**Szadek, dnia \_\_. 11. 2025 r.**

**nr sprawy \_\_\_\_\_\_**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**dotyczy:** postępowania o udzielenie zamówienia publicznego w trybie podstawowym bez przeprowadzenia negocjacji, o wartości nieprzekraczającej 221 000 Euro, na dostawę, montaż i konfigurację 3 szt. zasilaczy UPS, licencji oprogramowania do monitorowania infrastruktury informatycznej, licencji do oprogramowania do zarządzania i aktualizacji systemów operacyjnych Client Access License, 2 szt. serwerów typu RACK, 2 szt. serwerów dziedzinowych, 3 szt. Macierzy Dyskowych, oprogramowania Menadżera Logów oraz 4 szt. zarządzanych urządzeń sieciowych z obsługą standardu 802.1X, przeprowadzonego w ramach projektu “Cyberbezpieczny Samorząd”.

**Przedmiotem niniejszego zamówienia jest dostawa, montaż oraz konfiguracja:**

1. 3 szt. zasilaczy UPS,
2. 60 licencji oprogramowania do monitorowania infrastruktury informatycznej,
3. licencji do oprogramowania do zarządzania i aktualizacji systemów operacyjnych Client Access License,
4. 2 szt. serwerów typu RACK,
5. 2 szt. serwerów dziedzinowych,
6. 3 szt. Macierzy Dyskowych,
7. oprogramowania Menadżera Logów,
8. 4 szt. zarządzanych urządzeń sieciowych z obsługą standardu 802.1X,

szczegółowo opisanych poniżej.

1. **Zakup 3 szt. zasilaczy UPS wraz z dostawą oraz montażem**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa elementu, parametru lub cechy** | **Opis wymagań** |
| 1 | Moc pozorna | 3000 VA |
| 2 | Moc rzeczywista | 3000 W |
| 3 | Architektura UPSa | line-interactive |
| 4 | Liczba, typ gniazd wyj. z podtrzymaniem zasilania i ochroną przepięciową | 8 x IEC320 C13 (10A) + 2 x C19 (16A) |
| 5 | Segmentacja gniazd odbiorów | Gniazda odbiorcze muszą zawierać co najmniej 2 grupy 2 x IEC C13, których sterowanie odbywać się powinno za pomocą oprogramowania. Każdy segment musi umożliwiać pomiar zużycia energii. |
| 6 | Kształt napięcia wyjściowego przy pracy bateryjnej | Sinusoidalny |
| 7 | Typ gniazda wejściowego | IEC320 C14 (10A) |
| 8 | Czas podtrzymania przy obciążeniu 2000W min. | 6 minut |
| 9 | Wysokość w szafie | 2U |
| 10 | Typ obudowy | Uniwersalna Tower / Rack |
| 11 | Sprawność w trybie normalnym | > 96% |
| 12 | Zakres napięcia wejściowego w trybie podstawowym | 160V - 294 V (regulowane do 150V - 294V) |
| 13 | Zakres częstotliwości wejściowej bez użycia baterii | 47 do 70 Hz (sieć 50 Hz) |
| 14 | Poziom hałasu w trybie sieciowym | < 40 dBA |
| 15 | Zakres zmian napięcia wyjściowego | maksymalnie -10/+6% wartości nominalnej |
| 16 | Baterie wymieniane przez użytkownika "na gorąco" | Tak |
| 17 | Porty komunikacji | port szeregowy RS232, port USB, gniazdo rozszerzenia opcji komunikacji do instalacji karty SNMP/Web z możliwością monitorowania środowiska, port zdalnego wyłączania i włączania UPSa, mini złącze dla wyjściowego styku przekaźnikowego, styki bezpotencjałowe (3 wyjścia) |
| 18 | Pasek LED informujący o stanie UPS | Tak |
| 19 | Panel komunikacyjny | Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh) |
| 20 | Alarmy dźwiękowe | •  praca z baterii |
| •  awaria UPSa |
| •  przeciążenie UPSa |
| •  znaczne wyczerpanie baterii |
| 21 | Wyposażenie standardowe | •  kabel zasilający |
| •  kable sygnałowe USB i RS232 |
| •  kabel odbiorów 1.8m IEC320 C13/C14 - 2 szt. |
| •  system blokowania kabli - 2 szt. |
| •  zestaw montażowy do szafy 19" |
| •  podstawki do montażu tower |
| 22 | Wyposażenie dodatkowe | •  karta SNMP |
| 23 | Karta SNMP | • cyberbezpieczeństwo (szyfry TLS, MQTT) |
| • certyfikaty CA i PKl |
| • prędkość gigabit’owa (half-duplex, full-duplex) |
| • różne poziomy nadawania dostępu do konta administratora lub użytkownika |
| 24 | Oprogramowanie umożliwiające | • monitorowanie UPS oraz bezpieczne zamykanie urządzeń pracujących z systemami operacyjnymi Windows, Linux (RedHat, Fedora, (open) SUSE, Debian, Ubuntu), Unix (HP-UX, IBM Aix, Oracle (Sun) Solaris) |
| • podłączenie UPS zarówno za pomocą interfejsu USB lub RS-232, jak i przez sieć |
| • tworzenie scenariuszy wysyłania powiadomień email oraz uruchamiania własnych skryptów przy wystąpieniu wybranych zdarzeń |
| • tworzenie indywidualnych kont użytkowników z co najmniej dwoma poziomami dostępu do wyboru |
| •  zdalny dostęp do swojego interfejsu graficznego po lokalnej sieci |
| • wybór polskiej wersji językowej |
| 25 | System zarządzania pracą baterii | System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony. |
| 26 | Możliwość wydłużenia czasu potrzymania | Tak. Do min. 100 minut dla obciążenia 2000W poprzez dołączenie baterii zewnętrznych - automatyczna detekcja zewnętrznych jednostek bateryjnych. |
| 27 | Certyfikaty | Deklaracja zgodności oraz certyfikat ISO 9001 producenta lub równoważny, certyfikat Energy Star lub równoważny |
| 28 | Gwarancja producenta co najmniej | 3 lata na elektronikę, 2 lata na baterie |

1. **Oprogramowanie do monitorowania infrastruktury informatycznej – wznowienie 50 licencji oraz zakup 10 nowych licencji**

## **1. Oprogramowanie do zarządzania infrastrukturą IT**

Oprogramowanie posiada budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.

Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program wykorzystuje darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source dzięki czemu nie jest objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows.

Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., są odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Są one również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.

Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników.

Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów są logowane oznacza to, że program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta.

Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog. Lista kont użytkowników, w tym administratorów, może być synchronizowana z Active Directory, również przez szyfrowane połączenie LDAPS.

Program umożliwia konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityka pozawala na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymusza dostosowanie bieżących haseł do obowiązujących zasad.

Program zawiera mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA można skonfigurować okres, po którym należy ponownie zautoryzować logowanie.

W przypadku awarii autoryzacja logowania może być pominięta tylko w lokalnej konsoli serwera.

### **2. Moduł monitorowanie infrastruktury (bezagentowo)**

Program obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

* wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
* wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją OU)
* wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
* wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na

mapie do najbliższej linii siatki

* wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem

tła.

* wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
* wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach

dowolnym rozmiarze i kolorze

* wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
* wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do

którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny

* zablokowania mapy urządzeń przed przypadkową edycją
* serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych

serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów serwerów pocztowych:

* + program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty
  + program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
  + program ma możliwość wykonywania operacji testowych
  + program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
* monitorowania serwerów WWW i adresów URL
* cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
* obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
* obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
* obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
* monitoringu routerów i przełączników wg:
  + zmian stanu interfejsów sieciowych
  + ruchu sieciowego
  + podłączonych stacji roboczych – graficzna prezentacja panelu switcha
  + ruchu generowanego przez podłączone do portów stacje robocze
* serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
* wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
* monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
* zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
* wydajności systemów Windows: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.

Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0. Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

### **3. Moduł inwentaryzacji**

Program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

* Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
* Umożliwia odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
* Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
* Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
* Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
* Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
* Umożliwia odczytanie numeru seryjnego (klucze licencyjne).
* Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
* Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
* Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywanie metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
* Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.

Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

* przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
* przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,
* tworzenia powiązań między zasobami a urządzeniami,
* tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
* wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
* definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
* określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
* określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
* masową edycję atrybutów zasobów,
* definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
* importu danych z zewnętrznego źródła (.CSV),
* przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
* tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
* oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
* ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
* generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
* przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
* konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
* konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
* archiwizacji i porównywania audytów zasobów,
* tworzenia kodów kreskowych dla zasobów,
* drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
* inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
* możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
* inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
* definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:

* Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
* Informacje o aplikacjach używanych w organizacji.
* Tworzenie własnych wzorców aplikacji.
* Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
* Informacje o komputerach, na których aplikacja została wykryta.
* Zarządzanie posiadanymi licencjami.
* Wskazywanie osób odpowiedzialnych za licencję.
* Wskazanie użytkowników licencji.
* Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
* Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
* Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
* Zarządzanie posiadanymi licencjami: raport zgodności licencji.
* Możliwość przypisania do programów numerów seryjnych, wartości itp.

### **4. Moduł obsługi użytkowników**

Program umożliwia monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

* Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
* Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
* Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
* Informacji o edytowanych przez użytkownika dokumentach,
* Historii pracy (cykliczne zrzuty ekranowe),
* Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
* Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
* Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
* Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program ponadto posiada możliwość:

* wykrywania podejrzanej aktywności przez popularne „jigglery”, mającej na celu symulowanie faktycznej pracy.
* zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
* wyszczególnienia podejrzanej aktywności w raportach.
* wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
* automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
* blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
* integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
* skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
* automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
* blokowania ruchu na wskazanych portach TCP/IP,
* blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
* prowadzenia rejestru naruszeń blokad,
* wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze
* lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje
* określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
* przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
* definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.

Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.

Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

### **5. Moduł zdalnej pomocy użytkownikom**

W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połączenie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.

W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie pozwala na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System umożliwia użycie pośredniego statusu „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia.

Moduł ten zawiera również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat pozwala na:

* zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
* rozmowy również między „zwykłymi” użytkownikami
* przesyłanie plików między rozmówcami w trybie online
* tworzenie pokojów tematycznych, rozmów grupowych
* oznaczanie kontaktów jako „ulubionych” na liście kontaktów
* uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
* może być wyświetlany w trybie jasnym lub ciemnym

W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik ma możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów.

Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.

Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.

Moduł pomocy zdalnej umożliwia również:

* pobieranie listy użytkowników z Active Directory,
* wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,
* zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
* zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
* zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,
* zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,
* tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
* automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
* definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
* przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
* procesowanie zgłoszeń użytkowników z wiadomości e-mail,
* eksportowania listy zgłoszeń do plików CSV i XLSX,
* integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
* tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
* wykonywanie operacji na wielu zgłoszeniach równocześnie,
* dołączanie załączników do zgłoszeń,
* rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
* szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
* wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
* zrzuty ekranowe (podgląd pulpitu),
* zdalną modyfikację rejestrów,
* dystrybucję oprogramowania przez Agenty,
* definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
* przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
* dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
* zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
* możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
* możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
* planowanie nieobecności pracowników helpdesk,
* obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
* generowanie raportów obsługi helpdesk,
* zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
* zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
* wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.

### **6. Moduł ochrony danych przed wyciekiem**

Program umożliwia ochronę danych przed wyciekiem poprzez blokowanie urządzeń:

* Blokowanie urządzeń i nośników danych.
* Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
* Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
* Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
* Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
* Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
* Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
* Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
* Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
* Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
* Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
* Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
* Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:

* Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
* Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane.
* Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
* Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
* Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

* Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
* Podłączenie/odłączenie urządzenia przenośnego.

Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

Definiowanie reguł monitorowanych folderów w postaci list.

Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.)

Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.

### **7. Moduł zarządzania czasem i aktywnością użytkowników**

Program wspiera zarządzanie czasem i analizowanie aktywności użytkowników poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji może oznaczyć sesję aktywności jako czas prywatny, gdy wykonuje czynności prywatne na sprzęcie firmowym. Może również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp realizowany jest przez przeglądarkę internetową a strona może być wyświetlana w trybie jasnym lub ciemnym.

* Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
* Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.
* Statystyki aktywności podwładnych widoczne dla przełożonego.
* Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.
* Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.
* Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
* Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.
* Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.
* Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.
* Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).
* Wskaźnik czasu poświęconego na aktywność produktywną.
* Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.
* Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.
* Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.

### **8. Portal informacyjny w formie platformy**

Oprogramowanie posiada również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, których nazwy można zmieniać wg potrzeb. Na każdym z dashboardów widgety są rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych jest automatycznie odświeżana oraz może być:

* Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem.
* Wyświetlana w trybie jasnym lub ciemnym (nocnym).

Oprogramowanie umożliwia zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego. Widgety prezentują dane ze wszystkich modułów funkcjonalnych oprogramowania:

* Mapa sieci,
* Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,
* Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,
* Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW, naruszenia reguł blokad,
* Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,
* Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), informacje o stanie Bitlocker, Windows Defender, Windows Firewall, naruszenia reguł dostępu do nośników danych,
* Produktywność dla grupy, Statystyki czasu nieproduktywnego.

**Ochrona przed usunięciem**

Program jest zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.

**Funkcjonalność Agenta**

Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.

Program dostępny jest w języku polskim, wraz z Podręcznikiem Użytkownika w formie strony internetowej.

**Licencjonowanie oraz wsparcie techniczne**

Oprogramowanie będzie posiadać odpowiednią licencję umożliwiającą zarządzanie **60 stacjami roboczymi**.

Oprogramowanie zostanie dostarczone z **12-miesięcznym wsparciem producenta**, umożliwiającym aktualizacje produktu oraz pomoc techniczną.

## **9. Platforma szkoleniowa dla pracowników**

Platforma dostarczająca narzędzia i zasoby niezbędne do zapewnienia pracownikom wartościowej wiedzy i umiejętności w zakresie ochrony przed cyberzagrożeniami. Użytkownicy otrzymują dostęp do materiałów szkoleniowych oraz testów wiedzy. Menedżerowie grup oraz administratorzy zyskują wgląd w postęp nauki i poziom wiedzy w całej organizacji i dla poszczególnych grup.

Platforma udostępnia swoim użytkownikom kurs z zakresu cyberbezpieczeństwa, który składa się z modułów, lekcji i testów sprawdzających nabytą przez kursantów wiedzę. Każdy moduł składa się z lekcji w formie video oraz testu. Szkolenie zostanie przygotowane i odpowiednio ułożone przez ekspertów w dziedzinie cyberbezpieczeństwa, a informacje w nim zawarte będą aktualne, istotne i odnoszące się do realnych zagrożeń, na które użytkownik może natknąć się podczas codziennego korzystania z komputera w pracy i nie tylko.

### **Zakres tematyczny szkolenia:**

* Socjotechniki
* Bezpieczeństwo haseł
* Bezpieczeństwo poczty e-mail i ochrona przed SCAM-em
* Obrona przed phishingiem
* Bezpieczeństwo stron WWW i przeglądarek
* Ataki socjotechniczne z wykorzystaniem urządzeń
* Ataki za pośrednictwem telefonu
* Zagrożenia związane w urządzeniami mobilnymi
* Zagrożenia związane z sieciami Wi-Fi
* Zagrożenia w mediach społecznościowych
* Dobre praktyki bezpieczeństwa
* Prywatność, poufność i anonimowość w Internecie

1. **Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych Client Access License – 50 licencji**

Przedmiotem zamówienia jest dostawa licencji dostępowych CAL (Client Access License) umożliwiających dostęp do usług serwera w środowisku Zamawiającego, zgodnie z zasadami licencjonowania producenta.

2. Wymagania ogólne

Licencja CAL stanowi prawo do dostępu użytkownika lub urządzenia do usług serwera i nie obejmuje instalacji oprogramowania na serwerze.

Licencje muszą być oryginalne, pochodzące z oficjalnego kanału dystrybucji producenta.

Licencje muszą umożliwiać pełny, legalny dostęp do funkcjonalności serwera zgodnie z warunkami licencji producenta (np. Microsoft Product Terms / Product Use Rights).

3. Zakres funkcjonalny

Licencje CAL muszą umożliwiać dostęp do co najmniej następujących usług serwerowych:

* usługi katalogowe (np. Active Directory Domain Services),
* zarządzanie dostępem i uwierzytelnianiem,
* współdzielenie zasobów plikowych i drukowania (File & Print Services),
* dostęp do usług serwera aplikacyjnego/komunikacyjnego.

4. Rodzaj licencji

Zamawiający wymaga dostarczenia licencji w jednym z poniższych modeli (zgodnie z opisem w dokumentacji przetargowej):

a) User CAL (licencja dostępowa na użytkownika)

Uprawnia wskazanego użytkownika do korzystania z usług serwera z dowolnego urządzenia (komputer, terminal, urządzenie mobilne).

b) Device CAL (licencja dostępowa na urządzenie)

Uprawnia wskazane urządzenie do korzystania z usług serwera przez dowolną liczbę użytkowników.

Licencje muszą być przydzielane na stałe do użytkownika lub urządzenia zgodnie z wybraną opcją.

5. Zgodność z wersją serwera

Licencje CAL muszą być zgodne z wersją wykorzystywanego oprogramowania serwerowego lub nowsze.

Licencje CAL nie mogą być starsze niż wersja oprogramowania serwerowego, do którego zapewniają dostęp.

Przykład: CAL w wersji 2022 może uzyskać dostęp do serwera 2019, lecz CAL 2019 nie może uzyskać dostępu do serwera 2022.

6. Warunki licencjonowania

Licencje muszą być bezterminowe (perpetual).

Licencje muszą umożliwiać legalne użytkowanie w środowisku komercyjnym Zamawiającego.

1. **Zakup 2 szt. Serwerów typu RACK wraz z dostawą, montażem oraz konfiguracją oraz adaptacją do istniejącej konfiguracji zgodną z wytycznymi działu IT**

Obudowa

●     Typu RACK, wysokość nie więcej niż 1U;

●     Szyny umożliwiające wysunięcie serwera z szafy stelażowej;

●     Możliwość zainstalowania 8 dysków twardych hot plug 2,5” SATA, SAS;

●     Zainstalowane 2 szt. dysków SSD 1,92 GB HOT-PLUG;

Płyta główna

●     Wyprodukowana i zaprojektowana przez producenta serwera;

●     Możliwość instalacji procesora 160-rdzeniowego;

●     Moduł TPM 2.0;

●     2 złącza PCI Express x16;

●     Opcjonalnie możliwość uzyskania 3 slotów PCIe x16;

●     Opcjonalnie możliwość uzyskania 1 sloty typu FH;

●     12 gniazd pamięci RAM;

●     Obsługa 3 TB pamięci operacyjnej RAM DDR5;

●     Wsparcie dla technologii:

●     Bounded Fault;

●     SDDC;

●     ECC;

●     ECS;

●     Memory Mirroring;

●     Patrol/Demand Scrubbing;

●     Wewnętrzny slot na kartę Micro SD

Procesory

●     Procesor 16-rdzeniowy, taktowanie bazowe 3,0 GHz, architektura x86\_64;

●     osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 229 pkt. Wynik musi być opublikowany na stronie [http://spec.org](http://spec.org/) dla oferowanego serwera.

Pamięć RAM

384GB pamięci RAM;

●     DDR5 Registered 4800MHz;

●     Pamięci obsadzone w trybie maksymalnej wydajności;

Kontrolery LAN

●     Interfejsy LAN, nie zajmujące slotów PCI Express (OCP):

●     4x 1Gbit Base-T;

●     Możliwość uzyskania 2 interfejsów 100Gbit QSFP56 bez konieczności instalacji kart w slotach PCIe;

●     1x 1G Base-T dedykowany do zarządzania serwerem w trybie OOB;

Kontrolery I/O

●     Kontroler RAID dla dysków wewnętrznych SATA, SAS oraz NVMe obsługujący następujące poziomy RAID: 0,1,10,5,50,6,60 posiadający 4GB pamięci cache zabezpieczonej przed utratą danych na wypadek awarii zasilania (tzw. podtrzymanie pamięci cache), obsługa globalnych dysków Hot-Spare oraz rozszerzanie pojemności logicznych przestrzeni on-line;

Porty

●     Zintegrowana karta graficzna posiadająca 16MB pamięci rozdzielczość 1920x1200 przy 60 Hz, ze złączem VGA z tyłu serwera;

●     3 porty USB dostępne z tyłu serwera w tym dwa w wersji USB 3.1;

●     1 port USB 3.1 wewnętrzny;

●     2 porty USB na panelu przednim w tym jeden w wersji USB 3.1;

●     Jeden z frontowych portów USB musi posiadać możliwość zarządzania serwerem;

●     Dedykowany port do zarządzania i diagnostyki dostępny z przodu serwera;

●     Opcjonalny port serial;

●     Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

●     Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 1100W;

●     Redundantne dwuwirnikowe wentylatory hotplug dające gwarancję poprawnego działania serwera w temperaturze otoczenia nie przekraczającej 30 stopni Celsjusza;

Bezpieczeństwo

●     Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji;

●     Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej;

●     Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem;

●     Opcjonalne fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;

●     Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem;

●     Możliwość wyłączenia w BIOS funkcji przycisku zasilania;

●     Możliwość ustawienia hasła włączania serwera;

●     Możliwość ustawienia hasła administratora;

●     Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID;

Zarządzanie

●     Wymaga się aby serwer posiadał diody sygnalizujące awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.

●     Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser’ów PCIe, backplane’ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych;

●     Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera.

●     Funkcjonalność kontrolera zdalnego zarządzania:

●     Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna)

●     Uzyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja

●     Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.

●     Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.

●     Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3

●     Update systemowego firmware

●     Monitoring i możliwość ograniczenia poboru prądu

●     Zdalne włączanie/wyłączanie/restart

●     Zapis video zdalnych sesji

●     Podmontowanie lokalnych mediów z wykorzystaniem Java client

●     Przekierowanie konsoli szeregowej przez IPMI

●     Zrzut ekranu w momencie zawieszenia systemu

●     Możliwość przejęcia zdalnego ekranu

●     Możliwość zdalnej instalacji systemu operacyjnego

●     Alerty Syslog

●     Przekierowanie konsoli szeregowej przez SSH

●     Wsparcie dla dynamic DNS

●     Wyświetlanie danych aktualnych I historycznych dla zużycia energii oraz temperatury serwera

●     Wirtualna konsola z dostępem do myszy, klawiatury;

●     Montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy AciveX (musi działać w oparciu o HTML5)

●     Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS

●     Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę

●     wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API

●     Możliwość wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.

●     Kontroler zarządzania musi posiadać 4GB wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.

●     Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot’u.

●     Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.

●     Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.

●     Opcjonalne 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 w systemie operacyjnym

●     Automatyczne rozpoznawanie nowych serwerów poprzez protokół SLP oraz SSDP

●     Szczegółowy opis wykrytych systemów oraz ich komponentów

●     Możliwość eksportu danych min do formatu CSV

●     Grupowanie urządzeń w oparciu o kryteria użytkownika

●     Możliwość wizualizacji rozmieszczenia serwerów i zarządzanych urządzeń w szafach RACK

●     Tworzenie automatycznie grup urządzeń w oparciu o elementy konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji czy stanu np. firmware czy BIOS

●     Szybki podgląd stanu środowiska

●     Podsumowanie stanu dla każdego urządzenia

●     Szczegółowy status urządzenia/elementu/komponentu

●     Filtry raportów umożliwiające podgląd najważniejszych zdarzeń

●     Integracja z service desk producenta dostarczonej platformy sprzętowej, pozwalając min weryfikację statusu i wysyłanie paczek diagnostycznych

●     Możliwość przejęcia zdalnego pulpitu

●     Możliwość zamontowania wirtualnego napędu

●     Kreator umożliwiający dostosowanie akcji dla wybranych alertów

●     Przesyłanie alertów „as-is” do innych konsol firm trzecich

●     Możliwość definiowania ról administratorów

●     Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów

●     Aktualizacja oparta o repozytorium aktualizacji – budowanie repozytorium w sposób automatyczny ze stron producenta

●     Możliwość definiowania polityk aktualizacji (konkretne wersje firmware)

●     Automatyczna polityka aktualizacji „Najnowsze dostępne”

●     Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta na systemie operacyjnym

●     Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów

●     Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta

●     Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności czy powielania konfiguracji na inne serwery czy backup aktualnej konfiguracji.

●     Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile

●     Wykonanie restartu serwera i automatyczne wejście do BIOSu/UEFI

●     Zdalne bezpieczne usunięcie danych na dyskach SSD/HDD w serwerach

●     Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

●     Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:

●     wykonać zautomatyzowaną aktualizację firmware serwerów w clustrze Vmware do zdefiniowanej polityki poziomu mikrokodów

●     wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji

●     z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)

●     inwentaryzacja komponentów w serwerze i ich mikrokodów

●     historia min 24h poboru mocy i temperatury serwera

●     zbieranie danych diagnostycznych serwera do paczki

●     Integracja z środowiskiem Microsoft Admin Center pozwalająca z konsoli/plugin:

●     wykonać zautomatyzowaną aktualizację firmware serwerów w clustrze do zdefiniowanej polityki poziomu mikrokodów

●     z konsoli Admin Center uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)

●     aktualizacja sterowników systemowych Windows

●     inwentaryzacja komponentów w serwerze i ich mikrokodów

●     historia min 24h poboru mocy i temperatury serwera

●     zbieranie danych diagnostycznych serwera do paczki

●     Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Certyfikowane systemy operacyjne

●     Microsoft Windows Server 2025, 2022, 2019;

●     VMWare ESXi 8.0;

●     Suse Linux Enterprise Server 15;

●     Red Hat Enterprise Linux 10.x, 9.x, 8.x;

●     Ubuntu 22.04 LTS, 24.04 LTS,

●     Microsoft Windows 11

●     AlmaLinux 9.x, 8.x;

●     Rocky Linux 9.x, 8.x;

●     Xen Server 8.x;

Gwarancja

●     3 lata gwarancji producenta serwera w trybie on-site  z czasem reakcji następnego dnia roboczego. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.

●     Uszkodzone dyski nie podlegają zwrotowi organizacji serwisowej;

●     Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;

●     Firma serwisująca musi posiadać certyfikat ISO 9001:2015~~ISO 9001:2000~~ na świadczenie usług serwisowych lub certyfikat równoważny;

●     Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera w 24h od zgłoszenia usterki (podać koszt na dzień składania oferty).

Dokumentacja, inne

●     Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;

●     Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;

●     Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu na który można zgłaszać usterki;

●     Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

1. **Zakup 2 szt. Serwerów dziedzinowych wraz z dostawą, montażem, konfiguracją oraz adaptacją do istniejącej konfiguracji zgodną z wytycznymi działu IT**

|  |  |
| --- | --- |
| **Obudowa** | Do instalacji w szafie Rack 19”, wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i możliwością wysuwania do celów serwisowych. Możliwość instalacji maskownicy zamykanej na kluczyk.  Obudowa powinna umożliwiać instalację do 8 dysków 2,5” Hot Swap |
| **Procesor** | Architektura x86, maksymalny TDP dla procesora – maksymalnie 65W. Wymagana ilość rdzeni dla procesora – 8. Minimalna częstotliwość pracy procesora 2.7GHz. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być nizszy niż 83 punkty base w teście SPECrate 2017 Integer w konfiguracji jednoprocesorowej, opublikowanym przez SPEC.org ([www.spec.org](http://www.spec.org/)). Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. |
| **Płyta główna** | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania jednego procesora wykonującego 64-bitowe instrukcje |
| **Pamięć operacyjna** | Zainstalowane minimum 64GB pamięci RAM o częstotliwości 5600MHz. |
| **Zabezpieczenie pamięci** | ECC |
| **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.  1 port VGA na tylnym panelu. Możliwość zainstalowania drugiego portu VGA na przednim panelu serwera. |
| **Dyski/Rozbudowa dysków** | W chwili dostawy serwer musi posiadać zainstalowane minimum 4 sztuki dysków SSD o pojemności min. 480GB, połączone za pomocą sprzętowego kontrolera RAID.  Serwer powinien zawierać 8 wnęk na dyski, umożliwiające instalację nośników 2,5” hot-swap SSD/HDD w standardach SAS/SATA. |
| **Kontroler dyskowy** | W momencie dostawy serwer musi posiadać zainstalowany sprzętowy kontroler dyskowy, dedykowany przez producenta serwera.  Kontroler powinien posiadać pamięć cache min. 4GB oraz oferować poziomy zabezpieczeń typu RAID 0, 1, 10, 5, 50, 6, 60.  Kontroler powinien umożliwiać pracę dysków w trybie JBOD.  Kontroler powinien wspierać dyski SED.  Kontroler powinien mieć wbudowany dodatkowy kondensator, wspierający kopię danych do pamięci cache kontrolera.  Wymaga się obsługi globalnych dysków hot-spare. |
| **Zasilacz** | Minimum dwa zasilacze o mocy minimum 800W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji. |
| **Interfejsy sieciowe** | Wbudowana w płytę główną dwuportowa karta 1Gb Base-T.  Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. |
| **Sloty I/O PCIe** | Serwer powinien posiadać przynajmniej 2 sloty PCIe x8 generacji 4. |
| **Dodatkowe porty** | * z przodu obudowy: 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem). * z tyłu obudowy: 2x USB 3.2, 2x 1Gb Base-T , 1x VGA, 1x RJ-45 do zarządzania serwerem, 1x port szeregowy. |
| **Chłodzenie** | Cztery wentylatory zapewniające optymalne chłodzenie serwera |
| **Zarządzanie** | Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania. Wymagane funkcjonalności kontrolera zdalnego zarządzania:   * Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna * Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja * Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. * Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. * Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 * Update systemowego firmware * Monitoring i możliwość ograniczenia poboru prądu * Zdalne włączanie/wyłączanie/restart * Zapis video zdalnych sesji * Podmontowanie lokalnych mediow z wykorzystaniem Java client * Przekierowanie konsoli szeregowej przez IPMI * Zrzut ekranu w momencie zawieszenia systemu * Możliwość przejęcia zdalnego ekranu * Możliwość zdalnej instalacji systemu operacyjnego * Alerty Syslog * Przekierowanie konsoli szeregowej przez SSH * Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera * Możliwość mapowania obrazów ISO z lokalnego dysku operatora * Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS * Możliwość zamontowania minimum 4 obrazów ISO jednocześnie w czasie jednej sesji * Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę * Możliwość zdefiniowania minimum 12 użytkowników lokalnych na karcie zarządzającej * wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API * Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. * Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot’u. * Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. * Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.   Możliwość instalacji dodatkowego oprogramowania zarządzającego umożliwiającego:  - zarzadzanie infrastruktura serwerowni storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń  - możliwość skalowania do minimum 1000 urządzeń  - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2  - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych  - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia  - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii,  - konsola zarzadzania oparta o HTML 5  - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu,  - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja  - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania  - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań  - definiowanie roli użytkowników oprogramowania  - obsługa REST API oraz Windows PowerShell  - obsługa SNMP, SYSLOG, Email Forwarding  - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML  - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami  - przedstawianie historycznych aktywności użytkowników  -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych  - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem,  oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv  - Obsługa NTP  - przesyłanie alertów do konsoli firm trzecich  - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń)  - instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie  - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych,  Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami:  VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk. |
| **Funkcje zabezpieczeń** | Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł TPM2.0. Możliwość instalacji przedniego panelu zabezpieczającego, zamykanego na klucz. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączania portów USB na obudowie z poziomu UEFI. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej.  Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji |
| **Urządzenia hot swap** | Dyski twarde, zasilacze. |
| **Diagnostyka** | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID  Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez port USB na froncie serwera. |
| **Systemy operacyjne** | Microsoft Windows Server 2019, 2022,2025; Red Hat Enterprise Linux, 9.x, SUSE Linux Enterprise Server 15; VMware vSphere (ESXi) ESXI 8.x; Ubuntu 24.04 LTS |
| **Waga** | maximum: 13kg |
| **Gwarancja** | 60 miesięcy gwarancji producenta z czasem reakcji onsite w następnym dniu roboczym od momentu zgłoszenia usterki. Możliwość rozszerzenia gwarancji o gwarantowany czas naprawy w ciągu 24 godzin. Uszkodzone nośniki danych pozostają własnością zamawiającego. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających:  - Wykrywanie usterek sprzętowych z predykcją awarii.  - Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. |

1. **Zakup 3 szt. Macierzy Dyskowych wraz z dostawą, montażem, konfiguracją oraz adaptacją do istniejącej konfiguracji zgodną z wytycznymi działu IT**

|  |  |
| --- | --- |
| Procesor | Procesor osiągający wynik minimum 24 tysięcy punktów w teście PassMark. |
| Obudowa | Typu rack o wysokości maksymalnie 2U wraz z szynami przesuwnymi w zestawie. |
| Pamięć RAM | Minimum 128GB UDIMM w dowolnej konfiguracji. |
| Ilość obsługiwanych dysków | Minimum 12 dysków 3,5”/2,5” SATA 6 Gb/s o maksymalnej pojemności nie mniejszej niż 22TB każdy. |
| Zainstalowane dyski | 8 dysków HDD o pojemności 6TB każdy zgodnych z listą kompatybilności oferowanego serwera oraz charakteryzujących się następującymi parametrami:  - prędkość obrotowa: minimum 7200 RPM, - pamięć cache: minimum 250 MB, - gwarancja: minimum 60 miesięcy, - MTBF: minimum 2 miliony. |
| Interfejsy sieciowe | Minimum 2 porty 2.5GbE RJ-45,  Minimum 2 porty 10GbE RJ-45.  Obsługa agregacji łączy, VLAN i Jumbo Frame. |
| Porty i złącza | Minimum 2 porty USB 3.2 Gen 2 typu A (10 Gb/s) Minimum 2 złącza M.2 2280 PCIe Gen 5 x2 |
| Gniazda PCIe | Minimum 3 gniazda PCIe Gen4 x4 |
| Wskaźniki LED | Stan serwera, LAN, USB, HDD |
| Obsługa RAID | RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy. |
| Funkcje RAID | Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD. |
| Szyfrowanie | 256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych. |
| Wsparcie dla systemów operacyjnych | Minimum:   * Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux, * Microsoft Windows 10, 11, * Microsoft Windows Server 2019, 2022. |
| Protokoły | CIFS, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| Usługi | Stacja monitoringu, Windows ACL, Integracja w Windows Active Directory, Serwer WWW, Serwer plików, Manager plików przez web UI, Replikacja w czasie rzeczywistym, Serwer Syslog, |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów. |
| Język GUI | Polski |
| Gwarancja i serwis | Minimum 60 miesięcy gwarancji producenta. |
| Typowy pobór mocy podczas pracy | Maksymalnie 400 W |
| System plików | Dyski wewnętrzne - ZFS. Dyski zewnętrzne - EXT3, EXT4, NTFS, FAT32, HFS+. |
| Funkcje systemu plików | Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL |
| iSCSI | Obsługa MPIO, MC/S i SPC-3 Persistent Reservation |
| Zasilanie | Redundantny zasilacz o mocy pozwalającej na bezproblemową pracę w przypadku awarii jednego z modułów zasilania. |
| UPS | Obsługa sieciowych awaryjnych zasilaczy UPS. |

1. **Zakup Oprogramowania Menadżera Logów wraz z instalacją, konfiguracją oraz adaptacją do istniejącej konfiguracji zgodną z wytycznymi działu IT**

# **Wymagania funkcjonalne:**

1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
2. System musi pracować w oparciu o architekturę Linux.
3. System musi mieć możliwość centralnego zbierania i zarządzania logami
4. System działać w trybie zbliżonym do rzeczywistego
5. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu.
6. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
7. System musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20  GB danych dziennie
8. System musi zapewniać retencję danych w okresie minimum 365  dni.
9. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
10. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
11. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
12. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
13. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
14. System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu .
15. Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.
16. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.
17. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
18. Interfejs musi posiadać angielską lub polską wersję językową.
19. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
20. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
21. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius
22. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
23. System musi wspierać mechanizm logowania typu Single Sign On.
24. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
25. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
26. System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
27. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
28. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
29. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
30. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
31. System musi pozwalać na tworzenie parserów z poziomu GUI
32. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
33. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
34. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
35. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
36. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
37. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:

* Syslog, WEF, Flat file, Event log, WMI, SNMP trap, XML, JSON, JDBC/ODBC CSV, Email,

Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.

1. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
2. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.
3. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
4. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
5. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.
6. System musi posiadać predefiniowany zestaw parserów zdarzeń.
7. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
8. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
9. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
10. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
11. Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
12. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
13. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
14. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
15. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
16. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
17. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
18. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
19. Wykrycia dowolnej treści w logach,
20. Wykrycia wystąpienia wartości pola na wybranej liście,
21. Wykrycia niewystępowania wartości pola na wybranej liście,
22. Wykrycia zmiany jednego z kilku pól,
23. Wykrycia zdarzeń występujących z zadaną częstotliwością,
24. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
25. Wykrycia zaniku Wiadomości,
26. Wykrycia nowej wartości pola w zadanym okresie czasu,
27. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
28. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
29. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
30. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
31. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
32. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
33. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
34. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
35. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
36. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
37. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
38. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
39. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
40. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
41. System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
42. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
43. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
44. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
45. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
46. System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem community producenta na okres 1 roku.
47. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
48. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
49. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
50. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
51. System musi umożliwiać integrację z Mitre ATT@CK.

# **Reguły korelacyjne, alerty i obsługa incydentów**

1. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
2. System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.
3. System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
4. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
5. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit’u i wykrywania ukrytych procesów, plików, portów
6. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
7. System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP
8. Zamawiający wymaga wdrożenia systemu Security Information and Event Management (SIEM), który będzie zapewniał zaawansowane monitorowanie, analizę oraz korelację zdarzeń w infrastrukturze IT. System musi wspierać wykrywanie incydentów bezpieczeństwa oraz spełniać wymagania określone w aktualnych przepisach i normach dotyczących cyberbezpieczeństwa.

# **Wdrożenie i szkolenie**

1. Wdrożenie systemu SIEM musi zostać zrealizowane przez:

- Wykwalifikowanego integratora posiadającego doświadczenie w implementacji i konfiguracji systemów SIEM oraz stosowne certyfikaty potwierdzające kompetencje w zakresie cyberbezpieczeństwa i administracji systemami IT.

- Producenta oprogramowania SIEM, który zapewni pełne wsparcie w zakresie wdrożenia, integracji oraz dalszej eksploatacji systemu.

1. Wykonawca dostarczy voucher szkoleniowy dla 2-óch słuchaczy.
2. Szkolenie odbędzie się w formie zdalnej.
3. Szkolenie musi być prowadzone w języku polskim.
4. Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim.
5. Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania potwierdzające ich kompetencje w zakresie użytkowania i administrowania systemem.