Załącznik nr 1 do umowy – Szczegółowy Opis Przedmiotu Zamówienia

Dostawa sprzętu informatycznego oraz oprogramowania (wymagania minimalne):

1. **Dostosowanie usług katalogowych dla użytkowników, wraz z wdrożeniem Centralnego Systemu Bezpieczeństwa – 1 usługa w wysokości max. 168 godzin.**

W ramach zadania obowiązkiem Wykonawcy będzie dostosowanie usług katalogowych dla użytkowników, wraz z wdrożeniem Centralnego Systemu Bezpieczeństwa.

Z uwagi na minimalizowanie ingerencji w prace Urzędu, wdrożenie usług katalogowych wraz z wdrożeniem Centralnego Systemu Bezpieczeństwa nie może trwać dłużej niż 168 roboczogodzin, realizowanych w trakcie 90 dni przeznaczonych na realizacji projektu.

Obowiązkiem Wykonawcy jest omówienie harmonogramu wykonania usługi z Zamawiającym.

W harmonogramie powinna znaleźć się informacja o anonsowaniu planowanych prac przez Wykonawcę i forma jej potwierdzenia przez Zamawiającego. Harmonogram musi być zaakceptowany przez strony.

1.1 Wdrożenie i skonfigurowanie usług katalogowych musi zapewniać efektywne zarządzania dostępem do zasobów informatycznych u Zamawiającego. Obowiązkiem Wykonawcy będzie utworzenie struktury organizacyjnej, grup, kont użytkowników oraz polityk bezpieczeństwa. Szczegółowy zakres prac zawiera:

a. Analiza i Projektowanie:
- Ocena infrastruktury istniejącej w celu dostosowania projektu do istniejących zasobów.
- Zaprojektowanie struktury organizacyjnej usług katalogowych z uwzględnieniem potrzeb Zamawiającego.

Efektem działań będzie utworzenie dokumentu zawierającego ustalaną strukturę usług katalogowych. Dokument ten zostanie zatwierdzony przez zamawiającego w celu kontynuowania prac.

b. Wdrożenie:
- Instalacja na infrastrukturze Zamawiającego (serwerach z oprogramowaniem).
- Konfiguracja globalnych i lokalnych polityk bezpieczeństwa.
- Utworzenie grup użytkowników i przydzielanie odpowiednich uprawnień.
- Integracja usługi z istniejącymi systemami.

- Wpięcie 45 sztuk urządzeń klienckich, wraz z przeniesieniem profili użytkownika.
- Wsparcie w rozwiązaniu problemów związanych z wdrażaniem urządzeń klienckich.

Efektem działań będzie przekazanie maszyny z zainstalowaną i skonfigurowaną usługą katalogową.

c. Testowanie i akceptacja:
- Przeprowadzenie testów funkcjonalnych w celu potwierdzenia poprawności działania usługi katalogowej.
- Protokolarne przekazanie dokumentacji dotyczącej konfiguracji, w tym haseł dostępowych instrukcji i postępowania w razie problemów.

1.2 Wdrożenie oferowanego Centralnego Systemu Bezpieczeństwa (dalej CSB), polegające w szczególności na instalacji oraz uruchomieniu rozwiązania. Do obowiązków Wykonawcy należeć będą:

a) Instalacja fizyczna i konfiguracja funkcjonalna komponentów systemu CSB.
b) Konfiguracja systemu CSB w środowisku Zamawiającego. Zdefiniowanie niezbędnych do poprawnego działania systemu parametrów konfiguracyjnych.
c) Integracja z usługą katalogową w zakresie autentykacji użytkowników. Konfiguracja ról Użytkowników.
d) Podłączenie do 3 rodzajów źródeł zdarzeń (np. UTM, switch, serwer) rozpoznawanych przez system CSB. Wykonawca przekaże wytyczne dla Zamawiającego dotyczące koniecznej konfiguracji źródeł zdarzeń Zamawiającego.
e) Budowa minimum 1 parser dla źródeł zdarzeń nieobsługiwanych automatycznie przez system CSB.
f) Możliwość tworzenia niestandardowych reguł korelacyjnych/scenariuszy oraz aktywacja/konfiguracja wbudowanych reguł korelacyjnych
g) Konfiguracja polityk retencji danych
h) Przygotowanie dokumentacji powykonawczej, zawierającej co najmniej zbiór haseł dostępowych, instrukcji i postępowania w razie problemów
i) Przygotowanie i przetestowanie procedur kopii bezpieczeństwa i odtwarzania systemu po awarii
j) Instalacja najnowszej wersji składników systemu

Efektem wdrożenia musi być działanie CSB (systemu klasy SIEM) w środowisku IT Zamawiającego. Dodatkowe konfiguracje (aktualizacje) będą wykonywane w ramach Specjalistycznego wsparcia IT opisanego w dalszej części dokumentu.

2. <u>Specjalistyczne wsparcie IT w zakresie cyberbezpieczeństwa w wymiarze 8h stacjonarnie, 30h online - miesięcznie – łącznie usługa wsparcia trwać będzie nie dłużej jak do 25.03.2026 ;</u>

W ramach zadania obowiązkiem Wykonawcy będzie świadczenie specjalistycznego wsparcia IT w zakresie cyberbezpieczeństwa. Wnioskodawca w ramach każdej z zaoferowanych paczek roboczogodzin będzie świadczył specjalistyczne wsparcie IT w wymiarze 8h stacjonarnie, 30h online w następującym zakresie:

a) Wdrożenie reguł zgodności z przepisami prawnymi oraz standardami bezpieczeństwa.
b) Konfiguracja i zarządzanie firewallami, IDS/IPS i innymi mechanizmami obronnymi.
c) Zarządzanie dostępem i autoryzacją użytkowników.
d) Monitoring sieci i alarmowanie w czasie rzeczywistym.
e) Wdrożenie (na zlecenie) reguł dla Backupu i archiwizacji danych.
f) Szyfrowanie danych wrażliwych.
g) Zabezpieczenie przed oprogramowaniem złośliwym – konfiguracja: antywirus, antimalware.
h) Opracowanie i implementacja planu reagowania na incydenty bezpieczeństwa.
i) Analiza po incydentach i rekomendacje.
j) Stałe monitorowanie logów i zdarzeń związanych z bezpieczeństwem.
k) Zlecone raporty dotyczące stanu bezpieczeństwa.
l) Reagowanie na zgłoszone incydenty związane z bezpieczeństwem
m) Wsparcie w obsłudze wdrażonego w ramach projektu Centralnego Systemu Bezpieczeństwa – oprogramowania klasy SIEM.

Wszystkie zapisy rozumiane jako doradztwo i konfiguracja urządzeń oraz systemów zakupionych w ramach projektu będą realizowane zgodnie z założonymi incydentami. Incydenty będą mogły być zakładane przez Zamawiającego poprzez udostępnione przez Wykonawcę kanały komunikacji, takie jak co najmniej:

Strona www (24h)
Adres email (24h)
Telefon w dni robocze (7:30 – 15:30) – infolinia w języku polskim.

Dla wsparcia stacjonarnego, Wykonawca zapewni realizację incydentów zgodnie z SLA (1/3) co oznacza 1 dzień roboczy na reakcję na zgłoszenie i 3 dni roboczych na realizację.

Dla wsparcia online, Wykonawca zapewni realizację incydentów zgodnie z SLA (1/2) co oznacza 1 dzień roboczy na reakcję na zgłoszenie i 1 dzień robocze na realizację.

Projekt „Cyberbezpieczna Gmina Pacanów" dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd" z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

WSPARCIE STACJONARNE 8h w ramach paczki godzin.

W przypadku usług wykonywanych stacjonarnie, po zgłoszeniu przez Zamawiającego incydentu - konieczności wizyty stacjonarnej w Urzędzie, Wykonawca ma 3 dni robocze na realizację tego zadania. Wykonawca musi zaanonsować dzień swojej wizyty w Jednostce Zamawiającego w ramach czasu wskazanego na reakcję (1 dzień roboczy).
Wezwanie Wykonawcy do świadczenia usługi stacjonarnej odbywać będzie się maksymalnie w ramach dwóch wizyt w ramach jednej paczki godzin.
Każda wizyta i jej długość zostanie zaraportowana przez Wykonawcę i potwierdzona przez Zamawiającego. Raportowanie wykonanych godzin jest obowiązkiem Wykonawcy, może ono odbywać się z wykorzystaniem systemu informatycznego, lub w formie tradycyjnej (protokoły), jednak każdorazowo wykonanie usługi musi być potwierdzone przez Zamawiającego. Podpisane protokoły będą podstawą do wystawienia faktur (zgodnie z umową).

WSPARCIE ONLINE 30h w ramach paczki godzin.

W przypadku usług wykonywanych **online**, po zgłoszeniu przez Zamawiającego incydentu - konieczności wsparcia online, Wykonawca ma 1 dzień robocze na realizację tego zadania (1 dzień roboczy, następujący po dniu przeznaczonym na reakcje).
Wykonawca musi zaanonsować termin wykonywanych prac w ramach czasu wskazanego na reakcję (1 dzień roboczy).
Wezwanie Wykonawcy do świadczenia usługi wsparcia online odbywać będzie się maksymalnie w ramach 5 zleceń w ramach jednej paczki.
Każda usługa wsparcia online i jej długość zostanie zaraportowana przez Wykonawcę i potwierdzona przez Zamawiającego. Raportowanie wykonanych godzin jest obowiązkiem Wykonawcy, może ono odbywać się z wykorzystaniem systemu informatycznego, lub w formie tradycyjnej (protokoły), jednak każdorazowo wykonanie usługi musi być potwierdzone przez Zamawiającego. Podpisane protokoły będą podstawą do wystawienia faktur (zgodnie z umową).

Dla zgłoszeń obu typów incydentów Zamawiający przekaże wykonawcy imienną listę osób uprawnionych do zgłaszania i raportowania incydentów (maksymalnie 3 osoby).

WYKORZYSTANIE PACZEK GODZIN

W ramach zadania, Wykonawca świadczy na rzecz Zamawiającego usługę specjalistycznego wsparcia IT w 24 paczkach godzin w wymiarze 8h stacjonarnie, 30h online (dalej **paczka godzin**), a także pozostaje w trybie gotowości do podjęcia ww. zleceń w okresie o mniejszej intensyfikacji zgłoszeń.

Specjalistyczne wsparcie IT świadczone będzie od dnia podpisania umowy.

Wykonawca przez cały okres świadczenia usługi utrzymuje stan gotowości, do realizacji zleceń – incydentów na rzecz zamawiającego.

Paczka godzin, będzie wykorzystana maksymalnie w ciągu 30 dni.

Okres 30 dni stanowi okres rozliczeniowy dla każdej kolejnej paczki godzin, rozpoczynając od dnia podpisania umowy. Kolejne okresy rozliczeniowe będą liczone od dnia wykorzystania paczki godzin, lub upływie 30 dni.

Zamawiający w okresie 30 dni może wykorzystać maksymalnie 2 paczki godzin. Wykorzystanie większej ilości wsparcia – paczek godzin, może odbyć się tylko za obopólną zgodą Zmawiającego i Wykonawcy.

Wykorzystanie paczki godzin, klasyfikowane będzie zawsze dla okresu, w którym Zamawiający przekazał zgłoszenie incydentu, także w przypadkach, kiedy Wykonawca w jego obsłudze wyszedł poza okres trwania paczki godzin (np. zgłoszenie przekazane w 29 dniu okresu rozliczeniowego pierwszej paczki godzin, obsłużone w 32 dniu będzie zaliczane dla pierwszej paczki godzin).

W przypadku nie wykorzystania wszystkich godzin (stacjonarnych, lub online) w ciągu 30 dni, w ramach jednej paczki godzin niewykorzystane godziny nie przechodzą na kolejny okres. Nie zmienia to wynagrodzenia Wykonawcy, pod warunkiem pozostania w gotowości do wykonania zleceń incydentów na rzecz Zamawiającego.

Jeżeli Zamawiający wykorzysta jeden typ wsparcia (godziny stacjonarne, lub online) może wymienić typ wsparcia według przelicznika: 1 godzina stacjonarna = 6 godzin online.

Podmiot realizujący usługę musi posiadać kompetencje z wdrażanego w ramach projektu Centralnego Systemu Bezpieczeństwa – oprogramowania klasy SIEM - **Na wezwanie Zamawiającego, razem z podmiotowymi środkami dowodowymi, należy dołączyć certyfikat wystawiony przez producenta systemu potwierdzający kompetencje Wykonawcy (lub osób wskazanych do realizacji tego zadania) lub referencje z wdrożenia oferowanego systemu przez Wykonawcę (lub osoby wskazane do realizacji zadania).**

3. **<u>Centralny System Bezpieczeństwa. Oprogramowanie klasy SIEM z elementami XDR Extended Detection and Response, EDR Endpoint Detection and Response, oraz monitoringiem infrastruktury IT – 1 szt.;</u>**

LICENCJA

W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją bezterminową.

Oprogramowanie musi posiadać wsparcie do dnia 25-03-2026 roku, w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta.

Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.

WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA:

Automatyczne Odkrywanie: Centralny System Bezpieczeństwa (dalej CSB) musi używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI, i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci.

Monitorowanie Wysokiej Wydajności: CSB musi umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania (np. przez SNMP, ICMP, IPMI), CSB musi efektywnie zbierać dane o wydajności i dostępności urządzeń. System powinien być skalowalny i umożliwiać obsługę co najmniej 100 urządzeń i metryk.

Elastyczne Wyzwalacze: Wyzwalacze (akcje) w CSB powinny być wyrażeniami logicznymi, które określają warunki dla powiadomień alarmowych. W systemie musi być możliwość definiowania złożonych warunków dla generowania alertów, na przykład po przekroczeniu pewnych progów lub w przypadku wystąpienia określonych wzorców.

Wizualizacja Danych: CSB powinien posiadać intuicyjny i przejrzysty interface, umożliwiający wizualizację danych pod kontem ich analizy. System musi umożliwiać wizualizację przy wykorzystaniu m.in interaktywnych wykresów i grafik ponadto system musi posiadać wbudowaną zaawansowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności).

Alerty i Powiadomienia: CSB powinien umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS, czy integracje z systemami biletowymi. Użytkownicy powinni mieć możliwość ustawiania różnych poziomów priorytetów dla alertów, a także definiowania eskalacji dla poważniejszych problemów.

Raportowanie: CSB powinien umożliwiać użytkownikom generowanie szczegółowych raportów dotyczących wydajności i dostępności monitorowanych systemów.

Wsparcie dla Szyfrowania: CSB musi być systemem bezpiecznym, umożliwiającym szyfrowaną komunikację między agentami a serwerem, co zapewnia bezpieczeństwo danych monitorowania.

Skalowalność: Architektura CSB powinna być zaprojektowana z myślą o skalowalności, co powinno pozwalać na łatwą adaptację do rosnących wymagań w miarę rozwoju infrastruktury IT.

Przetwarzanie i Wyszukiwanie Danych: CSB pod kątem agregacji logów musi być oparty na technologii, która umożliwia indeksowanie, wyszukiwanie i analizowanie dużych ilości danych w czasie rzeczywistym. Użytkownicy powinni móc wykonywać skomplikowane zapytania, aby szybko odnaleźć konkretne informacje.

Szybkość i Wydajność: Zaprojektowany do szybkiego przetwarzania dużych ilości danych, co jest kluczowe w środowiskach produkcyjnych z intensywnym ruchem danych.

Elastyczne Zbieranie Danych: CSB musi gromadzić dane z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie).

Przetwarzanie i Wzbogacanie Danych: CSB musi posiadać bogaty zestaw filtrów do przetwarzania danych.

Odkrywanie i Analiza Danych: System musi umożliwia użytkownikom przeszukiwanie, przeglądanie i analizowanie zgromadzonych danych ułatwiając identyfikację wzorców i trendów.

Wsparcie dla Wielu Platform: CSB musi być kompatybilny z wieloma systemami operacyjnymi, co najmniej Linux, Windows, macOS.

Treści pojawiające się w interfejsie użytkowników CSB będą spełniać standardy WCAG 2.1 na poziomie AA.

Cały interfejs użytkownika powinien być dostosowany pod aktualne wymagania prawne związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami.

Na podstawie uzyskanych efektów serwis będzie mógł być udostępniony publicznie.

Treści multimedialne muszą być dostępne z poziomu klawiatury i oprogramowania dla osób niepełnosprawnych. Multimedia, które nie mogą być z przyczyn technicznych tak zbudowane, by uczynić je dostępnymi dla wszystkich użytkowników muszą posiadać alternatywny opis tekstowy, który wyjaśnia ich cel i funkcje zastosowania na stronie.

Zgodność ze standardami HTML i CSS całego serwisu www.

Kontrast kolorystyczny między tłem, a tekstem musi być zgodny z zaleceniami WCAG 2.1 AA.

System CSB musi rejestrować zdarzenia akcje i reakcje użytkowników w CSB. Historia akcji poszczególnych użytkowników musi być raportowana i możliwa do odtworzenia w logach systemowych – chronologicznie.

System musi posiadać budowę modułową, która będzie umożliwiać dodawanie nowych modułów oraz wyłączanie już uruchomionych. Dostarczony i uruchomiony system będzie posiadał co najmniej moduły:

1. **MODUŁ ANALIZY PODATNOŚCI**

1.1. Integracja ze stale aktualizowaną bazą danych CVE (Common Vulnerabilities and Exposures), gromadzącą informację na temat podatności urządzeń i oprogramowania.

System musi być zintegrowany z publicznym i stale aktualizowanym rejestrem gromadzącym i udostępniającym informację na temat znanych podatności w urządzeniach obsługiwanych przez system oraz oprogramowaniu zainstalowanym na urządzeniach Zamawiającego (np. UTM). Połączenie z bazą danych CVE odbywać się ma przy wykorzystaniu udostępnionego API i nie powinno wymagać od użytkowników końcowych konfiguracji.
Synchronizacja z bazą CVE oraz sprawdzenie dodania do niej nowych podatności dotyczących sprzętu i oprogramowania zainstalowanego w infrastrukturze sieciowej jednostki musi odbywać się przynajmniej raz dziennie. Po zalogowaniu do CSB i wybraniu modułu analizy podatności powinny być wyświetlane wszystkie zsynchronizowane informacje wraz z danymi historycznymi. Podatności "nowe", których użytkownik wcześniej nie widział powinny być w systemie oznaczone np. poprzez pogrubioną czcionkę lub inny kolor.

1.2. Automatyczne sprawdzenie możliwości występowania podatności w infrastrukturze sieciowej na podstawie zinwentaryzowanych urządzeń i oprogramowania.

System musi automatycznie sprawdzać możliwość wystąpienia nowej podatności tylko na urządzeniach i oprogramowaniu znajdującym się w infrastrukturze sieciowej jednostki, a dokładniej wyszczególnionych (dodanych) w module inwentaryzacji.

1.3. Powiadamianie użytkownika o nowych podatnościach występujących w jego środowisku IT.

System musi informować użytkownika/administratora o nowych podatnościach występujących w infrastrukturze sieciowej jednostki. System powinien posiadać możliwość włączenia powiadomień na przeglądarkę internetową oraz wskazany przez użytkownika/administratora adres e-mail. Ponadto użytkownik po zalogowaniu się do systemu i wybraniu modułu analizy podatności musi być powiadomiony przez system o występujących nowych podatnościach na poszczególnych hostach infrastruktury sieciowej poprzez np. graficzne wyróżnienie hosta i oprogramowania na nim

zainstalowanego. System musi informować użytkownika o treści podatności oraz jej sklasyfikowania (np. podatność krytyczna).

2. MODUŁ MONITORINGU ZASOBÓW

2.1. Monitorowanie zasobów hostów na podstawie zinwentaryzowanych w systemie urządzeń (monitoring obciążenia dysków, procesorów, ruchu sieciowego itp.)

System musi posiadać możliwość monitorowania zasobów wszystkich hostów dodanych w module inwentaryzacji. Monitorowanie, zbieranie informacji na temat obciążenia wybranego hosta musi odbywać się w sposób ciągły w ustalonych krótkich (co najmniej minutowych) odstępach czasowych. Użytkownik po zalogowaniu się do systemu i wybraniu modułu inwentaryzacji musi mieć możliwość wyświetlenia w formie graficznej (wykresów), przebiegów czasowych istotnych parametrów hosta, co najmniej takich jak: obciążenie procesora, obciążenie pamięci, obciążenie dysków, obciążenie ruchu sieciowego, skoki na procesorze, czas oczekiwania na dysk i odczyt i zapis na dysku. Ponadto system musi na bieżąco informować o aktualnym statusie hosta (dostępny, niedostępny).

2.2. Grupowanie hostów i korelacja obciążeń zasobów pomiędzy hostami

System musi mieć możliwość wyświetlania zgrupowanych wykresów hostów należących do tej samej grupy. Hosty muszą być pogrupowane w zasugerowany przez administratora sieci sposób w celu skorelowania ze sobą istotnych parametrów zasobów, co umożliwi porównanie zachowań poszczególnych hostów na tle grupy. Hosty powinny być podzielone co najmniej, na urządzenia sieciowe (np. serwery) oraz urządzenia końcowe (np. komputery pracowników). Użytkownik musi mieć możliwość filtrowania wykresów na poziomie poszczególnych hostów, oraz tworzenia w systemie nowych grup i wykresów parametrów dostępnych z wybieralnej listy.

2.3. Wysyłanie alertów i powiadomień dotyczących problemów i zdarzeń występujących na hostach

System musi posiadać funkcjonalność umożliwiającą użytkownikowi/administratorowi skonfigurowanie wysyłania alertów i powiadomień dotyczących problemów i zdarzeń. W systemie musi być możliwość ustawienia wysyłania wiadomości i powiadomień, poprzez wysyłanie komunikatów na przeglądarkę internetową, wysyłanie wiadomości e-mali lub wiadomości sms (w systemie powinna być możliwość dodania bramki sms - Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms). Wysyłane przez system wiadomości muszą zawierać co najmniej informacje na temat występującego zdarzenia/problemu tj. opis, sklasyfikowanie (np. błąd, ostrzeżenie, informacja), data i godzina. Użytkownik/Administrator powinien mieć możliwość ustawienia odbiorcy wiadomości poprzez podanie adresu e-mail, czy w przypadku wiadomości SMS numeru telefonu. Użytkownik musi mieć możliwość wyboru w systemie, przy jakiego typu zdarzeniach i problemach będzie wysyłana wiadomość.

2.4. Funkcja korelacji występujących problemów na hostach z modułem analizy logów

Moduł monitoringu zasobów oprócz przebiegów czasowych parametrów hostów powinien również zawierać informację na temat występujących problemów i zdarzeń na poszczególnych hostach. Użytkownik/Administrator po zalogowaniu się do systemu, wybraniu Modułu Monitoringu zasobów i wyborze konkretnego hosta musi posiadać możliwość prześledzenia zdarzeń i problemów naniesionych na osi czasu. Na osi czasu powinny być wyświetlane tylko "nowe" problemy i zdarzenia oraz te, których status nie został zmieniony na "rozwiązany" bądź "anulowany". Użytkownik/Administrator musi mieć możliwość zmiany statusu wybranego zdarzenia czy problemu wraz z dodaniem krótkiego opisu w jaki sposób problem został rozwiązany. Użytkownik/Administrator musi mieć możliwość stłumienia często powielającego się problemu, którego jest świadomy i musi poczekać na jego rozwiązanie (po włączeniu opcji tłumienia problemu, suystem przez pewien czas nie będzie o nim informował/alertował). Wszystkie problemy i zdarzenia raportowane w systemie muszą być skorelowane z logami pochodzącymi z konkretnych hostów. Użytkownik/Administrator po wybraniu w systemie konkretnego problemu występującego na konkretnym hoście po wybraniu zakładki logi musi zostać przekierowany do modułu analizy logów, w którym automatycznie wyświetlone będą tylko logi dotyczące hosta na którym wystąpił problem. Ponadto użytkownik/administrator w ramach tego modułu powinien mieć możliwość zgłoszenia wystąpienia konkretnego problemu do np. zewnętrznego wsparcia IT. W systemie powinna być możliwość integracji systemu z zewnętrznym systemem typu: "help-desk", przynajmniej poprzez podanie adresu e-mail, na który zostanie wysłane zgłoszenie.

2.5. Kategoryzacja istotności zdarzeń występujących w infrastrukturze sieciowej

Wszystkie zdarzenia i problemy raportowane w systemie muszą być skategoryzowane według ich poziomu istotności (priorytetów). W systemie powinny być identyfikowane problemy z priorytetami w co najmniej 4 stopniowej skali, np: Krytyczny, Wysoki, Średni, Niski. Ponadto, system powinien zapewniać dodatkowe dwa priorytety - zdarzenia nie istotne powinny być również sklasyfikowane w systemie jako informacja, a zdarzenia trudne do sklasyfikowania powinny posiadać priorytet o wartości (niesklasyfikowany).

2.6 Lista predefiniowanych zdarzeń najczęściej występujących w środowiskach IT

System musi być wyposażony w listę wcześniej zdefiniowanych zdarzeń/scenariuszy, które najczęściej występują w środowiskach IT. Użytkownik/Administrator powinien mieć możliwość wybrania konkretnego hosta lub grupy hostów i przypisania im predefiniowanych zdarzeń (np. brak miejsca na dyskach, czy zbyt wysoki ruch sieciowy). W predefiniowanych zdarzeniach/scenariuszach użytkownik/administrator powinien mieć możliwość ustawienia/edycji reguł oraz zmiany wykonywanych operacji, gdy warunki reguł zostaną spełnione. Użytkownik powinien mieć możliwość używania w regułach operatorów logicznych takich jak AND i OR oraz

operatorów relacyjnych takich jak: "==", "<=", ">=", "!=". Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

2.7 Dobór oraz dodawanie zdarzeń do konkretnego środowiska IT

System musi umożliwiać użytkownikowi/administratorowi dodawanie własnych zdarzeń/scenariuszy dostosowanych do jego konkretnych potrzeb. Tworzenie nowego zdarzenia w systemie powinno się odbywać poprzez podanie jego unikalnej nazwy, wybranie hosta lub grupy hostów, których dotyczy tworzone zdarzenie, zdefiniowanie warunków opisujących zdarzenie, oraz podanie operacji jakie mają być wykonane, gdy warunki zostaną spełnione. Warunki powinny korzystać z operatorów logicznych takich jak AND i OR oraz operatorów relacyjnych takich jak: "==", "<=", ">=", "!=". Użytkownik/Administrator systemu musi mieć możliwość ustawienia operacji różnego typu takich jak.: wysłanie wiadomości e-mail, wysłanie wiadomości SMS (Zamawiający dopuszcza wykorzystanie autorskiej bramki sms lub wskażę zew. bramkę/serwis sms), wysłanie zapytania (Request), czy uruchomienie predefiniowanego skryptu.

2.8 Zdalny dostęp do urządzeń końcowych

System musi umożliwiać zdalne połączenie się do wybranego hosta/urządzenia, które zostało wcześniej odpowiednio skonfigurowane. Zdalny dostęp musi odbywać się poprzez przeglądarkę internetową bez konieczności instalowania dodatkowego oprogramowania. Połączenie zdalne musi być możliwe przy wykorzystaniu co najmniej dwóch protokołów, konkretnie RDP i SSH.

2.9 Wywoływanie predefiniowanych skryptów na urządzeniach końcowych

System musi dawać możliwość wywołania podstawowych skryptów na hostach końcowych, na których został zainstalowany jego agent. Predefiniowane w systemie skrypty muszą obejmować co najmniej: wyłączenie i restart hosta, wysłanie wiadomości tekstowej do hosta, włączenie i wyłączenie blokady ruchu sieciowego, włączenie i wyłączenie trybu izolacji z infrastruktury sieciowej hosta z możliwością zdalnego połączenia się z nim.

2.10 Analiza ruchu sieciowego

System musi posiadać możliwość śledzenia logów pochodzących z urządzeń sieciowych typu UTM zwłaszcza tych najczęściej używanych i polecanych w środowiskach informatycznych. Użytkownik

systemu/administrator musi mieć możliwość filtrowania wyświetlanych informacji, co najmniej poprzez podanie przedziału czasowego i wyboru nazwy zinwentaryzowanego urządzenia typu UTM.

2.11 Monitorowanie problemów i zdarzeń występujących na drukarkach

System musi umożliwiać monitorowanie problemów występujących na drukarkach sieciowych wykorzystujących protokół SNMP. System powinien zbierać informacje na temat występujących problemów w osi czasu, umożliwiać tłumienie problemów, wskazywać ich istotność. Ponadto w systemie powinny znajdować się możliwe do pobrania wartości parametrów drukarki oraz informacji na temat dostępności urządzenia.

3. MODUŁ ANALIZY LOGÓW

3.1. Przegląd i analiza logów pochodzących z inwentaryzowanych urządzeń/maszyn.

Moduł Analizy Logów i Moduł Monitoringu Zasobów musi być powiązany z Modułem Inwentaryzacji i wykorzystywać informację przez niego posiadane. Użytkownik/Administrator systemu musi posiadać możliwość przeglądania i analizowania logów pochodzących z wszystkich hostów dodanych w Module inwentaryzacji. W ramach modułu system musi agregować logi pochodzące z systemów operacyjnych, aplikacji i systemów dziedzinowych. Agregacja logów powinna odbywać się w sposób ciągły i po osiągnięciu limitu związanego z zasobami dyskowymi serwera nadpisywać historyczne logi, począwszy od najstarszych.

3.2. Możliwość analizy tzw. „customowych" logów pochodzących z dowolnego oprogramowania, w tym systemów dziedzinowych.

System musi posiadać możliwość analizy logów pochodzących z dowolnego oprogramowania, a przede wszystkim z oprogramowania dziedzinowego stosowanego przez Zamawiającego. Użytkownik/Administrator musi mieć możliwość dodawania w module nazwy, lokalizacji i typu tzw. "customowych" logów, które będą agregowane w systemie, w celu późniejszej ich analizy. Zdefiniowane przez Użytkownika/Administratora logi powinny być skorelowane z problemami występującymi na hostach w module monitoringu zasobów. Jeśli wystąpi jakiś problem związany z działaniem np. systemu dziedzinowego, to użytkownik/administrator analizując problemy musi mieć opcję automatycznego przekierowania do logów związanych z tym system.

3.3. Zawansowane filtrowanie, zarówno po hostach jak i zainstalowanym na nich oprogramowaniu.

Moduł analizy logów musi być wyposażony w zaawanasowaną wyszukiwarkę umożliwiającą użytkownikowi/administratorowi wyszukiwanie i filtrowanie konkretnych logów. System powinien umożliwiać odfiltrowanie logów dla konkretnego hosta, grupy hostów, oprogramowania (w szczególności oprogramowania dziedzinowego - "customlogów"), kategorii, dowolnie wpisanej frazy oraz zakresu czasu (data – godzina, od -do). W Systemie muszą być zastosowane mechanizmy stronicowania, umożliwiające płynne przeglądanie dużej ilości informacji.

3.4. Przegląd i analiza logów dotyczących działań użytkowników.

W module analizy logów muszą być agregowane logi dotyczące działań użytkowników. W zależności od rodzaju systemu czy oprogramowania zainstalowanego na hoście w logach znajdują się informacje dotyczące różnej aktywności użytkowników (m.in. data zalogowania się użytkownika do systemu, data wylogowania, czy wybór konkretnej funkcjonalności). Użytkownik/Administrator CSB musi mieć możliwość sprawdzenia tych aktywności poprze wyszukanie i odfiltrowanie logów po nazwie użytkownika, typie aktywności, czy dowolnie wpisanej frazie.

3.6. Dostęp do logów historycznych.

System oprócz dostępu do aktualnych logów musi uwzględniać również logi historyczne. Użytkownik/Administrator musi mieć możliwość przeglądania wszystkich logów agregowanych na zasobach dyskowych. Ilość oraz zakres czasowy agregowanych logów limitowany ma być tylko zarezerwowaną przestrzenią dyskową na serwerze. Po osiągnięciu założonego limitu, system powinien nadpisywać logi począwszy od najstarszych. Użytkownik/Administrator podobnie jak w przypadku logów aktualnych musi mieć możliwość przeszukiwania oraz filtrowania logów historycznych po hostach, oprogramowaniu, czasie i dowolnie wpisanej frazie.

3.7. Informowanie i powiadomienia dotyczące pojawienia się nowych istotnych logów w obrębie całej infrastruktury sieciowej.

System musi być wyposażony w mechanizmy powiadamiające użytkownika/administratora o pojawieniu się istotnych logów pochodzących z urządzeń infrastruktury sieciowej. System musi posiadać możliwość konfiguracji tych powiadomień pod katem istotności pojawiającego się wpisu w lagach oraz wyboru typu logu (m.in. log systemowy, log "customowy"). Ponadto CSB musi informować użytkownika/administratora o "nowych" zagregowanych logach z poszczególnego hosta. Informacja ta powinna być wyświetlana w systemie po zalogowaniu użytkownika/administratora, a "nowe" logi to logi dodane do systemu od czasu ostatniego logowania użytkownika/administratora.

3.8. Kategoryzacja istotności logów (np.: informacja, ostrzeżenie, błąd).

System musi być wyposażony w mechanizmy kategoryzujące logi pod kontem ich istotności. System w szczególności powinien informować użytkownika/administratora o pojawieniu się logów dotyczących nieprawidłowości działania poszczególnych hostów, czy oprogramowania na nich zainstalowanych. Następnie w zależności od potrzeb użytkownika/administratora system powinien informować o pojawieniu się ostrzeżeń w oprogramowaniu kluczowym dla użytkownika. Jeśli log dotyczy tylko informacji takiej jak zalogowanie się, czy wyłączenie hosta, to użytkownik/administrator nie powinien otrzymywać powiadomienia (alertu), z wyjątkiem logów które użytkownik/administrator uzna za istotne (pomimo tego, że są skategoryzowane jako informacja).

4. MODUŁ EDR/XDR

4.1 Integracja z systemem EDR/XDR posiadanym przez Zamawiającego – ESET Enterprise Protect.

4.2. Podgląd informacji, alertów i zdarzeń występujących w środowisku IT

W CSB powinna być możliwość podglądnięcia statystyk incydentów/zdarzeń oraz ich kategorie. Użytkownik/Administrator z poziomu CSB powinien mieć możliwość uzyskania takich informacji jak rodzaj, nazwa lub źródło incydentu, opis, data wykrycia oraz kategoria/priorytet.

4.3. Bezpośrednie przekierowanie do zaawansowanych opcji zintegrowanego systemu EDR/XDR (panelu administracyjnego)

Poza integracją i prezentacją incydentów/zdarzeń występujących na poszczególnych hostach w module musi znajdować się funkcjonalność umożliwiająca użytkownikowi/administratorowi przejście do panelu administracyjnego systemu EDR/XDR udostępniającego zaawansowane opcje.

5. MODUŁ INWENTARYZACJI

5.1 Automatyczny (przy wykorzystaniu agentów), półautomatyczny (przy wykorzystaniu pliku CSV) lub ręczny sposób dodawania hostów oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

System musi dawać użytkownikowi/administratorowi możliwość dodawania hostów/urządzeń/oprogramowania należących do infrastruktury sieciowej na trzy różne sposoby. Pierwszy dotyczy automatycznego wykrywania i dodawania przy wykorzystaniu usług katalogowych. Wszystkie hosty i urządzenia należące do wybranej domeny powinny być automatycznie dodane do CSB wraz z zainstalowanym na nich oprogramowaniem. Drugi i trzeci sposób natomiast ma umożliwiać użytkownikowi/administratorowi dodanie

urządzeń/hostów/oprogramowania nie należących do domeny poprzez "ręczne" wpisanie informacji (wypełnienie formularza) lub wczytanie pliku w formacie CSV posiadającego usystematyzowaną strukturę. Moduł inwentaryzacji musi być ściśle skorelowany (powiązany) z pozostałymi modułami systemu CSB.

5.2 Gromadzenie pełnych informacji na temat urządzeń (tj. nazwa hosta, adres IP, główny użytkownik) jak i oprogramowania (nazwa, wersja)

Informacje o urządzeniach/hostach/oprogramowaniu, które muszą znaleźć się zarówno w formularzu jak i pliku CSV to m.in. dla hosta/urządzenia: nazwa, adres IP, przypisany użytkownik, typ urządzenia/hosta oraz lista zainstalowanego na nim oprogramowania wraz z wersjami. Przy wprowadzaniu "ręcznym" system musi umożliwiać użytkownikowi/administratorowi wybór nazwy i wersji oprogramowania z listy znajdującej się bazie CVE, bądź wpisanie własnych wartości.

6.3. Generowanie raportu w formacie PDF, CSV zawierającego aktualne informację na temat urządzeń oraz oprogramowania zainstalowanego w infrastrukturze sieciowej.

Moduł musi być wyposażony w funkcjonalności umożliwiającą użytkownikowi/administratorowi wygenerowania raportów z całej dodanej w systemie CSB infrastruktury sieciowej. Raporty powinny być generowane w co najmniej dwóch formatach tj. PDF i CSV oraz powinny zawierać wszystkie istotne informację na temat urządzenia/hosta/oprogramowania m. in takie jak: nazwa, adres, główny użytkownik, lista oprogramowania wraz z wersjami. Ponadto raport musi zawierać m.in. datę i godzinę wygenerowania, nazwę jednostki organizacyjnej oraz imię i nazwisko osoby generującej raport. Dokładny wzór (wizualny) generowanego raportu zostanie ustalony przez zamawiającego w trakcie realizacji zamówienia. Moduł musi umożliwiać generowanie raportów zarówno z całości jak i z odfiltrowanych urządzeń/hostów/oprogramowania. Użytkownik/Administrator musi mieć możliwość odfiltrowania informacji według co najmniej takich kategorii jak: nazwa użytkownika, grupa urządzeń, dowolnie wpisana fraza.

7. MODUŁ ZGŁASZANIA INCYDENTÓW (e-mail, system help-deskowy)

7.1. Integracja z systemem tiketowym.

System CSB musi w prosty i intuicyjny sposób umożliwiać użytkownikowi/administratorowi integrację z systemem typu: help-desk. Integracja powinna odbywać się poprzez ustawienie w konfiguracji CSB odpowiedniego adresu e-mail systemu help-deskowego, na który będą wysyłane zgłoszenia dotyczące problemów. Wysyłanie wiadomości ma się odbywać automatycznie po wybraniu przez użytkownika/administratora konkretnego zdarzenia w systemie CSB. Wiadomość e-mail powinna zwierać minimum nazwę jednostki organizacyjnej wysyłającej zgłoszenie, treść zgłoszenia oraz dane zgłaszającego: Imię Nazwisko, adres e-mail, numer telefonu.

7.2. Zgłaszanie incydentu/problemu, który został namierzony przez system.

Moduł zgłaszania incydentu powinien być ściśle powiązany z modułem monitoringu zasobów, a dokładniej z funkcjonalnością wyświetlającą zidentyfikowane na urządzeniach/hostach problemy. Użytkownik/Administrator systemu powinien posiadać możliwość wyboru problemu namierzonego przez CSB i automatycznego zgłoszenia go do help-desk, poprzez wybranie np. przycisku "Zgłoś Problem". Po wybraniu opcji zgłoszenia system powinien automatycznie wysyłać do systemu tiketowego zgłoszenie zawierające pełne informacje dotyczące wybranego problemu.

7.3. Bezpośrednie zgłaszane zagrożeń/cyberataków do CSIRT NASK.

System powinien umożliwiać generowanie co najmniej pliku w formacie pdf ze zgłoszeniem zagrożenia/incydentu/ cyberataku zgodnego z formularzem udostępnianym przez NASK.

8. MODUŁ WYKRYWANIA ZAGROŻEŃ

8.1. Wykrywanie zagrożeń na podstawie powszechnie znanych taktyk i technik wykorzystywanych przez cyberprzestępców udostępnione w ogólnodostępnej bazie danych MITRE ATT&CK.

System musi umożliwiać użytkownikowi/administratorowi włączenie reguł sprawdzających, czy w jego infrastrukturze sieciowej nie zostały zastosowane taktyki i techniki różnego rodzaju cyberataków. System musi być zintegrowany z powszechnie dostępną bazą danych MITRE ATT&CK zawierającą zbiór taktyk i technik zaobserwowanych przez specjalistów na całym świecie. System powinien posiadać wbudowane reguły umożliwiające wykrycie wielu zagrożeń opisanych w matrycy MITRE ATT&CK, system powinien wskazywać użytkownikowi, przed jakiego rodzaju taktykami i technikami jest chronione jego środowisko IT. System musi pokazywać ilość wbudowanych w nim reguł wraz z ilością włączonych reguł. Użytkownik/Administrator systemu musi mieć możliwość sprawdzenia w systemie ile reguł dotyczących konkretnej techniki jest włączonych, a ile jeszcze pozostało do wyłączenia. System musi pokazywać pokrycie matrycy MITRE ATT&CK ilościom włączonych/wyłączonych reguł wykrywających cyberzagrożenia.

8.2. Kategoryzacja oraz prezentacja wykrytych zagrożeń

System musi umożliwiać użytkownikowi/administratorowi sprawdzenie zagrożeń wykrytych na poszczególnych hostach/urządzeniach zinwentaryzowanych w module inwentaryzacji. Wykryte w systemie zagrożenia musza zawierać informację na temat: daty i czasu ich wystąpienia, rodzaju/treści oraz poziomu istotności. System powinien kategoryzować zagrożenia w co najmniej czterostopniowej skali: poziom zagrożenia niski, średni, wysoki, krytyczny.

8.3. Historia wykrytych zagrożeń

System musi posiadać możliwość sprawdzenia historii występowania zagrożeń na hostach/urządzeniach. System musi być wyposażony w rozbudowaną wyszukiwarkę hostów i zagrożeń umożliwiającą między innymi: wyszukanie hosta po nazwie, adresie IP, kategorii/priorytetów, daty wykrycia (przedziału czasowego).

8.4. Wsparcie/automatyczna ochrona po wykryciu zagrożenia

System musi posiadać możliwość włączenia "automatycznej ochrony" w wybrane dni tygodnia i w wybranych godzinach. Użytkownik/administrator musi mieć możliwość ustawienia automatycznej ochrony przed wybranymi taktykami i technikami działań cyberprzestępców poza godzinami jego pracy. System musi mieć możliwość ustawienia reakcji na wykrycie zagrożenia w zależności od wybranego poziomu istotności/priorytetu. Ponadto użytkownik/administrator musi mieć możliwość wybrania operacji/akcji z listy predefiniowanych operacji/akcji, która zostanie wykona w razie wykrycia zagrożenia o wybranym priorytecie. Lista operacji/akcji musi umożliwiać co najmniej wyłączenie/restart hosta/urządzenia na którym wykryto zagrożenie, przesłanie informacji o wystąpieniu zagrożenia do użytkownika/administratora przy wykorzystaniu poczty e-mail bądź bramki sms, blokowanie hosta na którym występuje zagrożenie.

9. MODUŁ RAPORTÓW

9.1. Tworzenie zestawień i raportów z danych pochodzących z pozostałych modułów

System musi posiadać możliwość tworzenie różnego rodzaju zestawień prowadzących do sporządzenia i wyeksportowania raportu w co najmniej dwóch formatach: csv, pdf. Podczas tworzenia zestawienia użytkownik/administrator musi mieć możliwość wyboru konkretnych hostów bądź grupy hostów, dla których tworzony jest raport. Użytkownik musi posiadać możliwość wyboru modułów oraz priorytetów zdarzeń w nich występujących. Ponadto użytkownik przez administrator musie mieć możliwość wyboru przedziału czasowego, dla którego zostanie wykonany raport.

10. PANEL UŻYTKOWNIKA

10.1. Intuicyjny i przejrzysty panel użytkownika dostępny z dowolnej lokalizacji poprzez stronę www.

Panel użytkownika CSB powinien być przejrzysty i intuicyjny oraz wykonany przy wykorzystaniu najnowszych standardów i technologii stosowanych we współczesnych systemach informatycznych. Panel użytkownika/administratora sytemu musi być dostępny poprzez podanie odpowiedniego adresu w przeglądarce internetowej. Dostęp do panelu użytkownika musi być bezpieczny poprzez szyfrowanie (zabezpieczenie certyfikatem SSL) oraz tzw. białą listę adresów

IP - która pozwala użytkownikowi/administratorowi systemu blokować dostęp z nie znajdujących się na niej adresów. Panel użytkownika powinien również spełniać wymagania związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami - WCAG 2.1 AA.

10.2. Wizualizacja statystyk zdarzeń i logów

Panel użytkownika CSB, powinien posiadać elementy umożliwiające prezentację statystyk zdarzeń i logów w sposób zrozumiały, ułatwiający analizę działania środowiska IT pod kątem cyberbezpieczeństwa. Wizualizacja statystyk zdarzeń i logów powinna dotyczyć przede wszystkim ilości "nowych" zdarzeń zarejestrowanych w systemie z podziałem na ich kategorię. Natomiast sposób prezentacji samych logów i zdarzeń musi być przejrzysty jasno podkreślający sklasyfikowanie zdarzenia czy wpisu do logów. Zdarzenia i logi powinny w systemie być wyświetlane w kolejności od najnowszych do najstarszych z możliwości odfiltrowania zakresu czasowego ich prezentowania.

10.3. Wykresy zdefiniowanych parametrów zasobowych aktualizowane na „żywo".

Wykresy prezentujące parametry zasobów urządzeń/hostów powinny być aktualizowane w systemie na "żywo", a dokładnie w zależności od ustaleń z zleceniodawcą system musi aktualizować wykresy w określonych odstępach czasowych (co najmniej, co minutę).

10.4. Filtrowanie wyświetlanych danych wg. hostów, oprogramowania, kategorii zdarzeń itd.

Panel użytkownika powinien być tak zaprojektowany, aby użytkownik/administrator w sposób intuicyjny mógł filtrować istotne dla niego informacje dotyczące zarówno obciążeń zasobów, zdarzeń (problemów, ostrzeżeń), czy logów. Panel użytkownika musi być wyposażony w wyszukiwarkę umożliwiająca filtrowanie informacji wg. m.in. nazwy hosta/urządzenia, nazwy oprogramowania czy kategorii zdarzeń i logów. Wyszukiwarka w panelu użytkownika powinna znajdować się w widocznym miejscu i posiadać precyzyjnie oznaczone możliwości filtrowania. Użytkownik/Administrator powinien mieć możliwość nakładania na siebie różnych filtrów.

10.5. Intuicyjny panel zarządzania regułami i definiowania "customowych" logów.

Panel użytkownika powinien być wyposażony w przejrzysty i intuicyjny panel zarządzania regułami (akcjami), na podstawie których użytkownik/administrator informowany jest o zaistniałym w środowisku IT problemie. W panelu tym musi znaleźć się między innymi lista już zdefiniowanych reguł z możliwością ich usunięcia i edycji oraz opcja umożliwiająca dodanie nowej reguły. Reguły w panelu użytkownika powinny być dodawane przy wykorzystaniu przejrzystego i

intuicyjnego formularza, w którym użytkownik/administrator musi podać nazwę reguły, dodać warunku oraz wybrać rodzaj operacji, która zostanie wykonana, gdy warunki będą spełnione. Użytkownik/administrator CSB musi mieć możliwość wyboru zarówno warunków, reguł jak i operacji z udostępnionych w systemie opcji. Ponad to panel użytkownika musi być wyposażony w panel zarządzania "customowymi" logami, w którym podobnie jak w przypadku reguł, użytkownik/administrator może wyświetlić listę zdefiniowanych "customlogów" wraz z możliwością ich usunięcia, edycji oraz zdefiniowania nowych. Dodanie do systemu "customlogów" musi być intuicyjne i ma polegać na podaniu unikalnej nazwy definiowanych logów, jego ścieżki (lub ścieżek) dostępu oraz nazwy hosta lub grupy hostów, których ma on dotyczyć.

4. Backup w chmurze – 1 szt.;

W ramach zadania obowiązkiem Wykonawcy będzie udostępnienie przestrzeni dyskowej na potrzeby przechowywania kopii zapasowych (backupów) danych. Usługa obejmuje:

1) Parametry główne

a) Udostępnienie przestrzeni dyskowej o minimalnej pojemności 200 GB.
b) Zapewnienie redundancji danych w celu zwiększenia bezpieczeństwa przechowywanych informacji.
c) Gwarancję dostępności danych (SLA na poziomie 99,9%).
d) Możliwość skalowania przestrzeni dyskowej w miarę wzrostu potrzeb.
e) Zapewnienie odpowiednich mechanizmów zabezpieczających dane, takich jak szyfrowanie, ochrona przed nieautoryzowanym dostępem oraz regularne testy odtwarzania danych.
f) Udostępnienie bezpiecznych, szyfrowanych połączeń dla transferu danych.

2) Specyfikacja Techniczna

a) **Pojemność Dyskowa**:

- Minimalna początkowa pojemność: 200 GB.

- Możliwość dodatkowego rozszerzenia pojemności w krokach co 100 GB.

b) **Bezpieczne Połączenia**:

- Wymóg stosowania bezpiecznych, szyfrowanych połączeń (TLS 1.2 lub nowszy) dla wszystkich operacji przesyłania danych.

- Certyfikaty SSL/TLS wydane przez zaufane urzędy certyfikacji (CA).

c) **Dostępność i Skalowalność**:

- Gwarantowana dostępność usługi na poziomie 99,9% (SLA).

- Skalowalność umożliwiająca dynamiczne zwiększanie przestrzeni dyskowej bez przerw w dostępie do usługi.

d) **Interfejsy Dostępu**:

- Dostęp przez protokoły NFS, SMB.

3) Dostęp do danych

a) Wykonawca zapewni Zamawiającemu dostęp do danych za pomocą narzędzi takich jak: Serwer plików, Serwer FTP, WebDav, Serwer WEB, Serwer kopii zapasowych.

4) Gwarancja i hosting

a) Przestrzeń dyskowa uruchomiona w ramach backupu w chmurze i gwarancja Wykonawcy świadczona będzie do dnia 25-03-2026 roku.

5. <u>Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych – 1 szt.;</u>

LICENCJA

W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją bezterminową.

Oprogramowanie musi posiadać wsparcie min. do dnia 25-03-2026 roku, w ramach wsparcia, Zamawiający musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji oprogramowania, zgłaszać błędy w Oprogramowaniu do serwisu producenta.

Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.

Dostarczona licencja na Oprogramowanie nie może limitować ilości urządzeń.

Licencja na dostarczone oprogramowanie musi umożliwiać działanie dla minimum 45 użytkowników.

OPROGRAMOWANIE

Oprogramowanie musi posiadać budowę modułową, składającą się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami musi być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Program musi umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.

Moduły muszą umożliwiać 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.

Oprogramowanie musi posiadać moduły opisane poniżej.

MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) – minimalne wymagania:

Musi obejmować m.in.: serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

1. Wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
2. Wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
3. Wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
4. Wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
5. Wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
6. Wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
7. Wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
8. Wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
9. Wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
10. Zablokowania mapy urządzeń przed przypadkową edycją
11. Serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
12. Serwerów pocztowych:
13. Monitorowanie czasu logowania do serwisu odbierającego oraz czas wysyłania poczty

14. 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)
15. Możliwość wykonywania operacji testowych
16. Możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
17. Monitorowanie serwerów WWW i adresów URL
18. Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
19. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail
20. Obsługa 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
21. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
22. Monitoring 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
23. Monitor m.in. serwisów Windows, który alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
24. Wyświetlanie 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
25. Monitorowanie stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
26. Zarządzanie stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
27. Podgląd wydajności systemów:
    - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

MODUŁ INWENTARYZACJA – minimalne wymagania:

1. Szczegółowe prezentacje dotyczące sprzętu m.in.: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Możliwość odczytu parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
3. Dane m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
4. Informuje o zainstalowanych aplikacjach oraz aktualizacjach systemu operacyjnego co bezpośrednio ma umożliwić audytowanie i weryfikację użytkowania licencji w organizacji.
5. Zbieranie informacji w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.

6. Posiadanie możliwości wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
7. Możliwość odczytania numeru seryjnego (klucze licencyjne).
8. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
9. Możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
10. Możliwość utworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików.

Moduł inwentaryzacji zasobów musi umożliwić 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 o 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").

MODUŁ OBSŁUGI UŻYTKOWNIKÓW – minimalne wymagania:

Badanie aktywności użytkowników 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.

Dodatkowo moduł musi posiadać funkcjonalność:

- 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.

Projekt „Cyberbezpieczna Gmina Pacanów" dofinansowany w ramach programu grantowego „Cyberbezpieczny Samorząd" z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

MODUŁ OCHRONY DANYCH PRZED WYCIEKIEM – minimalna funkcjonalność:

1. Blokowanie urządzeń i nośników danych. Program ma mieć 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.
2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
5. Funkcje wspierające bezpieczeństwo systemu
6. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
7. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
8. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
9. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
10. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:

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

Audyt operacji na plikach na urządzeniach przenośnych:

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

MODUŁ ZARZĄDZANIA CZASEM I ANALIZY UŻYTKOWNIKÓW – minimalne funkcjonalności:

1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.
3. Statystyki aktywności podwładnych widoczne dla przełożonego.
4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.

5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.
6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.
8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.
9. 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.
10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).
11. Wskaźnik czasu poświęconego na aktywność produktywną.
12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.
13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.
14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.

6. Serwer – 1 szt.;

Obudowa

1. Typu RACK, wysokość nie więcej niż 1U;
2. Szyny umożliwiające wysunięcie serwera z szafy stelażowej.
3. Możliwość zamontowania ramienia porządkującego ułożenie kabli z tyłu serwera;
4. Możliwość zainstalowania 8 dysków twardych hot plug 2,5";
5. Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
6. Zainstalowane 2 szt. dysków SSD SATA 240GB, HOT-PLUG;
7. Zainstalowane 6 szt. dysków SAS 12G 2,4TB, HOT-PLUG; 10000 RPM;
8. Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.

Płyta główna

1. Dwuprocesorowa;
2. Wyprodukowana i zaprojektowana przez producenta serwera;
3. Możliwość instalacji procesorów 60-rdzeniowych;
4. Zainstalowany moduł TPM 2.0;
5. 4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5;
    a) Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH;
6. 32 gniazda pamięci RAM;
7. Obsługa 8 TB pamięci operacyjnej RAM DDR5;
8. Wsparcie dla technologii:
    a) Memory Scrubbing;
    b) SDDC;
    c) ECC;
    d) Memory Mirroring;
    e) ADDDC;
9. Opcjonalna możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.
10. BIOS UEFI w specyfikacji 2.7.

Procesory

1. Jeden procesor 16-rdzeniowy, taktowanie bazowe 2,0 GHz, architektura x86_64;
2. osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 368 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera dwuprocesorowego z oferty producenta oferowanego serwera.

Pamięć RAM

1. 128 GB pamięci RAM;

2. DDR5 Registered 4800MT/s;

Kontrolery LAN

1. Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:
    a) 4x 1Gbit Base-T;
    b) Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;
2. Interfejsy LAN zainstalowane w slotach PCI-e:
    a) 2x 10Gbit Base-T.

Kontrolery I/O

Kontroler SAS RAID dla dysków wewnętrznych posiadający 2GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;

Porty

1. Zintegrowana karta graficzna ze złączem VGA z tyłu serwera (do złącza VGA wymaga się dołożenie przejściówki na złącze HDMI);
2. 2 porty USB 3.0 dostępne z tyłu serwera;
3. 2 porty USB 3.0 na panelu przednim;
4. Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
5. 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

1. Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy nie większej niż 550W;
2. Redundantne wentylatory hotplug.

Zarządzanie

1. Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;

a) informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:

- karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;
- procesory CPU;
- pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
- status karty zarządzającej serwera;
- wentylatory;
- bateria podtrzymująca ustawienia BIOS płyty głównej;
- zasilacze;
- system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);

2. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

a) Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;

b) Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;

c) Dostęp poprzez przeglądarkę Web, SSH;

d) Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;

e) Zarządzanie alarmami (zdarzenia poprzez SNMP);

f) Możliwość przejęcia konsoli tekstowej;

g) Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);

h) Obsługa serwerów proxy (autentykacja);

i) Obsługa VLAN;

j) Możliwość konfiguracji parametru Max. Transmission Unit (MTU);

k) Wsparcie dla protokołu SSDP;

l) Obsługa protokołów TLS 1.2, SSL v3;

m) Obsługa protokołu LDAP;

n) Synchronizacja czasu poprzez protokół NTP;

o) Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;

3. Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
4. Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
5. Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
6. Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane OS

1. Microsoft Windows Server 2022, 2019;
2. VMWare vSphere 8.0;
3. Suse Linux Enterprise Server 15;
4. Red Hat Enterprise Linux 9, 8;

5. Microsoft Hyper-V Server 2019

Gwarancja

1. 2 lat gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej **(długość gwarancji stanowi kryterium oceny ofert, deklarowaną długość gwarancji, należy podać w formularzu ofertowym)**;
2. Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
3. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
4. Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
5. Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.

Inne

1. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.
2. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE.
3. Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
4. W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;

5. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
6. Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;
7. Serwer musi być certyfikowany do pracy z systemem Ubuntu 22.04;
8. Zgodność z normami: CB, RoHS, WEEE, GS oraz CE.

7. System operacyjny do serwera – 1 szt.,

oraz

8. Licencje dostępowe do serwera – 45 szt.;

System operacyjny do serwera, oraz licencje dostępowe do serwera zostały opisane wspólnie z uwagi na zintegrowane parametry techniczne, obowiązkiem Wykonawcy jest podanie nazw i cen jednostkowych proponowanych rozwiązań, które spełnią poniższe wymagania zgodnie z podziałem zamieszczonym w załączniku nr 2 do SWZ wzór oferty.

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Wymaga się, aby oferowane licencje umożliwiały korzystanie 45 użytkownikom.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.

2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.

3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.

4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.

7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:

a) pozwalają na zmianę rozmiaru w czasie pracy systemu,

b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,

c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:

a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

18. Mechanizmy logowania w oparciu o:

a) Login i hasło,

b) Karty z certyfikatami (smartcard),

c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..

20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

b) 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:

i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

c) Zdalna dystrybucja oprogramowania na stacje robocze.

d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej

e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

i. Dystrybucję certyfikatów poprzez http

ii. Konsolidację CA dla wielu lasów domeny,

iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f) Szyfrowanie plików i folderów.

g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

i) Serwis udostępniania stron WWW.

j) Wsparcie dla protokołu IP w wersji 6 (IPv6),

k) Wsparcie dla algorytmów Suite B (RFC 4869),

l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

iii. Obsługi 4-KB sektorów dysków

iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

9. NAS Network Attached Storage – 2 szt.;

1. Procesor czterordzeniowy 64-bitowy o taktowaniu nie niższym niż 2.2GHz
2. Obudowa RACK 19" 1U – wraz z kompletem szyn przesuwnych umożliwiających zamontowanie w szafie RACK
3. Procesor - liczba rdzeni nie mniej niż 4
4. Pamięć RAM - Minimum 8 GB DDR4 ECC. Możliwość rozszerzenia pamięci RAM do 64GB
5. Całkowita liczba gniazd pamięci - Minimum 4
6. Liczba zatok na dyski twarde - Minimum 4
7. Obsługiwane dyski twarde:
   a) 3.5" SATA HDD / 2.5" SATA SSD – Hot Plug
   b) Zamawiający wymaga dostarczenia 4 dysków 3.5" SATA HDD o pojemności 8TB każdy o parametrach nie gorszych niż:
   - Prędkość obrotowa: 7200 RPM
   - MTTF: 2 000 000
   - Obciążenie roczne: 550 TB
   - Gwarancja – Zgodna z gwarancją zaproponowaną na urządzenie NAS.
   - Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera.
   - Dyski zgodne z listą kompatybilności producenta oferowanego serwera.
8. Wbudowane kieszenie dysków M.2 NVMe - Minimum 2
9. Możliwość podłączenia modułu rozszerzającego – Tak
10. Maksymalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż: 16
11. Porty na karty rozszerzeń - Minimum 1 x Gen3 x8 PCIe (x8 link)
12. Porty LAN - Wbudowane min. 4 x 1GbE RJ-45
13. Porty USB 3.2 - Minimum 2
14. Gniazdo rozszerzenia - Minimum 1
15. Zasilanie - Redundantny zasilacz o mocy minimalnej 150W
16. Mechanizm szyfrowania sprzętowego - Tak, min AES-NI
17. Wewnętrzny system plików BTRFS, EXT4
18. Obsługiwane tryby RAID - JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny
19. Uprawnienia - Uprawnienia listy kontroli dostępu systemu Windows (ACL)
20. Usługa katalogowa - Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station
21. Bezpieczeństwo - Zapora sieciowa, szyfrowanie folderu współdzielonego, 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), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.

22. Oprogramowanie do kopii zapasowej: Oferowany serwer powinien mieć oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. Minimalne wymagane funkcje oprogramowania do backupu:

- kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal,

- kopia zapasowa środowisk MacOS

- 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,

- automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej,
- 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

- zgodność współpracy oprogramowania do kopii zapasowej z oferowanym serwerem, potwierdzona przez producenta serwera.

23. 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 darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników.
- 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 1024 migawek na folder współdzielony i minimum 65000 migawek na cały system
- Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 60 jednoczesnych połączeń

24. Gwarancja producenta serwera min 24 miesiące – **(długość gwarancji stanowi kryterium oceny ofert, deklarowaną długość gwarancji, należy podać w formularzu ofertowym).**

10. UPS – 2 szt.;

1. Moc pozorna - 3000 VA
2. Moc rzeczywista - 3000 W
3. Topologia (klasyfikacja IEC 62040-3) - Line-interactive z AVR
4. Współczynnik mocy – 1
5. Czas przełączenia na baterię - <4 ms
6. Liczba, typ gniazd wyjściowych - 8 x IEC C13 (2 grupy gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza 2x2 IEC C13 10A), 1 x IEC C19 16A
7. Typ gniazda wejściowego - IEC C20 16A
8. Czas podtrzymania dla 2500W obciążenia - 4 min
9. Czas podtrzymania przy 1200W obciążenia -13 min
10. Czas podtrzymania przy 3000W obciążenia -17 min
    Dopuszcza się osiągnięcie czasu podtrzymania opisanego w punktach 8), 9), 10), za pomocą dodatkowych modułów bateryjnych.
11. Dodatkowe baterie - Możliwość dodania do 4 dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania do 84 minut dla 2500W obciążenia przy pf=1,0
12. Napięcie znamionowe - 200/208/220/230/240/250 V
13. Tolerancja napięci prostownika - 160 V – 294 V (regulacja programowa 150-294 V)

14. Częstotliwość znamionowa - 50/60 Hz autodetekcja
15. Tolerancja częstotliwości - 47– 70 Hz
16. Kształt napięcia – Sinusoidalny
17. Napięcie znamionowe wyjściowe - 200/208/220/230/240 V do wyboru przez użytkownika
18. Zakres zmian napięcia - +6/-10% napięcia nominalnego
19. Częstotliwość wyjściowa - 50/60 Hz
20. Współczynnik szczytu - 3:1
21. Baterie wymieniane przez użytkownika "na gorąco" – Tak
22. Ochrona przed przeładowaniem - Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
23. Ochrona przed głębokim rozładowaniem - Tak
24. Okresowy automatyczny test baterii – Tak
25. System zarządzania pracą baterii - System nieciągłego ładowania baterii. Na wezwanie Zamawiającego, razem z podmiotowymi środkami dowodowymi, należy dołączyć 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 uruchomienia bez napięcia w sieci "zimny start" – Tak
27. Baterie wewnętrzne o pojemności nie mniejszej niż - 9Ah 12V, minimum 6 szt.
28. Czas ładowania baterii do poziomu 90% - < 3 godz. do 90% pojemności użytkowej
29. Interfejs komunikacyjny:

a) USB
b) RS232 DB-9 żeński (HID)
c) styki przekaźnikowe
d) miniport wyłącznik ON/OFF
e) SNMP/Ethernet

30. Panel sterowania z wyświetlaczem LCD:

a) Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh).
b) Poziomy rząd przycisków sterowania
c) Poziomy rząd wskaźników stanu : zasialanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)
d) Sygnalizator akustyczny

31. Sygnały akustyczne, co najmniej na awarię, niski stan naładowania baterii, przeciążenie, oraz konieczność serwisu.
32. Przyciski sterujące i wskaźniki diodowe LED, co najmniej Przycisk Escape (anulowanie), Przyciski funkcyjne (przewijanie w górę i w dół), Przycisk Enter (potwierdzający), Przycisk

ON/OFF załączenia i wyłączenia, LED trybu zasilania z siec i(kolor zielony), LED trybu baterii (kolor żółty), LED usterki (kolor czerwony).

33. Typ obudowy uniwersalna Tower/Rack 2U
34. Dane techniczne karty SNMP:

a) **Network Support:** Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/

b) **Tymczasowe hasła**: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). **Blokowanie konta:** Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.

c) **Protokoły:** MQTT/RNDIS/LDAP/NVD/SSH/PKI

d) **Kamptybilność:** SNMP v1/v3 i IP v4/v6

e) **Interfejs:** HTML5

f) **Adresowanie IP:** DHCP/BootP/Manualne

g) **Szyfrowanie:** pakiet szyfrów TLS 1.2 z minimum SHA256

h) Dostępny port USB (microUSB - port serwisowy)

i) **Certyfikaty:** UL 2900-1, 2900-2-2, lub IEC62443-4-2

35. Dołączone oprogramowanie - Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie systemów operacyjnych.
36. Zgodność ze standardem Energy Star
37. Maksymalna szerokość - 438 mm
38. Maksymalna wysokość całkowita - 172 mm (4U)
39. Maksymalna głębokość - 603 mm
40. Maksymalny ciężar całkowity - 71 kg
41. Poziom hałasu w odl. 1m - do 40 dBA dla pracy normalnej
42. Znaki bezpieczeństwa - CE, Energy Star, IEC/EN 62040-1-1, IEC/EN 62040-2 class B, IEC/EN 62040-3
43. Możliwość montażu ręcznego bypassu serwisowego
44. Gwarancja producenta - 36 miesięcy dla elektroniki, 24 miesiące dla baterii (3 lata pełnej gwarancji po rejestracji produktu)

11. Switch zarządzalny sieciowy z obsługą VLAN, MACsec, standardu 802.1X – 2 szt.

1. Wymagania podstawowe

a) Przełącznik posiadający minimum 8 portów 1/10/Gb SFP+

b) Przełącznik posiadający 2 porty stakujące minimum 10Gb SFP+

c) Możliwość łączenia do 8 przełączników w stos

d) Wysokość urządzenia 1U
e) Pamięć operacyjna: minimum 2 GB pamięci DRAM
f) Pamięć flash minimum 1 GB
g) Bufor pakietów minimum 2MB
h) Pojemnośc tablicy MAC – minimum 32 000
i) Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
j) Obsługa 802.1v VLAN Klasyfikacja per Protokół oraz port
k) Obsługa Q-in-Q IEEE 802.1ad
l) Obsługa sieci wirtualnych protokołowych IEEE 802.1v
m) Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
n) Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
o) Obsługa Q-in-Q IEEE 802.1ad
p) Obsługa Quality of Service
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
q) Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
r) Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
s) Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
t) Moduł wentylatorów zapewniający ich redundancję
u) Wbudowany DHCP Serwer i klient
v) Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
w) 1 port Micro-USB do podpięcia zewnętrznego storage oraz do zarządzania przełącznikem
x) Port konsolowy USB oraz RJ45
y) Obsługa CDPv2 z obsługaVoice VLAN

2. <u>Obsługa Routingu IPv4</u>
a) Sprzętowa obsługa routingu IPv4 - forwarding
b) Pojemność tabeli routingu min. 8 tys. wpisów
c) Routing statyczny
d) Obsługa routingu dynamicznego IPv4
    a. RIP v1/v2
    b. OSPFv2
    c. BGP4, BGP+ - możliwość uruchomienia poprzez dodatkową licencję
    d. IS-IS możliwość uruchomienia poprzez dodatkową licencję

3. <u>Obsługa Routingu IPv6</u>
a) Sprzętowa obsługa routingu IPv6 - forwarding
b) Pojemność tabeli routingu min. 4 tys. wpisów
c) Routing statyczny
d) Obsługa routingu dynamicznego dla IPv6

- RIPng
- OSPF v3
- BGPv6 - możliwość uruchomienia poprzez dodatkową licencję
- IS-IS - możliwość uruchomienia poprzez dodatkową licencję

e) Ping dla IPv6
f) Obsługa MLDv1 (Multicast Listener Discovery version 1)
g) Obsługa MLDv2 (Multicast Listener Discovery version 2)
h) Minimum 16 instancji VRF
i) Policy based routing (PBR) for IPv4
j) Policy based routing (PBR) for IPv6

4. Obsługa Multicastów

a) Statyczne przyłączanie do grupy multicast
b) Obsługa PIM-SM
c) Obsługa PIM-SSM
d) Obsługa IGMP v1
e) Obsługa IGMP v2
f) Obsługa IGMP v3
g) Obsługa IGMP oraz MLD snooping
h) Obsługa IETF RFC1112 Host Extensions for IP Multicasting

5. Bezpieczeństwo

a) Obsługa Network Login
   - IEEE 802.1x - RFC 3580
   - Web-based Network Login
   - MAC based Network Login
b) Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
c) Możliwość integracji funkcjonalności Network Login z Microsoft NAP
d) Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
e) Obsługa Guest VLAN dla IEEE 802.1x
f) Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
g) Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication
h) Obsługa Identity Management
i) Wbudowana obrona procesora urządzenia przed atakami DoS
j) Obsługa TACACS+ (RFC 1492)
k) Obsługa RADIUS Authentication (RFC 2138)
l) Obsługa RADIUS Accounting (RFC 2139)
m) RADIUS and TACACS+ per-command Authentication
n) Bezpieczeństwo MAC adresów
   - ograniczenie liczby MAC adresów na porcie
   - zatrzaśnięcie MAC adresu na porcie
   - możliwość wpisania statycznych MAC adresów na port/vlan

o) Możliwość wyłączenia MAC learning
p) Obsługa SNMPv1/v2/v3
q) Klient SSH2
r) Zabezpieczenie przełącznika przed atakami DoS
   - Networks Ingress Filtering RFC 2267
   - SYN Attack Protection
   - Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
s) Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
   - Adres MAC źródłowy i docelowy plus maska
   - Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
   - Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
   - Numery portów źródłowych i docelowych TCP, UDP
   - Zakresy portów źródłowych i docelowych TCP, UDP
   - Identyfikator sieci VLAN - VLAN ID
   - Flagi TCP
   - Obsługa fragmentów
t) Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
u) Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania
v) Obsługa bezpiecznego transferu plików SCP/SFTP
w) Obsługa DHCP Option 82
x) Obsługa IP Security - Gratuitous ARP Protection
y) Obsługa IP Security - Trusted DHCP Server
z) Obsługa IP Security - DHCP Snooping
aa) Obsługa IP Security - DHCP Secured ARP/ARP Validation
bb) Obsługa IETF RFC 2474

6. Bezpieczeństwo sieciowe

a) Możliwość konfiguracji portu głównego i zapasowego
b) Obsługa redundancji routingu VRRP (RFC 2338)
c) Obsługa redundancji routingu VRRP na dwóch urządzeniach agregacyjnych pracujących w ramach MLAG w trybie Active-Active (obydwa urządzenia przeprowadzają routing)
d) Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
e) Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
f) Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
g) Obsługa PVST+
h) Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
i) Obsługa G.8032 v1/v2

j) Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie.
k) Obsługa MLAG - połączenie link aggregation do dwóch niezależnych przełączników.
l) Obsługa LACP w ramach MLAG
m) Obsługa protokołu MACsec – możliwość uruchomienia poprzez dodatkową licencję

7. Zarządzanie
a) Obsługa IETF RFC5905 NTPv4: Protocol and Algorithms Specification
b) Zarządzanie przez SNMP v1/v2/v3
c) Zarządzanie przez przeglądarkę WWW – protokół http i https
d) Możliwość zarządzania poprzez protokół XML
e) Możliwość zarządzania przełącznikiem z aplikacji Cloud
f) Możliwość zarzadzania przełącznikiem z dedykowanej aplikacji zarządzającej
g) Możliwość zarzadzania przełącznikiem z poziomu CLI
h) Wsparcie dla Zero-touch provisioning
i) Telnet Serwer/Klient
j) SSH2 Serwer/Klient
k) Ping dla IPv4 / IPv6
l) Traceroute dla IPv4 / IPv6
m) Obsługa SYSLOG
n) Sprzętowa obsługa sFlow
o) Sprzętowa obsługa IPFIX
p) Obsługa RMON min. 4 grupy: Status, History, Alarms, Events

8. Inne
a) Obsługa VXLAN: IETF RFC7358
b) Obsługa standardów Shortest Path Bridging (SPB) IEEE 802.1aq oraz IETF RFC 6329
c) Obsługa VXLAN Gateway
d) Obsługa Distributed Virtual Routing (DvR)
e) Obsługa 802.1Qbp Equal-Cost Multi-Path (Shortest Path Bridging)
f) Obsługa 802.1Qcj Automatic Attachment to Provider Backbone Bridging (PBB) Services
g) Obsługa 802.1ag Connectivity Fault Management
h) Obsługa 802.1ah Provider Backbone Bridges
i) Obsługa 802.1aq Shortest Path Bridging (SPB) MAC-in-MAC
j) Obsługa IETF RFC 6329 IS-IS Extensions supporting IEEE 80 2.1aq SPB
k) Wsparcie dla AVB – Audio Video Bridging
l) Zakres temperatury pracy od 0 do 50 stopni C

9. Wymaganie szczegółowe
a) Przełącznik 48 portów 1 Gbits
b) Przełącznik posiadający minimum 48 portów 10/100/1000BASE-T
c) Nieblokująca architektura o wydajności przełączania minimum 256 Gb/s

d) Szybkość przełączania minimum 190 milionów pakietów na sekundę

10. Gwarancja
    a) Gwarancja producenta minimum 24 miesiace.