.		Zamawiający wymaga, aby przełącznik posiadał gwarancję typu „limited lifetime”, która zapewnia wymianę niesprawnego urządzenia przez producenta, po jego wcześniejszym dostarczeniu do producenta, w okresie do 5 lat od momentu ogłoszenia zakończenia sprzedaży danego modelu urządzenia Dodatkowo: zamawiający wymaga, aby przełącznik posiadał roczny serwis gwarancyjny na sprzęt. Wymiana uszkodzonego elementu w trybie 9x5xNBD, wraz z dostępem do najnowszych wersji oprogramowania.

12. S27. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X (switch) – typ III – 5 sztuk – kompatybilność z posiadanym Fortinet OT Security Platform

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 10 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganiem jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
 - a) 8 porty GE RJ-45.
 - d) 2 porty GE, SFP.

Zarządzanie

- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 20 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 30 Mpps.
- Tablica adresów MAC o pojemności co najmniej 8 k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 5 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
 - Centralne zarządzanie konfiguracją urządzenia
 - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
 - Centralne zarządzanie sieciami VLAN.
 - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
 - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
 - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
 - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
 - Automatyczna detekcja i rekomendacje konfiguracji.
 - Przesyłanie logów na zewnętrzny serwer syslog.
 - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
 - Obsługa białych i czarnych list adresów MAC.
 - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania.

13. S27. Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X (switch) – typ IV – 1 sztuka – kompatybilność z posiadanym Fortinet OT Security Platform

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 30 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganiem jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
 - a) 24 porty GE RJ-45.
 - e) 4 porty 10 GE SFP+.

Zarządzanie

- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
 - Centralne zarządzanie konfiguracją urządzenia
 - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
 - Centralne zarządzanie sieciami VLAN.
 - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
 - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
 - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
 - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
 - Automatyczna detekcja i rekomendacje konfiguracji.
 - Przesyłanie logów na zewnętrzny serwer syslog.
 - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
 - Obsługa białych i czarnych list adresów MAC.
 - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.

3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania.

14. S34. Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise – 15 sztuk

Access Point – kompatybilny z posiadanym FortiGate Integrated Wi-Fi controller

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
 - a. Temperatura 0–50°C,
 - b. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać co najmniej następujące standardy:
 - a. 2.4 GHz 802.11b/g/n/ax,
 - b. 5 GHz 802.11a/n/ac/ax,
 - c. 6 GHz 802.11ax/be
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w co najmniej jeden interfejs Ethernet (RJ45) wspierający co najmniej szybkości 1G/2.5G/5.0G.
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. Maksymalne zużycie energii nie może przekraczać 17W przy wykorzystaniu wszystkich funkcji urządzenia.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
 - a. Tunnel,
 - b. Bridge,

- c. Mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
 - a. MIMO – 2x2,
 - b. Wymagana przepustowość dla poszczególnych modułów radiowych:
 - i. min. 688 Mbps;
 - ii. min. 2882 Mbps;
 - iii. min. 5765 Mbps;
 - c. Wymagana moc nadawania:
 - i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
 - ii. min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
 - iii. min. 22 dBm dla pasma 6GHz z możliwością zmiany co 1dBm
 - d. Wsparcie dla kanałów 20/40/80/160/320MHz,
 - e. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5dBi dla pasma 6GHz.
 - f. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy.
 - g. Każdy z modułów radiowych musi posiadać możliwość pracy jako dedykowany skaner.
12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 256.
13. Funkcje dodatkowe:
 - a. OFDMA UL i DL
 - b. Spatial Reuse (BSS Coloring)
 - c. UL-MU-MIMO
 - d. DL-MU-MIMO
 - e. Enhanced Target Wake Time (TWT)
 - f. Wbudowany analizator widma
 - g. Wbudowane mechanizmy WIPS/WIDS

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.

15. S02. NGFW (Next Gen FireWall) – licencje - typ I

Cecha/Funkcjonalność	Minimalne parametry wymagane przez Zamawiającego
Licencje dostępne	
Licencje dostępne – 50 sztuk	1. W ramach postępowania musi zostać dostarczone co najmniej 50 tokenów programowych współpracujących z posiadanym przez Zamawiającego urządzeniem FortiGate, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów oraz w ramach połączeń VPN typu client-to-site. 2. Wsparcie dla tokenów programowych (software token) dla

	takich systemów operacyjnych jak iOS, Android oraz Windows 10 Mobile. 3. Dla tokenów na system iOS i Android wymaga się: • aktywacji z systemu firewall FortiGate • generowania kodu (cyfr) co 30 lub 60 sekund, • możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), • ochrony dostępu poprzez konfigurowalny kod PIN.
--	---

16. S02. NGFW (Next Gen FireWall) wraz z integralnym O18. Oprogramowanie WAF (Web Application Firewall) – typ II – 3 sztuki

Wymagania ogólne	Zamawiający wymaga dostarczenia 3 sztuk licencji na okres 12 miesięcy do posiadanych urządzeń Fortinet Fortigate 40F. 1. Dostarczone licencje muszą: a) być fabrycznie nowe, b) pochodzić z autoryzowanego kanału sprzedaży producenta, c) być przeznaczone do użytkowania na terenie Unii Europejskiej, d) umożliwiać rejestrację na koncie Zamawiającego, e) zapewniać bieżące aktualizacje sygnatur bezpieczeństwa i dostęp do aktualizacji firmware. 2. Zamawiający wymaga dostarczenia poniższych licencji: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Weryfikacja zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia) na okres 12 miesięcy. b) Identyfikację urządzeń OT/ICS, wykrywanie zasobów przemysłowych, segmentację ruchu sieciowego, monitorowanie protokołów przemysłowych, takich jak Modbus TCP, Siemens S7, PROFINET, MQTT, możliwość definiowania polityk bezpieczeństwa dla środowisk OT, automatyzację reakcji na incydenty bezpieczeństwa, minimalizację ryzyka zakłóceń PLC/SCADA na okres 12 miesięcy. c) Zarządzanie urządzeniami bezpieczeństwa, możliwość grupowania urządzeń, zarządzanie konfiguracją urządzeń, wykonywanie kopii zapasowych konfiguracji, centralne zbieranie logów, podgląd zdarzeń bezpieczeństwa, generowanie alarmów i powiadomień, dashboardsy bezpieczeństwa, możliwość wyszukiwania i filtrowania logów, raportowanie incydentów bezpieczeństwa, możliwość eksportu raportów, wspieranie segmentacji środowisk przemysłowych, uwierzytelnianie wieloskładnikowe (MFA), role administracyjne RBAC, szyfrowanie transmisji danych, rejestrowanie działań administratorów, możliwość integracji z usługami katalogowymi na okres 12 miesięcy. Rozwiązanie musi zapewniać: przechowywanie logów w chmurze, możliwość retencji danych przez minimum 365 dni. Wykonawca zobowiązany jest do dostarczenia kluczy/licencji w formie elektronicznej lub aktywacji licencji na koncie Zamawiającego, wskazania numerów subskrypcji/licencji oraz dostarczenia dokumentów
------------------	---

	potwierdzających legalność pochodzenia licencji.
--	--

17. S02. NGFW (Next Gen FireWall) wraz z integralnym O18. Oprogramowanie WAF (Web Application Firewall) – typ III - 2 szt

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastr Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

- 4 portami Gigabit Ethernet RJ-45.
- 2. System Firewall posiada wbudowany port konsoli szeregowej.
- 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- 4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 500 tys. jednoczesnych połączeń oraz 25 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 3 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 750 Mbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 450 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - OpenStack.
 - VMware NSX.
 - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łącz WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv6), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub

licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.

8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.
7. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.

4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wymagane są stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.
3. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
4. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
5. Możliwość włączenia logowania per reguła w polityce firewall.
6. System zapewnia możliwość logowania do serwera SYSLOG.
7. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

- a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/ domen, Weryfikacja zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia) na okres 12 miesięcy.
- b) Ochrona systemów przemysłowych SCADA na okres 12 miesięcy.
- c) Logowanie i raportowanie w oparciu o usługę realizowaną w chmurze, z czasem retencji logów minimum 1 rok, na okres 12 miesięcy

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne.

18. S02. NGFW (Next Gen FireWall) uwzględniające integralnie O18. Oprogramowanie WAF w ramach pełnionej funkcji – licencje – typ IV

Serwisy i licencje	1. Licencje do posiadanych już przez Zamawiającego – urządzeń FortiGate 100F – 2 szt 2. Dwie dostarczone licencje muszą: a) być fabrycznie nowe, b) pochodzić z autoryzowanego kanału sprzedaży producenta, c) być przeznaczone do użytkowania na terenie Unii Europejskiej, d) umożliwiać rejestrację na koncie Zamawiającego, e) zapewniać pełną kompatybilność z urządzeniem klasy FortiGate 100F f) zapewniać bieżące aktualizacje sygnatur bezpieczeństwa i dostęp do aktualizacji firmware. 3. Zamawiający wymaga dostarczenia poniższych licencji: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Weryfikacja zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia) na okres 12 miesięcy. b) Identyfikację urządzeń OT/ICS, wykrywanie zasobów przemysłowych, segmentację ruchu sieciowego, monitorowanie protokołów przemysłowych, takich jak Modbus TCP, Siemens S7, PROFINET, MQTT, możliwość definiowania polityk bezpieczeństwa dla środowisk OT, automatyzację reakcji na incydenty bezpieczeństwa, minimalizację ryzyka zakłóceń PLC/SCADA na okres 12 miesięcy. c) Zarządzanie urządzeniami bezpieczeństwa, możliwość grupowania urządzeń, zarządzanie konfiguracją urządzeń, wykonywanie kopii zapasowych konfiguracji, centralne zbieranie logów, podgląd zdarzeń bezpieczeństwa, generowanie alarmów i powiadomień, dashboardy bezpieczeństwa, możliwość wyszukiwania i filtrowania logów, raportowanie incydentów bezpieczeństwa, możliwość eksportu raportów, wspieranie segmentacji środowisk przemysłowych, uwierzytelnianie wieloskładnikowe (MFA), role administracyjne RBAC, szyfrowanie transmisji danych, rejestrowanie działań administratorów, możliwość integracji z usługami katalogowymi na okres 12 miesięcy. Rozwiązanie musi zapewniać: przechowywanie logów w chmurze, możliwość retencji danych przez minimum 365 dni. Wykonawca zobowiązany jest do dostarczenia kluczy/licencji w formie elektronicznej lub aktywacji licencji na koncie Zamawiającego, wskazania numerów subskrypcji/licencji oraz dostarczenia dokumentów potwierdzających legalność pochodzenia licencji.
Gwarancja	System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Dwa rozszerzenie licencji – o system zarządzania zdalnym dostępem VPN i ochrony dla stacji roboczych wraz z serwerem centralnego zarządzania.

W ramach postępowania wymagany jest dostarczenie rozwiązania do zarządzania konfiguracją dostępu VPN i ochrony dla stacji roboczych wraz z mechanizmami centralnego zarządzania.

Dostarczone rozwiązanie musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się, aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.

Parametry systemu zarządzania dostępem VPN i ochrony dla stacji roboczych.

1. Elementy systemu zarządzania dostępem i ochrony dla stacji roboczych muszą zawierać następujące funkcje i mechanizmy:
 - 1) Kontrola antywirusowa
 - Mechanizmy Anti-Ransomware pozwalające na behawioralne wykrywanie podejrzanej aktywności złośliwego oprogramowania typu Ransomware
 - Mechanizm Antiexploit pozwalający na ochronę popularnych aplikacji przed atakami typu 0-day
 - Możliwość blokowania podejrzanych adresów URL i niebezpiecznych stron
 - Mechanizmy antywirusowe oparte o:
 - Sygnaturach aktualizowanych min. co godzinę
 - Baz reputacji plików opartych o funkcję skrótu dostępnych on-line i działających w czasie rzeczywistym
 - Możliwość integracji z systemami typu sandbox w chmurze oraz on-prem, wraz z możliwością zarówno wysyłania plików jak i korzystania z informacji o wykrytych zagrożeniach
 - 2) Kategoryzacja URL
 - URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.
 - Możliwość integracji z wtyczką do przeglądarki internetowej, celem analizy kategorii WWW dla ruchu SSL/HTTPS
 - 3) Analiza podatności
 - Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.
 - Mechanizmy pozwalające na wymuszenie aktualizacji systemu lub popularnych aplikacji
 - 4) Dostęp VPN
 - Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
 - Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
 - Rozwiązanie musi umożliwiać realizowanie funkcjonalności split tunneling w oparciu o aplikacje, przykładowo musi istnieć możliwość wykluczenia aplikacji wymagających dużej ilości pasma np.: Microsoft Office 365, Microsoft Teams, Skype, GoToMeeting, Zoom, WebEx, YouTube
 - Rozwiązanie musi umożliwiać realizowanie funkcjonalności split tunneling w oparciu o domeny (FQDN)
 - Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.
 - Mechanizmy uwierzytelniania dwuskładnikowego.
 - System musi umożliwiać zastosowanie protokołu SAML dla SSL VPN
2. Funkcjonalność kontroli i blokowania urządzeń USB
3. Kontrola ruchu sieciowego
 - 1) Kontrola ruchu sieciowego pochodzącego z aplikacji - w oparciu o wbudowany Firewall aplikacyjny.

4. Centralne logowanie i raportowanie
 - 1) System musi umożliwiać wysyłanie logów ze stacji roboczych do centralnego systemu logowania i raportowania
5. Centralne zarządzanie
 - 1) System musi umożliwiać centralne zarządzania stacjami roboczymi
6. Poszczególne mechanizmy muszą być dostępne dla następujących wersji systemów operacyjnych Windows oraz Mac OS: Microsoft Windows 11 (64-bit), Microsoft Windows 10 (32-bit, 64-bit), Windows Server 2022, Windows Server 2019, Mac OS X v15, OS X v14, OS X v13.

Parametry systemu centralnego zarządzania.

1. Wymaga się aby elementy wchodzące w skład systemu centralnego zarządzania były dostarczone w postaci oprogramowania jako usługi (ang. software as a service, w skrócie SaaS).
2. System powinien umożliwiać automatyczną aktualizację oprogramowania na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall, Sandbox
3. Ponadto wymagane jest aby system zapewniał:
 - 3.1. Integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD.
 - 3.2. Definiowanie różnych profili (wersji konfiguracji) dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie.
 - 3.3. Zautomatyzowany proces zarządzania aplikacją kliencką.
 - 3.4. Przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS, w których administrator może określić komponenty instalatora dla stacji roboczych przynajmniej takie jak :
 - filtrowanie URL,
 - analiza podatności,
 - application firewall
 - antywirus
 - 3.5. Możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym.
 - 3.6. Panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych.
 - 3.7. Panel w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych: System musi umożliwiać wyświetlanie w konsoli zarządzania informacji o stacjach roboczych, które mogą służyć do diagnozy problemów oraz stanu stacji min:
 - Typ połączenia (Ethernet/Wifi)
 - Adres IP
 - Adres IP domyślnej bramy
 - Adres MAC
 - Adres MAC bramy sieciowej
 - Nazwa sieci WiFi (SSID)
 - Model sprzętu
 - Producent sprzętu
 - Informacje o procesorze
 - Informacje o pamięci RAM
 - Numer seryjny
 - Informacje o dysku twardym (rozmiar)
 - 3.8. Możliwość wymuszenia aktualizowania systemu i aplikacji z racji wykrytych podatności na stacjach roboczych.
 - 3.9. Automatyczne wykrywanie stacji klienckich w grupach roboczych.
 - 3.10. System musi umożliwiać określanie czy dana stacja znajduje się w wewnętrznej sieci chronionej, czy poza nią, na podstawie reguł budowanych w oparciu cechy :
 - Parametrów DHCP

- Serwerów DNS
 - Połączenia ze stacją zarządzającą
 - Adresacją sieci
 - Bramą domyślną (Default Gateway) (adres IP lub adres MAC)
 - Publiczny adres IP
 - Tunel VPN
 - Dostępny IP za pomocą PING
 - Typ połączenia (Ethernet lub WiFi)
- 3.11. Reguły określające czy stacja należy do sieci zaufanej muszą być budowane w oparciu o różne kombinacje powyższych parametrów
- 3.12. Reguły muszą pozwalać na przydzielenie różnych profili bezpieczeństwa zależnie od określenia przynależności do sieci zaufanej
- 3.13. Logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcją filtrów oraz możliwością pobierania logów przez administratora.
- 3.14. Generowanie alarmów: związanych z zarządzaniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach.
- 3.15. Definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcją przypisywania uprawnień do elementów panelu konfiguracyjnego.
- 3.16. Zarządzanie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN.
- 3.17. Automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji.
- 3.18. Możliwość przeniesienia stacji/urządzenia do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi.
- 3.19. Możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie,
- 3.20. Możliwość skonfigurowania weryfikacji zgodności (posture check) w celu sprawdzenia czy na stacji końcowej jest:
- Uruchomiony AV i ma zaktualizowaną bazę ,
 - Zainstalowana odpowiednia wersja systemu operacyjnego,
 - Uruchomiony odpowiedni proces,
 - Zainstalowany odpowiedni Certyfikat,
 - Odpowiedni wpis w rejestrach systemowych,
 - Stworzony odpowiedni plik,
 - Użytkownik zalogowany do konkretnej domeny AD,
- 3.21. Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system.
- 3.22. Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne.

Licencje oraz serwisy.

W ramach postępowania wraz z konsolą centralnego zarządzania muszą zostać dostarczone niezbędne licencje upoważniające do:

1. Zainstalowania i centralnego zarządzania minimum 50 licencji aplikacjami klienckimi na stacjach roboczych przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
2. Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować funkcjonalności:

- a. Filtrowanie adresów URL oraz filmów wideo
- b. Możliwość zarządzania stacjami roboczymi i profilami SSL i IPsec VPN
- c. Możliwość wykonywania analizy podatności systemów operacyjnych i zainstalowanych aplikacji
- d. Centralne zarządzanie
- e. Centralne logowanie i raportowanie

19. U09. Wdrożenie urządzeń oraz oprogramowania – z pozycji 1-18 - oprogramowania/rozwiązania z zakresu bezpieczeństwa.

Wdrożenie obejmuje:

- U39. Usługi konfiguracji i hardeningu systemów/urządzeń IT/OT/ICS/IIoT,
- U41. Usługa segmentacji sieci IT/OT/ICS/IIoT,

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 urządzeń do sieci LAN Zamawiającego
- instalacja i konfiguracja serwerów
- instalacja i konfiguracja przełączników LAN
- instalacja i konfiguracja NGFW
- wykonanie weryfikacji prawidłowego działania dostarczonych urządzeń oraz oprogramowania
- instalacja i konfiguracja serwerów
- instalacja i konfiguracja macierzy dyskowej
- instalacja i konfiguracja NAS
- Instalacja i konfiguracja oprogramowania oraz rozwiązań typu NGFW
- Konfiguracja kopii zapasowej

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.

System centralnego gromadzenia logów zostanie wdrożony w zakresie dostarczanych komponentów sprzętowo-programowych wraz z instruktażem zdalnym, z administracji systemem, obejmującym m.in. zagadnienia dotyczące podłączania źródeł bezagentowych (np. syslog)

20. Dostawa i wdrożenie platformy XDR oraz świadczenie usługi zarządzania cyberbezpieczeństwem SOC/MDR z wykorzystaniem wdrożonego rozwiązania XDR.

W skład pozycji wchodzi:

- O35. Oprogramowanie do badania podatności systemów informatycznych | Pakiet uzupełniających się rozwiązań: Oprogramowanie do badania podatności systemów informatycznych, do zarządzania podatnościami
- O12. Oprogramowanie typu EDR (Endpoint Detection and Response) | Pakiet uzupełniających się rozwiązań: System typu EDR, Oprogramowanie antywirusowe
- O14. Oprogramowanie typu NDR (Network Detection & Response) | System typu NDR
- Usługa typu MDR (Managed Detection and Response) IT/OT/ICS/IIoT | Usługa typu MDR (Managed Detection and Response)
- U12. Usługa SOC (Security Operation Center) IT/OT/ICS/IIoT | Pakiet uzupełniających się rozwiązań: Usługa SOC (Security Operation Center), Usługi reagowania na incydenty w środowisku IT/OT/ICS, Analiza i zabezpieczanie dowodów cyfrowych

Szczegółowy opis:

1. Usługa zarządzania cyberbezpieczeństwem musi być świadczona przez okres 12 miesięcy.
2. Usługa zarządzania cyberbezpieczeństwem musi być świadczona przez Wykonawcę w czasie rzeczywistym, w trybie ciągłym 24 godziny na dobę, 7 dni w tygodniu, przez 365 dni w roku (24/7/365).
3. Wykonawca, w terminie uzgodnionym z Zamawiającym, zobowiązany jest do przeprowadzenia analizy przedwdrożeniowej oraz rozruchu usługi zarządzania cyberbezpieczeństwem. W ramach tych działań Wykonawca zobowiązany jest do:
 - 3.1. dostosowania i uzgodnienia z Zamawiającym zasad współpracy;
 - 3.2. identyfikacji urządzeń końcowych (stacji roboczych i serwerów), które zostaną objęte usługą zarządzania cyberbezpieczeństwem;
 - 3.3. opracowania reguł bezpieczeństwa, klasyfikacji incydentów oraz scenariuszy reakcji;
 - 3.4. wdrożenia systemu zapewniającego kompleksową ochronę przed zagrożeniami w technologii Extended Detection & Response (XDR), o którym mowa w „9.Wymagania dla systemu XDR”:

Zamawiający wymaga dostarczenia licencji systemu XDR obejmującego ochroną 110 urządzeń końcowych na okres 12 miesięcy.
 - 3.5. zainstalować i skonfigurować na stacjach roboczych i serwerach dostarczane oprogramowanie

XDR, w tym przenieść wszystkie polityki bezpieczeństwa z obecnie użytkowanego oprogramowania antywirusowego;

3.6. przeprowadzić min. jednodniowy instruktaż z dostarczonego systemu XDR dla personelu IT Zamawiającego.

3.7. Zakończenie analizy przedwdrożeniowej i rozruchu usługi zarządzania cyberbezpieczeństwem zostanie potwierdzone protokołem odbioru.

4. Wykonawca zobowiązany jest do zapewnienia pełnego wsparcia eksperckiego, merytorycznego i administracyjnego w zakresie realizacji przedmiotu zamówienia, zgodnie z najlepszymi praktykami i zgodnie z najnowszymi wytycznymi branżowymi i technologicznymi w tym zakresie, jak również wytycznymi z audytów przeprowadzanych przez instytucje zewnętrzne, którym podlega Zamawiający przez cały okres obowiązywania umowy.
5. Wykonawca zobowiązany jest do udostępnienia Zamawiającemu stałego dostępu do dedykowanego panelu klienta, w celu bezpośredniego monitorowania i weryfikowania parametrów infrastruktury teleinformatycznej objętej usługą zarządzania cyberbezpieczeństwem.
6. Wykonawca zobowiązany jest do instruktażu 2 administratorów Zamawiającego z administrowania i obsługi dostarczonego systemu XDR. Zakres instruktażu musi przygotować administratorów do pełnego wykorzystania funkcjonalności systemu XDR. Forma instruktażu zostanie ustalona podczas analizy przedwdrożeniowej.
7. Wykonawca musi monitorować oraz reagować na incydenty bezpieczeństwa na podstawie alarmów z wdrożonego systemu XDR, a także zintegrowanych z nim, na etapie wdrożenia, innych systemów cyberbezpieczeństwa.
8. Wykonawca zobowiązany jest do dostarczenia i wdrożenia systemu XDR wraz dokumentacją powykonawczą oraz wsparciem technicznym producenta na cały okres świadczenia Usługi zarządzania cyberbezpieczeństwem.
9. Wymagania dla systemu XDR:

W ramach Usługi Wykonawca dostarczy, wdroży i będzie utrzymywał system zapewniający kompleksową ochronę przed zagrożeniami przy użyciu następujących funkcjonalności: Endpoint Detection & Response, Endpoint Protection Platform, Network Detection & Response, ochrona tożsamości, Extended Detection and Response, Security Orchestration Automation and Response, technologia deprecji, ochrona poczty e-mail, filtrowanie domen, filtrowanie treści webowych, zarządzanie stanem zabezpieczeń w chmurze i aplikacjach SaaS, zarządzanie zewnętrznym obszarem podatnym na ataki cybernetyczne, zarządzanie stanem zabezpieczeń punktów końcowych, centralne zarządzanie logami, analiza behawioralna użytkowników, wbudowana usługa MDR działająca 24/7/365.

Który:

- 9.1. musi zapewniać centralne zarządzanie ochroną wszystkich typów urządzeń końcowych (stacje robocze, serwery) i automatyzację reakcji na incydenty;
- 9.2. musi umożliwiać wdrożenie we wszystkich trzech modelach: cloud (SaaS), on-premise oraz hybrydowo;
- 9.3. musi zapewniać centralną konsolę zarządzającą, dostępna przez przeglądarkę, wspierać autentykację wieloskładnikową (MFA) i mechanizm pojedynczego logowania (SSO) oraz granularne role i uprawnienia, jak również integrację z Active Directory;
- 9.4. musi obsługiwać automatyczne wykrywanie i instalowanie agentów na nowych urządzeniach oraz

zapewniać szybkie, bezobsługowe wdrożenie aktualizacji (bez potrzeby restartów);

- 9.5. musi zapewniać możliwość komunikacji przez publiczne API;
- 9.6. musi zapewniać integrację z narzędziami do monitorowania, analizowania i reagowania na zagrożenia w czasie rzeczywistym klasy SIEM;
- 9.7. musi zapewniać możliwość zdalnego monitorowania i zarządzania Remote Monitoring and Management (RMM);
- 9.8. musi zapewniać możliwość integracji z platformami certyfikacji bezpieczeństwa dla sprzętu, oprogramowania i urządzeń Internetu Rzeczy (IoT) Platform Security Architecture (PSA);
- 9.9. musi natywnie oferować, bez konieczności dokupywania modułów zewnętrznych:
 - a. możliwość instalacji agenta ochrony na następujących systemach operacyjnych: Windows XP, Windows 7 i nowsze, Windows Server od 2008 R2 i nowsze, każda wiodąca dystrybucja Linux (wg. W3Techs), macOS (Intel & Apple Silicon);
 - b. kompleksową ochronę przed szeroką gamą zagrożeń, obejmującą: wirusy, ransomware, oprogramowanie szpiegujące (spyware), oprogramowanie typu rootkit, cryptominers, ataki typu fileless, exploits (w tym ataki na krytyczne komponenty OS), narzędzia hakerskie, phishing;
 - c. wsparcie zaawansowanej heurystyki oraz uczenia maszynowego do analizy zachowania, a także dynamiczną analizę podejrzanych plików w czasie rzeczywistym (sandbox), umożliwiającą wykrywanie także zagrożeń typu zero-day;
 - d. rozbudowane mechanizmy analizy zachowań użytkowników (User & Behavioral Analytics), wykrywania ruchu lateralnego (lateral movement), automatycznej detekcji anomalii oraz pełną widoczność ruchu procesów, plików, rejestru, systemu i sieci (detection living-off-the-land);
 - e. wbudowane mechanizmy automatycznej reakcji na incydenty, w tym: izolacja stacji lub hosta, blokowanie kont użytkowników, natychmiastowe zamykanie procesów, kwarantanna plików, przywrócenie stanu systemu sprzed incydentu (rollback);
 - f. możliwość blokowania urządzeń (device control) podłączanych za pomocą USB;
 - g. zaawansowany threat hunting, możliwość eksportu i importu wskaźników kompromitacji IOC, integrację z syslog, SIEM oraz publiczne API dla zarządzania i automatyzacji;
 - h. natywne mechanizmy deception, czyli: fałszywe pliki, pułapki na hostach i endpointach, pułapki w sieci lokalnej, honeypoty;
 - i. pełną kompatybilność i koegzystencję z innym legalnie wykorzystywanym w organizacji oprogramowaniem antywirusowym lub zabezpieczającym;
- 9.10. musi umożliwiać wykrywanie, blokowanie i automatyczną reakcję na poniższe techniki, bazując na MITRE ATT&CK, musi umożliwiać korelację poniższych technik, ich wizualizację, automatyzację reakcji oraz pełną dokumentację incydentów z poziomu jednej konsoli:
 - a. wykrywanie oraz blokowanie prób pozyskania credentiali przy nieszyfrowanych poświadczeniach (Unsecured Credentials);
 - b. pełne monitorowanie procesów, wykrywanie prób enumeracji i blokowanie nieautoryzowanego dostępu do informacji o uruchomionych procesach (Process Discovery);
 - c. blokowanie prób wyłączania kluczowych usług i komponentów systemowych (Service Stop);
 - d. wykrywanie i blokowanie interpretatorów komend/skryptów (np. PowerShell, WMI, Bash, CMD) i

ich szkodliwego użycia (Command and Scripting Interpreter);

- e. wykrywanie prób automatycznego zbierania danych na stacjach (Automated Collection);
 - f. detekcja prób automatyzowanej eksfiltracji danych (Automated Exfiltration);
 - g. wykrywanie i blokowanie prób wycieku danych przez kanały Command & Control np. HTTP/S, DNS, ICMP (Exfiltration Over C2 Channel);
 - h. analiza i alertowanie obfuskacji plików, kodu, informacji (Obfuscated Files or Information);
 - i. detekcja prób obejścia narzędzi bezpieczeństwa (Debugger Evasion);
 - j. monitoring i detekcja prób enumeracji użytkowników systemowych (System Owner/User Discovery);
 - k. kontrola oraz widoczność zmian i zapytań do konfiguracji sieciowej systemów (System Network Configuration Discovery);
 - l. detekcja prób zbierania informacji o systemie/hostach (System Information Discovery);
 - m. identyfikacja i blokowanie niestandardowych mechanizmów uruchamiania, blokada rozwiązań typu guardrail (Execution Guardrails);
 - n. monitoring kluczy rejestru przechowujących dane uwierzytelniające (Credentials in Registry);
 - o. alertowanie przy enumeracji plików i folderów (File and Directory Discovery);
 - p. wykrywanie i blokowanie prób wyłączania/omijania zabezpieczeń (Impair Defenses);
 - q. analiza, wykrywanie i blokowanie nadużycia legalnych (valid) kont (Valid Accounts);
 - r. wykrywanie oraz blokowanie destrukcji danych (Data Destruction);
 - s. detekcja i blokowanie działania ransomware oraz szyfrowania masowego plików (Data Encrypted for Impact);
 - t. monitoring i zapobieganie czyszczeniu śladów/logów przez atakujących (Indicator Removal on Host);
- 9.11. Wymaga się, aby oferowane rozwiązanie bezpieczeństwa wykazało skuteczność potwierdzoną w niezależnych badaniach MITRE ATT&CK Evaluations Enterprise, z roku 2024 lub nowszym, na poziomie co najmniej:
- a. 98% skuteczności w zakresie Detection Visibility (widoczność/detekcja wszystkich kroków ataku),
 - b. 98% skuteczności w zakresie Protection Rate (blokowanie złośliwych kroków ataku),
 - c. 98% skuteczności w zakresie Prevention (blokowanie ataków na etapie pierwszych kroków).

Dostawca musi przedłożyć oficjalne materiały producenta lub raporty z MITRE ATT&CK Evaluations potwierdzające spełnienie powyższych progów.

- 9.12. musi zapewnić ochronę offline, czyli zachowanie kluczowych funkcji nawet bez stałego połączenia z serwerem zarządzającym;

- 9.13. musi posiadać wbudowany system decepcji który umożliwia:

- a. automatyczne generowania pułapek będących imitacją endpointów i serwerów i automatyczny sygnał ostrzegawczy po wejściu lub aktywności atakującego na takim deceptive node;
 - b. umieszczanie plików-pułapek zachęcających do kradzieży, z funkcją monitorowania akcji i generowania alertów;
 - c. system powiadomień i automatycznej reakcji po każdej nieuprawnionej próbie dostępu;
 - d. tworzenie kont użytkowników-pułapek, monitorowanie prób logowania oraz wszelkich interakcji z tymi kontami;
 - e. wykorzystanie deception do szybkiej identyfikacji lateral movement i prób eskalacji uprawnień przez atakującego;
- 9.14. musi zapewniać File Integrity Monitoring (FIM) – egzekwowanie polityk w zakresie zmiany plików/zasobów;
- 9.15. musi zapewniać możliwość szybkiej weryfikacji podatności na poziomie punktów końcowych, łącznie z wykrywaniem i naprawą błędnych konfiguracji punktów końcowych oraz wykrywaniem podatnych aplikacji w na poziomie punktów końcowych,
- 9.16. musi zapewniać wykrywanie skanowania sieci: detekcja aktywności skanowania na poziomie segmentu sieci oraz hosta, wykrywanie prób identyfikacji usług, portów oraz rozpoznawanie różnych technik skanowania (szybkie, wolne, rozproszone);
- 9.17. musi zapewniać wykrywanie zatrufania sieci: monitoring prób zatrufania tablic ARP, wykrywanie ataków typu DNS spoofing, technik man-in-the-middle, identyfikacja podszywania się pod urządzenia lub serwery w sieci;
- 9.18. musi zapewniać wykrywanie tunelowania eksfiltracji: identyfikacja nietypowego, tunelowanego ruchu mającego na celu eksfiltrację (DNS tunneling, ICMP tunneling, HTTP/S tunneling), alertowanie przy transferze danych do nieautoryzowanych lokalizacji oraz detekcja długotrwałych i ukrytych połączeń;
- 9.19. musi zapewniać zarządzanie i reagowanie poprzez moduł NDR dostępny z poziomu tej samej konsoli zarządzającej;
- 9.20. musi zapewniać zaawansowane zarządzanie zasobami sprzętowymi i programowymi (asset management), risk scoring (ocena ryzyka każdego składnika);
- 9.21. musi zapewniać pełny logging oraz retencje danych zgodnie z wymogami Zamawiającego (integracja z SIEM, IOC, threat hunting);
- 9.22. musi zapewniać możliwość zaawansowanej i personalizowanej automatyzacji reakcji na incydenty (predefiniowane oraz własne playbooks);
- 9.23. musi oferować tzw. lekkiego agenta - agent na endpointy nie powinien zużywać więcej niż 250MB RAM oraz 5% CPU;
- 9.24. musi zapewniać granularne role/uprawnienia administracyjne, możliwość blokowania zmian ustawień przez użytkowników;
- 9.25. musi zapewniać, że Wszystkie metadane, telemetria, logi i dane użytkownika muszą być przechowywane wyłącznie na terytorium Unii Europejskiej – zgodnie z RODO i normami UE. M
- 9.26. musi posiadać pełną dokumentację licencyjną i wdrożeniową w języku polskim lub angielskim.

10. Wykonawca zobowiązany jest do monitorowania incydentów, zdarzeń i anomalii z dostarczonego systemu XDR, a także zintegrowanych z nim, na etapie wdrożenia, innych systemów cyberbezpieczeństwa.
11. Wykonawca zobowiązany jest do analizy incydentów według procedur uzgodnionych z Zamawiającym.
12. Wykonawca zobowiązany jest do obsługi incydentów zgodnie z ustalonymi z Zamawiającym scenariuszami reakcji, w tym ich kategoryzacji i priorytetyzacji.
13. Wykonawca zobowiązany jest do klasyfikacji wykrytych lub zgłoszonych incydentów według następujących kategorii:
 - 13.1. Incydenty krytyczne – powodujące poważne zakłócenia lub przerwanie ciągłości operacyjnej Zamawiającego w obszarach krytycznych;
 - 13.2. Incydenty niekrytyczne – pozostałe incydenty niezaliczane do kategorii krytycznych;
 - 13.3. False positive – błędne detekcje lub zgłoszenia, które nie wymagają reakcji zgodnie z umową, tj. nie stanowią rzeczywistego incydentu bezpieczeństwa.
14. Za podjęcie incydentu uznaje się rozpoczęcie działań przez operatora usługi zarządzania bezpieczeństwem, polegających na jego segregacji oraz analizie. Terminy reakcji i realizacji są następujące:
 - 14.1. Incydent Krytyczny: reakcja do 2 godzin,
 - 14.2. Incydent Niekrytyczny: reakcja do 4 godzin,
15. Wykonawca zobowiązany jest do obsługi zdarzeń i incydentów zgodnie z najlepszymi praktykami branżowymi z uwzględnieniem właściwego nadania priorytetów.
16. Wykonawca zobowiązany jest do przysyłania comiesięcznych raportów z wykonanych działań. Raporty będą przysyłane na adres e-mail wskazany w umowie. Wzór raportu zostanie opracowany wspólnie przez Zamawiającego i Wykonawcę na etapie analizy przedwdrożeniowej i rozruchu usługi zarządzania bezpieczeństwem.
17. W zakresie świadczenia usługi zarządzania bezpieczeństwem Wykonawca:
 - 17.1. musi monitorować i reagować na incydenty bezpieczeństwa w trybie ciągłym (24/7/365) z systemu XDR, a także zintegrowanych z nim, na etapie wdrożenia, innych systemów cyberbezpieczeństwa, w szczególności uwzględniać:
 - a. powiadomienia o zagrożeniach ze stacji roboczych oraz serwerów, w szczególności generowanych z narzędzi ochrony,
 - b. powiadomienia o dezaktywacji narzędzi bezpieczeństwa na danym urządzeniu końcowym;
 - c. zdarzenia związane z modyfikacją mechanizmów harmonogramu w systemach operacyjnych;
 - d. zdarzenia związane z modyfikacją dzienników zdarzeń i dzienników systemowych;
 - e. zdarzenia dotyczące integralności plików mogące świadczyć o zainfekowaniu oprogramowaniem złośliwym;
 - 17.2. musi dokonywać wstępnej oceny zdarzeń, analizy i obsługi incydentów w zakresie posiadanych kompetencji, zgodnie z ustalonymi scenariuszami reakcji;
 - 17.3. musi kontaktować się z Zamawiającym w przypadku konieczności dokonania zmian w infrastrukturze, niezbędnych do eliminacji przyczyny incydentu;

- 17.4. musi eskalować incydent zgodnie z ustalonym scenariuszem reakcji z wykorzystaniem ustalonych kanałów komunikacji;
- 17.5. musi dokumentować wykonane czynności zgodnie z przygotowanymi i zaakceptowanymi scenariuszami reakcji;
- 17.6. musi przygotowywać miesięczne raporty wykrytych zdarzeń bezpieczeństwa;
- 17.7. musi dostosowywać polityki bezpieczeństwa systemów XDR, SIEM oraz NDR, celem dostosowania ich do skuteczniejszego wykrywania zagrożeń.
- 17.8. musi zapewnić dostępność zespołu serwisowego 12/5, świadczącego usługę wsparcia przy usuwaniu awarii systemów XDR, SIEM oraz NDR, w tym:
 - a. wsparcie telefoniczne zespołu inżynierów;
 - b. pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji urządzeń;
 - c. doradztwo w zakresie konfiguracji;
 - d. zdalne wsparcie techniczne;
 - e. pomoc w zakładaniu zgłoszeń serwisowych u producenta;
 - f. przegląd konfiguracji;
 - g. zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta;
 - h. konfiguracja polityk bezpieczeństwa

21. Dostawa i wdrożenie oprogramowania klasy SIEM wraz z gwarancją i wsparciem technicznym.

W skład pozycji wchodzi:

- O14. Oprogramowanie typu NDR (Network Detection & Response)
- O19. Oprogramowanie SIEM (Security Information and Event Management) | Pakiet uzupełniających się rozwiązań: System typu SIEM, Menadżer logów, Oprogramowanie do monitorowania infrastruktury informatycznej

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

1.1 Systemy Zamawiającego wymagające monitorowania

System SIEM będący przedmiotem zamówienia, musi zbierać logi/dane z poniższych elementów infrastruktury IT: Active Directory, Windows Server, Linux Server, Stacje robocze (Windows oraz Linux), DNS, DHCP, Systemy bezpieczeństwa np.: agent antywirusowy, Web Application Firewall, NAC, DLP, EDR, Serwer poczty, system antyspamowy, Firewall/UTM, IPS/IDS, VPN, Przełączniki sieci LAN, punkty dostępowe WiFi.

1.2 Wymagania dla Systemu Zbierania i Analizy Logów oraz Systemu SIEM.

- a) W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
- b) Rozwiązanie musi zostać dostarczone w postaci maszyn wirtualnej instalowanych w środowisku Vmware lub Windows Hyper-V
- c) Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach.
- d) Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.
- e) Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.
- f) Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.
- g) Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.
- h) Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.
- i) Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).
- j) Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.
- k) Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.
- l) Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).
- m) Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.
- n) Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeolP).
- o) Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów).
- p) Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.
- q) Rozwiązanie musi umożliwiać tworzenie statycznych raportów.
- r) Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF.
- s) Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.
- t) Rozwiązanie musi umożliwiać tworzenie własnych raportów.
- u) Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.
- v) Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.
- w) System zbierania logów musi wspierać hiperwizory: Vmware ESXi, Microsoft Hyper-V oraz Proxmox VE.

1.3 Wymagania dla Systemu SIEM.

- a) W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące incydenty na urządzeniach sieciowych Zamawiającego
- b) Rozwiązanie musi w pełni realizować swoją funkcjonalność lokalnie (instalacja on-prem)
- c) Architektura rozwiązania musi być oparta o fizyczne lub wirtualne sondy monitorujące, których rolą jest odbieranie kopii ruchu sieciowego, generowanie alarmów oraz/lub metadanych o zdarzeniach, przygotowanie przechwyconych plików do dalszej analizy oraz przekazywanie przetworzonych danych do urządzenia administracyjnego.

- d) Architektura rozwiązania musi być oparta także o fizyczne urządzenie administrujące, którego rolą jest zarządzanie sondami, włącznie z regułami detekcji, sygnaturami i nadzorem stanu, dogłębna analiza odebranych plików, prezentacja wyników detekcji, a także przekazywanie danych do rozwiązań stron trzecich.
- e) Platformy muszą obsługiwać szyfrowanie dysków.
- f) Rozwiązanie musi wspierać implementację na środowisku wirtualnym takim jak m.in. VMWare, Hyper-V, Proxmox VE, KVM, OVM, OVF.
- g) Konsola rozwiązania musi szacować poziom ryzyka dla każdego wykrytego zagrożenia.
- h) Licencja z gwarancją i wsparciem technicznym musi bazować na ilości aktywnie występujących w ruchu sieciowym adresów IP. Ilość adresów, objętych monitorowaniem: min. 100.
- i) Musi posiadać moduły zabezpieczone połączeniem (HTTPS) w przeglądarce
- j) Konsola rozwiązania musi zawierać informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, sygnatury czasowe.
- k) Konsola rozwiązania musi dawać możliwość tagowania zdarzeń i załączania opisu (notatek).
- l) Rozwiązanie musi obsługiwać silniki detekcji takie jak Analiza Shellcode i Powershell, tj. detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wywoływania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach.
- m) Rozwiązanie musi umożliwiać analizowanie całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń.
- n) System musi być dostarczony z gwarancją oraz wsparciem technicznym obejmującym: dostęp do najnowszych wersji systemu SIEM, aktualizacji, poprawek; aktualizację silnika korelującego zbierane logi z regułami bezpieczeństwa systemu SIEM; aktualizację bazy scenariuszy postępowania dla rozpoznanych zagrożeń; kontakt z certyfikowanym inżynierem Wykonawcy lub producenta; dostęp do zdalnej pomocy technicznej Wykonawcy lub producenta w ilości min. 2 godziny tygodniowo;

1.5 Agent dla urządzeń końcowych

Wykonawca wraz z systemem SIEM musi dostarczyć moduł agenta dla urządzeń końcowych w modelu licencji wieczystej wraz z centralną konsolą zarządzającą dla min. 100 adresów IP oraz gwarancją i wsparciem technicznym na okres min. 12 miesięcy

Minimalne wymagania dla modułu agenta dla urządzeń końcowych:

1. Rozwiązanie musi posiadać moduł agenta urządzeń końcowych dla systemów Windows oraz MacOS umożliwiający bezproblemową współpracę z systemem antywirusowym do ochrony stacji roboczych, użytkowanym przez Zamawiającego.
2. Rozwiązanie musi zawierać centralną konsolę administracyjną umożliwiającą monitorowanie oraz wizualizację zebranych danych z zarządzanych urządzeń.
3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej.
4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

5. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
6. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, nazwę komputera, grupę, użytkownika.
7. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, rozmiar pliku.
8. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne lub niebezpieczne.
9. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.
10. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania komend zdalnych.
11. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
12. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
13. Rozwiązanie musi umożliwiać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
14. Rozwiązanie musi zapewniać integrację z przynajmniej takimi systemami jak: konsola programu antywirusowego, moduł EDR.
15. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: numer seryjny, informacje o systemie, procesor, pamięć RAM, karty sieciowe).
16. Serwer administracyjny musi posiadać możliwość tworzenia grup komputerów.
17. Rozwiązanie musi zapewniać korzystanie z min. 100 szablonów raportów, przygotowanych przez producenta lub własnych raportów tworzonych przez administratora.
18. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email oraz do dziennika syslog.
19. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami.
20. Rozwiązanie musi informować administratora o niezainstalowanych aktualizacjach systemowych.

1.6 NDR (Network Detection and Response).

Wykonawca wraz z systemem SIEM musi dostarczyć moduł Network Detection and Response wraz z centralną konsolą zarządzającą dla min. 100 adresów IP w modelu licencji wieczystej oraz gwarancją i wsparciem technicznym na okres min. 12 miesięcy.

Minimalne wymagania dla modułu NDR:

1. Wielowątkowy silnik detekcji umożliwiający obsługę ruchu liczonego w dziesiątkach Gigabitów
 - Możliwość obsługi wielu podsieci VLAN
 - Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
 - Obsługa biblioteki wyrażeń regularnych HyperScan
 - Możliwość aktualizacji reguł bez wyłączania/ponownego uruchamiania silnika detekcji
2. Obsługa wielowątkowości procesora
3. Możliwość analizy kopii ruchu w sieci LAN w czasie rzeczywistym bez ingerencji w ruch sieciowy
4. Rejestracja żądań HTTP

5. Rejestracja i przechowywanie certyfikatów TLS
6. Możliwość wyodrębnienia plików z analizowanego ruchu sieciowego i zapisania ich na dysku do późniejszej analizy
7. Możliwość przechwytywania pakietów danych przesyłanych w sieci LAN i zapisywanie ich dla późniejszej analizy offline
8. Tworzenie raportów w przypadku wykrycia ruchu opisanego regułami jako ruch niebezpieczny
9. Rejestrowanie i dogłębna analiza ruchu szyfrowanego TLS/SSL
10. Rejestrowanie wszystkich kluczy wymiany do analizy oraz w celu zapobiegania podmiennie
11. Rejestrowanie, zapisywanie ruchu HTTP z dowolnego portu do pliku w celu późniejszej analizy
12. Możliwość identyfikacji, wyodrębniania i rejestrowania plików w ruchu HTTP
13. Rejestracja wszystkich zapytań i odpowiedzi DNS
14. Funkcja wykrywania włamań sieciowych
15. Funkcja zapobiegania włamaniom sieciowym
16. funkcja monitorowania bezpieczeństwa sieci LAN
17. Pełne wsparcie dla protokołu IPv6
18. Możliwość dekodowania tuneli: IP-IP, IP6-IP4, IP4-IP6, GRE, VXLAN, Geneve, Teredo
19. Silnik analizy strumienia danych TCP
20. Defragmentacja pakietów w celu poddania ich analizie IPS
21. Możliwość obsługi wielu podsieci VLAN
22. Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
23. Możliwość modyfikacji reguł
24. Możliwość zdefiniowania niebezpiecznych plików przez parametry: wielkość, nazwa, rozszerzenie
25. Możliwość wykrywania złośliwego oprogramowania w oparciu o odcisk palca JA3, JA3S
26. Możliwość wykrywania złośliwego oprogramowania w oparciu o metodę HASSH
27. Obsługa dekodowania pakietów: IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, PPP, PPPoE, Raw, SLL, VLAN, QINQ, MPLS, ERSPAN, VXLAN
28. Dekodowanie warstwy aplikacji: HTTP, HTTP/2, SSL, TLS, SMB, DCERPC, MODBUS TCP, SMTP, FTP, SSH, DNS, ETHERNET/IP, ENIP/CIP, DNP3, NFS, NTP, DHCP, TFTP, KRB5, IKEv2, SIP, SNMP, RDP, RFB
29. Możliwość tworzenia raportów zgodnych z standardem JSON, SYSLOG,
30. Możliwość filtrowania alertów z podziałem na wagę/priorytet
31. Możliwość filtrowania alertów dla wybranej reguły z podziałem na wagę/priorytet
32. Wspierane systemy operacyjne: Windows, Linux, FreeBSD, OpenBSD, MacOS, Mac OS X
33. Obsługa przekazywania alertów „dalej” do systemów takich jak: syslog, eve.log, JSON, Unified
34. Filtrowanie alertów na poziomie: reguł, hostów, sieci

1.7 Oprogramowanie do monitorowania infrastruktury informatycznej

W ramach realizacji zadania Wykonawca musi dostarczyć system w modelu licencji wieczystej objęty gwarancją i wsparciem technicznym na okres min. 12 miesięcy, dokona instalacji, konfiguracji oraz podłączenia wszystkich wymaganych systemów będących celem monitorowania.

System musi spełniać poniższe wymagania minimalne oraz zapewniać możliwość:

1. Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat.

2. Zapewnienia równoległego dostępu do systemu dla wielu użytkowników.
3. Ograniczania użytkownikom dostępu do wybranych grup hostów.
4. Monitorowania serwerów fizycznych.
5. Monitorowania urządzeń sieciowych.
6. Monitorowania stanu połączeń.
7. Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów
8. Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux.
9. Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych
10. Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń.
11. Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu.
12. Grupowanie hostów.
13. Definiowanie planowanych przerw serwisowych dla hostów i usług.
14. Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).
15. Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych).
16. Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).
17. Monitorowanie serwerów za pomocą agentów
18. Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server.
19. Monitorowanie Active Directory.
20. Monitorowanie serwerów plików, udziałów sieciowych.
21. Monitorowanie statusu serwerów Apache.
22. Monitorowanie baz danych: ORACLE, MySQL, Postgress, MSSQL Server, DB2
23. Monitorowanie urządzeń przez następujące protokoły: SNMP, WMI, IPMI
24. Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW.
25. Monitorowanie poprawności działania DNS.
26. Monitorowanie środowisk: VMware, Hyper-V, Proxmox
27. Monitorowanie działania serwera czasu NTP.
28. Monitorowanie offsetu czasu na serwerach.
29. Monitorowanie ping - czasy odpowiedzi, straty pakietów.
30. Monitorowanie zajętości miejsca na poszczególnych partycjach.
31. Monitorowanie obciążenia dysków.
32. Monitorowanie wykorzystania pamięci RAM.
33. Monitorowanie obciążenia CPU.
34. Monitorowanie logów systemowych Windows.
35. Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia.
36. Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane.
37. Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix.
38. Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence)
39. Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe
40. Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów).
41. Wykrywanie niestabilnie działających usług.
42. Monitorowanie dostępności stron internetowych.
43. Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń).
44. Prezentację stanu urządzeń na mapie.
45. Prezentację danych na dashboardach.
46. Elastyczną konfigurację dashboardów, wybór elementów.
47. Wizualizację stanu działania całej infrastruktury na jednym dashboardzie.
48. Tworzenie indywidualnych dashboardów przez użytkowników.
49. Globalne wyłączanie powiadomień.

50. Powiadamianie użytkownika o problemach przez e-mail.
51. Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie.
52. Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników.
53. Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług
54. Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW
55. Automatyczna konfiguracja i działanie z REST-API
56. Centralne zarządzanie agentami
57. Integracja danych z różnych źródeł danych (JSON, XML, SNMP)
58. System posiada własny kolektor logów syslog
59. Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps
60. Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event
61. Klasyfikuje wiadomości bazując zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe.
62. System monitoruje urządzenia klasy UTM minimum w zakresie:
 - a) wykrywania włamań i szybkości blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika
 - b) stanu synchronizacji klastra High-Availability. Status „zsynchronizowany” jest uważany za OK, a status „niezsynchronizowany” CRIT.
 - c) ogólnego stanu alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz” (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda” (1).
 - d) aktualnej liczby sesji na urządzeniu
 - e) liczby dostępnych tuneli IPSec VPN
 - f) wykrywania wirusów i szybkości blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika.
 - g) poziomu wykorzystania procesora. Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne.
63. System ma możliwość odbierania i prezentacji danych z urządzenia UTM z wykorzystaniem kolektora logów syslog.
64. System ma możliwość odbierania danych z systemu z agenta dla urządzeń końcowych wykorzystaniem kolektora logów syslog.
65. W ramach wsparcia technicznego Wykonawca musi monitorować następujące elementy infrastruktury IT Zamawiającego: Serwery fizyczne, maszyny wirtualne Windows/Linux, serwery Active Directory, Macierze, serwery plików NAS, przełączniki sieciowe, zasilacze awaryjne.

22. Kompleksowe rozwiązanie klasy Privileged Access Management w modelu licencji wieczystej oraz wsparciem technicznym na 12 miesięcy.

W skład pozycji wchodzi:

- O27. Oprogramowanie do zarządzania uprzywilejowanego dostępu (PAM- Privileged Access Management/ PIM - Privileged Identity Management) | Pakiet uzupełniających się rozwiązań: System typu PAM, Oprogramowanie do zarządzania tożsamością i dostępem, System typu Centralny menedżer haseł

Kompleksowe rozwiązanie klasy Privileged Access Management w modelu licencji wieczystej oraz wsparciem technicznym na 12 miesięcy.

Parametry minimalne rozwiązania:

1. Rozwiązania działające jako PROXY, bez potrzeby instalacji przez administratora agentów na systemach chronionych rozwiązaniem PAM.
2. Rejestracja i podgląd sesji uprzywilejowanych użytkowników (polecenia i zrealizowane działania) umożliwiając funkcje bezpieczeństwa niezaprzeczalności wykonanych działań i zabezpieczenie materiału dla celów sądowych.
3. Rozwiązanie powinno wspierać platformy chmurowe Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, platformy wirtualne Kernel-based Virtual Machine (KVM), Microsoft Hyper-V, OpenStack, VMware vSphere oraz platformę sprzętową.
4. Rozwiązanie powinno być dostarczone jako jednolity System. Bez potrzeby instalacji na wskazanym systemie operacyjnym. Cały System powinien być wspierany przez dostawcę, to jest zarówno warstwa systemu operacyjnego, jak i aplikacji.
5. Rozwiązanie powinno wspierać natywnie połączenia dla protokołów SSH i RDP do PROXY, oraz SSH/TELNET/RLOGIN/RDP/VNC od PROXY do systemów chronionych.
6. Dla niestandardowych protokołów (nie wspieranych natywnie przez rozwiązanie dostawcy) powinna istnieć możliwość wywołania klienta, wspierającego taki protokół, na stacji przesiadkowej, w taki sposób, aby jedynie klient i przypisane mu zasoby były widoczne dla użytkownika.
7. Dla niestandardowych protokołów i wywołania ich klienta, rozwiązanie powinno wspierać technologie dla Microsoft RemoteApp.
8. Możliwość przydzielania uprawnień administracyjnych, dostępowych dla użytkowników na podstawie profili ustawień.
9. W przypadku dostępu audytora profil użytkownika powinien co najmniej oferować możliwość ograniczenia dostępu do nagrań wybranych grup użytkowników i grup systemów docelowych wraz z konfigurowanymi dla nich kontami uprzywilejowanymi.
10. Konfiguracja profilu użytkownika powinna zawierać możliwość filtrowania połączeń przychodzących w oparciu o adres źródłowy IP. Tworząc tym samym listy kontroli dostępu (ACL) dla użytkowników z przypisanym profilem użytkownika. Definicja ograniczenia powinna dopuszczać format: adres IP, adres sieci i maska sieci lub FQDN.
11. Rozwiązanie powinno pozwalać na określenie polityki dostępu przez przypisanie wybranej grupy użytkowników do wskazanej grupy systemów docelowych.
12. Podgląd zarejestrowanych danych musi uwzględniać zapis video sesji oraz transkrypcje nagrania przedstawiającą wszystkie metadane dotyczące sesji (RDP) oraz pełny zapis wyświetlanych danych dla konsoli (SSH).
13. Monitorowanie połączeń w czasie rzeczywistym, w tym możliwość podglądu sesji w czasie rzeczywistym z możliwością jej natychmiastowego zakończenia.
14. Zarządzanie zbiorami reguł (polityką) haseł lokalnych użytkowników i administratorów.
15. Możliwość włączenia/wyłączenia rejestrowania sesji dla wybranych grup użytkowników.
16. Możliwość ustawienia dostępu przez portal internetowy, przeglądarkę, co najmniej dla sesji SSH i RDP, bez potrzeby instalacji dedykowanej wtyczki w przeglądarce.
17. Rozwiązanie umożliwia integrację z Microsoft Active Directory bez potrzeby synchronizacji informacji o użytkownikach. To znaczy, że użytkownik Active Directory dodany do grupy użytkowników automatycznie, w tej samej chwili jest rozpoznany przez rozwiązanie do zarządzania dostępem.
18. Możliwość definiowania systemów docelowych przez określenie adresu IP, nazwy DNS lub możliwość określania przez adres IP sieci i maski.
19. Dla sesji RDP „meta-dane” powinny zawierać informację na temat:
 - a. zmiany aktywnego okna,
 - b. operacji wyboru danego przycisku w oknie systemu Windows,
 - c. operacji wyboru przycisków typu „radio button” lub zaznaczenie opcji typu „check box” w oknie,
 - d. zmiany treści w polu tekstowym w oknie systemu Windows,

- e. rozpoczęcia i zakończenia procesu,
 - f. wymiany plików przez schowek systemu Windows,
 - g. wymiany plików przez przekierowane zasoby sieciowe systemu Windows.
20. Dla sesji RDP możliwość blokowania połączeń TCP wychodzących na stacji docelowej, serwera Microsoft Windows.
 21. Dla sesji RDP możliwość blokowania wybranych procesów na stacji docelowej, serwer Microsoft Windows.
 22. Dla sesji SSH i RDP możliwość tworzenia wzorców regex dla wykonywanych poleceń, a w przypadku wykrycia takiego wzorca możliwość ustawienia jednej z akcji: zakończenie sesji lub powiadomienie o wykryciu wzorca.
 23. Określanie wzorców wykonywanych poleceń dla SSH i RDP powinno odbywać się na poziomie tworzenia grup użytkowników, dla których kreowany jest dostęp lub na poziomie grupy systemów docelowych, do których dostęp jest chroniony i monitorowany przez rozwiązanie PAM.
 24. Wsparcie funkcjonalności współdzielenia co najmniej sesji RDP nawiązanej przez użytkownika Systemu z Audytorem, rozumianej jako pełna interakcja - wprowadzanie znaków z klawiatury oraz ruchów myszką.
 25. Rozwiązanie powinno umożliwiać uwierzytelnienie użytkownika Systemu certyfikatem oraz użycie tego samego certyfikatu przy logowaniu do docelowego systemu.
 26. Ochrona haseł wprowadzanych do sesji poprzez wykrycie kursora wejściowego w polach wprowadzania hasła lub w oknie kontrola konta użytkownika UAC (User Account Control).
 27. Uwierzytelnienie użytkownika przez login/hasło, certyfikat X.509, klucz w SSH.
 28. Wsparcie dla protokołów, uwierzytelniania: KERBEROS, RADIUS, Microsoft Active Directory, LDAP, TACACS+.
 29. Możliwość ustawienia dodatkowego zatwierdzenia dostępu dla połączeń do wybranej grupy serwerów przez wskazaną liczbę użytkowników do tego wskazanych.
 30. Możliwość ustawienia dodatkowego zatwierdzenia dostępu w zależności od czasu logowania, np. nie wymagać zatwierdzenia dostępu od Poniedziałku do Piątku, w godzinach 8:00-16:00, a we wszystkich pozostałych dniach i godzinach jej wymagać.
 31. Możliwość automatycznego wyszukiwania nowych urządzeń w sieci oraz dodawania jako nowych obiektów chronionych w systemie PAM.
 32. Możliwość udostępniania w czasie rzeczywistym statystyk oraz kluczowych wskaźników wydajności.
 33. Możliwość tworzenia własnych powiadomień mailowych wysyłanych przez system PAM.
 34. Wsparcie tworzenia skryptów logowania dla protokołów połączeniowych Telnet / RLOGIN.
 35. Rozwiązanie powinno wspierać natywnie nagrywanie połączenia przy zastosowaniu protokołu WinSCP.
 36. Wsparcie integracji systemu PAM z rozwiązaniami klasy SIEM wraz z możliwością filtrowania zdarzeń, które mają być wysyłane do systemu SIEM.
 37. Możliwość zarządzania polityką retencji danych gromadzonych przez system PAM.
 38. System powinien wspierać agregację połączeń sieciowych.
 39. System powinien udostępniać informacje o pakiecie, opcjach oraz metryce posiadanej licencji.
 40. System musi wspierać klucze ECDSA dla hostów SSH.
 41. Rozwiązanie powinno wspierać tryb konfiguracji klastra wysokiej dostępności (ang. HA – High Availability), w którym będą co najwyżej dwa węzły zainstalowanego Systemu.
 42. Możliwość automatycznego rotowania haseł i kluczy SSH dla określonych hostów lub grup kont.
 43. Możliwość tworzenia wyjątków dla automatycznego rotowania haseł i kluczy SSH.
 44. Tworzenie różnych harmonogramów automatycznej zmiany haseł na systemach docelowych.
 45. Generować hasła jednorazowe oraz zmieniać je automatycznie po ich użyciu.
 46. Możliwość tworzenia własnych polityk / wymagań dla haseł:
 - a. Wymagalność minimalnej ilości znaków,
 - b. Wykluczenie określonych przez administratora znaków,
 - c. Wymagalność wielkich i małych liter,
 - d. Wymagalność znaków specjalnych,
 - e. Wymagalność minimalnej liczby znaków specjalnych.
 47. Wymagalność ustawienia różnych polityk/wymagań haseł dla różnych grup hostów lub grup kont.
 48. Ustawienie ważności hasła w określonym przedziale czasu.
 49. Kontrola haseł znajdujących się w plikach poprzez ich ukrycie lub dekodowanie.

50. Zapewnienie wtyczek pozwalających na zmianę haseł dla systemów: AIX, F5 BIG IP, SAP IQ, AWS IAM, Checkpoint, ESX, Fortinet Fortigate, HP iLO, MS SQL Server, ORACLE, Stormshield, Teradata, Unix, Microsoft Windows, Cisco, Dell iDRAC, IBM 3270, Juniper SRX, LDAP, MySQL, Palo Alto PA-500, Grafana.
51. Rozwiązanie musi umożliwiać zmianę haseł za pośrednictwem interfejsu API (co najmniej REST API/SCIM API).
52. Zarządzanie oraz cykliczne rotowanie haseł kont serwisowych.
53. Możliwość integracji Systemu z rozwiązaniami AV/DLP przez zastosowanie protokołu ICAP.
54. Dla protokołów WinSCP oraz SFTP wsparcie analizowania zawartości przesyłanych plików oraz ich blokowania.
55. Możliwość integracji Systemu z systemami klasy ITSM (ang. IT Service Management).
56. Rozwiązanie musi posiadać Wsparcie Techniczne producenta na okres co najmniej 12 miesięcy.
57. Wsparcie Techniczne powinno być świadczone co najmniej w dni robocze (od poniedziałku do piątku) w godzinach od 8:00 do 19:00 (z wyłączeniem dni wolnych ustawowo od pracy).
58. Zgłoszenie problemu technicznego będzie możliwe przez co najmniej dwa kanały komunikacyjne: przez dedykowany numer telefoniczny oraz przez Portal Wsparcia Technicznego dostępny przez przeglądarkę internetową umożliwiający zdalne zgłaszanie i monitorowanie statusu zgłoszenia biletu problemowego.
59. W ramach udzielonego Wsparcia Technicznego Zamawiający musi mieć możliwość zgłaszania awarii i zapytań o pomoc techniczną bez ograniczeń co do liczby zgłoszeń.
60. Dostęp do Portalu Wsparcia Technicznego musi być udzielony dla co najmniej 2 kont użytkowników.
61. Obsługa zgłoszeń musi obejmować co najmniej rozwiązywanie problemów technicznych i konfigurację oprogramowania Systemu.
62. Reakcja na zgłoszenie problemu technicznego nie może być dłuższa niż 1 dzień roboczy.
63. Usługa Wsparcia Technicznego musi gwarantować dostęp do aktualnych wersji Systemu oraz poprawek (ang. Hotfix), jak też dokumentacji technicznej – co najmniej instrukcji użytkownika i administratora Systemu.
64. Oferowane produkty będą pochodziły z oficjalnego kanału dystrybucyjnego producenta na terenie Unii Europejskiej.
65. Oferowane oprogramowanie musi być oprogramowaniem w wersji aktualnej (tzn. najnowszej opublikowanej przez producenta) na dzień dostawy Systemu.
66. System musi mieć możliwość ochrony nie mniej niż 50 systemów np. serwerów typu Linux, Windows, aktywnych urządzeń sieciowych, jak przełączniki, routery oraz aplikacje np. konsole do zarządzania.
67. Licencja na System PAM nie powinna limitować ilości sesji równoległych.
68. Licencja na System PAM nie powinna ograniczać liczby użytkowników systemu PAM.
69. System musi umożliwiać realizację klastra wysokiej dostępności składającego się z dwóch węzłów produktu bez ponoszenia dodatkowych opłat.
70. Udzielana licencja musi być oferowana w modelu wieczystym.

23. Dostawa i wdrożenie kompleksowego rozwiązania składającego się z oprogramowania do zarządzania urządzeniami końcowymi i mobilnymi z funkcjonalnością ochrony danych wrażliwych w modelu licencji wieczystej i wsparciem technicznym producenta na 12 miesięcy oraz technologii autentykacji wieloskładnikowej dla użytkowników.

W skład pozycji wchodzi:

- O34. Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych | Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych, system zarządzania urządzeniami mobilnymi (MDM), System typu DLP, System typu MFA

1. Przedmiotem zamówienia jest dostawa i wdrożenie kompleksowego rozwiązania składającego się z oprogramowania do zarządzania urządzeniami końcowymi i mobilnymi z funkcjonalnością ochrony danych wrażliwych w modelu licencji wieczystej i wsparciem technicznym producenta na 12 miesięcy oraz technologii autentykacji wieloskładnikowej dla użytkowników.
2. Rozwiązanie ma służyć do poprawy poziomu cyberbezpieczeństwa, automatyzacji administracji IT, centralizacji zarządzania urządzeniami końcowymi oraz wsparcia zgodności z wymaganiami NIS2 i KSC.

2.1. Przedmiot zamówienia obejmuje:

1. Dostawę licencji Oprogramowania dla 110 urządzeń końcowych oraz 70 urządzeń mobilnych.
2. Dostawę i wdrożenie technologii autentykacji wieloskładnikowej dla użytkowników.
3. Zapewnienie wsparcia technicznego producenta przez okres 12 miesięcy od dnia odbioru Oprogramowania.
4. Wdrożenie Oprogramowania w środowisku Zamawiającego.
5. Konfigurację systemu zgodnie z wymaganiami Zamawiającego.
6. Integrację z istniejącą infrastrukturą Zamawiającego.
7. Przygotowanie dokumentacji powdrożeniowej.
8. Przeprowadzenie szkolenia administratorów.
9. Przekazanie Zamawiającemu dostępu do dokumentacji technicznej, bazy wiedzy i aktualizacji.:

2.2 Wymagania oferowanego rozwiązania:

2.3. Oprogramowanie musi umożliwiać zarządzanie co najmniej następującymi klasami urządzeń: 1. Stacje robocze Windows. 2. Serwery Windows. 3. Komputery macOS. 4. Urządzenia Linux. 5. Smartfony i tablety Android. 6. Urządzenia iOS oraz iPadOS. 7. Urządzenia sieciowe SNMP. 8. Wybrane urządzenia OT/ICS. 9. Urządzenia znajdujące się poza siecią LAN Zamawiającego. 10. Urządzenia pracujące w trybie offline lub z okresowym dostępem do sieci.

2.4. Oprogramowanie musi umożliwiać co najmniej: 1. Inwentaryzację sprzętu i oprogramowania. 2. Dystrybucję oprogramowania. 3. Automatyzację instalacji aplikacji. 4. Patch management systemów

operacyjnych. 5. Wdrażanie systemów operacyjnych. 6. Zarządzanie konfiguracją. 7. Zarządzanie lokalnymi kontami administracyjnymi. 8. Zarządzanie urządzeniami mobilnymi. 9. Zdalne wsparcie użytkownika. 10. Obsługę urządzeń poza LAN bez stałego VPN. 11. Integrację z Service Desk, SIEM lub innymi systemami zewnętrznymi.

3. Dostawa

3.1. Dostawa licencji ma zostać dokonana w dni robocze w godzinach pracy Zamawiającego, chyba, że Zamawiający i Wykonawca uzgodnią inaczej.

3.2. Dostarczone licencje muszą obejmować dostęp do najnowszej wersji Oprogramowania udostępnionej przez Producenta na dzień dostawy.

3.3. Licencje oraz Oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucji Producenta.

3.4. Wykonawca zobowiązany jest do przekazania Zamawiającemu zestawienia dostarczonych licencji w wersji elektronicznej.

3.5. Oferowane rozwiązanie musi być dostarczone w modelu licencji wieczystej. Wykonawca zobowiązany jest dostarczyć potwierdzenie prawa Zamawiającego do bezterminowego korzystania z Oprogramowania w postaci certyfikatu, zgodnie z warunkami Producenta.

4. Wsparcie techniczne i aktualizacje

4.1. Wykonawca zobowiązuje się zapewnić Zamawiającemu wsparcie techniczne dla dostarczonego Oprogramowania oraz wszystkich licencji przez okres 12 miesięcy od dnia odbioru Oprogramowania.

4.2. Minimalny zakres wsparcia technicznego musi obejmować: 1. Dostęp do aktualnej dokumentacji technicznej Producenta. 2. Dostęp do bazy wiedzy Producenta. 3. Dostęp do aktualizacji Oprogramowania. 4. Dostęp do poprawek bezpieczeństwa. 5. Dostęp do nowych wersji Oprogramowania w ramach posiadanego wsparcia. 6. Możliwość zgłaszania incydentów technicznych. 7. Możliwość pobierania plików instalacyjnych, obrazów, aktualizacji, komponentów i agentów

4.3. Wykonawca musi zapewnić obsługę zgłoszeń w języku polskim lub angielskim.

4.4. Wykonawca musi zapewnić możliwość eskalacji zgłoszeń do Producenta.

4.5. Wykonawca musi zapewnić minimum następujące czasy reakcji: 1. Incydent krytyczny – do 4 godzin roboczych. 2. Incydent wysoki – do 8 godzin roboczych. 3. Incydent standardowy – do [2] dni roboczych.

Za incydent krytyczny uznaje się awarię uniemożliwiającą korzystanie z kluczowych funkcji Oprogramowania, w szczególności zarządzania agentami, dystrybucji poprawek, pracy konsoli administracyjnej lub komunikacji z urządzeniami.

5. Terminy realizacji

5.1. Wykonawca zobowiązany jest zrealizować dostawę licencji w ustalonym terminie wynikającym z harmonogramu wdrożeniowego.

5.2. Wdrożenie Oprogramowania powinno zostać wykonane w ustalonym terminie wynikającym z harmonogramu wdrożeniowego.

5.3. Szkolenie administratorów powinno zostać wykonane w terminie uzgodnionym z Zamawiającym, lecz nie później niż do dnia odbioru końcowego.

6. Szczegółowe wymagania dla Oprogramowania

6.1. Informacje ogólne

6.1.1. Oprogramowanie musi być rozwiązaniem klasy Unified Endpoint Management umożliwiającym centralne zarządzanie wszystkimi wymaganymi modułami z poziomu jednej spójnej konsoli administracyjnej w postaci aplikacji desktopowej.

6.1.2. Oprogramowanie musi umożliwiać centralne zarządzanie co najmniej: 1. Stacjami roboczymi Windows. 2. Serwerami Windows. 3. Urządzeniami macOS. 4. Urządzeniami Linux. 5. Urządzeniami mobilnymi Android. 6. Urządzeniami mobilnymi iOS/iPadOS. 7. Urządzeniami sieciowymi SNMP. 8. Wybranymi urządzeniami OT/ICS.

- 6.1.3. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji administratora w konsoli zarządzającej oraz umożliwiać jednoczesną pracę wielu administratorów.
- 6.1.4. Logowanie administratorów do konsoli zarządzającej musi umożliwiać integrację z Active Directory.
- 6.1.5. Oprogramowanie musi umożliwiać stosowanie MFA dla logowań administracyjnych.
- 6.1.6. Oprogramowanie musi umożliwiać jednoczesną pracę wielu administratorów.
- 6.1.7. Oprogramowanie musi posiadać system ról i uprawnień umożliwiający przypisywanie wybranych grup stanowisk, urządzeń, użytkowników lub funkcjonalności do poszczególnych administratorów.
- 6.1.8. Wszelkie raporty, zestawienia oraz funkcje grupowe muszą respektować uprawnienia nadane administratorowi i obejmować wyłącznie te obiekty, do których administrator posiada dostęp.
- 6.1.9. Oprogramowanie musi umożliwiać ukrywanie danych osobowych użytkowników końcowych, takich jak imię, nazwisko, login lub identyfikator użytkownika, przed wskazanymi administratorami.
- 6.1.10. Oprogramowanie musi umożliwiać wysyłanie powiadomień e-mail z serwera aplikacyjnego, w szczególności dotyczących statusu zadań, błędów, zdarzeń systemowych, alertów, raportów lub powiadomień administracyjnych.
- 6.1.11. Oprogramowanie musi umożliwiać eksport dowolnego widoku konsoli administracyjnej co najmniej do formatu Excel/XLSX lub CSV.
- 6.1.12. Oprogramowanie musi posiadać architekturę trójwarstwową obejmującą co najmniej: 1. Bazę danych. 2. Serwer aplikacyjny / zarządzający. 3. Agenta lub komponent zarządzający na urządzeniu końcowym.
- 6.1.13. Oprogramowanie, niezależnie od liczby funkcjonalności lub zarządzanych urządzeń końcowych, musi działać na urządzeniu końcowym Windows w oparciu o jeden podstawowy agent zarządzający, z możliwością rozszerzania funkcjonalności bez instalowania wielu niezależnych agentów dla każdego modułu.
- 6.1.14. Oprogramowanie musi umożliwiać rozbudowę o dodatkowe moduły lub funkcjonalności bez konieczności reinstalacji całego środowiska serwerowego.
- 6.1.15. Oprogramowanie musi umożliwiać zwiększenie liczby zarządzanych urządzeń bez konieczności reinstalacji serwera, w szczególności przez zmianę, aktualizację lub rozszerzenie licencji.

6.1.16. Oprogramowanie musi umożliwiać aktualizację licencji online, bez konieczności ręcznej wymiany plików licencyjnych, o ile środowisko Zamawiającego posiada dostęp do wymaganych usług online Producenta.

6.2. Wymagania techniczne i kompatybilność platform

6.2.1. Wymagania dla serwera zarządzającego: Oprogramowanie musi wspierać instalację serwera zarządzającego co najmniej na: 1. Microsoft Windows Server 2016 Standard/Datacenter – wersja z GUI. 2. Microsoft Windows Server 2019 Standard/Datacenter – wersja z GUI. 3. Microsoft Windows Server 2022 Standard/Datacenter – wersja z GUI. 4. Microsoft Windows Server 2025 Standard/Datacenter – jeżeli wsparcie jest dostępne w aktualnej wersji Oprogramowania.

6.2.2. Dla komponentów serwerowych Zamawiający wymaga stosowania systemów operacyjnych pozostających w okresie wsparcia Producenta systemu operacyjnego.

6.2.3. Oprogramowanie musi współpracować z Microsoft SQL Server co najmniej w wersjach: 1. Microsoft SQL Server 2016 SP3 – dopuszczalnie jako wersja starsza/deprecated, jeżeli wspierana przez Producenta Oprogramowania. 2. Microsoft SQL Server 2017. 3. Microsoft SQL Server 2019. 4. Microsoft SQL Server 2022. 5. Microsoft SQL Server 2025 – jeżeli wsparcie jest dostępne w aktualnej wersji Oprogramowania.

6.2.4. Oprogramowanie musi wymagać co najmniej poziomu kompatybilności bazy danych zgodnego z Microsoft SQL Server 2016 lub nowszym, jeżeli wynika to z dokumentacji Producenta.

6.2.5 Oprogramowanie musi umożliwiać wykorzystanie Microsoft SQL Server Express dla małych środowisk testowych lub niewielkich instalacji, z zastrzeżeniem ograniczeń Producenta Microsoft oraz ograniczeń rozmiaru bazy danych SQL Express.

6.2.6. Zamawiający może wyrazić na stosowanie systemów operacyjnych innych niż pozostających w okresie wsparcia Producenta.

6.2.7. Minimalne wymagania sprzętowe dla serwera zarządzającego: 1. Procesor: minimum 4 rdzenie. 2. Pamięć RAM: minimum 8 GB, rekomendowane minimum 16 GB. 3. Karta sieciowa: minimum 1 Gbps. 4. Przestrzeń dyskowa dla instalacji systemu: minimum 20 GB. 5. Dodatkowa przestrzeń dyskowa na repozytoria, paczki, aktualizacje, systemy operacyjne, logi oraz kopie robocze – zgodnie z rozmiarem środowiska Zamawiającego.

6.2.8. Dla serwera repozytorium / Distribution Point / DIP należy przewidzieć dodatkową przestrzeń dyskową co najmniej na:

1. Aplikacje dystrybuowane do urządzeń końcowych. 2. Repozytorium Managed Software / aplikacje firm trzecich. 3. Obrazy systemów operacyjnych. 4. Sterowniki. 5. Paczki instalacyjne agentów. 6. Aktualizacje i komponenty wdrożeniowe.

6.2.9. Oprogramowanie musi wspierać środowiska wirtualne, w szczególności środowiska VMware, Hyper-V, Proxmox VE lub inne platformy wirtualizacyjne wspierane przez system operacyjny serwera.

6.2.10. Oprogramowanie musi wspierać aktualne wymagane komponenty Microsoft .NET, w szczególności ASP.NET Core Shared Framework oraz Microsoft Windows Desktop Runtime w wersjach wymaganych przez Producenta Oprogramowania.

6.2.11. Wymagania dla stacji administracyjnej: Konsola administracyjna musi wspierać uruchomienie na współczesnych wersjach systemów Microsoft Windows, co najmniej: 1. Windows 10. 2. Windows 11. 3. Wspieranych wersjach Windows Server, jeżeli uruchomienie konsoli na serwerze jest dopuszczone przez Producenta.

6.2.12. Konsola administracyjna powinna wspierać minimalną rozdzielczość 1024 × 768, przy czym rekomendowana jest rozdzielczość co najmniej 1280 × 800 lub wyższa.

6.2.13. Zakres obsługi systemów Windows jako endpointów: Oprogramowanie musi umożliwiać zarządzanie aktualnymi wersjami systemów Windows, co najmniej: 1. Windows 10 Pro / Enterprise. 2. Windows 10 LTSC/LTSB, jeżeli jest wspierany przez Producenta. 3. Windows 11 Pro / Enterprise. 4. Windows 11 24H2, z uwzględnieniem wymagań i ograniczeń Producenta, w szczególności dotyczących komponentu VBScript. 5. Windows Server 2016. 6. Windows Server 2019. 7. Windows Server 2022. 8. Windows Server 2025, jeżeli jest wspierany przez aktualną wersję Oprogramowania, także z ograniczeniami opisanymi w dokumentacji Producenta.

6.2.14. Oprogramowanie powinno umożliwiać obsługę starszych systemów Windows w zakresie dopuszczonym przez Producenta, w szczególności: 1. Windows 8.1 – wsparcie ograniczone, jeśli jest dostępne. 2. Windows 7 – wsparcie ograniczone, jeśli jest dostępne. 3. Windows Server 2012 / 2012 R2 – wsparcie ograniczone, jeśli jest dostępne. 4. Windows XP SP3 – wyłącznie w zakresie legacy, jeśli środowisko Zamawiającego tego wymaga i jeżeli Producent dopuszcza pracę starszego agenta.

6.2.15. Dla Windows XP SP3 Zamawiający dopuszcza obsługę wyłącznie jako środowisko legacy, z zastrzeżeniem, że aktualny agent Oprogramowania może nie być wykonywalny na Windows XP, a obsługa

może wymagać starszej wersji agenta. Wymaganie to nie dotyczy funkcjonalności takich jak Remote Desk, OS Install, automatyczny deployment agenta lub funkcji bezpieczeństwa niedostępnych dla systemów poza wsparciem Microsoft.

6.2.16. Dla systemów Windows znajdujących się poza wsparciem Producenta systemu operacyjnego Zamawiający dopuszcza ograniczoną funkcjonalność oraz brak gwarancji działania wszystkich nowych funkcji, pod warunkiem, że Wykonawca jasno wskaże zakres wsparcia i ograniczenia.

6.2.17. Zakres obsługi macOS: Oprogramowanie musi umożliwiać zarządzanie aktualnymi wersjami macOS wspieranymi przez Producenta Oprogramowania, co najmniej: 1. macOS 13 Ventura. 2. macOS 14 Sonoma. 3. macOS 15 Sequoia. 4. macOS 26 Tahoe – jeżeli jest wspierany przez aktualną wersję Oprogramowania.

6.2.18. Zamawiający dopuszcza brak wsparcia dla starszych wersji macOS, takich jak Catalina, Big Sur lub Monterey, jeżeli zostały wycofane z aktualnej listy wsparcia Producenta Oprogramowania.

6.2.19. Zakres obsługi Android: Oprogramowanie musi umożliwiać zarządzanie urządzeniami Android Enterprise w aktualnych wersjach systemu, co najmniej: 1. Android 10. 2. Android 11. 3. Android 12. 4. Android 13. 5. Android 14. 6. Android 15. 7. Android 16 – jeżeli jest wspierany przez aktualną wersję Oprogramowania.

6.2.20. Zamawiający dopuszcza ograniczone wsparcie dla Android 8 i Android 7, w szczególności brak wsparcia dla wybranych nowych funkcji lub brak wsparcia dla zero-touch, jeśli wynika to z dokumentacji Producenta.

6.2.21. Zakres obsługi iOS/iPadOS: Oprogramowanie musi umożliwiać zarządzanie urządzeniami iOS/iPadOS w aktualnych wersjach systemu, co najmniej: 1. iOS/iPadOS 12. 2. iOS/iPadOS 13. 3. iOS/iPadOS 14. 4. iOS/iPadOS 15. 5. iOS/iPadOS 16. 6. iOS/iPadOS 17. 7. iOS/iPadOS 18. 8. iOS/iPadOS 26 – jeżeli jest wspierany przez aktualną wersję Oprogramowania.

6.2.22. Zamawiający dopuszcza brak wsparcia dla iOS 10 i iOS 11, jeżeli zostały wycofane z aktualnej listy wsparcia Producenta Oprogramowania.

6.2.23. Zakres obsługi Linux Oprogramowanie musi umożliwiać agentowe lub SSH-based zarządzanie systemami Linux, co najmniej dla: 1. Debian 12 lub nowszy. 2. Ubuntu LTS 22.04 lub nowszy. 3. Ubuntu LTS 24.04 lub nowszy. 4. Rocky Linux 9 lub nowszy. 5. Red Hat Enterprise Linux 9 lub nowszy. 6. OpenSUSE 15 lub nowszy.

6.2.24. Oprogramowanie powinno wspierać zarządzanie pakietami Linux poprzez co najmniej: 1. APT. 2. DNF. 3. Zypper. 4. Snap. 5. Flatpak.

6.2.25. Dla Debian 11 Zamawiający dopuszcza tryb SSH-only lub wsparcie ograniczone, jeśli wynika to z dokumentacji Producenta.

6.2.26. Wymagania dla komponentu Gateway / Proxy: Oprogramowanie musi posiadać komponent bramy / gateway / proxy umożliwiający komunikację z urządzeniami znajdującymi się poza siecią LAN Zamawiającego bez konieczności zestawiania klasycznego połączenia VPN.

6.2.27. Komponent Gateway powinien być możliwy do instalacji w strefie DMZ i nie powinien wymagać instalacji na tym samym serwerze co główny serwer zarządzający.

6.2.28. Komunikacja pomiędzy agentem, bramą i serwerem musi odbywać się z wykorzystaniem szyfrowanego protokołu HTTPS lub równoważnego mechanizmu zabezpieczającego transmisję.

6.3. Architektura platformy

6.3.1. Oprogramowanie musi posiadać architekturę skalowalną, umożliwiającą obsługę środowisk rozproszonych terytorialnie.

6.3.2. Oprogramowanie musi wspierać więcej niż jeden serwer repozytorium / Distribution Point / DIP w celu optymalizacji dystrybucji pakietów, aktualizacji i systemów operacyjnych.

6.3.3. Oprogramowanie musi umożliwiać indywidualną synchronizację pomiędzy serwerami repozytoriów, z możliwością ograniczania harmonogramu synchronizacji oraz przepustowości łącza.

6.3.4. Oprogramowanie musi wspierać PXE Relay lub równoważny mechanizm umożliwiający wdrażanie systemów operacyjnych przez sieć.

6.3.5. Oprogramowanie musi wspierać Wake-Up Points lub równoważny mechanizm umożliwiający wzbudzanie urządzeń w lokalizacjach rozproszonych.

6.3.6. Oprogramowanie musi posiadać możliwość integracji z Active Directory w trybie niewymagającym rozszerzenia schematu AD.

6.3.7. Oprogramowanie musi posiadać dostęp read-only do Active Directory dla celów synchronizacji, chyba że określona funkcjonalność wymaga innych uprawnień i zostanie to udokumentowane.

6.3.8. Oprogramowanie musi umożliwiać pobieranie informacji z Active Directory oraz automatyczne rejestrowanie urządzeń, użytkowników lub grup w systemie zarządzającym.

6.3.9. Oprogramowanie musi umożliwiać zarządzanie urządzeniami zarówno według struktury organizacyjnej, jak i według grup logicznych, dynamicznych, lokalizacji, atrybutów, statusów, systemów operacyjnych lub innych kryteriów.

6.4. Komunikacja serwer–klient

6.4.1. Oprogramowanie musi obsługiwać komunikację z agentami przy niewielkim obciążeniu łącza w zakresie kontroli agentów, pobierania statusów i przesyłania informacji zwrotnych.

6.4.2. Oprogramowanie musi umożliwiać ograniczanie wykorzystania pasma przy dystrybucji pakietów, aktualizacji, obrazów i innych danych.

6.4.3. Oprogramowanie musi wspierać tryby zadań: 1. Push. 2. Pull. 3. Shutdown. 4. Wake-on-LAN. 5. Zadania cykliczne. 6. Zadania inicjowane przez użytkownika końcowego.

6.4.4. Oprogramowanie musi umożliwiać komunikację z urządzeniami poza siecią LAN przez bramkę instalowaną w DMZ lub równoważny komponent pośredniczący.

6.4.5. Oprogramowanie musi zapewniać możliwość obsługi urządzeń zdalnych i offline, w tym urządzeń pracujących okresowo poza siecią organizacji.

6.4.6. Oprogramowanie musi umożliwiać synchronizację statusów urządzeń i zadań po ponownym połączeniu urządzenia z systemem.

6.5. Operacje wykonywane przez Oprogramowanie

6.5.1. Oprogramowanie musi umożliwiać pracę wielu administratorów równocześnie w jednej konsoli zarządzającej.

6.5.2. Oprogramowanie musi wyświetlać informacje o stanie urządzeń, zadań, operacji i błędów w czasie rzeczywistym lub bliskim rzeczywistemu, z uwzględnieniem znacznika czasu.

6.5.3. W przypadku zakończenia zadania błędem administrator musi otrzymać w konsoli szczegółową informację o przyczynie błędu.

6.5.4. Komunikaty błędów muszą obejmować co najmniej: 1. Identyfikację urządzenia. 2. System operacyjny urządzenia. 3. Nazwę zadania. 4. Status wykonania. 5. Kod błędu, jeżeli jest dostępny. 6. Opis przyczyny błędu. 7. Czas wystąpienia błędu.

6.5.5. Oprogramowanie musi umożliwiać definiowanie dodatkowych pól i zmiennych przechowywanych w tej samej bazie danych, np. informacji o lokalizacji, gnieździe sieciowym, osobie odpowiedzialnej, leasingu, gwarancji, dziale, kosztach, numerze inwentarzowym lub danych supportowych.

6.5.6. Oprogramowanie musi wspierać grupy dynamiczne wykorzystywane do indywidualnych widoków, raportów, przypisać zadań oraz automatyzacji.

6.5.7. Oprogramowanie musi umożliwiać przypisywanie zadań urządzeniom spełniającym wskazane warunki dynamiczne, np. system operacyjny, wersja systemu, wolne miejsce na dysku, obecność aplikacji, stan aktualizacji, lokalizacja, adres IP, podsieć, typ urządzenia lub przynależność do grupy AD.

6.6. Minimum możliwości w zakresie zadań i automatyzacji

6.6.1. Oprogramowanie musi umożliwiać wysyłanie poleceń do urządzeń końcowych w trybie Push.

6.6.2. Oprogramowanie musi umożliwiać pobieranie zadań przez urządzenia końcowe w trybie Pull.

6.6.3. Oprogramowanie musi umożliwiać wykonywanie zadań typu Shutdown, Restart lub Logoff, zgodnie z uprawnieniami administratora.

6.6.4. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on-LAN.

6.6.5. Oprogramowanie musi umożliwiać automatyczne generowanie i wysyłanie zadań powtarzających się.

6.6.6. Oprogramowanie musi umożliwiać uruchamianie zadań z poziomu użytkownika końcowego przez kiosk samoobsługowy / Self-Service dostępny przez przeglądarkę lub aplikację użytkownika.

6.6.7. Zawartość Kiosku / Self-Service musi być definiowana co najmniej: 1. Per użytkownik. 2. Per grupa użytkowników. 3. Per urządzenie. 4. Per grupa urządzeń. 5. Per jednostka organizacyjna.

6.6.8. Oprogramowanie musi umożliwiać interakcję użytkownika końcowego w trakcie wykonywania zadania, w szczególności: 1. Opóźnienie instalacji. 2. Przypomnienie później. 3. Akceptację instalacji. 4. Odmowę lub odroczenie, jeśli polityka administratora na to pozwala. 5. Informowanie użytkownika o czasie pozostałym do restartu lub rozpoczęcia zadania.

6.6.9. Oprogramowanie musi umożliwiać definiowanie okien serwisowych dla urządzeń, grup urządzeń lub zadań.

6.6.10. Oprogramowanie musi umożliwiać wymuszenie uruchomienia zadania poza standardowym oknem, jeśli administrator posiada odpowiednie uprawnienia.

6.7. Dystrybucja i instalacja oprogramowania

6.7.1. Oprogramowanie musi umożliwiać dystrybucję dowolnego oprogramowania, nie tylko paczek MSI, ale również instalatorów typu EXE, InstallShield, InnoSetup, NullSoft, Wise Installer oraz innych powszechnie stosowanych mechanizmów instalacyjnych oraz tzw. custom'owych.

6.7.2. Oprogramowanie musi posiadać kreator do tworzenia pakietów instalacyjnych obejmujących różnorodne oprogramowanie.

6.7.3. Oprogramowanie musi umożliwiać wykrywanie i obsługę wielu mechanizmów instalacji, w szczególności MSI, EXE, InnoSetup, InstallShield, NullSoft i innych.

6.7.4. Oprogramowanie musi umożliwiać automatyzowanie instalatorów wraz z możliwością dostosowywania instalatorów tak, aby możliwe było nadpisywanie pól opisowych, parametrów instalacji, katalogów docelowych, przełączników, kluczy rejestru, plików konfiguracyjnych oraz innych ustawień.

6.7.5. Oprogramowanie musi umożliwiać administratorowi zautomatyzowanie procesu instalacji w taki sposób, aby na urządzeniu końcowym nie było wymagane podanie jakichkolwiek opcji przez użytkownika.

6.7.6. Oprogramowanie musi umożliwiać instalację w trybie cichym oraz graficznym.

6.7.7. Oprogramowanie musi umożliwiać dodawanie w ramach instalatora lub zadania co najmniej następujących akcji: 1. Blokowanie klawiatury i myszy. 2. Zmiany w rejestrze systemowym. 3. Działania na plikach i folderach. 4. Uruchomienie skryptu PowerShell. 5. Uruchomienie skryptu BAT/CMD. 6. Uruchomienie skryptu VBS, jeżeli wspierany przez system operacyjny. 7. Zatrzymanie i wznowienie usług. 8. Zatrzymanie i uruchomienie procesów. 9. Utworzenie skrótów. 10. Skopiowanie plików. 11. Ustawienie katalogu roboczego. 12. Zmianę uprawnień lub kontekstu uruchomienia.

6.7.8. Zdalna dystrybucja oprogramowania musi wykorzystywać natywną logikę instalatora i nie może wymagać wyłącznie technologii snapshotingu jako podstawowego mechanizmu pakietowania.

6.7.9. Oprogramowanie musi umożliwiać harmonogramowanie dystrybucji: 1. W zadanym przedziale czasowym. 2. Cyklicznie, np. wybrany dzień tygodnia i godzina. 3. Jednorazowo na żądanie. 4. Według warunków dynamicznych. 5. Według okien serwisowych.

6.7.10. Oprogramowanie musi umożliwiać tworzenie zależności między aplikacjami, np. wymóg instalacji komponentu A przed instalacją aplikacji B.

6.7.11. W przypadku braku aplikacji zależnej na urządzeniu końcowym system musi umożliwiać automatyczne wdrożenie aplikacji zależnej przed instalacją aplikacji docelowej.

6.7.12. Oprogramowanie musi umożliwiać integrację procedury odinstalowania aplikacji.

6.7.13. Oprogramowanie musi umożliwiać transparentną instalację pakietów, z zapisem w logach informacji o rzeczywistych parametrach instalacji, np. komendzie instalatora, kodach zwrotnych i statusie wykonania.

6.7.14. Oprogramowanie musi umożliwiać różnorodną weryfikację instalacji, w szczególności poprzez: 1. Kod zwrotny programu instalacyjnego. 2. Występowanie pliku. 3. Występowanie katalogu. 4. Wpis w rejestrze. 5. Obecność usługi. 6. Obecność procesu. 7. Wersję aplikacji. 8. Wynik skryptu weryfikacyjnego.

6.7.15. Oprogramowanie musi umożliwiać ustawienie kontekstu bezpieczeństwa, w jakim dana paczka ma zostać zainstalowana na urządzeniu końcowym.

6.7.16. Oprogramowanie musi umożliwiać tworzenie plików transformacji MST dla pakietów MSI.

6.7.17. Oprogramowanie musi umożliwiać tworzenie pakietów instalacyjnych obejmujących instalację wielu aplikacji oraz wykonanie szeregu dodatkowych funkcji związanych np. z inwentaryzacją, konfiguracją, kontrolą zgodności lub wykonaniem skryptów.

6.7.18. Oprogramowanie musi posiadać środowisko skryptowe umożliwiające tworzenie własnych skryptów i ich dystrybucję z poziomu konsoli.

6.7.19. Środowisko skryptowe powinno umożliwiać proste tworzenie skryptów metodą drag and drop lub zbliżoną metodą graficzną.

6.7.20. Oprogramowanie musi posiadać zestaw standardowych poleceń skryptowych oraz pomoc kontekstową.

6.7.21. Oprogramowanie musi umożliwiać tryb testowy step-by-step dla tworzonych automatyzacji lub pakietów.

6.7.22. Oprogramowanie musi posiadać możliwość sterowania również interfejsami niestandardowymi, w tym aplikacjami opartymi np. o Java lub inną technologię, jeżeli jest to technicznie możliwe.

6.8. Patch Management i aktualizacje systemów Microsoft

6.8.1. Oprogramowanie musi umożliwiać centralne zarządzanie poprawkami bezpieczeństwa dla systemów klienckich oraz serwerowych Microsoft Windows.

6.8.2. Oprogramowanie musi umożliwiać dystrybucję poprawek Windows bez konieczności wykorzystywania WSUS jako jedynego mechanizmu dystrybucji.

6.8.3. Oprogramowanie może umożliwiać integrację lub triggerowanie z poziomu WSUS, jeżeli Zamawiający wykorzystuje WSUS w swoim środowisku.

6.8.4. Oprogramowanie musi umożliwiać obsługę aktualizacji dla aktualnych systemów Windows, co najmniej Windows 10, Windows 11 oraz Windows Server 2016/2019/2022/2025, jeżeli systemy te są wspierane przez Producenta.

6.8.5. Oprogramowanie powinno umożliwiać obsługę starszych systemów Windows w zakresie wspieranym przez Producenta, z uwzględnieniem ograniczeń systemów pozostających poza wsparciem Microsoft.

6.8.6. Producent Oprogramowania musi zapewniać stały dostęp do bazy danych poprawek Microsoft lub równoważnego mechanizmu pozwalającego na identyfikację wymaganych aktualizacji.

6.8.7. Baza poprawek lub katalog aktualizacji musi być dostępny z poziomu konsoli Oprogramowania po jego aktualizacji przez Producenta.

6.8.8. Oprogramowanie musi umożliwiać określanie ścisłych wymagań czasowych dla instalacji poprawek Microsoft oraz kontrolowanie ich wykonania.

6.8.9. Oprogramowanie musi umożliwiać rozdzielenie procesu sprawdzania brakujących poprawek od procesu instalacji poprawek.

6.8.10. Poprawki muszą być możliwe do zatwierdzania automatycznie lub ręcznie.

6.8.11. Oprogramowanie musi umożliwiać definiowanie różnych reguł patch management dla różnych grup urządzeń, np. stacji roboczych, serwerów, urządzeń testowych, urządzeń produkcyjnych lub urządzeń krytycznych.

6.8.12. Oprogramowanie musi umożliwiać raportowanie: 1. Brakujących poprawek. 2. Zainstalowanych poprawek. 3. Statusu instalacji. 4. Błędów instalacji. 5. Urządzeń wymagających restartu. 6. Poziomu zgodności patchingowej.

6.8.13. Oprogramowanie musi umożliwiać zarządzanie restartami po instalacji poprawek, w tym odroczenia, komunikaty dla użytkownika, harmonogramy restartów i wymuszenie restartu zgodnie z polityką administratora.

6.8.14. Oprogramowanie musi umożliwiać instalację poprawek w ramach zdefiniowanych okien serwisowych.

6.8.15. Oprogramowanie nie może wymagać korzystania z wycofanych mechanizmów patchowania klasycznego, jeżeli zostały usunięte z aktualnej wersji systemu. Wymagane jest wykorzystanie aktualnego mechanizmu Update Management.

6.9. Aktualizacja aplikacji firm trzecich / Managed Software

6.9.1. Oprogramowanie musi zawierać gotowe repozytorium aktualizacji aplikacji firm trzecich lub równoważny mechanizm utrzymywany przez Producenta.

6.9.2. Repozytorium powinno obejmować popularne aplikacje biznesowe, narzędziowe, przeglądarki, komponenty runtime oraz aplikacje powszechnie występujące w środowiskach organizacji, np. Adobe, Java, przeglądarki internetowe, narzędzia komunikacyjne, narzędzia konferencyjne i inne.

6.9.3. Repozytorium aktualizacji aplikacji firm trzecich powinno dostarczać paczki pozbawione niepożądanych dodatków reklamowych, toolbarów lub komponentów adware, o ile dotyczy.

6.9.4. Oprogramowanie musi umożliwiać automatyczną aktualizację aplikacji firm trzecich.

6.9.5. Oprogramowanie musi umożliwiać definiowanie poziomów zatwierdzania aktualizacji aplikacji firm trzecich.

6.9.6. Oprogramowanie musi umożliwiać raportowanie statusu aktualizacji aplikacji firm trzecich.

6.9.7. Oprogramowanie musi umożliwiać konfigurację aktualizacji w sposób pozwalający na najpierw wdrożenie do grupy testowej, a następnie do grup produkcyjnych

6.10. Zarządzanie systemami operacyjnymi / OS Install

6.10.1. Oprogramowanie musi umożliwiać automatyczną i natywną instalację systemów operacyjnych Windows.

6.10.2. Oprogramowanie musi umożliwiać wdrażanie systemów Windows przez sieć z wykorzystaniem PXE lub równoważnego mechanizmu.

6.10.3. Oprogramowanie musi umożliwiać obsługę obrazów Windows PE.

6.10.4. Oprogramowanie musi umożliwiać automatyczne przygotowanie i personalizację instalacji systemu operacyjnego.

6.10.5. Oprogramowanie musi umożliwiać przypisywanie sterowników do sprzętu lub profili sprzętowych.

6.10.6. Oprogramowanie musi umożliwiać automatyzację procesu migracji systemów Windows, w szczególności migracji do Windows 11.

6.10.7. Oprogramowanie musi umożliwiać instalację systemu operacyjnego wraz z aplikacjami, konfiguracjami oraz zadaniami powdrożeniowymi.

6.10.8. Oprogramowanie musi umożliwiać wykorzystanie profili sprzętowych i przypisania sterowników do określonych klas urządzeń.

6.10.9. Oprogramowanie powinno wspierać DHCP Option 82 lub równoważny mechanizm, jeśli jest wymagany w środowisku sieciowym Zamawiającego.

6.11. Inwentaryzacja sprzętu i oprogramowania

6.11.1. Oprogramowanie musi umożliwiać automatyczne skanowanie komputerów, serwerów, urządzeń mobilnych, urządzeń Linux, urządzeń macOS, urządzeń sieciowych oraz wybranych urządzeń OT/ICS.

6.11.2. Oprogramowanie musi umożliwiać inwentaryzację sprzętu obejmującą co najmniej: 1. Producenta urządzenia. 2. Model. 3. Numer seryjny. 4. Procesor. 5. Pamięć RAM. 6. Dyski. 7. Karty sieciowe. 8. Adresy IP. 9. Adresy MAC. 10. BIOS/UEFI. 11. TPM, jeżeli dostępne. 12. Informacje o baterii, jeżeli dotyczy.

6.11.3. Oprogramowanie musi umożliwiać inwentaryzację oprogramowania obejmującą co najmniej: 1. Nazwę aplikacji. 2. Wersję. 3. Producenta. 4. Datę instalacji, jeżeli dostępna. 5. Informację o ostatnim uruchomieniu aplikacji, jeżeli dostępna. 6. Informację o użyciu aplikacji, jeżeli dostępna.

6.11.4. Oprogramowanie musi umożliwiać identyfikację stopnia wykorzystania oprogramowania w celu wsparcia zarządzania licencjami i optymalizacji kosztów.

6.11.5. Oprogramowanie musi umożliwiać kontrolę przypisanych licencji do konta, użytkownika, urządzenia lub zasobu.

6.11.6. Oprogramowanie musi umożliwiać przechowywanie historii zmian wybranych danych inwentaryzacyjnych.

6.11.7. Oprogramowanie musi umożliwiać przypisywanie zasobów do użytkowników lub grup, a nie wyłącznie do urządzeń, jeżeli taka funkcjonalność jest dostępna w aktualnej wersji systemu.

6.12. Network Discovery, urządzenia sieciowe i OT/ICS

6.12.1. Oprogramowanie musi umożliwiać automatyczne skanowanie sieci firmowej.

6.12.2. Oprogramowanie musi umożliwiać identyfikację urządzeń SNMP, takich jak drukarki, routery, przełączniki, urządzenia sieciowe, urządzenia przemysłowe oraz inne urządzenia wspierające SNMP.

6.12.3. Oprogramowanie musi wspierać SNMP v1, SNMP v2c oraz SNMP v3.

6.12.4. Dla SNMP v3 Oprogramowanie powinno wspierać silne mechanizmy uwierzytelnienia, w tym SHA384/SHA512, jeżeli są wspierane przez urządzenia i Producenta Oprogramowania.

6.12.5. Oprogramowanie musi umożliwiać konfigurację wielu community strings dla skanowania SNMP.

6.12.6. Oprogramowanie musi umożliwiać powtarzalne harmonogramowanie zadań network discovery.

6.12.7. Oprogramowanie musi umożliwiać import wyników network discovery z plików, jeżeli środowisko Zamawiającego wymaga skanowania offline.

6.12.8. Oprogramowanie musi umożliwiać przypisywanie wykrytych urządzeń do odpowiednich klas, grup lub widoków.

6.12.9. Oprogramowanie musi umożliwiać konwersję wykrytego urządzenia sieciowego do typu Windows lub Linux, jeżeli urządzenie zostanie zidentyfikowane jako możliwe do zarządzania agentem.

6.12.10. Oprogramowanie musi posiadać skaner do wykrywania urządzeń w sieci.

6.12.11. Oprogramowanie musi umożliwiać identyfikację i inwentaryzację wybranych urządzeń OT/ICS, co najmniej przez: 1. SNMP. 2. OPC UA. 3. Siemens S7Comm.

6.12.12. Oprogramowanie powinno wspierać identyfikację urządzeń Siemens SIMATIC S7 1200 i S7 1500 oraz protokół S7Comm dla Siemens SIMATIC S7 300 i S7 400.

6.12.13. Oprogramowanie powinno wspierać OPC UA dla niezależnego od producenta wykrywania sterowników PLC z aktywnym serwerem OPC UA.

6.12.14. Oprogramowanie musi umożliwiać wizualizację topologii sieci lub co najmniej prezentację zależności i informacji o wykrytych urządzeniach sieciowych.

6.13. Zarządzanie urządzeniami mobilnymi / MDM

6.13.1. Oprogramowanie musi umożliwiać zautomatyzowane zarządzanie urządzeniami mobilnymi Android, iOS oraz iPadOS.

6.13.2. Oprogramowanie musi wspierać Android Enterprise.

6.13.3. Oprogramowanie musi umożliwiać obsługę urządzeń Android co najmniej w trybach: 1. Fully Managed. 2. Work Profile. 3. Dedicated Device. 4. Corporate-Owned Personally Enabled, jeżeli wspierane przez Producenta i Android Enterprise.

6.13.4. Oprogramowanie musi umożliwiać zarządzanie urządzeniami Apple z wykorzystaniem mechanizmów MDM Apple.

6.13.5. Oprogramowanie powinno wspierać Apple Business Manager / Apple School Manager, jeżeli Zamawiający korzysta z tych usług.

6.13.6. Oprogramowanie musi umożliwiać: 1. Rejestrację urządzeń mobilnych. 2. Wymuszanie polityk bezpieczeństwa. 3. Zarządzanie profilami konfiguracyjnymi. 4. Zarządzanie aplikacjami. 5. Blokowanie urządzeń. 6. Zdalne wymazanie urządzenia. 7. Zdalne wymazanie danych firmowych, jeżeli platforma to wspiera. 8. Egzekwowanie wymagań hasła lub kodu PIN. 9. Szyfrowanie urządzenia, jeżeli platforma to wspiera. 10. Weryfikację zgodności urządzenia. 11. Raportowanie statusu urządzeń.

6.13.7. Oprogramowanie musi umożliwiać per-app VPN, tj. zestawianie połączenia VPN dla wybranych aplikacji, a nie wyłącznie dla całego urządzenia.

6.13.8. Oprogramowanie musi umożliwiać konfigurację ograniczeń bezpieczeństwa urządzeń mobilnych.

6.13.9. Oprogramowanie musi umożliwiać blokowanie funkcji wybranych przez administratora.

6.13.10. Oprogramowanie powinno umożliwiać wykonywanie poleceń na urządzeniach mobilnych, w tym wyświetlenie komunikatu użytkownikowi, ustawienie parametrów urządzenia, wymuszenie synchronizacji lub podobne działania administracyjne.

6.13.11. Oprogramowanie musi umożliwiać raportowanie zgodności urządzeń mobilnych.

6.14. Zarządzanie Linux

6.14.1. Oprogramowanie musi umożliwiać zarządzanie urządzeniami Linux z wykorzystaniem agenta lub trybu SSH, zgodnie z zakresem wspieranym przez Producenta.

6.14.2. Oprogramowanie musi umożliwiać inwentaryzację urządzeń Linux.

6.14.3. Oprogramowanie musi umożliwiać wykonywanie własnych skryptów lokalnie na urządzeniu Linux.

6.14.4. Oprogramowanie musi umożliwiać sprawdzanie statusu aktualizacji pakietów Linux.

6.14.5. Oprogramowanie musi umożliwiać aktualizację pakietów Linux przy wykorzystaniu wspieranych managerów pakietów.

6.14.6. Oprogramowanie musi wspierać co najmniej APT, DNF, Zypper, Snap oraz Flatpak, jeżeli są dostępne na zarządzanym systemie.

6.14.7. Oprogramowanie musi umożliwiać prezentację informacji o pakietach zainstalowanych, brakujących, zablokowanych lub wymagających aktualizacji.

6.14.8. Oprogramowanie musi umożliwiać wykorzystanie dynamicznych grup dla urządzeń Linux na podstawie kryteriów takich jak architektura procesora, status aktualizacji pakietów, dystrybucja, wersja systemu lub tryb uruchomienia.

6.15. Zarządzanie macOS

6.15.1. Oprogramowanie musi umożliwiać zarządzanie urządzeniami macOS w zakresie wspieranym przez Producenta.

6.15.2. Oprogramowanie musi umożliwiać inwentaryzację urządzeń macOS.

6.15.3. Oprogramowanie musi umożliwiać raportowanie statusu urządzeń macOS.

6.15.4. Oprogramowanie powinno umożliwiać konfigurację profili macOS, w tym profili Wi-Fi, bezpieczeństwa i zgodności, jeżeli jest to wspierane przez Producenta.

6.15.5. Oprogramowanie powinno umożliwiać zarządzanie zgodnością urządzeń macOS w kontekście co-management i Conditional Access.

6.16. Zdalne wsparcie i zdalny dostęp

6.16.1. Oprogramowanie musi umożliwiać bezpośrednie połączenie z urządzeniami końcowymi w celu zdalnego wsparcia użytkownika.

6.16.2. Oprogramowanie musi umożliwiać zdalny dostęp do urządzeń w sieci LAN.

6.16.3. Oprogramowanie musi umożliwiać zdalny dostęp do urządzeń poza siecią LAN, bez konieczności zestawiania VPN, za pośrednictwem Gateway/Proxy lub równoważnego mechanizmu.

6.16.4. Oprogramowanie musi umożliwiać zdalne wsparcie urządzeń mobilnych Android/iOS/iPadOS, jeżeli Zamawiający zakupi odpowiedni moduł lub dodatek.

6.16.5. Oprogramowanie musi umożliwiać kontrolę uprawnień do zdalnego dostępu.

6.16.6. Oprogramowanie musi umożliwiać audyt lub rejestrację informacji o sesjach zdalnych, jeżeli jest to wspierane przez moduł zdalnego wsparcia.

6.16.7. Oprogramowanie musi umożliwiać obsługę zdalnego dostępu zgodnie z zasadami bezpieczeństwa Zamawiającego, w tym wymóg zgody użytkownika, jeżeli Zamawiający wymaga takiego trybu.

8. Zgodność z NIS2 i KSC

8.1. Oprogramowanie musi wspierać Zamawiającego w realizacji wymagań związanych z cyberbezpieczeństwem, w szczególności wynikających z dyrektywy NIS2, ustawy o krajowym systemie cyberbezpieczeństwa oraz dobrych praktyk bezpieczeństwa IT

9. Wymagania dla Producenta

9.1. Producent Oprogramowania musi posiadać aktualny certyfikat ISO/IEC 27001:2022 lub równoważny.

9.2. Certyfikat musi obejmować co najmniej procesy związane z rozwojem, utrzymaniem, eksploatacją lub bezpieczeństwem produktów programistycznych Producenta.

9.3. Producent musi zapewniać regularne aktualizacje Oprogramowania.

9.4. Producent musi publikować dokumentację techniczną oraz informacje o wymaganiach systemowych.

9.5. Producent musi zapewniać dostęp do poprawek bezpieczeństwa.

9.6. Producent musi prowadzić rozwój Oprogramowania w obszarach zarządzania endpointami, bezpieczeństwa, automatyzacji, raportowania i integracji..

Technologia autentykacji wieloskładnikowej dla użytkowników:

Rozwiązanie musi umożliwiać zastosowanie sprzętowych kluczy bezpieczeństwa do realizacji silnego wieloskładnikowego uwierzytelniania (MFA) oraz zabezpieczenia dostępu do systemów i stanowisk pracy zgodnie ze standardami FIDO2/WebAuthn.

Zamawiający wymaga dostarczenia i wdrożenia 70 sztuk sprzętowych kluczy bezpieczeństwa.

Sprzętowe klucze bezpieczeństwa muszą spełniać następujące wymagania techniczne:

1. Typ urządzenia: sprzętowy klucz bezpieczeństwa FIDO2/U2F przeznaczony do uwierzytelniania wieloskładnikowego.
2. Interfejs komunikacyjny: USB-A.
3. Obsługiwane standardy: FIDO2.1, WebAuthn, FIDO U2F, CTAP2.1.
4. Obsługiwane funkcjonalności: passkeys, logowanie bezhasłowe, MFA, HOTP, TOTP, PIV oraz OpenPGP.
5. Ochrona kodem PIN: możliwość wymuszania złożoności kodu PIN na poziomie oprogramowania układowego urządzenia.
6. Liczba przechowywanych poświadczeń FIDO2: co najmniej 300 rekordów Resident Keys / Discoverable Credentials.
7. Obsługa OTP: możliwość przechowywania co najmniej 50 profili TOTP/HOTP za pośrednictwem aplikacji oraz obsługa co najmniej jednego profilu HOTP przez interfejs HID
8. Autoryzacja fizyczna: pojemnościowy sensor dotykowy umożliwiający potwierdzanie operacji wymagających fizycznej interakcji użytkownika.
9. Obsługiwane mechanizmy kryptograficzne: ECDSA, SHA-256, AES, HMAC oraz ECDH.
10. Obsługiwane algorytmy i krzywe kryptograficzne: RSA o długości klucza 2048, 3072 i 4096 bitów, ECC secp256r1, secp256k1, secp384r1 i secp521r1, Ed25519 oraz X25519.
11. Funkcjonalności dla środowisk enterprise: obsługa PIV Smart Card, OpenPGP oraz uwierzytelniania SSH z wykorzystaniem kluczy sprzętowych, w tym ecdsa-sk i ed25519-sk.
12. Wymiary: nie większe niż $42,1 \times 17 \times 6$ mm.
13. Masa: nie większa niż 5 g.
14. Zasilanie: przez interfejs USB, napięcie 5 V DC, pobór prądu nie większy niż 35 mA.
15. Odporność i trwałość: zabezpieczenie płytki elektronicznej powłoką ochronną zwiększającą odporność na wilgoć, deklarowana żywotność co najmniej 10 lat oraz trwałość co najmniej 100 000 cykli programowania.

24. Usługa kopii zapasowych w chmurze obliczeniowej IT/OT/ICS

Informacje wstępne

- 1.1. Zamawiający obecnie wykonuje standardowe zadania backupu maszyn wirtualnych do lokalnego repozytorium zgodnie z ustanowioną polityką kopii zapasowych. Zamawiający oczekuje dostarczenia kompletnego rozwiązania, realizującego kopie wyniesione.

- 1.2. Zamawiający oczekuje dostarczenia jednego, kompletnego oprogramowania spełniającego wszystkie wymagania. Nie dopuszcza się dostarczenia dwóch odrębnych, zintegrowanych rozwiązań. Wykonawca zapewni licencje/subskrypcje ściśle dostosowane jakościowo i ilościowo do wymagań postępowania.

Wymagania dot. systemu kopii wyniesionych (off-site backup)

- 1.3. System musi zapewniać automatyczne wykonywanie i przechowywanie kopii zapasowych poza siedzibą Zamawiającego przez co najmniej 12 miesięcy od wdrożenia.
- 1.4. Komunikacja między infrastrukturą Zamawiającego a zdalnym miejscem składowania danych off-site musi odbywać się przy użyciu bezpiecznego protokołu (min. SSL/TLS lub IPSec).
- 1.5. System po stronie Wykonawcy nie może przyjmować ani przechowywać niezaszyfrowanych kopii zapasowych – wszystkie dane przesyłane off-site muszą być szyfrowane po stronie źródła.
- 1.6. Na żądanie Zamawiającego Wykonawca udostępni szczegółową lokalizację fizyczną (adres budynku, nr szafy/działu w centrum danych) urządzeń, na których przechowywane są wyniesione kopie danych.
- 1.7. Wykonawca zapewni samoobsługowy portal usługi kopii wyniesionych, umożliwiający:
 - 1.7.1. zdalne monitorowanie i zarządzanie kopiami zapasowymi z poziomu jednego, przyjaznego interfejsu WWW;
 - 1.7.2. zabezpieczenie dostępu do portalu przy użyciu SSL oraz wieloskładnikowej autentykacji (MFA – login, hasło i token);
 - 1.7.3. podgląd bieżącego i historycznego stanu zadań backupu oraz eksport raportów do pliku;
 - 1.7.4. możliwość uruchamiania, zatrzymywania, wznowiania zadań backupu oraz przeglądania ich logów (rejestrów zdarzeń);
 - 1.7.5. obsługę alarmów związanych z backupem i stanem usługi oraz eksport zdarzeń do pliku;
 - 1.7.6. funkcje raportowania i rozliczeń zasobów: przegląd wykorzystania przydzielonej przestrzeni, liczby chronionych serwerów/stacji/VM, generowanie raportów statystycznych;
 - 1.7.7. portal powinien udostępniać funkcje umożliwiające scentralizowane zarządzanie, monitorowanie oraz raportowanie usług backupu typu Backup-as-a-Service (BaaS) i Disaster Recovery-as-a-Service (DRaaS).
- 1.8. Dopuszczalne jest wykorzystanie technologii w trybie multi-tenant do realizacji kopiowania i przechowywania danych off-site (z zachowaniem izolacji klientów i szyfrowania transportu danych).
- 1.9. Wykonawca udostępni Zamawiającemu repozytorium na kopie zapasowe o pojemności 10 TB z możliwością rozbudowy do minimum 200 TB (wielkość dodatkowej rozbudowy repozytorium nie jest elementem oferty).
- 1.10. Zamawiający wymaga, aby dostarczone licencje/subskrypcje umożliwiały wykonywanie kopii zapasowych dla 15 maszyn wirtualnych.
- 1.11. Sprzęt pamięci masowej musi wspierać transfer wielowątkowy danych, mieć redundancję wszystkich komponentów (brak pojedynczych punktów awarii – awaria jednego elementu nie przerywa pracy) oraz pozwalać na rozbudowę i aktualizację (firmware) w trybie online.
- 1.12. Architektura repozytorium musi gwarantować, że awaria dowolnego dysku, półki dyskowej, kontrolera, węzła czy zasilacza nie przerwie dostępu do pozostałych danych.
- 1.13. Awaryjne odtwarzanie danych z wyniesionego miejsca składowania danych musi odbywać się automatycznie za pomocą lokalnego interfejsu systemu kopii zapasowych Zamawiającego, bez udziału pracowników Wykonawcy.
- 1.14. Wykonawca zapewni wsparcie techniczne i utrzymanie rozwiązania przez cały okres 12 miesięcy. Na potrzeby zgłaszania zmian konfiguracji i awarii Wykonawca udostępni dedykowany kanał mailowy. Wykonawca gwarantuje:
 - 1.14.1. podjęcie zgłoszenia awarii w czasie nie dłuższym niż 4 godziny;
 - 1.14.2. usunięcie awarii w czasie nie dłuższym niż 24 godziny;
 - 1.14.3. podjęcie zgłoszenia zmiany konfiguracji w czasie nie dłuższym niż 8 godzin;
 - 1.14.4. realizację zgłoszenia zmiany konfiguracji wykonywania kopii wyniesionych w czasie nie dłuższym niż 2 dni robocze.
- 1.15. Wykonawca zobowiązany jest do zapewnienia pełnego wsparcia eksperckiego, merytorycznego i administracyjnego w zakresie realizacji przedmiotu zamówienia, zgodnie z najlepszymi praktykami i zgodnie z najnowszymi wytycznymi branżowymi i technologicznymi w tym zakresie, jak również wytycznymi z audytów przeprowadzanych przez instytucje zewnętrzne, którym podlega Zamawiający, przez cały okres obowiązywania umowy.
- 1.16. Wykonawca przygotuje dokumentację użytkownika i administratora wdrożonego systemu.

- 1.17. Wykonawca zobowiązany jest do instruktażu 2 administratorów Zamawiającego z administrowania i obsługi dostarczonego rozwiązania.
- 1.18. Wykonawca jest odpowiedzialny za testowanie kopii zapasowych Zamawiającego pod kątem poprawności przechowywanych danych oraz konfiguracji oraz przeprowadzenie testów odtworzeniowych nie rzadziej niż dwa razy w ciągu roku.

Wymagania dot. centrum przetwarzania danych, w którym składowane będą kopie wyniesione

- 1.19. Centrum przetwarzania danych, w którym będą składowane wyniesione kopie zapasowe, musi spełniać co najmniej standard TIER III (poziom z pełną redundancją krytycznych systemów i możliwością utrzymania bez przerywania pracy centrum danych, zapewniający wysoką dostępność) lub równoważne.
- 1.20. Infrastruktura w centrum przetwarzania danych, spełnia co najmniej następujące wymagania:
- 1.20.1. posiada aktywne elementy infrastruktury IT zapewniające pracę w modelu n+1;
 - 1.20.2. musi posiadać redundantne wewnętrzne linie chłodu;
 - 1.20.3. musi posiadać możliwość odłączania każdego elementu linii dystrybucji energii elektrycznej i chłodu w celu poddania czynnościom serwisowym, tak aby nie zakłócić normalnej pracy urządzeń dwu-zasilaczowych;
 - 1.20.4. musi posiadać wdrożoną strefową kontrolę dostępu w oparciu o karty zbliżeniowe lub rozwiązanie równoważne;
 - 1.20.5. musi posiadać całodobową ochronę fizyczną z rejestracją kamer monitoringu wizyjnego na zewnątrz i wewnątrz budynku;
 - 1.20.6. musi być zlokalizowane na terenie Polski w odległości nie mniejszej niż 25 km w linii prostej od siedziby Zamawiającego, gdzie znajduje się lokalne repozytorium backupu;
 - 1.20.7. musi posiadać niezależne strefy pożarowe oraz system wczesnej detekcji dymu i ognia, a pomieszczenia ze sprzętem IT muszą być wyposażone w zautomatyzowaną aparaturę gaśniczą;
 - 1.20.8. musi mieć zapewnione zasilanie z dwóch niezależnych linii energetycznych oraz rezerwowe zasilanie realizowane przy pomocy UPS oraz agregatu prądotwórczego;
 - 1.20.9. musi posiadać zasilanie gwarantowane w układzie n+1, zapewniające nieprzerwane zasilanie;
 - 1.20.10. dystrybucja energii elektrycznej odbywa się z wykorzystaniem niezależnych torów zasilania, z osobnym zabezpieczeniem nadmiarowo prądowym z gwarantowanym podtrzymaniem zasilania z wykorzystaniem UPS i agregatu prądotwórczego;
 - 1.20.11. podstawowe i zapasowe łącza internetowe symetryczne każde o przepustowości nie mniejszej niż 1 Gb/s do infrastruktury, na której składowane będą wyniesione kopie zapasowe (Wykonawca nie zapewnia łącza po stronie Zamawiającego).

WARUNKI REALIZACJI CZĘŚCI II

Przedmiot Części II obejmuje kompletną dostawę, wdrożenie, konfigurację, uruchomienie i integrację rozwiązań wskazanych w tabeli szczegółowych parametrów, wraz z dokumentacją, szkoleniem, gwarancją, aktualizacjami i wsparciem technicznym. Obowiązki określone poniżej stosuje się wyłącznie do zakresu Części II.

1. Dokumentacja Analizy Przedwdrożeniowej

Przed rozpoczęciem prac ingerujących w środowisko produkcyjne Wykonawca opracuje Dokumentację Analizy Przedwdrożeniowej (DAP), podlegającą uzgodnieniu i zatwierdzeniu przez Zamawiającego na zasadach określonych w projektowanych postanowieniach umowy.

- opis stanu istniejącego w zakresie niezbędnym do realizacji Części II;
- opis docelowej architektury wdrażanych rozwiązań;
- wykaz sprzętu, oprogramowania, licencji, subskrypcji, modułów i komponentów;
- sposób integracji z infrastrukturą Zamawiającego;
- model licencjonowania i okresy obowiązywania licencji, subskrypcji, aktualizacji i wsparcia;
- harmonogram prac, okna serwisowe, plan migracji, plan wycofania zmiany oraz plan testów odbiorowych;
- zasady komunikacji, raportowania, zarządzania ryzykiem i obsługi zmian.

2. Dostawa, wdrożenie i integracja

Szczegółowy opis wdrożenia znajduje się w pozycji – 19.

3. Licencje i subskrypcje

Licencje i subskrypcje muszą pochodzić z legalnego źródła, obejmować wszystkie jednostki licencyjne wskazane w tabeli części II oraz zapewniać dostęp do pełnej wymaganej funkcjonalności, aktualizacji bezpieczeństwa i wsparcia producenta. Okres subskrypcji powinien rozpocząć się nie wcześniej niż w terminie uzgodnionym z Zamawiającym, co do zasady nie wcześniej niż w dniu uruchomienia albo odbioru danego rozwiązania; dla Usług Ciągłych – od dnia wskazanego w Protokole Uruchomienia Usługi.

4. Dokumentacja powykonawcza

Wykonawca prześle w języku polskim dokumentację powykonawczą w formacie PDF oraz – w odniesieniu do dokumentów opracowanych przez Wykonawcę – również w formacie edytowalnym.

- wykaz dostarczonego sprzętu, oprogramowania, licencji i subskrypcji;
- opis wdrożonej architektury, konfiguracji i integracji;
- instrukcje administracyjne, eksploatacyjne, aktualizacyjne i odtworzeniowe;
- dokumenty licencyjne, gwarancyjne i serwisowe;
- raport z przeprowadzonych testów i wykaz ewentualnych ograniczeń.

5. Szkolenie administratorów

Wykonawca przeprowadzi szkolenie lub instruktaż administratorów wskazanych przez Zamawiającego, obejmujący architekturę rozwiązania, bieżącą administrację, tworzenie polityk bezpieczeństwa, analizę

alarmów i zdarzeń, aktualizacje, kopie konfiguracji, obsługę awarii oraz korzystanie ze wsparcia producenta. Wykonawca przekaze materiały szkoleniowe w języku polskim.

6. Gwarancja, serwis i wsparcie

Wykonawca zapewni gwarancję, aktualizacje i wsparcie techniczne przez okres wskazany w tabeli części II i projektowanych postanowieniach umowy. Priorytety zgłoszeń, czasy reakcji, czasy przywrócenia działania lub usunięcia awarii oraz zasady eskalacji określono w opisach poszczególnych pozycji niniejszego OPZ; projektowane postanowienia umowy odsyłają do tych parametrów.

7. Odbiór części II

Warunkiem odbioru Części II (Protokół Odbioru Wdrożenia) jest łączne:

- dostarczenie wszystkich wymaganych urządzeń, licencji, subskrypcji i komponentów;
- wykonanie instalacji, konfiguracji, integracji i uruchomienia;
- pozytywne zakończenie testów określonych w zatwierdzonej DAP;
- usunięcie wad i niezgodności uniemożliwiających bezpieczną eksploatację;
- przekazanie kompletnej dokumentacji i dokumentów licencyjnych;
- przeprowadzenie szkolenia administratorów;
- podpisanie protokołu odbioru przez Zamawiającego.



Podpisany elektronicznie przez
Ewelina Ewa Głęńsk
23.10.2026
12:47:28 +02'00'