

RZK.271.2.2.2025

Szczegółowy Opis Przedmiotu Zamówienia

„Cyberbezpieczny Samorząd - Gmina Piecki”

W ramach projektu „Cyberbezpieczny Samorząd”

Priorytet II: Zaawansowane usługi cyfrowe

Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa

Fundusze Europejskie na Rozwój Cyfrowy 2021-2027

Spis treści

Wstęp	3
Wymagania ogólne	3
Wymagania dot. wdrożenia	3
Zakup i wdrożenie sprzętu.....	6
Serwer wirtualizacyjny- 1 szt.....	6
Cyfrowy bunkier – 1 zestaw	10
Serwer LOGów – 1 szt.....	17
Przełącznik dostępowy – 1 szt.....	21
Macierz – rozbudowa	25
Macierz – przedłużenie wsparcia / gwarancji	25
UTM zakup wsparcia – Urząd Gminy	25
DLP	25
UTM zakup i wdrożenie – Gminy Ośrodek Pomocy Społecznej w Pieckach.....	38
UPS do serwerowni 3kVA – 1 szt.....	45
UPS centralny – 20kVA/20kW – 1 szt.....	48
Oprogramowanie systemowe	50
Centralny system logów	50
Oprogramowanie do wirtualizacji.....	56
Oprogramowanie antywirusowe – rozbudowa posiadanej licencji	57
Oprogramowanie do zarządzania infrastrukturą – rozbudowa	58
Instalacja dostarczonych urządzeń.....	59
Usługa segmentacji sieci.....	59
Serwery.....	59
Macierz dyskowa	60
Przełączniki sieciowe.....	60
Zabezpieczenie usług.....	60
Firewall – UTM	60
Kopie zapasowe	61
UPSy	61
Instruktaże.....	62
Gwarancja.....	62
Przygotowanie i dostarczenie dokumentacji powykonawczej.....	62
Szkolenia pracowników	64
Pakiet szkoleń dla pracowników Zamawiającego	64
Szkolenia specjalistyczne dla działu IT	66
Szkolenie specjalistyczne – Audytor Wiodący ISO 27001.....	72
Opracowanie / aktualizacja dokumentacji SZBI	73

Wstęp

Niniejszy dokument stanowi Szczegółowy Opis Przedmiotu Zamówienia (dalej SzOPZ lub OPZ) w zakresie dostawy oraz wdrożenia sprzętu i oprogramowania, służącego zabezpieczeniu działania infrastruktury Zamawiającego. Wszystkie parametry techniczne określone w niniejszym OPZ określają graniczne (minimalne lub maksymalne - zgodnie z opisem) wymagania stawiane oferowanym urządzeniom i oprogramowaniu, co oznacza, że jeśli Wykonawca zaoferuje przedmioty posiadające więcej funkcji niż wymagane minimum lub w lepszym stopniu, nie zostaną mu przyznane żadne dodatkowe punkty, poza punktami w kryterium oceny oferty „parametry techniczne oferowanego sprzętu” (wskazane w rozdziale 17 SWZ). Wykonawca może zaoferować rozwiązania równoważne spełniające minimum opisane w OPZ.

Wymagania ogólne

Zamawiający wymaga, by dostarczony sprzęt i oprogramowanie były w wersji aktualnej na dzień jego instalacji.

System musi mieć możliwość pracy użytkowej przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.

Dla dostarczonego sprzętu i oprogramowania należy dostarczyć: licencje, nośniki instalacyjne, instrukcje użytkownika i administratora (w formie elektronicznej).

Dla dostarczonego oprogramowania należy dostarczyć: bezterminowe licencje użytkowe oraz subskrypcyjne okresowe [np. na aktualizację systemu zabezpieczeń] na min. okres zaoferowanej gwarancji na urządzenie na którym licencje są instalowane; nośniki instalacyjne, instrukcje.

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2023, poz. 1582 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Minimalny okres gwarancji - 24 msc. - dotyczy wszystkich elementów systemu – o ile w specyfikacji lub niniejszym opisie nie wskazano inaczej.

Wymagania dot. wdrożenia

1. Wykonawca dokona instalacji, konfiguracji, parametryzacji i integracji dostarczanego sprzętu i oprogramowania.
2. Prace muszą być prowadzone w sposób niekolidujący z działalnością Zamawiającego. Każda przerwa w funkcjonowaniu obecnego oprogramowania musi zostać uzgodniona z Zamawiającym na co najmniej 2 dni przed planowaną przerwą.

3. Zamawiający wymaga, aby moduły oprogramowania, wdrożone przez Wykonawcę w ramach realizacji przedmiotu zamówienia były wdrożone do pełnej wymaganej funkcjonalności opisanej w SWZ i załącznikach oraz dokumentacji realizacji projektu.
4. Instalacja i wdrożenie winny odbywać się w godzinach pracy pracowników Zamawiającego - w dni robocze w godzinach 7.00-15.00. Zamawiający dopuszcza wykonanie pracy w innym czasie niż wskazany, po uzgodnieniu i akceptacji Zamawiającego.
5. Wdrożenie powinno odbywać się bezpośrednio na miejscu u Zamawiającego. Wdrożenie nie powinno odbywać się w formie pracy zdalnej, chyba że zachodzą ku temu nieprzewidziane przesłanki. W takim przypadku wymagana jest zgoda i ustalenia z Zamawiającym.
6. **Wykonawca dokona integracji oraz migracji danych z obecnie posiadanych przez Zamawiającego systemów informatycznych, tj.:**
 - a. **Migracja serwerów wirtualnych opartych na Windows Server 2016 do najnowszej wersji Windows Server (kontroler domeny, serwer plików, serwer systemu dziedzicznego, itp.) – sposób migracji wybiera Wykonawca, w efekcie jednak Zamawiający oczekuje że domena zostanie zaktualizowana do najnowszej wersji i będzie działać w trybie HA.**
 - b. **Migracja serwerów wirtualnych ze starego klastra wirtualizacyjnego pracującego na Hyper-V na nowy – Wykonawca musi zmigrować (przekonwertować) wszystkie maszyny obecnie pracujące na serwerach wirtualizacyjnych do nowego klastra i skonfigurować klaster do pracy w trybie HA.**
 - c. **Docelowo w ramach nowego klastra powinno zostać uruchomionych min. 6 maszyn wirtualnych opartych o system Windows Server 2022 lub nowszy (należy utworzyć i aktywować dodatkowe czyste maszyny VM Windows Server 2022 lub nowsze) oraz co najmniej 2 maszyny oparte na systemie typu LINUX.**
7. Zamawiający wymaga dostarczenia oprogramowania kompletnego tj. zawierającego wszystkie niezbędne składniki wymagane do zainstalowania, wdrożenia i eksploatacji dostarczanego oprogramowania tj. systemy operacyjne, bazy danych, oprogramowania narzędziowe i inne niezbędne oprogramowanie firm trzecich. Dostarczane oprogramowanie firm trzecich musi być zgodne z postanowieniami licencyjnymi producenta na instalację u Zamawiającego i infrastrukturze posiadanej przez Zamawiającego.
8. Wykonawca przed przystąpieniem do wdrożenia winien przeprowadzić analizę przedwdrożeniową oraz określić ramowy harmonogram wdrożenia poszczególnych modułów oferowanego oprogramowania uwzględniając uzgodnienia z Zamawiającym.
9. Po uruchomieniu produkcyjnym całości oprogramowania Wykonawca zapewni dostępność swoich pracowników w wymiarze min. 20 roboczogodzin w celu wsparcia użytkowników przy obsłudze oprogramowania, bieżącego usuwania problemów z działaniem oraz jego dostrajania.

10. Wykonawca przygotowuje dokumentację powdrożeniową wdrażanego oprogramowania wymaganą w SWZ i załącznikach tj. instrukcje, procedury.
11. Wykonawca po zakończeniu wdrożenia przekaze Zamawiającemu wszystkie konta i hasła administracyjne do każdego elementu dostarczanego oprogramowania oraz bazy danych.
12. Wykonawca w ramach wdrożenia skonfiguruje backup oprogramowania i bazy danych oraz przetestuje poprawność jego wykonywania.
13. Po dokonaniu instalacji i wdrożenia docelowo system powinien:
 - a) spełniać wymagania określone w SWZ i Załącznikach do SWZ,
 - b) uwzględniać charakter prowadzonej przez Zamawiającego działalności oraz spełniać wymagania obowiązujących przepisów prawa, w szczególności ustaw i rozporządzeń.

Zakup i wdrożenie sprzętu

Poniżej przedstawiono parametry graniczne jakie dostarczany sprzęt musi spełniać. W przypadku gdy do realizacji funkcjonalności opisanych w niniejszym Opisie Przedmiotu Zamówienia wymagany jest sprzęt/oprogramowanie/licencje nieujęte w poniższym zestawieniu, a wynikają ze specyfiki zaoferowanego przez Wykonawcę rozwiązania - Wykonawca musi go dostarczyć w ramach złożonej oferty i wykazać w wykazie asortymentowo-cenowym.

Serwer wirtualizacyjny– 1 szt.

Element konfiguracji	Wymagania minimalne
Obudowa	<p>Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do mocowania kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia).</p> <p>Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.</p> <p>Serwer z możliwością wyposażenia w zdejmowany panel przedni z zamkiem chroniący przed nieuprawnionym dostępem do dysków.</p> <p>Możliwość wyposażenia serwera w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający:</p> <ul style="list-style-type: none">a. wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOSb. wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczyc. przywracanie konta administratorad. wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwerae. wyświetlanie w czasie rzeczywistym temperatury procesorówf. konfigurowanie ustawień sieciowych modułu zarządzania.
Procesor	<p>Dwa procesory piątej generacji dwunastordzeniowe, x86 - 64 bity, pracujące z częstotliwością bazową min. 2.4GHz, osiągający w testach SPECrate2017_fp_base wynik nie gorszy niż 330 punktów, dla testu oferowanego modelu serwera z 2 procesorami.</p> <p>Wynik testu musi być opublikowany na stronie www.spec.org oraz dołączony do oferty.</p> <p>Płyta główna wspierająca zastosowanie procesorów od 8 do 64 rdzeni, mocy do min. 385W i taktowaniu CPU do min. 3.7GHz.</p>
Pamięć operacyjna	<p>Min. 256GB RDIMM DDR5 5600 MT/s w modułach pamięci o pojemności min. 32 GB każdy.</p> <p>Płyta główna z minimum 32 slotami na pamięć i umożliwiającą instalację do minimum 8TB.</p> <p>Zabezpieczenie pamięci:</p> <ul style="list-style-type: none">a. Memory mirroringb. ECCc. patrol scrubbing

- d. SDDC
- e. memory thermal throttling
- f. ADDDC-SR
- g. PPR
- h. Memory SMBus hang recovery.

Sloty rozszerzeń	Min. 2 aktywne gniazda PCI-Express generacji 5, x16 (szybkość slotu – bus width). Możliwość dołożenia trzeciego gniazda PCI-Express generacji 5, x16 (szybkość slotu – bus width). Dwa sloty OCP 3.0 możliwe do obsadzenia poprzez karty sieciowe w dowolnej konfiguracji.
Dysk twardy	Serwer pozwalający na instalację 8 dysków SAS/SATA/NVMe, 2,5” z możliwością rozbudowy o 2 dodatkowe wnęki dyskowe na dyski SAS/SATA 2.5” Zainstalowane min. 4szt. dyski SSD 480GB każdy.
Kontroler	Kontroler sprzętowy wyposażony w min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę napędów dyskowych SATA/SAS/NVMe.
Interfejsy sieciowe	Jedna czteroportowa karta 1Gb nie zajmująca gniazd PCIe. Jedna dwuportowa karta 10Gb SFP+ z kompletem wkładek SR MM nie zajmująca gniazd PCIe. Dodatkowa dwuportowa karta FC 16Gb z kompletem wkładek kompatybilnych z posiadaną macierzą.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Porty	Min. 4 x USB, z czego min. 3 szt. w wersji USB 3.0 Dodatkowo USB TYP-C na przednim panelu, które musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS; 1 x VGA z tyłu obudowy Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1600W, klasy Titanium. W komplecie z zasilaczami należy dostarczyć kable zasilające o długości min. 2m.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Bezpieczeństwo	Serwer wyposażony w moduł TPM 2.0.

Karta/moduł zarządzający	<p>Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiającą:</p> <ul style="list-style-type: none"> a. monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), b. monitorowanie w czasie rzeczywistym poboru prądu przez serwer, c. zbieranie logów błędów hardware, d. przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, e. montowanie wirtualnych napędów, f. zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, g. wysyłanie zawiadomień drogą mailową i poprzez SNMP h. wsparcia dla IPMI, SSH, Redfish i. wsparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows, j. nadawanie ról użytkownikom, k. możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, LCD, l. możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem.
Oprogramowanie zarządzające i diagnostyczne	<p>Wraz ze serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:</p> <ul style="list-style-type: none"> a. włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów. b. tworzenie szablonów instalacyjnych dla systemów operacyjnych. c. tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów. d. zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera. e. aktualizacja sterowników i BIOS serwerów. f. zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.
System operacyjny	<p>Zamawiający wymaga dostarczenia wirtualizacyjnego systemu operacyjnego kompatybilnego z posiadanym obecnie oprogramowaniem wirtualizacyjnym (VMware 8.0) umożliwiające</p>

włączenie serwera do obecnego klastra wirtualizacyjnego oraz przedłużenie wsparcia dla całego klastra o 36 miesięcy.

Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2022+ Ubuntu 20.04 LTS, 22.04 LTS Red Hat Enterprise Linux (RHEL) 8.6, 9.0 VMware ESXi 7.0 U3, 8.0, 8.0 U1/U2
Wsparcie techniczne	<p>Urządzenie objęte minimum 36 miesięcznym okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej Next Business Day od momentu zgłoszenia usterki.</p> <p>Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera lub przez autoryzowanego partnera serwisowego producenta.</p> <p>Uszkodzone dyski zostają u zamawiającego (disk retention).</p> <p>Usługi gwarancyjne świadczone przez producenta lub autoryzowanego partnera serwisowego producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny.</p> <p>Wymagane oświadczenie producenta potwierdzające, że elementy, z których zbudowany jest serwer, są produktami producenta tych serwerów lub są przez niego certyfikowane oraz całe są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.</p> <p>Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:</p> <ul style="list-style-type: none"> i. możliwość pobierania najnowszego firmware, ii. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń, iii. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta, iv. otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.
Inne	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.</p>

<p>Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001, ISO 14001, ISO 27001 oraz ISO 50001.</p> <p>Deklaracja zgodności CE.</p>

Cyfrowy bunkier – 1 zestaw

1. Sprzęt musi być fabrycznie nowy, wyprodukowany nie wcześniej niż 9 miesięcy przed dostawą.
2. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.
3. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:
 - a. Obudowa: 1U lub maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do mocowania kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia).
 - b. Procesor: 6-rdzeniowy/12-wątkowy procesor x86 o taktowaniu min. 2GHz, procesor musi posiadać co najmniej 12MB cache
 - c. Pamięć operacyjna: Min. 16 GB DIMM DDR4 lub DDR5
 - d. Dysk twardy: Zainstalowane min. 2 dyski SSD M.2 NVMe o pojemności min. 200GB każdy w konfiguracji RAID 1.
 - e. Zainstalowane dyski o pojemności łącznej min. 24 TB w konfiguracji RAID 5, przestrzeń musi być osiągnięta przez minimum 4 dyski fizyczne.
 - f. Interfejsy sieciowe: Jedna min. dwuportowa karta 1Gb niezajmująca gniazd PCIe. dodatkowa dwuportowa karta 10Gb SFP+ z kompletem wkładek SR MM. Port Ethernet do zarządzania.
 - g. Redundantne zasilanie, min. 600W każdy zasilacz.
 - h. Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego.
4. Produkt dostępny w polskiej wersji językowej.
5. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
6. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków
7. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów
8. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych
9. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
10. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
11. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe
12. System zarządzania nie może być oparty o relacyjne bazy danych.

13. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
14. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
15. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
16. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
17. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
18. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
19. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
20. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
21. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
22. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
23. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
24. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
25. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
26. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
27. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
28. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało

zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.

29. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
30. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
31. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
32. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
33. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
34. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
35. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
36. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
37. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
38. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
39. System musi pozwalać na automatyczne aktualizacje oprogramowania.
40. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
41. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
42. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
43. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.

44. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
45. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
46. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
47. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
48. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
49. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
50. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
51. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
52. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental,
53. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
54. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Google Cloud Storage, magazyny zgodne z S3
55. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb,S3, nfs, iscsi
56. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
57. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniem zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
58. Możliwość generowania raportów dobowych w oparciu o harmonogram
59. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego (datacenter powinno być zlokalizowane na terenie Polski)

60. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)
61. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
62. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienie e-mail. (poziom definiowany indywidualnie dla każdego magazynu).
63. Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:
 - Debian: 9+,
 - Ubuntu: 16.04+,
 - Fedora: 29+,
 - RHEL: 6+,
 - openSUSE: 15+,
 - SUSE Enterprise Linux(SLES): 12 SP2+,
 - macOS: 10.13+,
 - Windows: 10 / 11,
 - Windows Server: 2016 +,Środowisk wirtualnych:
 - Hyper-V 2016+,
 - VMware: 6.7+.
64. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.
65. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
66. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
67. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
68. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
69. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego skalania danych.
70. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
71. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu

- źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
72. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
 73. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
 74. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
 75. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
 76. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
 77. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).
 78. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.
 79. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
 80. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
 81. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
 82. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
 83. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

84. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
85. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.
86. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.
87. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)
88. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
89. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi
90. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.
91. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.
92. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.
93. System musi umożliwiać zabezpieczenie środowisk Jira
94. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.
95. Wszystkie linie supportu muszą być obsługiwane w języku polskim.
96. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.
97. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.
98. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)
99. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
100. W ramach wsparcia technicznego Zamawiający musi mieć dostęp do tzw. Dedicated Customer Success Managera, tj. osoby po stronie Dostawcy dedykowanej do obsługi zgłoszeń technicznych, doraźnej pomocy i bieżącej pomocy w utrzymaniu infrastruktury Zamawiającego.
101. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do Dedicated Customer Success Managera.

102. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.
103. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu.
104. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
105. System powinien umożliwiać wykorzystanie wbudowanego menadżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
106. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
107. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.
108. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu.

Serwer LOGów – 1 szt.

Element konfiguracji	Wymagania minimalne
Obudowa	<p>Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do mocowania kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia).</p> <p>Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.</p> <p>Serwer z możliwością wyposażenia w zdejmowany panel przedni z zamkiem chroniący przed nieuprawnionym dostępem do dysków.</p> <p>Możliwość wyposażenia serwera w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający:</p> <ol style="list-style-type: none"> a. wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS b. wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy c. przywracanie konta administratora d. wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera

- e. wyświetlanie w czasie rzeczywistym temperatury procesorów
- f. konfigurowanie ustawień sieciowych modułu zarządzania.

Procesor	<p>Procesor min. piątej generacji dwunastordzeniowy, x86 - 64 bity, pracujące z częstotliwością bazową min. 2.4GHz, osiągający w testach SPECrate2017_fp_base wynik nie gorszy niż 370 punktów, dla testu oferowanego modelu serwera z 2 procesorami.</p> <p>Wynik testu musi być opublikowany na stronie www.spec.org oraz dołączony do oferty.</p> <p>Płyta główna wspierająca zastosowanie procesorów od 8 do 64 rdzeni, mocy do min. 385W i taktowaniu CPU do min. 3.7GHz.</p>
Pamięć operacyjna	<p>Min. 32GB RDIMM DDR5 5600 MT/s.</p> <p>Płyta główna z minimum 32 slotami na pamięć i umożliwiającą instalację do minimum 4TB.</p> <p>Zabezpieczenie pamięci:</p> <ul style="list-style-type: none"> a. Memory mirroring b. ECC c. patrol scrubbing d. SDDC e. memory thermal throttling f. ADDDC-SR g. PPR h. Memory SMBus hang recovery.
Sloty rozszerzeń	<p>Min. 3 aktywne gniazda PCI-Express generacji 5, z czego min. 1 slot x16 (szybkość slotu – bus width). Możliwość dołożenia trzech slotów PCI-Express generacji 5, x16 (szybkość slotu – bus width).</p>
Dysk	<p>Serwer pozwalający na instalację 12 dysków SAS/SATA 3,5" z możliwością rozbudowy o 4 dodatkowe wnęki dyskowe na dyski SAS/SATA 2.5"</p> <p>Zainstalowane 2 dyski serwerowe SSD M.2 Read-Intensive Hot-Plug o pojemności min. 480 GB każdy. Dyski muszą być skonfigurowane w RAID1 przez dedykowany kontroler sprzętowy i nie mogą zajmować kieszeni na dyski 3.5".</p> <p>Zainstalowane min. 6 szt. dysków NLSAS 7.2k RPM 8TB każdy.</p>
Kontroler	<p>Kontroler sprzętowy wyposażony w min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę napędów dyskowych SATA/SAS.</p>
Interfejsy sieciowe	<p>Jedna dwuportowa karta 10Gb SFP+ z kompletem wkładek SR MM nie zajmująca gniazd PCIe.</p> <p>Jedna czteroportowa karta 1Gb BaseT.</p>

Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Porty	<p>Min. 4 x USB, z czego min. 3 szt. w wersji USB 3.0</p> <p>Dodatkowo USB TYP-C na przednim panelu, które musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS;</p> <p>1 x VGA z tyłu obudowy</p> <p>Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.</p>
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1600W, klasy Titanium. W komplecie z zasilaczami należy dostarczyć kable zasilające o długości min. 2m.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Bezpieczeństwo	Serwer wyposażony w moduł TPM 2.0.
Karta/moduł zarządzający	<p>Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca:</p> <ul style="list-style-type: none"> a. monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), b. monitorowanie w czasie rzeczywistym poboru prądu przez serwer, c. zbieranie logów błędów hardware, d. przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, e. montowanie wirtualnych napędów, f. zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, g. wysyłanie zawiadomień drogą mailową i poprzez SNMP h. wsparcia dla IPMI, SSH, Redfish i. wsparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows, j. nadawanie ról użytkownikom, k. możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, LCD, l. możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem.
Oprogramowanie zarządzające i diagnostyczne	Wraz ze serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem),

	<p>posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:</p> <ul style="list-style-type: none"> a. włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów. b. tworzenie szablonów instalacyjnych dla systemów operacyjnych. c. tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów. d. zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera. e. aktualizacja sterowników i BIOS serwerów. f. zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.
System operacyjny	<p>Zamawiający wymaga dostarczenia systemu operacyjnego wraz z wymaganymi licencjami kompatybilnego z oferowanym centralnym systemem logów oraz z systemem zarządzania siecią (np. jeśli system zarządzania siecią potrzebuje systemu Windows Server to należy taka licencję dostarczyć).</p>
Wsparcie techniczne	<p>Urządzenie objęte minimum 36 miesięcznym okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej Next Business Day od momentu zgłoszenia usterki.</p> <p>Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera lub przez autoryzowanego partnera serwisowego producenta.</p> <p>Uszkodzone dyski zostają u zamawiającego (disk retention).</p> <p>Usługi gwarancyjne świadczone przez producenta lub autoryzowanego partnera serwisowego producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny.</p> <p>Wymagane oświadczenie producenta potwierdzające, że elementy, z których zbudowany jest serwer, są produktami producenta tych serwerów lub są przez niego certyfikowane oraz całe są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:</p> <ul style="list-style-type: none"> i. możliwość pobierania najnowszego firmware, ii. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń, iii. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,

	iv. otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.
Inne	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.</p> <p>Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001, ISO 14001, ISO 27001 oraz ISO 50001.</p> <p>Deklaracja zgodności CE.</p>

Przełącznik dostępowy – 1 szt.

Wymagania:

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagane parametry fizyczne:
 - a. możliwość montażu w stelażu/szafie 19"
 - b. wysokość maksymalna 1U
 - c. głębokość bez zainstalowanego zasilacza nie większa niż 35 cm
 - d. minimum jeden zasilacz 230V AC
 - e. zakres temperatur pracy ciągłej co najmniej od 0°C do +45 °C
 - f. zakres wilgotności pracy co najmniej 5% - 90%
 - g. waga bez zainstalowanego zasilacza nie większa niż 4,7 kg
3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:
 - a. 48 portów 100/1000BASE-T – WSZYSTKIE PORTY MUSZĄ BYĆ REDUNDANTNE!
 - b. 6 portów 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T (RJ45), kabli DAC
4. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
5. Przełącznik musi posiadać następujące porty służące do zarządzania:
 - a. Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45
6. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
 - a. Zarządzanie stosem poprzez jeden adres IP

- b. Do min. 9 jednostek w stosie
 - c. Porty do stackowania mogą być współdzielone z portami typu uplink.
 - d. Magistrala stackująca o wydajności minimum 80Gb/s
 - e. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
 - f. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
 - g. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
- 7. Układ przełączający o wydajności min. 180 Gbps, wydajność przełączania przynajmniej 160 Mpps
 - 8. Obsługa min. 32 500 adresów MAC
 - 9. Wbudowana pamięć RAM min. 1GB.
 - 10. Procesor wielordzeniowy. Minimalne taktowanie procesora 1000MHz
 - 11. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB
 - 12. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
 - 13. Możliwość skonfigurowania min. 32 interfejsów vlan interface SVI działających równocześnie
 - 14. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad
 - 15. Obsługa minimum 120 grup LAG
 - 16. Obsługa ramek jumbo o wielkości min. 9216 bajtów
 - 17. Obsługa sFlow
 - 18. Wsparcie dla G.8032 ERPS
 - 19. Obsługa protokołu VRRP
 - 20. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
 - 21. Wsparcie dla mechanizmu PVST+.
 - 22. Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng, IS-IS, BGP. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
 - 23. Obsługa min. 6 100 tras dla routingu IPv4
 - 24. Obsługa min. 2 000 tras dla routingu IPv6
 - 25. Obsługa min. 2 000 IPv6 neighbor discovery (ND)
 - 26. Obsługa protokołów związanych z obsługą ruchu typu multicast:
 - a. IGMP v1, v2 i v3
 - b. IGMP Snooping v2 i v3
 - c. PIM-SM, PIM-SSM i PIM-DM
 - d. MSDP i MLD Snooping
 - e. minimum 2000 tras multicast dla IPv4 i minimum 1000 tras multicast dla IPv6
 - 27. Minimalny rozmiar tablicy ARP 4000 wpisów
 - 28. Obsługa protokołów LLDP i LLDP-MED.

29. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client

30. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

- a. min. 3 poziomy dostęp administracyjny poprzez konsolę
- b. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL
- c. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
- d. obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1500 reguł ACL
- e. zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2
- f. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP
- g. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard
- h. możliwość synchronizacji czasu zgodnie z NTP lub SNTP

31. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:

- a. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
- b. wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ

32. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).

33. Wymagane opcje zarządzania:

- a. możliwość lokalnej obserwacji ruchu na określonym porcie
- b. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)
- c. wsparcie dla skryptów python uruchamianych na urządzeniu
- d. wsparcie dla RMON

34. Wraz z urządzeniami muszą zostać dostarczone:

- a. pełna dokumentacja w języku polskim lub angielskim
- b. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana

35. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 9 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy

36. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie

producenta oferowanych switchy, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

37. Zamawiający wymaga, aby urządzenia posiadały 60 miesięczny serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
38. Usługa serwisu musi być świadczona w języku polskim.
39. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
40. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
41. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.
42. System centralnego zarządzania może być dostarczony w formie:
 - a. Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej
 - b. Lub dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.
43. Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.
44. W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.
45. System centralnego zarządzania musi umożliwiać:
 - a. tworzenie VLANów
 - b. ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu
 - c. tworzenie połączeń zagregowanych
 - d. monitorowanie statusu pracy przełącznika i portów
 - e. możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania
 - f. możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego
 - g. interfejs do zarządzania w języku polskim lub angielskim

Do przełącznika będzie podłączony „cyfrowy bunkier” , który wymaga łączya wysokiej przepustowości, dlatego należy połączyć szafę dystrybucyjną z serwerownią kablem światłowodowym – wymagana wizja lokalna w celu ustalenia trasy i wyceny kosztu instalacji kabla.

Macierz – rozbudowa

Posiadaną przez Zamawiającego macierz PowerVault ME5012 należy rozbudować o co najmniej 4 szt. dysków SSD Read Intensive SAS 24Gb/s, Hot-Plug, wymienionych na liście kompatybilności producenta macierzy o pojemności min. 1,9TB każdy. Zamawiający posiada obecnie 4 wolne sloty na dyski.

Macierz – przedłużenie wsparcia / gwarancji

Zamawiający posiada macierz Dell Storage SCv3020, dla której należy przedłużyć wsparcie / gwarancję minimum na okres udzielenia gwarancji na resztę dostarczanego sprzętu. Gwarancja musi zapewniać realizację zgłoszeń serwisowych na poziomie NBD.

UTM zakup wsparcia – Urząd Gminy

Zamawiający posiada UTM FortiGate 61F, w ramach postępowania wymagane jest dostarczenie wsparcia i rozszerzenia gwarancji / wsparcia dla urządzenia.

W skład pakietu usług wsparcia wchodzi:

- czas reakcji serwisu (w języku polskim) na zgłoszenie: do 1h,
- zgłoszenia telefoniczne i przez portal,
- dostarczenie zastępczego urządzenia w czasie do 8h w razie awarii,
- zdalne wdrożenie urządzenia,
- pomoc i wsparcie techniczne,
- konsultacje architekta bezpieczeństwa,
- zdalne zmiany konfiguracji przez technika,
- przegląd konfiguracji i logów,
- upgrade firmware.

DLP

Zamawiający wymaga aby w ramach postępowania wdrożony został system DLP (Data Leak Prevention). Zamawiający zezwala aby wdrożenie polegało na rozszerzeniu funkcjonalności posiadanego urządzenia UTM lub poprzez rozbudowę posiadanego oprogramowania antywirusowego lub poprzez źródło dedykowanego rozwiązania DLP. Niezależnie od sposobu implementacji, Zamawiający wymaga aby system został skonfigurowany a Administrator przeszkolony z konfiguracji i użytkowania rozwiązania. Jeśli rozwiązanie będzie polegało na instalacji agenta na komputerach użytkowników i licencji na każde stanowisko, należy dostarczyć min. 50 licencji a Wykonawca zainstaluje oprogramowanie na każdej stacji roboczej.

Wymagania:

1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 50 Klientów jednocześnie.
2. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, polityk, pomoc i inne wbudowane bazy wiedzy.
3. Agent musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.

4. System zapewnia możliwość stworzenia instalatora (.exe) z wbudowanymi, zaszyfrowanymi poświadczeniami dla dowolnego konta. Funkcja ta umożliwia instalację usługi bezpośrednio na kontach użytkowników – zarówno lokalnych, jak i domenowych, korzystając z uprawnień zdefiniowanych dla instalatora w konsoli systemu.
5. Agent musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).
6. System powinien umożliwiać generowanie unikatowego identyfikatora Agentów – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.
7. Agent musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.
8. Agent musi wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu Agentów.
9. System musi umożliwiać komunikację pomiędzy Agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.
10. System musi mieć możliwość współpracy komponentów Agent i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami Agentów.
11. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem.
12. Automaty powinny realizować co najmniej: usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nie przyrostowe, zmniejszanie bazy danych).
13. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartości parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie.
14. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).
15. Agent musi działać na systemach 32 i 64 bitowych: Windows Server 2019/2022, Windows 10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.
16. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2

17. Serwer www oraz SQL muszą działać na komercyjnych systemach 64 bitowych, np.: Windows Server 2019/2022, Windows 10/11 lub Linux RedHat v8 lub nowszym.
18. Baza danych musi działać na silniku SQL w wersji 64 bitowych komercyjnym lub bezpłatnym (np. Microsoft SQL Server Express Edition).
19. Jeśli do instalacji systemu na serwerze wymagane będą jakiekolwiek licencje systemów operacyjnych bądź bazodanowych – należy je dostarczyć.
20. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
21. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
22. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.
23. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS.
24. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny.
25. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV.
26. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switchy itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, dacie zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.
27. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.
28. System zapewnia integrację z modelem LLM.
29. System musi umożliwiać pełne zdalne zarządzanie Agentami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania Agenta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (polecen systemu operacyjnego).
30. Agent musi mieć możliwość konfiguracji zakresu skanowania plików.
31. Agent musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej, konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkownika, który go wyświetlił.
32. Konsola musi być w pełni polskojęzyczna.
33. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie). Konsola administracyjna musi posiadać dashboard – dashboard użytkownika,

- dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.
34. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widżety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.
 35. Dane na widżetach muszą być aktualizowane automatycznie.
 36. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność).
 37. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu.
 38. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego.
 39. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.
 40. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.
 41. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).
 42. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja Klienta, stanu Klienta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.
 43. Konsola musi zawierać w sobie pełną dokumentację systemu.
 44. System powinien prezentować podgląd zainstalowanych systemów operacyjnych, pakietów oraz aplikacji na komputerach z informacjami o: nazwie, wersji, producencie, typie licencji.
 45. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 4 tys. wzorców aplikacji, 1,3 tys. Producentów.
 46. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.
 47. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.
 48. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone.

Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.

49. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).
50. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.
51. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).
52. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.
53. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza poczynawszy od wskazanego miejsca w hierarchii kluczy rejestru.
54. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).
55. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).
56. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.
57. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.
58. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).
59. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne).
60. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.
61. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik)
62. System umożliwia dodawanie notatek do każdej pozycji sprzętu.
63. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).
64. System musi umożliwiać definiowanie typów serwisów
65. System musi umożliwiać definiowanie wartości serwisu
66. System musi umożliwiać definiowanie daty ważności serwisu oraz daty gwarancji
67. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.
68. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkownika, likwidacja).

69. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.) System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.
70. System musi ewidencjonować historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).
71. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/portcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.
72. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.
73. System musi zbierać informacje o jakości połączenia:
- a. Czas odpowiedzi serwisów (usług) podawany w milisekundach:
 - b. Średni czas odpowiedzi.
 - c. Minimalny czas odpowiedzi.
 - d. Maksymalny czas odpowiedzi.
 - e. Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.
74. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają Klienta.
75. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci
76. Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług.
77. System musi umożliwiać administratorowi definiowanie dodatkowych portów do monitorowania i przypisywanie do nich usług, a także modyfikowanie istniejących rekordów, obejmujących: port TCP, kategorię, nazwę usługi oraz nazwę skróconą.
78. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.
79. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.
80. System ma automatycznie wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.
81. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu Windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.
82. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert,

- pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory Windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.
83. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).
84. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, Windows PowerShell. System posiada co najmniej 70 predefiniowanych poleceń. System musi umożliwiać użytkownikom automatyczne definiowanie poleceń cmd/PowerShell. Funkcjonalność ta pozwala na wprowadzanie opisów zadanych czynności, a następnie, wykorzystując zaawansowane algorytmy AI, system automatycznie generuje adekwatne skrypty.
85. Zaawansowany Asystent AI do Przygotowywania Skryptów do precyzyjnego tworzenia szczegółowych skryptów
86. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).
87. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)
88. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.
89. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/ drugi/ trzeci/ czwarty/ ostatni, poniedziałek/ wtorek/ środa/ czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni, co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.
90. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie.
91. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.
92. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.
93. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).
94. System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie

usługami i restart komputera, zdalną instalacją oprogramowania, poprawek i aktualizacji (service pack, patch).

95. System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.
96. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.
97. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejścia dostępu).
98. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.
99. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.
100. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości pomiędzy użytkownikiem komputera z zainstalowanym Klientem a administratorem systemu.
101. Powinien zapewniać możliwość inicjowania czatu przez administratora.
102. Użytkownik powinien mieć opcję rozpoczęcia rozmowy za pomocą ikony na pasku zadań, która automatycznie uruchamia się zgodnie z konfiguracją Klienta.
103. System musi przechowywać historię konwersacji.
104. Powinien informować administratora poprzez powiadomienie w konsoli systemowej o nowych wiadomościach od użytkowników.
105. System powinien umożliwiać wysyłanie jednorazowych wiadomości w trybie natychmiastowym jako ALERT.
106. Musi oferować możliwość wysłania wiadomości z opcją odłożenia na później (na 10 minut, 1, 2, 4 godziny) dla późniejszego odczytu.
107. Powinien zapewniać historię wysyłania i odbierania wiadomości przez użytkowników, z możliwością edycji treści w edytorze HTML.
108. Wiadomość powinna być dostępna do wysłania do określonej grupy, wybranych komputerów lub użytkowników.
109. System musi umożliwiać konfigurację czasu wygaśnięcia wiadomości.
110. Powinien pozwalać na tworzenie szablonów wiadomości do regularnego użytku.
111. Musi zapewniać funkcję odłożenia wysyłania wiadomości dla późniejszego odczytu, z możliwością edycji treści w edytorze HTML.
112. System powinien rejestrować historię wysyłania i odczytywania wiadomości przez użytkowników.
113. Powinien umożliwiać wysłanie wiadomości do zdefiniowanej grupy, wybranych komputerów lub użytkowników.
114. Musi oferować opcję konfiguracji terminu, po którym wiadomość wygaśnie.
115. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”.
116. Formatowanie treści musi być zgodne z HTML.

117. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).
118. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.
119. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualnie i dźwiękowo o otrzymaniu nowej wiadomości.
120. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.
121. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).
122. System musi posiadać wbudowaną centralną bazę systemu umożliwiającą import i eksport niektórych danych zarówno poprzez API jak też za pomocą wbudowanego import/eksportu.
123. System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników.
124. System musi umożliwiać definiowanie dowolnej ilości grup użytkowników przypisanych do dowolnej ilości przełożonych. System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną.
125. System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących.
126. System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami.
127. System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią).
128. System musi na bieżąco monitorować i chronić za pomocą odpowiednio zdefiniowanych polityk i reguł dane w ruchu, dane w spoczynku oraz dane w użyciu.
129. Przez dane w spoczynku rozumie się dane, które nie są (ale mogą być) w ruchu lub w użyciu, wymagają inwentaryzacji i zabezpieczenia.
130. Przez dane w użyciu należy rozumieć dane, które są aktywnie przetwarzane przez dowolną aplikację i/lub punkt końcowy (komputer). Przykłady danych w użyciu: edycja dokumentu MS Word, Excel, PowerPoint, edycja pliku tekstowego CSV, TXT, tworzenie pliku, przechwytywanie ekranu (screenshot), kopiowanie / wklejanie danych.
131. Przez dane w ruchu należy rozumieć dane, które są przesyłane, np. kopiowanie danych (plików) z dysku sieciowego na nośnik USB, kopiowanie danych (plików) z komputera na komputer, przesyłanie danych e-mailem w treści lub w postaci załącznika, pobieranie danych z serwera FTP, przesyłanie danych za pomocą komunikatora.
132. Obiekty docelowe reguł muszą być definiowalne za pomocą parametrów takich jak: nazwa komputera, adres IP, unikatowy identyfikator agenta, status połączenia

- do systemu (online/offline), zainstalowany system operacyjny, nazwę zalogowanego użytkownika, model komputera, producent komputera, dostawca komputera, budżet, z którego zakupiony został komputer, strukturę organizacyjną
133. Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych.
134. System musi posiadać funkcjonalności monitorowania, blokowania, powiadomieniu użytkownika o wystąpieniu naruszenia zdefiniowanej polityki oraz pełnego logowania zdarzeń dotyczących polityki dla celów administracyjnych (powiadomienie administratora systemu).
135. System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP.
136. System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.
137. Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę.
138. System musi mieć możliwość określenia ram czasowych działania danej reguły.
139. System musi dysponować mechanizmami dostępu do plików na poziomie jądra systemu operacyjnego MS Windows (32-bit i 64-bit), co uniemożliwia obejście zabezpieczeń nawet osobie z uprawnieniami administratora na poziomie systemu operacyjnego.
140. System musi w pełni wspierać następujące polityki ochrony danych:
- a. Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione.
 - b. Monitorowanie wykonywanych zrzutów ekranu, blokowanie możliwości zapisania i wykorzystania zrzutów ekranu.
 - c. Przechwytywanie zrzutów ekranu z komputerów użytkowników wyzwalany akcją użytkownika lub na życzenie administratora zgodnie z wcześniej ustawionym interwałem czasowym.
 - d. Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputera.
 - e. Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).
141. Kontrola i ochrona urządzeń
- a. Blokowanie dostępu do wybranych typów urządzeń od strony sprzętowej. Wsparcie dla CD-ROM, portów USB, kart sieciowych, GPS, kart graficznych, modemów, klawiatur, czytników kart, drukarek, urządzeń Bluetooth i innych, monitorowanie podłączanych urządzeń.
 - b. Blokowanie dostępu do urządzeń USB, tworzenie czarnych list urządzeń, monitorowane podłączanych urządzeń USB.
 - c. Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www.

- d. Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych.
142. Klasyfikacja i ochrona dokumentów
- a. Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami.
 - b. Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu.
 - c. Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.
143. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS_AES_256 i AES_128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/desyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych, zarówno lokalnie, jak i zdalnie (poza NATem). Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany.
144. Ochrona danych w użyciu
- a. Podjęcie działania w momencie uruchomienia określonego procesu.
 - b. Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka.
145. Ochrona danych w ruchu
- a. Monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów.
 - b. Monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą.
146. System musi umożliwiać wyeksportowanie wybranych lub wszystkich danych do formatu .xls, .xlsx, .csv, .calc (OpenOffice), .html, .mht, .xml, .jpeg, .png, .gif, .bmp.
147. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów, przy czym generowanie raportu musi odbywać się po stronie serwera www.
148. System powinien umożliwiać eksport danych z raportu do formatów: pdf, xls, doc, rtf.
149. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).
150. System musi istnieć możliwość tworzenia i dodawania własnych raportów przez użytkownika.
151. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.
152. Uwierzytelnianie do systemu musi być realizowane:

- a. z wykorzystaniem imiennego konta użytkownika i hasła,
 - b. z wykorzystaniem imiennego konta administratorów aplikacji i hasła,
 - c. za pośrednictwem uwierzytelniania poprzez Active Directory,
 - d. za pośrednictwem uwierzytelniania poprzez CAS,
153. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.
154. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).
155. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie (MFA).
156. Uwierzytelnianie z wykorzystaniem obrazu wideo.
157. Uwierzytelnianie z jednorazowym kodem wysłanym na e-mail użytkownika.
158. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP.
159. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256.
160. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 10/11 i Windows Server 2019+.
161. System musi umożliwiać blokadę dostępu po nieudanej próbie zalogowania się do systemu. Ponadto, system powinien oferować:
162. Podgląd wszystkich zablokowanych administratorów systemu, w tym informacje o typie, elemencie, czasie trwania blokady [s] oraz o ostatniej aktywności.
163. Możliwość odblokowania zablokowanego administratora systemu z poziomu konsoli administracyjnej przez osobę uprawnioną.
164. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport.
165. System musi oferować możliwość podglądu wszystkich aktualnie otwartych sesji administratorów w konsoli administracyjnej, obejmując takie informacje jak: data utworzenia sesji, login, IP oraz SID.
166. Dodatkowo, system powinien umożliwiać wyszukiwanie zalogowanych administratorów po nazwie.
167. System musi udostępniać historię działań wybranych użytkowników/administratorów w zakresie, adresy URL i nagłówki http.
168. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy Klientami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera.
169. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.

170. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.
171. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).
172. System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od Klientów.
173. System musi zapewniać:
- a. Pełne logowanie błędów w celu weryfikowania nieprawidłowości.
 - b. Przechowywanie logów systemowych.
 - c. Przechowywanie logów bezpieczeństwa.
 - d. Przechowywanie logów aktywności użytkowników i administratorów.
 - e. Pobieranie logów z Klientów z poziomu konsoli administracyjnej.
 - f. Możliwość eksportu logów.
 - g. Definiowanie maksymalnego czasu przechowywania plików log.
 - h. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.
 - i. Definiowanie ścieżki do kopii zapasowej
 - j. Definiowanie ścieżki do importu danych
 - k. Definiowanie ścieżki do zapisu raportów
 - l. Definiowanie serwera do importu danych
174. System musi posiadać dokumentację w postaci min. 5 filmów instruktażowych/nagrań z webinarów w języku polskim.
175. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.
176. Czas trwania Usługi Utrzymania Oprogramowania wynosi 24 miesiące od dnia zakupu i obejmują:
- a. asystę techniczną,
 - b. obsługa zgłoszeń w zakresie:
 - c. reakcja na zgłoszenia błędów w określonym czasie reakcji;
 - d. dokonywanie analizy przyczyn błędów;
 - e. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich;
 - f. zapewnianie obejścia dla błędów występujących z przyczyn leżących po stronie infrastruktury zamawiającego;
 - g. usuwania błędów w czasie naprawy;
 - h. usuwania błędów występujących z przyczyn leżących po stronie oprogramowania podmiotów trzecich – po udostępnieniu odpowiedniej aktualizacji przez producenta tego oprogramowania oraz jej uzyskaniu – w czasie naprawy;
 - i. zapewnienia dostępności Oprogramowania.

UTM zakup i wdrożenie – Gminy Ośrodek Pomocy Społecznej w Pieckach

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.

17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
27. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
28. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
29. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
30. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
31. Ochrona antyspam ma działać w oparciu o:
 - białe/czarne listy,
 - DNS RBL,
 - Skaner heurystyczny.
32. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.

33. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
34. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
35. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
- PPTP VPN,
 - IPSec VPN,
 - SSL VPN.
36. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
37. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
38. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
39. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
40. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
41. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
42. Urządzenie ma posiadać wbudowany filtr URL.
43. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
44. Administrator ma mieć możliwość dodawania własnych kategorii URL.
45. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
- blokowanie dostępu do adresu URL,
 - zezwolenie na dostęp do adresu URL,
 - blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
46. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
47. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
48. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
49. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
50. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
- lokalną bazę użytkowników (wewnętrzny LDAP),
 - zewnętrzną bazę użytkowników (zewnętrzny LDAP),
 - usługę katalogową Microsoft Active Directory.
51. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.

52. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
- SSL,
 - Radius,
 - Kerberos.
53. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
54. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
55. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
56. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
57. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
58. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
59. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
60. Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:
- równoważenie względem adresu źródłowego,
 - równoważenie względem połączenia.
61. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
62. Urządzenie ma umożliwiać przełączenie na łączy zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).
63. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy.
64. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).
65. Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.
66. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
67. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego.
68. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).

69. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
70. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
71. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
72. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
73. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
74. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
75. Urządzenie ma umożliwiać zarządzania z poziomu konsoli (SSH)
76. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
77. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
78. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
79. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
80. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
81. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
82. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
83. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
84. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
85. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
86. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
- manualnego eksportu do pliku w dowolnym momencie czasu,
 - automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

87. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
88. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
89. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
90. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
91. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
92. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
93. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
94. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
95. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
96. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
97. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
98. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
99. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
100. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
101. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
102. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
103. Urządzenie ma posiadać usługę DNS Proxy.
104. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
105. Urządzenie musi mieć zaimplementowane Open API
106. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
107. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

108. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
109. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
110. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
111. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
112. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
113. Liczba portów Ethernet 2,5Gbps – min. 8.
114. Liczba portów światłowodowych 1Gbps – min. 1.
115. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
116. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
117. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
118. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
119. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
120. Maksymalna liczba tuneli VPN IPSec – minimum 100.
121. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
122. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
123. Obsługa interfejsów 802.11q (VLAN) – minimum 128
124. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
125. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
126. Urządzenie nie ma limitu na liczbę użytkowników.
127. Liczba reguł filtrowania – minimum 8 192.
128. Liczba tras statycznego routingu – minimum 512.
129. Liczba tras dynamicznego routingu – minimum 10 000.
130. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
131. Urządzenie musi być wyposażone w moduł TPM.
132. Gwarancja
 - a. Urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także muszą być objęte serwisem producenta na terenie RP.
 - b. Urządzenia objęte minimum 24 miesięcznym okresem gwarancji.

- c. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
- d. Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego rozwiązania, potwierdzające pochodzenie urządzeń z licencjami z oficjalnego kanału dystrybucyjnego producenta.
- e. Zamawiający dopuszcza realizację gwarancji przez autoryzowanego partnera serwisowego producenta.
- f. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
 - i. możliwość pobierania najnowszego firmware,
 - ii. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
 - iii. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
 - iv. otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.

UPS do serwerowni 3kVA – 1 szt.

Nazwa elementu, parametru Opis wymagań
lub cechy

Współczynnik mocy	1
Topologia (klasyfikacja IEC 62040-3)	Line-interactive (czysta sinusoida, AVR) lub On-Line
Typ obudowy	Uniwersalna (Tower/Rack), maks. 4U
Liczba, typ gniazd wyjściowych, możliwość sterowania	8x IEC C13 (10A), 2x IEC C19 (16A), W tym 2 grupy gniazd z możliwością sterowania: <ol style="list-style-type: none"> 1. 2x IEC C13 2. 2x IEC C13 + 1x IEC C19
Typ gniazda wejściowego	Gniazdo IEC C20 (16A)
Czas podtrzymania	Min. 20 minut przy obciążeniu 100%, możliwość wydłużenia czasu podtrzymania poprzez dołożenie kolejnych modułów bateryjnych
Napięcie znamionowe	230 V
Tolerancja napięcia prostownika	160 - 290 V
Częstotliwość znamionowa	50/60 Hz autodetekcja
Tolerancja częstotliwości	47 - 70 Hz (system 50 Hz)
Napięcie znamionowe wyjściowe	230 V (domyślnie) / 220/240 V
Częstotliwość wyjściowa	50/60 Hz

Baterie wymieniane przez użytkownika "na gorąco"	Tak
Ochrona przed przeładowaniem	Tak
Ochrona przed głębokim rozładowaniem	Tak
Okresowy automatyczny test baterii	Tak
Zimny start	Tak
System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
Interfejs komunikacyjny	<ul style="list-style-type: none"> • USB i RS232 • karta Web/SNMP • złącze dla zdalnego awaryjnego wyłączenia • złącze dla zdalnego załączenia/wyłączenia • złącze dla wyjściowego styku przekaźnikowego
Panel sterowania z wyświetlaczem LCD	<p>Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS-a) ze wskazaniem chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh)</p> <ul style="list-style-type: none"> • Przyciski sterowania • Kolorowe wskaźniki stanu: trybu normalnego (zielony), trybu bateryjnego (żółty), usterki (czerwony) • Sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie)

Wyposażenie	<ul style="list-style-type: none"> • instrukcja obsługi, instrukcja bezpieczeństwa • przewód zasilający • kabel RS232 • kabel USB • uchwyty kablowe • podstawki do montażu pionowego (Tower) • 2 przewody IEC 10 A • zestaw szyn montażowych do szafy 19"
Karta Web/SNMP	<ul style="list-style-type: none"> • cyberbezpieczeństwo (certyfikaty UL 2900-2-2/IEC62443/HTTPS/MQTT/RNDIS/LDAP/NVD/SSH/PKI, • pakiet szyfrów TLS 1.2 z minimum SHA256) • certyfikaty CA i PKI • prędkość: Gigabit Ethernet • różne poziomy nadawania dostępu do konta administratora lub użytkownika
Oprogramowanie zarządzające	<p>Wymagane oprogramowanie producenta UPS-a do monitorowania i zarządzania, umożliwiające:</p> <ul style="list-style-type: none"> - tworzenie scenariuszy zasilania ukierunkowanych na pojedyncze maszyny wirtualne, grupy maszyn wirtualnych lub automatyczne grupy maszyn wirtualnych - tworzenie scenariuszy zasilania ukierunkowanych na klastry - tworzenie scenariuszy zasilania z sekwencyjnym wyłączaniem poszczególnych maszyn wirtualnych
Wyposażenie dodatkowe	<p>Zestaw gniazd wyjściowych PDU o prądzie nominalnym 16A podłączany do gniazda wyjściowego IEC C19 w zasilaczu awaryjnym UPS, obudowa 1U do montażu w szafie Rack (19") z możliwością montażu w wielu położeniach, z 12 szt. gniazd IEC C13 (10A) i 1 szt. IEC C19 (16A), z 2 bezpiecznikami nadmiarowoprądowymi, z zaciskami zabezpieczającymi przed przypadkowym wyciągnięciem kabla zasilającego na gnieździe wejściowym i gniazdach wyjściowych IEC C13.</p>
Poziom hałas (przy standardowym obciążeniu)	< 40 dB
Zgodność z normami UE	Deklaracja zgodności CE
Dodatkowe certyfikaty	Raport CB (TUV), ISO 9001 dla producenta urządzenia

UPS centralny – 20kVA/20kW – 1 szt.

1. Moc wyjściowa UPS-a 20 kVA / 20 kW, w obszarze pracy współczynnika mocy obciążenia od 0,8 indukcyjny do 0,8 pojemnościowy.
2. Urządzenie ma być przystosowane do przyszłej rozbudowy w układzie pracy równoległej (min. 4 UPS). Układ połączeń logicznych pomiędzy poszczególnymi UPS'ami nie może stanowić pojedynczego punktu awarii, to znaczy przerwanie połączenia logicznego między UPS'ami pracującymi równolegle nie może spowodować utraty funkcjonalności systemu zasilania gwarantowanego. Opis technologii powinien być materiałem firmowym producenta.
3. Ilość faz 3/3 trzy fazy wejściowe i trzy fazy wyjściowe
4. Napięcie wejściowe – wyjściowe 3x400 V zgodne z wartościami zapisanymi w Polskiej Normie PN-IEC 60038, z tolerancją minimum 325V do 475V przy 100% obciążeniu bez korzystania z energii z baterii.
5. Urządzenie powinno posiadać:
 - a. Wejście trójfazowe 5-cio przewodowe (TN-S)
 - b. Wyjście trójfazowe 5-cio przewodowe (TN-S)
6. Częstotliwość wejściowa 50 Hz zgodna z wartościami zapisanymi w Polskiej Normie PN-IEC 60038 z tolerancją min. 40Hz do 70Hz
7. Urządzenie powinno zapewnić ciągłe bezprzerwowe zasilanie w trybie TRUE ON-LINE z podwójną konwersją przy zupełnych lub chwilowych zanikach napięcia i wahaniach częstotliwości w sieci elektrycznej przez cały czas pracy urządzenia. Zgodnie z normą PN-EN 62040-3, urządzenie klasy VFI-SS-111.
8. Czas pracy autonomicznej urządzenia przy 100% obciążeniu 20 kW musi wynosić co najmniej 8 minut, w temperaturze 25°C i na początku okresu eksploatacji.
9. Urządzenie powinno być wyposażone w system nieciągłego ładowania baterii. Do oferty należy dołączyć opis sposobu zarządzania pracą baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Opis powinien być materiałem firmowym producenta.
10. Urządzenie powinno być wyposażone w dotykowy, graficzny wyświetlacz LCD, z komunikatami w języku polskim.
11. Wymiary UPS nie powinny przekraczać następujących wartości:
 - a. szer. max. 350 mm
 - b. głęb. max. 750 mm
 - c. wys. max. 1300 mm
12. Poziom hałasu urządzenia nie może przekraczać 60dBA z odl. 1m.
13. Zasilacz musi być wyposażony w wewnętrzny elektroniczny układ obejściowy oraz zewnętrzny, mechaniczny, naścienny serwisowy układ obejściowy umożliwiający bezprzerwowe odłączenie UPS. Bypass zewnętrzny musi być wyprodukowany przez tego samego producenta co UPS.
14. UPS powinien być wyposażony w układ zabezpieczający przed zwrotnym podaniem energii do sieci (backfeed protection, zgodnie z normą IEC 62040), w torze bypassu statycznego.

15. Urządzenie musi posiadać możliwość przełączenia pracy w tryb oszczędzający energię charakteryzujący się zapewnieniem zasilania odbiorników z tolerancją parametrów napięcia i częstotliwości ustawioną w torze obejściowym, pozwalając na osiągnięcie sprawności długookresowej na poziomie min. 98,5% przy obciążeniu liniowym w zakresie 50-100% mocy znamionowej. Czas przełączania z trybu oszczędzania energii na tryb podwójnej konwersji wynosi do 2 ms.
16. Stabilizacja napięcia wyjściowego $< 1\% U_n$ przy obciążeniu statycznym, Stabilizacja napięcia wyjściowego $< 4\% U_n$ przy obciążeniu dynamicznym zmieniającym się od 0% do 100% i odwrotnie w czasie odbudowy maks. 100 ms.
17. Sprawność $> 95\%$ w trybie TRUE ONLINE w przedziale 50%-100% obciążenia znamionowego.
18. Wejściowy współczynnik mocy $\cos \varphi$ min. 0,99, THDi nie wyższe niż 3%.
19. Wyjściowy współczynnik mocy $\cos \varphi = 1$, TDHu wyjściowe dla obciążenia liniowego nie wyższe niż 1,5%.
20. Możliwość pracy z niesymetrycznym obciążeniem poszczególnych faz, w zakresie 0-100% obciążenia.
21. Urządzenie musi posiadać panel komunikacyjny, w którym powinny być zainstalowane gniazdo komunikacji RS-232, port komunikacyjny USB, gniazdo wyłącznika awaryjnego p.poż., karta sieciowa Web/SNMP.
22. Karta SNMP musi posiadać certyfikaty cyberbezpieczeństwa (szyfry TLS, MQTT) oraz certyfikaty CA i PKI. Musi cechować się prędkością gigabit'ową (half-duplex, full-duplex). Dostawca musi zapewnić możliwość automatycznego uaktualniania oprogramowania sprzętowego (firmware) karty poprzez sieć LAN.
23. Wymagana deklaracja producenta zgodności produktu z normami: EN 62040-1: 2008, EN 62040-2: 2006 oraz spełnienia dyrektyw: 2006/95/EC i 2004/108/EC wraz z rokiem przyznania znaku CE.
24. Wymaga się, aby dostarczone urządzenia objęte były gwarancją producenta na okres min. 24 miesiące.
25. Zamawiający po dostawie wykona pomiary i testy funkcjonalne potwierdzające spełnianie przez urządzenie zadeklarowanych parametrów układu zasilania. Jeżeli którykolwiek parametr nie zostanie spełniony Zamawiający rozwiąże umowę z Dostawcą zaś Dostawca zobowiązany będzie do wykonania demontażu i odebrania urządzenia na własny koszt.
26. Oferowane urządzenie do bezprzerwowego zasilania zwane dalej urządzeniem ma być fabrycznie nowe i ma pochodzić z seryjnej produkcji. Data jego wyprodukowania nie może być wcześniejsza niż 6 miesięcy przed terminem złożenia ofert.
27. Producent oferowanego urządzenia powinien spełniać wymagania międzynarodowego standardu jakości ISO 9001, co powinno być potwierdzone ważnym certyfikatem.
28. Dostawca urządzenia ma zapewnić dostawę części zamiennych przez okres co najmniej 7 lat od daty zakończenia produkcji oferowanego modelu urządzenia.
29. Urządzenie powinno być wyprodukowane w kraju należącym do Unii Europejskiej.

30. Wykonawca zapewni wykonanie, w ramach zaoferowanej ceny, wymagane przez producenta przeglądy okresowe/gwarancyjne/serwisowe w okresie udzielonej gwarancji.

Oprogramowanie systemowe

Centralny system logów

1. System musi pełnić funkcję zbierania logów, skanowania podatności oraz analizy danych i incydentów z całej infrastruktury IT.
2. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
3. System musi pracować w oparciu o architekturę Linux.
4. System musi mieć możliwość centralnego zbierania i zarządzania logami
5. System działać w trybie zbliżonym do rzeczywistego
6. System musi umożliwiać funkcjonowanie bez dostępu do sieci Internet
7. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwością centralnego dostępu.
8. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
9. System musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20 GB danych dziennie
10. System musi zapewniać retencję danych w okresie minimum 365 dni.
11. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
12. Licencja na oferowany system nie może ograniczać ilości źródeł danych, z których pobierane są dane i zdarzenia.
13. System musi umożliwiać rozbudowę bez potrzeby wyłączenia lub restartu środowiska.
14. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
15. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
16. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
17. System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregośkolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu .
18. Komunikacja pomiędzy komponentami systemu odpowiadającymi za agregacji, retencję i wizualizację danych musi odbywać się w sposób szyfrowany z wykorzystaniem protokołu TLS w wersji minimum 1.3.
19. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.
20. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.

21. Interfejs musi posiadać polską wersję językową.
22. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
23. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
24. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius
25. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
26. System musi wspierać mechanizm logowania typu Single Sign On.
27. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
28. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
29. System powinien umożliwiać zarządzanie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
30. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
31. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
32. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
33. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
34. System musi pozwalać na tworzenie parserów z poziomu GUI
35. System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.
36. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
37. System musi być wyposażony w zaawansowane metody analizy danych oparte na algorytmach sztucznej inteligencji.
38. Algorytmy sztucznej inteligencji muszą umożliwiać przewidywanie zachowań systemu poprzez zrozumienie liczby generowanych zdarzeń oraz wartości liczbowych w tych zdarzeniach, takich jak wysłane bajty (sent_bytes), rozmiar pliku (file_size) i czas trwania sesji (session_duration).
39. Algorytmy sztucznej inteligencji muszą wspierać pracę operatora w wykrywaniu anomalii w danych: pojedynczego parametru liczbowego, wielu parametrów liczbowych, tekstu oraz danych mieszanych. Oczekuje się, że wykrywanie anomalii będzie połączone z obliczaniem punktów, co umożliwi operatorowi skoncentrowanie swojej pracy na zdarzeniach o najwyższych wynikach.

40. Algorytmy sztucznej inteligencji muszą umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
41. Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
42. Algorytmy sztucznej inteligencji musi umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
43. Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
44. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
45. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
46. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
47. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
48. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:
- Syslog,
 - WEF,
 - Flat file,
 - Event log,
 - WMI,
 - SNMP trap,
 - XML,
 - JSON,
 - JDBC/ODBC
 - CSV,
 - Email,

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

49. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
50. System musi umożliwiać gromadzenie danych z baz danych relacyjnych, NoSQL, czasu rzeczywistego, m.in. MSSQL, Oracle, PostgreSQL, SQL Server, MongoDB, Apache Cassandra, InfluxDB i Apache Kafka
51. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.

52. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
53. Operacja z rekordami bazy danych musi być wykonywane jedynie za pomocą składni JSON z wykorzystaniem udokumentowanego API.
54. Wykorzystanie bazy danych musi odbywać się za pomocą REST API z pominięciem wykorzystania klienta typu SQL client.
55. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
56. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.
57. System musi posiadać predefiniowany zestaw parserów zdarzeń.
58. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
59. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
60. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
61. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
62. Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
63. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
64. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
65. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
66. System musi posiadać wbudowany komponent budowania elektronicznej dokumentacji z możliwością ręcznego i automatycznego dodawania treści oraz uzupełniania jej o wartości pochodzące ze zgromadzonych w Systemie danych.
67. Komponent budowania elektronicznej dokumentacji musi mieć możliwość m.in. tworzenia lub dodawania diagramów architektury zasobów informatycznych, tabel oraz list.
68. System musi umożliwiać łączenie wyników dwóch niezależnych zapytań w postaci jednej odpowiedzi, bez użycia składni SQL.
69. System musi posiadać interfejs umożliwiający zmianę wybranej wartości w zgromadzonych danych.
70. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi

umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.

71. System musi umożliwiać budowanie zapytań z wykorzystaniem składni SQL.
72. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
73. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
74. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
 - a. Wykrycia dowolnej treści w logach,
 - b. Wykrycia wystąpienia wartości pola na wybranej liście,
 - c. Wykrycia niewystępowania wartości pola na wybranej liście,
 - d. Wykrycia zmiany jednego z kilku pól,
 - e. Wykrycia zdarzeń występujących z zadaną częstotliwością,
 - f. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
 - g. Wykrycia zaniku Wiadomości,
 - h. Wykrycia nowej wartości pola w zadanym okresie czasu,
 - i. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
75. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
76. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
77. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
78. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
79. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
80. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
81. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
82. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
83. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
84. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.

85. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
86. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
87. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
88. System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
89. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
90. System musi posiadać wbudowany, dostępny z poziomu GUI moduł tworzenia i edycji elektronicznej dokumentacji bazującej oraz wzbogacającej dane gromadzone ze środowiska informatycznego.
91. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
92. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
93. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
94. System musi być dostarczony z licencją wieczystą oraz wsparciem producenta na okres minimum 24 miesięcy.
95. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
96. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
97. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
98. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
99. System musi być dostarczony z repozytorium danych IoC utrzymywanym i rozwijanym przez producenta.
100. System musi umożliwiać integrację z Mitre [ATT@CK](#).
101. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
102. System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.

103. System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
104. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
105. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów
106. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
107. System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP
108. System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.
109. Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
110. Mechanizm archiwizacji musi umożliwiać pozwalając na przywracanie danych do systemu celem analizy online.
111. Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych
112. Dokumentacja techniczna i baza wiedzy dotycząca oferowanego systemu musi być opublikowana na ogólnodostępnej stronie internetowej producenta.
113. Producent systemu musi umożliwiać rozbudowę oferowanego rozwiązania o moduł funkcjonalny SOAR lub zapewnić gotową integrację z systemem SOAR tego samego producenta.
114. Zamawiający wymaga licencji wieczystych z gwarancją i serwisem na okres minimum 24 miesięcy, z możliwością przedłużenia. Serwis powinien obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.
115. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
116. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
117. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Oprogramowanie do wirtualizacji

Zamawiający posiada klastrer wirtualizacyjny oparty o środowisko VMWare 8 + Vcenter (VMware vSphere 8 Essentials Kit for 3 hosts (Max 2 CPU per host, 32 cores/CPU), 1YR VMware SNS). Nowy serwer wirtualizacyjny należy podłączyć do obecnego klastra i zapewnić wsparcie producenta dla całego klastra minimum na okres udzielonej gwarancji.

Zamawiający nie przewiduje wymiany oprogramowania klastra wirtualizacyjnego. Wszystkie licencje muszą być kompatybilne i umożliwiać zarządzanie klastrem z jednej konsoli Vcenter. Licencje muszą pozwalać na uruchomienie wirtualizacji na wszystkich procesorach w klastrze.

Oprogramowanie antywirusowe – rozbudowa posiadanej licencji

Zamawiający posiada oprogramowanie antywirusowe Bitdefender (GravityZone Business Security Premium dla 50 użytkowników (data wygaśnięcia 21 Feb 2025) + GravityZone Full Disk Encryption dla 10 użytkowników (data wygaśnięcia 27 Feb 2025). Zamawiający wymaga przedłużenia wsparcia producenta (w tym aktualizacji sygnatur) i rozbudowy wszystkich licencji do min. 50 stanowisk ze wsparciem dla EDR oraz centralnej konsoli do zarządzania stanowiskami.

W przypadku dostarczenia oprogramowania alternatywnego, dostarczone przez Wykonawcę oprogramowanie antywirusowe musi wspierać min. następujące funkcjonalności posiadanego przez Zamawiającego oprogramowania:

- Antimalware
- Antiphishing
- Anti-Exploit
- Process Inspector
- Ransomware Mitigation
- Automatic Disinfection and Removal
- Firewall
- Web Threat Protection
- Application Control (Blacklisting)
- Network Attack Defense
- Web Access Control
- Device Control
- Analytics
- Executive Summary
- Threats Explorer
- Endpoint Risk Analytics
- Add-Ons (Purchased Separately)
- Patch Management
- Full Disk Encryption
- Security for Mobile
- Security for Email
- Integrity Monitoring

Powyższe funkcjonalności stanowią listę nazw własnych producenta oprogramowania Bitdefender i Wykonawca musi zapewnić, że alternatywne oprogramowanie lub jego moduły będzie/będą miały takie same lub lepsze funkcjonalności niezależnie od nazw własnych użytych przez producenta alternatywnego oprogramowania. Wraz z ofertą należy przekazać listę modułów wraz z ich dokładnym opisem funkcjonalności jakie oferuje.

Oprogramowanie do zarządzania infrastrukturą – rozbudowa

Zamawiający posiada oprogramowanie Axence nVision (moduły „Inwentaryzacja” oraz „Data Guard”) licencje na 40 stanowisk, które należy rozbudować o licencje HelpDesk dla wszystkich pracowników. Dodatkowo należy zwiększyć ilość licencji stanowiskowych do 50 szt. oraz zapewnić usługę wysyłania alarmowych wiadomości SMS z oprogramowania nVision do administratora (minimum 500 szt. wiadomości miesięcznie). Usługa musi posiadać otwarte API pozwalające na dołączanie dowolnych innych systemów wspierających funkcjonalność wysyłania SMSów przez API.

Wykonawca może dostarczyć oprogramowanie alternatywne posiadające taką samą funkcjonalność w ramach nowych oraz już posiadanych modułów oprogramowania nVision. W przypadku zaoferowania oprogramowania alternatywnego należy dostarczyć wraz z ofertą dokładny opis modułów i ich funkcjonalności.

Instalacja dostarczonych urządzeń i oprogramowania

Wszystkie dostarczane urządzenia muszą zostać zainstalowane [tj. wypakowane, zmontowane, zamontowane w szafach rack, (zamawiający powiada szafę rack o głębokości 900mm!) uruchomione i skonfigurowane] w docelowym miejscu pracy [wskazany przez Zamawiającego] w terminie wskazanym przez Zamawiającego [miejsce i termin dostawy oraz instalacji należy uzgodnić na min. 5 dni roboczych przed planowaną dostawą urządzeń].

W systemie zarządzania dla każdego urządzenia należy utworzyć dwóch użytkowników z administracyjnymi [jeden dla ASI, jeden dla serwisu]. Jeśli interfejs posiada konto „gościa” należy je wyłączyć. Wszystkie możliwe protokoły sieciowe [ssh, http, https, telnet, itp.] muszą zostać zabezpieczone przed niepożądanym dostępem, a niebezpieczne protokoły wyłączone.

Zamawiający wymaga od Wykonawcy instalacji i konfiguracji dostarczonego oprogramowania na sprzęcie dostarczonym lub wskazanym przez Zamawiającego.

Oprogramowanie do zarządzania siecią i zbierania logów planowane jest do uruchomienia na dostarczonym serwerze logów jako odrębne maszyny wirtualne. Oprogramowanie do wirtualizacji należy zainstalować na serwerach wirtualizacyjnych.

Usługa segmentacji sieci

Zamawiający wymaga aby Wykonawca w porozumieniu z Administratorem IT Zamawiającego stworzył polityki zezwalające na ruch pomiędzy segmentami sieci. Wykonawca podzieli logicznie sieć na min. 5 vlanów: Management, Serwery, Komputery użytkowników, Drukarki, Hot-Spot WiFi. Wykonawca wspólnie z zamawiającym ustali minimalne zakresy portów i/lub usług jakie mogą działać pomiędzy strefami i wdroży odpowiednie dla każdej z grup polityki bezpieczeństwa (np. HotSpot WiFi – tylko internet (dns, http/s, pop/s, imap/s, itp.)), stworzy profile bezpieczeństwa na UTM/przełącznikach. Wykonawca skonfiguruje UTM (w zakresie vlanów, routingu, profili bezpieczeństwa) przełączniki sieciowe (w zakresie vlanów, grup lag, itp.) Vmware (w zakresie vlanów, grup lag na vswitch i kartach fizycznych). W efekcie prac Wykonawcy cała infrastruktura Zamawiającego musi być skonfigurowana do pracy w odseparowanych od siebie sieci vlan (jeśli wymagana będzie konfiguracja usług takich jak DHCP, DNS, RIP, itp. Wykonawca musi je wykonać).

Serwery

Na serwerach wirtualizacyjnych należy zainstalować system wirtualizacji i skonfigurować go do korzystania z zasobów dyskowych macierzy oraz podłączyć do centralnie zarządzanego klastra wirtualizacyjnego i ustawić polityki HA. Wykonawca w uzgodnieniu z Zamawiającym zaprojektuje i wdroży system backupu min. maszyn wirtualnych. Serwer logów musi zostać skonfigurowany do zbierania logów z urządzeń sieciowych i serwerów za pomocą standardowych protokołów. Interfejs przeglądania logów musi być zabezpieczony przed dostępem osób niepożądanych oraz szyfrowany za pomocą certyfikatu SSL.

Macierz dyskowa

Macierz musi zostać rozbudowana o dodatkowe dyski. Dyski muszą być skonfigurowane w systemie zarządzania macierzą. Dostępna przestrzeń musi być rozszerzona przez dodatkowe dyski. Oprogramowanie wewnętrzne obydwu macierzy i dysków należy dodatkowo zaktualizować do najnowszych obsługiwanych wersji.

Przełączniki sieciowe

Na wszystkich przełącznikach sieciowych należy skonfigurować SNMP oraz SNMP traps do korzystania z systemu monitorowania i przesyłania alarmów do ASI oraz centralnego systemu logów. Na wszystkich przełącznikach muszą zostać skonfigurowane vLany oraz reguły zabezpieczenia DHCP [jeśli wymagane]. Sieć zarządzania należy wydzielić do oddzielnego vLANu. Wszystkie przełączniki muszą mieć przypisany adres IP do interfejsu zarządzania.

Wykonawca musi w szczególności wykonać następujące czynności:

- Połączenie przełączników z istniejącymi elementami infrastruktury,
- Konfiguracja uzgodnionej funkcjonalności L2 (VLANy, agregacje, UDLD/DLDP, STP),
- Konfiguracja uzgodnionej funkcjonalności L3 (adresy, bramy, DNSy, NTP, syslog),
- Konfiguracja uzgodnionych funkcjonalności bezpieczeństwa.

Przełączniki należy skonfigurować do obsługi użytkowników końcowych – skonfigurować odpowiednie vlany i polityki ochrony oraz dostępu zgodnie z miejscem instalacji.

Zabezpieczenie usług

Wykonawca dokona instalacji fizycznej wszystkich wymaganych urządzeń teletechnicznych oraz dostarczanego sprzętu. Wszystkie urządzenia muszą zostać podłączone i uruchomione.

Wykonawca wdroży [tj. zainstaluje, uruchomi, skonfiguruje i przetestuje] infrastrukturę zapasową serwerów wirtualnych oraz procedurę przełączania usług. Na serwerze fizycznym Wykonawca utworzy infrastrukturę serwerów wirtualnych. Serwery wirtualne należy skonfigurować do korzystania z zasobów sieciowych i dyskowych. Wszystkie maszyny wirtualne muszą zostać skonfigurowane zgodnie z ich przeznaczeniem [np.: Active Directory, DHCP, DNS, RDP, etc.].

Firewall – UTM

Urządzenia muszą zostać zainstalowane w miejscu użytkowania – wskazanym przez Zamawiającego (Urząd Gminy i Gminny Ośrodek Pomocy Społecznej). W konfiguracji urządzeń muszą zostać włączone min. usługi:

- ochrony przed atakami typu DoS/DDoS, itp.,
- ochrony antywirusowej,
- web filter,
- IDS/IPS/DLP.

UTMy muszą zostać skonfigurowane w taki sposób, aby serwis techniczny Wykonawcy mógł łączyć się z urządzeniami w serwerowni za pośrednictwem bezpiecznego kanału transmisji – VPN.

Instalowane urządzenia muszą chronić zainstalowane wewnątrz sieci Zamawiającego serwery aplikacyjne usług [głównie przed atakami typu DoS oraz MitM].

W szczególności Wykonawca musi wykonać następujące czynności:

- aktualizacja do najnowszej zalecanej wersji oprogramowania,
- stworzenie segmentów sieci (VLANów) (również na przełącznikach),
- ustawienie polityk ruchu w taki sposób aby działały usługi udostępniane przez Zamawiającego na obecnych urządzeniach / serwerach,
- stworzenie polityk zezwalających na ruch pomiędzy segmentami sieci – w ustaleniu z Zamawiającym (min. w zakresie: 5 vlanów: Management, Serwery, Komputery użytkowników, Drukarki, Hot-Spot WiFi) – Wykonawca wspólnie z zamawiającym ustali minimalne zakresy portów i/lub usług jakie mogą działać pomiędzy strefami i wdroży odpowiednie dla każdej z grup polityki bezpieczeństwa (np. HotSpot WiFi – tylko internet (dns, http/s, pop/s, imap/s, itp.))
- stworzenie profili bezpieczeństwa,
- przełączenie sieci na firewall/UTM.

Kopie zapasowe

Wykonawca we współpracy z ASI zweryfikuje i w razie konieczności zaktualizuje politykę kopii bezpieczeństwa uwzględniając możliwości techniczne po wdrożeniu Projektu. Na podstawie polityki Wykonawca skonfiguruje systemy i usługi do wykonywania kopii bezpieczeństwa zgodnie z harmonogramami. Przetestuje działanie mechanizmu automatycznego wykonywania kopii bezpieczeństwa i po okresie 30 dni od uruchomienia harmonogramu oceni skuteczność wdrożonych mechanizmów. W ramach wdrożenia musi zostać dostarczona instrukcja odtwarzania danych w różnych zakresach [np.: pojedynczy plik, cały katalog, użytkownik wraz z plikami, maszyna, itp.]. Wykonawca razem z Administratorem ustali miejsce składowania oraz retencję kopii.

UPSy

Wykonawca zainstaluje UPSy w serwerowni zgodnie z wytycznymi producenta.

UPS 3kVA musi zostać zainstalowany w szafie RACK lub bezpośrednio w jej okolicy.

UPS 20kVA musi zostać zainstalowany w miejscu obecnego UPSa i podłączony do instalacji energetycznej Zamawiającego zgodnie z obecną dokumentacją.

Obydwa UPSy muszą być zmontowane, zainstalowane, skonfigurowane, uruchomione i przetestowane. Interfejsy zarządzające muszą być skonfigurowane i podłączone do sieci LAN. Wykonawca wspólnie z Zamawiającym ustali nazwy użytkowników i hasła.

Wykonawca zainstaluje dostarczone oprogramowanie do zarządzania UPS 3kVA i wdroży scenariusz automatycznego zamykania wirtualnych serwerów i fizycznych maszyn w przypadku długotrwałego zaniku napięcia. Czasy i kolejność zamykania maszyn Wykonawca ustali z Administratorem podczas wdrożenia.

Instruktaże

Przewiduje się przeprowadzenie instruktażu z wdrażanych rozwiązań dla pracowników działu IT. Instruktaż odbywać się będzie w trakcie instalacji i/lub po instalacji urządzeń i oprogramowania.

Zakres instruktaży dla każdego z urządzeń/systemu zostanie dostosowany do stopnia wiedzy pracowników. Instruktaże dla administratorów systemu będą miały charakter stanowiskowy w zakresie obsługi i administracji systemami.

Instruktaże dla administratorów będą musiały spełniać minimum następujące wymagania:

- 1) powinny odbywać się w godzinach od godz. 8.00 do 15.00,
- 2) instruktaże odbywać się będą w siedzibie Zamawiającego (lub jednostce podległej jeśli tam będzie instalowane urządzenie).

Instruktaże mają na celu umożliwienie pracownikom działu IT sprawne poruszanie się po panelach zarządzania dostarczoną infrastrukturą i zrozumienie wprowadzonych polityk bezpieczeństwa.

Gwarancja

Świadczenie usługi gwarancji ma na celu zapewnienie ciągłości sprawnego działania Systemu poprzez realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych Dysfunkcji systemów, niewłaściwego działania systemu, spadku wydajności, wykryciu zagrożenia włamania, itp.

W ramach usługi Wykonawca zobowiązany jest do nieodpłatnego usuwania dysfunkcji:

- z przyczyn zawinionych przez Wykonawcę będących konsekwencją wystąpienia: Dysfunkcji w Systemie, błędu lub wady fizycznej pakietu aktualizacyjnego lub instalacyjnego, błędu w dokumentacji administratora lub w dokumentacji użytkownika, błędu w wykonaniu usług przez Wykonawcę;
- związanych z realizacją usługi wdrożenia Systemu;
- spowodowanych aktualizacjami Systemu instalowanymi na polecenie lub w wyniku rekomendacji Wykonawcy.

Przygotowanie i dostarczenie dokumentacji powykonawczej

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Administratora – zawierającą ogólny opis wymaganych czynności i działań związanych z instalacją i konfiguracją danego elementu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego (platformy sprzętowej, systemowej, bazodanowej i aplikacyjnej). Dokumentacja musi zawierać wszystkie niezbędne loginy, hasła, kody dostępu, itp. pozwalające na odtworzenie pełnego zakresu systemu po awarii, zarządzanie w pełnym zakresie dostarczonym rozwiązaniem oraz pełnienie usługi serwisu przez inny podmiot po okresie trwałości projektu. Loginy i hasła należy dostarczyć na pendrive w formie zaszyfrowanej bazy danych (np. Keepass) lub w oddzielnej kopercie.

Dokumentacja techniczna dostarczonego rozwiązania musi być sporządzona w języku polskim i dostarczona w wersji elektronicznej z możliwością przeszukiwania treści – dla systemów. Powyższe nie dotyczy standardowej dokumentacji producenta sprzętu i oprogramowania a jedynie dokumentacji projektowej.

Szkolenia pracowników

Pakiet szkoleń dla pracowników Zamawiającego

Kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness), umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w internecie.

Zamawiający wymaga przeprowadzenia szkolenia „na miejscu” w siedzibie zamawiającego dla wszystkich pracowników urzędu w grupach maksymalnie po 20 osób w minimalnym wymiarze czasowym równym 4 godzin dla każdej z grup. Wykonawca przygotowuje listy obecności dla pracowników i dostarczy po zakończeniu szkolenia imienne zaświadczenia o odbytym szkoleniu. Każde szkolenie musi pokrywać minimum następujące zakresy:

- ✓ Podstawy bezpiecznego internetu (w tym e-mail)
- ✓ Phishing - podstawy
- ✓ Spyware/malware - podstawy
- ✓ Bezpieczeństwo danych osobowych RODO/GDRP

Wykonawca musi dostarczyć ponadto dedykowaną użytkownikom Zamawiającego i świadczoną przez okres min. 3 miesięcy platformę e-Learningową.

Usługa e-Learningowa musi zawierać:

1. Platformę szkoleniową zawierającą minimum 45 szkoleń, dostępnych w języku polskim (oraz w jęz. angielskim), w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.

a) Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:

- ✓ Podstawy bezpiecznego internetu
- ✓ Bezpieczeństwo poczty
- ✓ Załączniki w poczcie elektronicznej
- ✓ Phishing
- ✓ Spyware/malware
- ✓ Bezpieczeństwo danych osobowych RODO/GDRP
- ✓ Bezpieczne hasła
- ✓ Menedżery haseł
- ✓ Bezpieczeństwo urządzeń mobilnych
- ✓ Uwierzytelnianie wieloskładnikowe (MFA)
- ✓ Bezpieczna praca zdalna
- ✓ Bezpieczna praca w biurze
- ✓ Sieci społeczne
- ✓ Socjotechnika stosowana
- ✓ Zakupy w internecie

b) Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.

c) Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 8 godzin.

2. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:

- a) z linkiem prowadzącym do stronnym internetowej,
- b) z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,
- c) z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,
- d) z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.

W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.

3. dedykowaną platformę dostarczającą raporty obejmujące minimum:

- a) status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,
- b) status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zawierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.

W ramach świadczonej usługi usługodawca musi:

- przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,
- zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,
- zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
- dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,
- wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników (nie więcej niż 5 zmian w okresie trwania usługi).
- przeprowadzić minimum 4 kampanie phishingowe

Wymagania dodatkowe:

Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma

szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.

Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Do oferty należy załączyć oświadczenie usługodawcy o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001.

Szkolenia specjalistyczne dla działu IT

Szkolenie UTM

Celem szkolenia jest zaprezentowanie najczęściej stosowanych funkcji i metod zarządzania dostarczonymi urządzeniami UTM.

Zdobycie umiejętności samodzielnej konfiguracji poszczególnych modułów bezpieczeństwa takich, jak: AntyVirus, AntySpam, WebFilter, IPS.

Poznanie funkcjonalności modułu umożliwiającego kontrolę aplikacji.

Zaprezentowanie dostępnych rozwiązań VPN.

Szkolenie przeprowadzane w formie warsztatów ze znaczną liczbą praktycznych laboratoriów. Zakres tematyczny oraz część warsztatowa musi zostać dostosowana do poziomu wiedzy i potrzeb uczestników szkolenia.

Szkolenie oparte o oprogramowanie w wersji jakiej został dostarczony UTM.

Plan szkolenia:

Produkty - rodzaje, pozycjonowanie, wymiarowanie

Podstawowe czynności administracyjne:

- konfiguracja domyślna
- update firmware
- kopia zapasowa
- konfiguracja licencji
- wstępna konfiguracja trybu pracy
- konfiguracja interfejsów sieciowych
- konfiguracja serwera DHCP
- dodatkowe ustawienia sieciowe
- dostęp administracyjny

Logowanie - metody logowania i ich praktyczna konfiguracja

- Syslog
- pamięć RAM

Konfiguracja zapory ogniowej - elementy podstawowe obiekty i grupy

- reguły zapory ogniowej
- translacja adresów SNAT i DNAT

Konfiguracja zapory ogniowej - uwierzytelnianie metody uwierzytelniania użytkowników

- lokalna baza użytkowników grupy użytkowników
- użytkownicy AD

Routing statyczny

- Ping Server
- metryka i priorytety

Zarządzanie zagrożeniami, moduł antywirusowy, moduł antyspamowy

- filtrowanie stron WWW kontrola aplikacji
- moduł IPS i DLP

Wirtualne Sieci Prywatne VPN SSL-VPN vs IPSec VPN

- konfiguracja tuneli VPN

Uczestnicy szkolenia mają otrzymać certyfikat wystawiony imiennie oraz na Zamawiającego sygnowany przez Certyfikowane Centrum Edukacyjne dostarczonego urządzenia UTM.

Wykonawca ustali termin przeprowadzenia szkoleń z pracownikami IT Zamawiającego lub przekaże vouchery na szkolenia uprawniające do przeprowadzenia szkolenia min. w terminie jednego roku.

Szkolenie Active Directory – zarządzanie

Zamawiający wymaga aby szkolenie pozwalało na uzyskanie wiedzy i praktycznych umiejętności w zakresie zarządzania usługami domenowymi Active Directory w systemie Windows Server. W tym zapoznanie się z:

- Dostępnymi rozwiązaniami do zarządzania tożsamością.
- Wdrażaniem i administracją AD DS w systemie Windows Server.
- Bezpiecznym wdrożeniem AD DS.
- Wdrażaniem i konfiguracją lokacji AD DS oraz zarządzaniem replikacją.
- Wdrażaniem i zarządzaniem zasadami grupy.
- Zarządzaniem ustawieniami użytkowników za pomocą zasad grupy.
- Procesem implementacji hierarchii urzędu certyfikacji za pomocą usług AD CS i sposobami zarządzania urzędami certyfikacji.
- Wdrażaniem i zarządzaniem certyfikatami.
- Wdrażaniem i zarządzaniem AD RMS.
- Wdrażaniem i zarządzaniem usługami AD FS.
- Zabezpieczaniem i zapewnianiem dostępu do danych za pomocą technologii takich jak dynamiczna kontrola dostępu, foldery robocze i dołączanie do miejsca pracy.
- Procesem monitorowania, rozwiązywania problemów i zapewnieniem ciągłości działania usług AD DS.
- Procesem implementacji usługi Windows Azure Active Directory.
- Wdrażaniem i zarządzaniem usługami Active Directory Lightweight Directory Services (AD LDS).

Wykonawca zapewni:

- szkolenie w języku polskim,
- materiały w języku polskim lub angielskim,
- szkolenie i materiały odnoszące się do aktualnej wersji systemu wirtualizacji
- szkolenie prowadzone może być w formie kursu on-line lub w siedzibie Wykonawcy
- w przypadku szkolenia w siedzibie Wykonawcy Wykonawca zapewni wyżywienie i ewentualne noclegi

Minimalny zakres szkolenia:

1. Przegląd ochrony dostępu i informacji
 - Wprowadzenie do rozwiązań w zakresie dostępu i ochrony informacji
 - Omówienie rozwiązań AIP w systemie Windows Server
 - Przegląd FIM 2010 R2
2. Zaawansowane wdrażanie i administrowanie AD DS
 - Wdrażanie usług AD DS
 - Wdrażanie i klonowanie wirtualnych kontrolerów domeny
 - Wdrażanie kontrolerów domeny w systemie Windows Azure
 - Administrowanie AD DS
3. Zabezpieczanie AD DS
 - Zabezpieczanie kontrolerów domeny
 - Wdrażanie bezpieczeństwa konta
 - Wdrażanie uwierzytelnienia kontroli
4. Wdrażanie i administrowanie lokacjami AD DS i replikacją
 - Omówienie replikacji usług AD DS
 - Konfigurowanie witryn AD DS
 - Konfigurowanie i monitorowanie replikacji usług AD DS
5. Wdrażanie zasad grupy
 - Wprowadzenie do zasad grupy
 - Wdrażanie i administrowanie obiektami GPO
 - Zakres zasad grupy i przetwarzanie zasad grupy
 - Rozwiązywanie problemów z zastosowaniem obiektów zasad grupy
6. Zarządzanie ustawieniami użytkownika za pomocą zasad grupy
 - Wdrażanie szablonów administracyjnych
 - Konfigurowanie przekierowania folderu i skryptów
 - Konfigurowanie preferencji zasad grupy
7. Wdrażanie i zarządzanie usługami AD CS
 - Wdrażanie urzędów certyfikacji
 - Administrowanie urzędami certyfikacji
 - Rozwiązywanie problemów, utrzymanie i monitorowanie urzędów certyfikacji
8. Wdrażanie i zarządzanie certyfikatami
 - Korzystanie z certyfikatów w środowisku biznesowym
 - Wdrażanie i zarządzanie szablonami certyfikatów

- Zarządzanie wdrażaniem, unieważnianiem i odzyskiwaniem certyfikatów
 - Wdrażanie i zarządzanie kartami inteligentnymi
9. Wdrażanie i zarządzanie AD RMS
- Omówienie AD RMS
 - Wdrażanie i zarządzanie infrastrukturą AD RMS
 - Konfigurowanie ochrony treści AD RMS
 - Konfigurowanie zewnętrznego dostępu do AD RMS
 - Wdrażanie i zarządzanie usługami AD FS
 - Omówienie usług AD FS
 - Wdrażanie usług AD FS
 - Implementowanie AD FS dla pojedynczej organizacji
 - Wdrażanie usług AD FS w scenariuszu federacji między przedsiębiorstwami
 - Rozszerzenie usług AD FS na klientów zewnętrznych
10. Wdrażanie bezpiecznego dostępu do udostępnionego pliku
- Przegląd dynamicznej kontroli dostępu
 - Wdrażanie komponentów DAC
 - Wdrożenie DAC do kontroli dostępu
 - Wdrażanie pomocy odmowy dostępu
 - Wdrażanie i zarządzanie folderami roboczymi
 - Wdrażanie przyłączenia do miejsca pracy
11. Monitorowanie, zarządzanie i odzyskiwanie usług AD DS
- Monitorowanie AD DS
 - Zarządzanie bazą danych AD DS
 - Opcje tworzenia kopii zapasowych i odzyskiwania AD DS oraz innych rozwiązań w zakresie tożsamości i dostępu
12. Implementowanie Windows Azure Active Directory
- Omówienie usługi Windows Azure AD
 - Zarządzanie kontami Windows Azure AD
13. Wdrażanie i zarządzanie AD LDS
- Przegląd AD LDS
 - Wdrażanie usług AD LDS
 - Konfigurowanie wystąpień i partycji AD LDS
 - Konfigurowanie replikacji usług AD LDS
 - Integracja AD LDS z AD DS

Certyfikowane szkolenie z oprogramowania antywirusowego

Szkolenie musi obejmować min.:

- Omówienie podstaw systemu antywirusowego
- Tworzenie dostępu do konsoli
- Instalacja serwera bezpieczeństwa i konsoli zarządzania

- Tworzenie pakietów instalacyjnych i ich wdrożenie ręczne oraz zdalne na systemach Windows oraz ręczne na systemach Linux
- Tworzenie paczek .msi
- Konfiguracja szablonów polityk bezpieczeństwa wraz z omówieniem występujących opcji, zwróceniem uwagi na najważniejsze ustawienia pod kątem stacji roboczych i serwerów
- Konfiguracja modułu Antymalware
- Konfiguracja reguł Zapory sieciowej
- Konfiguracja blokowania stron internetowych
- Konfiguracja i blokowanie urządzeń podłączanych do komputerów
- Obsługa systemu EDR
- Obsługa Analizatora Sandbox
- Wyjaśnienie zarządzanie ryzykiem
- Konfiguracja powiadomień i raportów
- Rozwiązywanie podstawowych problemów przy administracji
- Szkolenie może być prowadzone w formie on-line
- Minimalny czas szkolenie: 4h zegarowe
- Szkolenie musi zakończyć się wystawieniem imiennego certyfikatu
- Szkolenie musi być prowadzone w języku polskim

Certyfikowane szkolenie z administrowania dostarczonym Systemem zarządzania infrastrukturą

Szkolenie w formie warsztatów dostarczające kompletu informacji i umiejętności niezbędnych do skutecznego zarządzania IT w dostarczonym systemie. Minimalny zakres szkolenia prowadzonego w języku polskim:

1. Ogólne omówienie Systemu.
2. Wymagania i instalacja systemu.
3. Wstępna konfiguracja systemu i instalacja.
4. Konfiguracja i praca w module Sieciowym.
5. Konfiguracja i praca w module Inwentaryzacji.
6. Konfiguracja i praca w module Użytkowników.
7. Konfiguracja i praca w module HelpDesk.
8. Konfiguracja i praca w module DataGuard.
9. Konfiguracja i praca w Konsoli Administracyjnej.
10. Rozwiązywanie najczęstszych problemów.
11. Egzamin certyfikujący.

Szkolenie 12h zegarowych (dwudniowe).

W ramach usługi Wykonawca musi dostarczyć:

- pakiet materiałów szkoleniowych,
- egzamin,
- certyfikat dla uczestnika,
- 14-dniowy czas na konsultacje z trenerem po szkoleniu,
- wyżywienie i nocleg.

Szkolenie z zarządzania systemem wirtualizacji

Minimalny zakres szkolenia:

1. Omówienie podstaw wirtualizacji
2. Instalacja oprogramowania hostów
3. Instalacja klastra wirtualizacji
4. Konfigurowanie hostów wirtualizacji i klastra wirtualizacyjnego
5. Zarządzanie klastrem wirtualizacji za pomocą centralnej konsoli
6. Konfigurowanie i zarządzanie siecią w systemie wirtualizacji
7. Konfigurowanie i zarządzanie pamięcią masową w klastrze
8. Wdrażanie maszyn wirtualnych
9. Zarządzanie wirtualnymi maszynami
10. Konfiguracja kopii bezpieczeństwa
11. Monitorowanie usług w klastrze wirtualizacyjnym

Wykonawca zapewni:

- szkolenie w języku polskim,
- materiały w języku polskim lub angielskim,
- szkolenie i materiały odnoszące się do aktualnej wersji systemu wirtualizacji
- szkolenie prowadzone może być w formie kursu on-line lub w siedzibie Wykonawcy
- w przypadku szkolenia w siedzibie Wykonawcy Wykonawca zapewni wyżywienie i ewentualne noclegi
- po szkoleniu musi być możliwość podejścia do certyfikowanego egzaminu

Ukończenie szkolenia da uczestnikowi następujące umiejętności i wiedzę:

- Instalację oraz konfigurację hostów
- Wdrożenie i skonfigurowanie konsoli centralnej
- Używanie klienta do tworzenia zasobów i przypisywania ról użytkownikom
- Skonfigurowanie wysokiej dostępności hostów VM i konsoli
- Tworzenie i konfigurowanie sieci wirtualnej przy użyciu standardowych i rozproszonych przełączników
- Tworzenie i konfigurowanie datastorów przy użyciu technologii pamięci masowej
- Tworzenia maszyn wirtualnych, template'ów, klonów i migawek
- Skonfigurowanie repozytorium tools'ów i zarządzanie nim
- Tworzenie content library do zarządzania template'ami i deploy'u maszyn wirtualnych
- Zarządzanie wykorzystaniem zasobów maszyny wirtualnej
- Migrowanie maszyn wirtualnych
- Zarządzanie update'ami, aby aktualizować Konsolę, hosty i maszyny wirtualne
- Skonfigurowanie i zarządzanie siecią i pamięcią masową dla dużego i zaawansowanego przedsiębiorstwa
- Używanie profili hosta do zarządzania zgodnością hosta
- Monitorowanie wydajności Konsoli, hostów i maszyn wirtualnych.

Szkolenie specjalistyczne – Audytor Wiodący ISO 27001

Zamawiający wymaga aby w ramach szkoleń, Wykonawca przeszkolił jednego pracownika Zamawiającego w zakresie audytora wiodącego Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001. Zakres szkolenia musi obejmować teoretyczne i praktyczne przygotowanie pracownika do egzaminu i dalszej samodzielnej pracy jako Audytor Wiodący ISO27001 zgodnie z normą PN-EN ISO/IEC 27001:2023-08 lub nowsza obowiązującą w momencie składania oferty.

W ramach szkolenia Zamawiający wymaga aby Wykonawca przeprowadził certyfikację (egzamin zakończony wydaniem certyfikatu imiennego) przeszkolonego pracownika w zakresie Audytora wiodącego wg. ISO 27001.

Szkolenie musi być prowadzone w języku polskim.

Wykonawca zapewni materiały, nocleg i wyżywienie na okres szkolenia.

Opracowanie / aktualizacja dokumentacji SZBI

Zakres prac:

1) Aktualizacja lub opracowanie (w przypadku braku dokumentu) dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwanej „SZBI”), w skład której wchodzi następujące dokumenty:

- a) Polityka Bezpieczeństwa Informacji;
- b) Polityka ochrony danych osobowych;
- c) Instrukcja zarządzania systemem informatycznym;
- d) Polityka zarządzania ciągłością działania;
- e) Procedura zarządzania incydentami cyberbezpieczeństwa;
- f) Analiza ryzyka w zakresie Bezpieczeństwa Informacji;

2) Wdrożenie SZBI w jednostkach we współpracy z kierownikami jednostek lub osobami wyznaczonymi do wdrożenia SZBI,

3) 24 roboczogodziny konsultacji realizowanych w ramach doradztwa przy oraz po wdrożeniu dokumentacji SZBI (zakres ten może ulec zwiększeniu w zależności od potrzeb w ramach realizacji zamówienia)

4) W ramach dokumentacji SZBI ujęte zostaną następujące procedury:

- a) procedury korzystania z urządzeń mobilnych
- b) procedury pracy zdalnej
- c) postępowanie z nośnikami
- d) procedury kontroli dostępu
- e) zabezpieczenie pomieszczeń i obiektów
- f) procedury czystego biurka
- g) procedury czystego ekranu
- h) procedury kopii zapasowych
- i) procedury ochrony logów
- j) bezpieczeństwo komunikacji
- k) zarządzanie bezpieczeństwem sieci
- l) przesyłanie informacji
- m) plany ciągłości działania
- n) procedury zarządzania incydentami
- o) prywatność i ochrona danych osobowych
- p) szacowanie ryzyka w obszarze bezpieczeństwa informacji
- q) szkolenia personelu

Zamawiający wymaga opracowania/aktualizacji i wdrożenia SZBI w:

- Urząd Gminy Piecki
- Gminy Ośrodek Pomocy Społecznej w Pieckach
- Środowiskowy Dom Pomocy w Pieckach
- Zespół Obsługi Placówek Oświatowych w Pieckach

Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zamawiającego i wdrażanej jednostki w oparciu o wzajemne ustalenia dokonane we współpracy pomiędzy Stronami

na etapie analizy wstępnej oraz wszelkich innych informacji uzyskanych przez Wykonawcę w trakcie realizacji Umowy mogących mieć wpływ na treść dokumentacji. Usługi dotyczące czynności wdrażających dokumentację zostanie uznana za wykonaną po przekazaniu Zleceniodawcy przez Zleceniobiorcę całości dokumentacji SZBI i podpisaniu protokołu odbioru przez Zamawiającego.