

Sprawa nr ZK-TOS.252.5.2026

Opis Przedmiotu Zamówienia

„Wzmocnienie systemu cyberbezpieczeństwa w Zakładzie Komunalnym w Dębem Wielkim”

*W ramach projektu „Cyberbezpieczne Wodociągi”
C3.1.1. Cyberbezpieczeństwo - CyberPL
Krajowy Plan Odbudowy i Zwiększania Odporności*

Zamawiający:
Zakład Komunalny w Dębem Wielkim
ul. Zielona 3,
05-311 Dębe Wielkie
NIP: 8222278065

Spis treści

Wstęp	3
Ogólny zarys projektu	3
Wymagania ogólne	3
Wymagania dot. wdrożenia	3
Równoważność	4
Zakup i wdrożenie sprzętu oraz oprogramowania.....	6
Serwery pod rozwiązania bezpieczeństwa – 1 kpl.....	6
Serwery do wykonywania kopii zapasowych – 2 szt.	14
Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa – 2 szt.	15
Zarządzalny switch szkieletowy - 1 szt.	15
Zarządzalny switch dostępowy – 1 szt.	17
Zarządzalne switchy dostępowe z PoE – 2 szt.	18
Oprogramowanie typu EDR /XDR – 20 szt.....	20
Zestaw urządzeń do magazynowania i zarządzania energią elektryczną – 1 kpl.	25
NGFW z licencją UTM – 1 szt.	28
Sprzętowe sondy/sensory do monitorowania sieci OT – 1 kpl.	33
Instruktaże	37
Gwarancja.....	37
Instalacja i konfiguracja dostarczonych systemów	37
Przygotowanie i dostarczenie dokumentacji powykonawczej.....	39
Procedura odbioru przedmiotu zamówienia	40

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 oraz niezbędnych szkoleń. 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. Wykonawca może zaoferować rozwiązania równoważne spełniające minimum opisane w OPZ.

Ogólny zarys projektu

Celem projektu jest kompleksowe wdrożenie nowoczesnych systemów zabezpieczeń infrastruktury i danych Zamawiającego (tj. zaprojektowanie, dostarczenie, zainstalowanie, uruchomienie i przeszkolenie). Zamawiający oczekuje dostarczenia systemów informatycznych, uruchomienia (w tym instalacja i parametryzacja), przeprowadzenia instruktażu personelu oraz zapewnienie usługi utrzymania dostarczonych systemów.

Zamawiający wymaga aby w efekcie realizacji projektu powstała infrastruktura serwerowa odporna na awarie pojedynczych elementów (HA). W tym celu zamierza zainstalować serwery pracujące w klastrze wirtualizacyjnym, przechowującym dane na szybkiej pamięci sieciowej.

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.

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 2004, Nr 229, poz. 2315 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 i/lub ofercie nie wyszczególniono inaczej.

Przez gwarancję Zamawiający rozumie utrzymanie prawidłowego działania w okresie gwarancji wszystkich funkcjonalności opisanych w OPZ i dostarczonych przez Wykonawcę.

Wymagania dot. wdrożenia

1. Wykonawca po podpisaniu umowy, a przed przystąpieniem do prac wdrożeniowych, musi dokonać analizy przedwdrożeniowej (uwzględniając: potwierdzenie stanu istniejącego i przeprowadzenie inwentaryzacji wdrożeniowej) i potwierdzić zgodność opisanych w niniejszym OPZ rozwiązań z możliwym wdrożeniem uwzględniając specyfikę działalności Zamawiającego.
2. Wykonawca dokona instalacji, konfiguracji, parametryzacji i integracji dostarczanego sprzętu i oprogramowania.

3. 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.
4. 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.
5. 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.
6. 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.
7. Wykonawca przygotowuje dokumentację powdrożeniową wdrażanego oprogramowania wymaganą w SWZ i załącznikach tj. instrukcje, procedury, opisy, itd.
8. Wykonawca po zakończeniu wdrożenia przekaze Zamawiającemu wszystkie konta i hasła administracyjne do każdego elementu dostarczanego oprogramowania oraz bazy danych.
9. 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,
 - c) spełniać wymagania określone we wniosku o dofinansowanie (zwłaszcza w zakresie wskaźników projektu).

Równoważność

1. Jeżeli dokumentacja przetargowa (SWZ z załącznikami) wskazywałaby w odniesieniu do niektórych materiałów lub urządzeń znaki towarowe, patenty lub pochodzenie, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, Zamawiający zgodnie z art. 99 ust. 5 ustawy Pzp dopuszcza oferowanie materiałów lub urządzeń równoważnych.
2. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry techniczne, eksploatacyjne, użytkowe, jakościowe i funkcjonalne jakimi muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego.
3. Pod pojęciem „minimalne parametry techniczne, eksploatacyjne, użytkowe, jakościowe i funkcjonalne”, Zamawiający rozumie wymagania dotyczące materiałów lub urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów itp.
4. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania.
5. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretnych produktów przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach technicznych, eksploatacyjnych, użytkowych, jakościowych i funkcjonalnych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Oznacza, że wskazaniom tym towarzyszą wyrazy „lub równoważny”.
6. W sytuacji, gdyby dokumentach opisujących przedmiot zamówienia, zawarto odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów

referencji technicznych, a takim odniesieniem nie towarzyszyło wyrażenie „lub równoważne”, to Zamawiający dopuszcza rozwiązanie równoważne opisywanym w każdej normie, europejskiej ocenie technicznej, aprobacie, specyfikacji technicznej, systemowi referencji technicznych. W związku z powyższym należy przyjąć, że każdej normie, europejskiej ocenie technicznej, aprobacie, specyfikacji technicznej, systemowi referencji technicznych występujących w opisie przedmiotu zamówienia towarzyszą wyrazy „lub równoważne”.

8. Kryteria stosowane w celu oceny równoważności:

Wykonawca, który powołuje się na rozwiązania równoważne, jest zobowiązany wykazać w ofercie, że oferowane przez niego rozwiązanie, spełnia wymagania określone przez Zamawiającego.

W takim przypadku Wykonawca zobowiązany jest:

- a) podać w ofercie – Poprzez wypełnienie tabeli pod nazwą: „Wykaz materiałów i urządzeń równoważnych oraz rozwiązań równoważnych”, znajdującej się na Formularzu oferty, podając: Nazwę (typ, rodzaj) materiału/urządzenia lub/oraz opis rozwiązania (norma, europejska ocena techniczna, aprobata, specyfikacja techniczna, system referencji technicznej) oryginalnego: (wynikających z dokumentacji) oraz nazwę (typ, rodzaj) materiału/urządzenia równoważnego lub/oraz opis rozwiązania równoważnego (norma, europejska ocena techniczna, aprobata, specyfikacja techniczna, system referencji technicznej), a także podać nazwę producenta materiału/urządzenia równoważnego;
- b) Przedłożyć wraz z ofertą odpowiednie dokumenty (w języku polskim) np. karty techniczne, karty katalogowe producenta, wymagane przepisami prawa certyfikaty, inne dokumenty, opisujące techniczne parametry zaoferowanych materiałów i urządzeń równoważnych, lub/oraz inne dokumenty dotyczące norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, pozwalające jednoznacznie stwierdzić, że są one rzeczywiście równoważne.
- c) Równoważność pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów technicznych nie gorszych od założonych w niniejszej SWZ. W przypadku niewskazania przez Wykonawcę w ofercie rozwiązania równoważnego, Zamawiający uzna, iż Wykonawca będzie realizował przedmiot zamówienia zgodnie z rozwiązaniami wskazanymi w SWZ i jej załącznikach.
- d) Zastosowane materiały i urządzenia winny być dopuszczone do obrotu i stosowania na terenie RP.

Uwaga:

W przypadku niedostarczenia odpowiednich dokumentów pozwalających jednocześnie stwierdzić, że oferowane produkty i/lub systemy są rzeczywiście równoważne, wskutek czego Zamawiający nie będzie w stanie stwierdzić rzeczywistej równoważności, Zamawiający uzna treść oferty Wykonawcy za nieopowiadającą treści SWZ, a tym samym, oferta Wykonawcy zostanie odrzucona.

Zakup i wdrożenie sprzętu oraz oprogramowania

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 specyfikacji zaoferowanego przez Wykonawcę rozwiązania - Wykonawca musi go dostarczyć w ramach złożonej oferty.

Serwery pod rozwiązanie bezpieczeństwa – 1 kpl.

Przedmiotem zamówienia jest zestaw składający się z 2 szt. serwerów przeznaczonych pod rozwiązanie bezpieczeństwa.

Wymagania:

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków 3,5".
2. Serweru wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
3. Serwery muszą być dostarczone wraz z przednim panelem zamykanym na klucz, zabezpieczającym dyski przed nieuprawnionym wyjęciem.
4. Płyta główna z możliwością zainstalowania do dwóch procesorów.
5. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
6. Zainstalowany procesor min. 16-rdzeniowy o taktowaniu min. 2.8GHz (base frequency) umożliwiający osiągnięcie w teście SPECrate2017_fp_base wyniku min. 500 pkt. w konfiguracji dwuprocesorowej dla oferowanego serwera.
7. Pamięć RAM min. 128 GB RAM DDR5 RDIMM 5600MT/s w kościach po min. 32 GB.
8. Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM.
9. Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200.
10. Wbudowane porty:
 - a. 4 porty USB z czego nie mniej niż 1 port USB 3.x na przednim panelu obudowy, 2 porty USB 3.x na tylnym panelu obudowy oraz 1 port USB na płycie głównej.
 - b. Złącze 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.
 - c. 1 port VGA na tylnym panelu obudowy.
 - d. Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
11. Minimum 3 aktywne sloty PCI-E 5.0 x16.
12. Zainstalowane i w pełni funkcjonalne interfejsy sieciowe:
 - a. minimum 1 x RJ-45 Ethernet management port,
 - b. minimum 2 porty 10Gb/s Ethernet w standardzie SFP+ wraz z odpowiednimi wkładkami optycznymi SFP+ Multimode,
 - c. minimum 4 porty 1Gb/s Ethernet w standardzie Base-T.
13. Zainstalowane 2 dyski serwerowe SSD SATA Read-Intensive o pojemności min. 480GB każdy.
14. Zainstalowane 5 dysków serwerowych HDD SATA o pojemności min. 8 TB każdy.
15. Zainstalowany sprzętowy kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 10, 5, 50. Kontroler wyposażony w 4GB Cache i podtrzymanie bateryjne. Kontroler powinien posiadać wsparcie dla dysków SAS oraz SATA.
16. Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo.
17. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).

18. Dwa identyczne zasilacze o mocy min. 1500W klasy Titanium zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera. W komplecie z zasilaczami należy dostarczyć kable zasilające o długości min. 2m.
19. Bezpieczeństwo:
 - a. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
 - b. Moduł TPM 2.0.
20. Serwer wyposażony w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający:
 - 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.
21. Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca:
 - 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. wsparcie 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.
22. Wraz z serwerami 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:
 - 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 i pamięci, które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów.
 - d. dalsze 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.

23. Wraz z serwerami wymagane jest dostarczenie licencji na serwerowy system operacyjny wspierający rozwiązanie do cyberbezpieczeństwa (najnowsza wersja dostępna w dniu składania ofert) na 4 maszyny wirtualne w każdym z serwerów w ilości pokrywającej zapotrzebowanie na wszystkie fizyczne rdzenie procesorów w serwerach pod rozwiązania bezpieczeństwa oraz z licencjami dostępowymi na 20 urządzeń na cały zestaw. Wymagania dotyczące rozwiązania – oprogramowanie musi spełniać co najmniej wymagania:

- a. Oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzicznego użytkowanego aktualnie przez Zamawiającego oraz pełną współpracę z Active Directory. Licencja zostanie wykorzystana do uruchomienia oprogramowania na serwerze zakupionym w ramach niniejszego postępowania.
- b. Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.
- c. Licencja bez ograniczeń czasowych.
- d. Instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym;
- e. Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych);
- f. Wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB;
- g. Obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu;
- h. Praca w roli klienta domeny Microsoft Active Directory;
- i. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory;
- j. Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP);
- k. Zawarta możliwość uruchomienia roli serwera DNS;
- l. Możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
- m. Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP);
- n. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
- o. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
- p. Zawarta możliwość uruchomienia roli serwera stron WWW;
- q. Zawarta funkcjonalność szyfrowania dysków
- r. Dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera;
- s. W ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego;
- t. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów);
- u. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
- v. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;

- w. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
 - x. Obsługa zdalnego pulpitu;
 - y. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
 - z. Obsługa PowerShell 4.0;
 - aa. Obsługa WiFi i Bluetooth;
 - bb. Możliwość współdzielenia zasobów GPU między hostami.
24. Razem z zestawem serwerów należy dostarczyć system bezpieczeństwa informatycznego, który integruje różnorodne funkcje monitorowania, analizy oraz reakcji na zagrożenia w celu kompleksowej ochrony infrastruktury IT. System musi bazować na nowoczesnych technologiach klasy SIEM (Security Information and Event Management), a także umożliwia holistyczne podejście do bezpieczeństwa oraz zarządzanie incydentami w sposób wysoce zautomatyzowany i skalowalny. Zamówienie obejmuje dostawę licencji wieczystej. Zakres funkcjonalny:
- a. System musi gromadzić dane z różnorodnych źródeł, takich jak:
 - i. Logi systemowe (systemów operacyjnych, serwerów, aplikacji, urządzeń sieciowych).
 - ii. Informacje o zdarzeniach (np. próby logowania, zmiany uprawnień, działania użytkowników).
 - iii. Dane dotyczące konfiguracji infrastruktury IT (np. plików konfiguracyjnych, polityk bezpieczeństwa).
 - b. System musi automatycznie analizować te dane w czasie rzeczywistym, identyfikując potencjalne zagrożenia oraz anomalie na podstawie wcześniej zdefiniowanych reguł, sygnatur oraz zaawansowanych algorytmów analitycznych.
 - c. Ciągłe monitorowanie stanu bezpieczeństwa w czasie rzeczywistym. System musi umożliwiać:
 - i. Wczesne wykrywanie zagrożeń: Wykorzystanie analizy behawioralnej oraz sztucznej inteligencji do identyfikacji nietypowych zachowań użytkowników, urządzeń i aplikacji.
 - ii. Pełna widoczność nad wszystkimi elementami infrastruktury IT, w tym także nad środowiskami wirtualnymi i chmurowymi.
 - iii. Analiza historyczna zdarzeń: System musi umożliwiać retrospektywne badanie logów i zdarzeń, co jest niezbędne do dochodzeń powłamanionych i audytów bezpieczeństwa.
 - d. System musi posiadać zaawansowane wykrywanie zagrożeń w różnych środowiskach, takich jak:
 - i. Środowiska chmurowe (AWS, Azure, Google Cloud).
 - ii. Kontenery (Docker, Kubernetes).
 - iii. Urządzenia końcowe.
 - e. Oraz rozszerzać możliwości SIEM, pozwalając na:
 - i. Skoordynowane wykrywanie zagrożeń w całym środowisku IT.
 - ii. Szybkie reagowanie na incydenty dzięki integracji z innymi narzędziami do zarządzania i automatyzacji (np. firewalle, narzędzia do zarządzania zasobami IT).
 - iii. Automatyzację działań naprawczych, co redukuje czas reakcji na zagrożenia oraz minimalizuje ryzyko.
 - f. System musi wspierać zarządzanie incydentami bezpieczeństwa poprzez:

- i. Automatyczne powiadomienia o wykrytych zagrożeniach, pozwalające administratorom na szybkie podjęcie działań.
 - ii. Raportowanie incydentów z pełnym zestawem informacji potrzebnych do analizy i dalszych działań naprawczych.
 - iii. Korelowanie zdarzeń z różnych źródeł w celu lepszego zrozumienia zagrożeń i zidentyfikowania ich źródła.
 - g. System musi pomagać organizacji w utrzymywaniu zgodności z regulacjami prawnymi i standardami bezpieczeństwa poprzez:
 - i. Monitorowanie działań użytkowników i zapis zmian w systemach, co pozwala na śledzenie operacji oraz wykrywanie nieautoryzowanych działań.
 - ii. Automatyczne generowanie raportów audytowych i zgodności, które można przedstawić audytorom oraz organom nadzoru.
 - iii. Tworzenie alertów zgodności, które informują o potencjalnych naruszeniach polityk bezpieczeństwa.
 - h. System musi oferować wysoką skalowalność oraz zapewniać integrację z szeroką gamą innych rozwiązań i narzędzi używanych w ramach zabezpieczeń IT.
25. Razem z zestawem serwerów należy dostarczyć system monitoringu infrastruktury IT.

Wymagania:

- a. Architektura
 - i. Licencja: Oprogramowanie musi być rozwiązaniem opartym na licencji wieczystej. Zamawiający doszcza rozwiązanie na licencji open-source, wolnym od kosztów licencyjnych z góry (np. na licencji AGPLv3).
 - ii. Architektura rozproszona: System musi pozwalać na poziome skalowanie poprzez wdrażanie nielimitowanej liczby serwerów pośredniczących (proxy). Oprogramowanie to powinno umożliwiać monitorowanie zasobów w odizolowanych sieciach lokalnych, za zaporami sieciowymi oraz kompresować ruch przesyłany do serwera centralnego.
 - iii. Odporność na awarie (HA): Architektura musi wspierać Wysoką Dostępność (High Availability) zarówno dla serwera backendowego, jak i wielu instancji interfejsu webowego, zapewniając automatyczne równoważenie obciążenia (Load Balancing).
 - iv. Zarządzanie danymi: Rozwiązanie musi pozwalać na definiowanie zróżnicowanych polityk retencji danych, pozwalających na niezależne określanie czasu przechowywania np. dokładnych danych historycznych (np. 6 miesięcy) i danych zagregowanych/trendów (np. 2 lata).
- b. Gromadzenie danych i monitorowanie środowiska
 - i. Elastyczność odpytowania: System musi wspierać monitorowanie oparte o agentów dla wielu systemów operacyjnych (Linux, Windows, macOS, BSD, AIX, Solaris) z możliwością zbierania danych w trybie aktywnym (push) i pasywnym (pull).
 - ii. Monitorowanie bezagentowe: Możliwość pozyskiwania metryk z wykorzystaniem branżowych standardów i protokołów takich jak: SNMP, IPMI, SSH, Telnet, ODBC, ICMP, PromQL (Prometheus), Java JMX, Modbus oraz MQTT.
 - iii. Monitorowanie syntetyczne i aplikacyjne: Rozwiązanie musi umożliwiać konfigurację wielokrokowych scenariuszy opartych na przeglądarce w celu emulacji rzeczywistych transakcji użytkowników, jak również umożliwiać monitorowanie endpointów HTTP/HTTPS i interfejsów API.
 - iv. Transformacja danych: System musi być w stanie na bieżąco normalizować i optymalizować napływające dane (np. wykorzystując wyrażenia regularne,

- JSONPath, XPath, konwersję CSV do JSON, zliczanie różnic lub skrypty JavaScript).
- v. Gotowe wsparcie dla chmur i virtualizacji: Rozwiązanie musi zapewniać automatyczne wykrywanie i monitorowanie środowisk kontenerowych (Kubernetes, Docker), chmurowych (AWS, Azure, GCP) oraz środowisk wirtualnych (VMware, m.in. maszyny gości, hypervisory, datastores).
- c. Wykrywanie problemów i analiza biznesowa
- i. Zaawansowane progi alarmowe: Oprogramowanie musi umożliwiać elastyczne zdefiniowanie progów powiadamiania przy użyciu wielu poziomów krytyczności, z wykorzystaniem predykcji trendów i wykrywania anomalii w oparciu o bieżącą analizę danych historycznych (tzw. baseline).
 - ii. Korelacja i analiza przyczyn (Root Cause Analysis): System musi dostarczać mechanizmy pozwalające odseparować pierwotną przyczynę awarii od zdarzeń pochodnych (symptomów), zapobiegając nadmiarowi powiadomień powiązanych ze sobą urządzeń.
 - iii. Monitorowanie usług biznesowych (SLA): Obliczanie faktycznej dostępności i przestojów dla usług biznesowych z użyciem hierarchicznych drzew zależności i wag przypisanych do składowych infrastruktury.
- d. Powiadamianie i automatyzacja działań naprawczych
- i. Wielokanałowe komunikaty: System powinien domyślnie pozwalać na przekazywanie alertów poprzez pocztę e-mail, bramki SMS, webhooki, komunikatory (np. Slack, MS Teams) i zapewniać integrację z popularnymi platformami ITSM (np. ServiceNow, Jira).
 - ii. Złożone schematy eskalacji: Możliwość definiowania wielostopniowych procesów, w tym powiadomień opóźnionych, cyklicznych przypomnień do momentu rozwiązania problemu oraz powiadomień przypisanych do różnego szeregu pracowników w zależności od czasu trwania awarii.
 - iii. Automatyczne działania naprawcze (Auto-remediation): Możliwość zdalnego i automatycznego egzekwowania skryptów lub poleceń na urządzeniach (np. zrestartowanie usługi) bezpośrednio w odpowiedzi na wykrytą anomalię.
- e. Wizualizacja i mapowanie topologii
- i. Dashboards: Możliwość personalizacji wielostronicowych kokpitów w oparciu o widżety prezentujące wykresy, statusy problemów czy usługi SLA, ze wsparciem metody przeciągnij-i-upuść.
 - ii. Interaktywne mapy i zagnieżdżanie: System musi pozwolić na rysowanie map topologii infrastruktury IT uwzględniających stan poszczególnych elementów w czasie rzeczywistym. Wymagana jest możliwość tworzenia struktury zagnieżdżonych pod-map do łatwiejszej nawigacji po systemie.
 - iii. Raportowanie cykliczne: Mechanizm pozwalający na generowanie i regularne (dziennie, tygodniowe, miesięczne) wysyłanie raportów z podsumowaniem stanu infrastruktury w formacie PDF bezpośrednio na skrzynki e-mail.
- f. Wymagania z zakresu bezpieczeństwa (Security & Access Control)
- i. Szyfrowanie i uwierzytelnianie: Wsparcie dla szyfrowania ruchu wewnątrz platformy monitorującej za pomocą certyfikatów lub uwierzytelnienia PSK. Uwierzytelnianie operatorów musi integrować się z usługami katalogowymi (LDAP, Active Directory), wykorzystywać SAML/SSO oraz zapewniać autoryzację wieloskładnikową (MFA/TOTP).
 - ii. Wielodostęp (Multi-tenancy) i autoryzacja: System musi oferować zaawansowany system praw i przypisywania ról oparty na

odczyt/zapis (Read/Write/Deny) lub pozwalających wyizolować widoczność elementów (np. do celów udostępnienia wglądu zewnętrznym klientom - tenants).

- iii. Ochrona poświadczeń: Obsługa zewnętrznych magazynów haseł (tzw. Secret Vault, np. CyberArk, HashiCorp), aby poufne informacje o uwierzytelnianiu nie były przechowywane w systemie i nie mogły być odzyskane za pomocą interfejsu API.
- iv. Audyt: Rejestr audytowy (Audit log) przechowujący wszystkie zmiany w konfiguracji przypisane do wprowadzającego użytkownika i adresu IP z opcją eksportu logów.

g. Automatyzacja zarządzania i wdrażania

- i. Automatyczne wykrywanie sieci (Discovery): System z wbudowanym silnikiem skanowania adresacji IP oraz z automatycznym tworzeniem progów alarmowych, wskaźników lub wykresów po podłączeniu odpowiedniego zasobu do sieci.
- ii. Zarządzanie API: System musi posiadać otwarty interfejs (JSON RPC API), do pełnego, zautomatyzowanego sterowania procesami wdrażania konfiguracji czy też w celu eksportu i strumieniowania danych z systemu monitorowania.

26. Razem z zestawem serwerów należy dostarczyć system klasy ITSM (IT Service Management) oraz ITAM (IT Asset Management). Narzędzie ma na celu usprawnienie obsługi zgłoszeń użytkowników, kompleksową inwentaryzację infrastruktury sprzętowej oraz oprogramowania, a także optymalizację procesów zarządzania usługami IT. System musi charakteryzować się modułową budową, zapewniającą pełną integrację procesów wsparcia użytkowników z ewidencją zasobów IT. Wymagane jest wdrożenie następujących obszarów funkcjonalnych:

a. Zarządzanie Zasobami i Baza CMDB (Asset Management)

- i. Inwentaryzacja sprzętu i oprogramowania: Automatyczna oraz manualna ewidencja stacji roboczych i serwerów (w tym systemów operacyjnych, wersji, numerów seryjnych, statusów, lokalizacji i przypisanych użytkowników), monitorów, urządzeń sieciowych (przełączników, routerów, zapór sieciowych), drukarek i urządzeń peryferyjnych, a także telefonów i kart SIM.
- ii. Zarządzanie licencjami: Rejestrowanie posiadanych licencji i ich wersji z możliwością ścisłego powiązania ich z oprogramowaniem zainstalowanym na zasobach.
- iii. Fizyczna i pasywna struktura sieci: Śledzenie urządzeń pasywnych, okablowania (identyfikacja łączonych elementów) oraz materiałów eksploatacyjnych.
- iv. Graficzne zarządzanie centrum danych: Możliwość odwzorowania struktury fizycznej serwerowni, w tym graficzny układ budynków, pomieszczeń oraz szaf rackowych (front/tył) wraz z zarządzaniem zasilaniem (PDUs) i okablowaniem.
- v. Automatyczna kontrola unikalności: Blokowanie dodawania duplikatów urządzeń na podstawie unikalnych pól (np. numerów seryjnych) przy rejestracji ręcznej i automatycznej.

b. Obsługa Zgłoszeń i Wsparcie Użytkowników (Helpdesk)

- i. Zarządzanie Incydentami i Wnioskami (Tickets): Podział zgłoszeń na incydenty oraz wnioski o usługi, przypisywanie ich do odpowiednich grup lub osób, priorytetyzacja (wpływ, pilność) oraz definiowanie poziomów obsługi (SLA) i eskalacji.

- ii. Zarządzanie Problemami i Zmianami (Problems & Changes):
Rejestrowanie problemów w celu identyfikacji przyczyn źródłowych oraz planowanie, harmonogramowanie i budżetowanie zmian w infrastrukturze IT.
 - iii. Automatyzacja i cykliczność: Możliwość definiowania powtarzalnych (rekurencyjnych) zgłoszeń i zmian (np. cotygodniowe zadania konserwacyjne).
 - iv. Formularze i portal samoobsługowy: Dostęp do bezpłatnego interfejsu samoobsługowego dla użytkowników końcowych oraz kreator spersonalizowanych formularzy zgłoszeniowych.
 - v. Integracja z pocztą e-mail: Automatyczne przekształcanie wiadomości przychodzących na skrzynki e-mail w zgłoszenia serwisowe w systemie.
 - c. Zarządzanie Finansami i Kontraktami (Management)
 - i. Budżetowanie i dostawcy: Rejestrowanie budżetów powiązanych z zasobami i asystą techniczną, zarządzanie bazą dostawców oraz kontaktami zewnętrznymi.
 - ii. Umowy i domeny: Ewidencja i monitorowanie umów wsparcia IT (okresy rozliczeniowe, czas reakcji), domen internetowych oraz certyfikatów SSL (z automatyczną kontrolą dat ważności).
 - d. Narzędzia Organizacyjne i Pomocnicze (Tools)
 - e. Zarządzanie projektami: Planowanie zadań dla zespołów z wizualizacją w formie wykresu Gantta lub tablicy Kanban.
 - f. Baza wiedzy: Centralny rejestr wiedzy wewnętrznej oraz publiczne FAQ dla użytkowników w celu ułatwienia samodzielnego rozwiązywania prostych problemów.
 - g. Rezerwacja zasobów: Moduł pozwalający na rezerwację sprzętu współdzielonego przez użytkowników.
27. Zgodność z normą ISO 9001, ISO 14001, ISO 27001 oraz ISO 50001 lub równoważnymi.
28. Serwer musi posiadać deklarację CE.
29. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
30. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
31. Gwarancja:
- a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem producenta na terenie RP.
 - b. Urządzenie objęte minimum 36-miesięcznym okresem gwarancji w trybie On-Site z gwarantowanym czasem reakcji najpóźniej Next Business Day od momentu zgłoszenia usterki.
 - c. Uszkodzone dyski zostają u Zamawiającego.
 - d. Zamawiający dopuszcza realizację gwarancji przez autoryzowanego partnera serwisowego producenta.
 - e. 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.
 - f. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta

oferowanego serwera, że wymagany poziom serwisu z wymaganym SLA został zaoferowany na potrzeby oferty w niniejszym postępowaniu.

- g. Na wezwanie Zamawiającego Wykonawca musi dostarczyć 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.
- h. 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.

Serwery do wykonywania kopii zapasowych – 2 szt.

Przedmiotem zamówienia są 2 szt. serwerów do przechowywania danych.

Wymagania:

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 zatokami na dyski SATA HDD i SSD o wielkości 3,5 cala oraz 2,5 cala.
2. Serwer wraz z kompletem szyn umożliwiających montaż w szafie rack.
3. Zainstalowany 1 procesor klasy x86 min. 4-rdzeniowy o taktowaniu min. 2.2GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 4 400 pkt. Wynik testów dla oferowanego modelu procesora należy dołączyć do oferty.
4. Pamięć RAM min. 32 GB RAM DDR4
5. Wbudowane porty min. 2 porty USB 3.2.
6. Powyższe porty USB nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
7. Min. 1 aktywny slot PCI-E 3.0 x8 umożliwiający instalację dodatkowych kart rozszerzeń, takich jak karty sieciowe, karty SSD NVMe lub inne, które mogą zwiększyć funkcjonalność i wydajność systemu.
8. Zainstalowane i w pełni funkcjonalne minimum 2 porty 2.5GbE RJ45. Porty nie mogą zajmować slotów PCI-E
9. Kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 5, 6, 10.
10. Zainstalowane min. 5 dysków HDD SATA o pojemności min. 8 TB każdy.
11. Min. 2 wentylatory.
12. Min. 2 zasilacze o mocy min. 550W, zainstalowane wewnątrz serwera, pracujące redundantnie w celu zapewnienia ciągłości pracy w przypadku awarii jednego z nich.
13. Urządzenie powinno oferować zaawansowane funkcje zabezpieczeń, takie jak szyfrowanie AES-NI.
14. Diody LED umieszczone z przodu obudowy serwera informujące o statusie: dysków i zasilaniu.
15. Wraz ze serwerem dostarczone powinno być oprogramowanie do tworzenia kopii zapasowych i odzyskiwania danych komputerów, serwerów i maszyn wirtualnych w środowiskach wirtualizacyjnych. Oprogramowanie powinno zapewniać pełne bezpieczeństwo danych, niezawodność, oraz wsparcie dla popularnych platform wirtualizacji. Wymagania:
 - a. Zaawansowane funkcje tworzenia kopii zapasowych

- b. Ochrona integralności danych oraz infrastruktury IT
 - c. Natychmiastowe odzyskiwanie po awarii
 - d. Deduplikacja
 - e. Szyfrowanie i kompresja
 - f. Statystyki użycia
 - g. Wstrzymywanie i wznowianie tworzenia kopii zapasowych
16. Zgodność z normą ISO 9001 oraz ISO 14001 lub równoważnych.
17. Serwer musi posiadać deklarację CE.
18. Zainstalowany specjalistyczny system operacyjny przeznaczony dla serwerów do przechowywania danych.
19. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
20. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta.
21. Serwer musi być kompatybilny z popularnymi systemami backupu oraz oprogramowaniem do wirtualizacji.
22. Gwarancja:
- a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP.
 - b. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji.
 - c. Zamawiający dopuszcza realizację gwarancji przez autoryzowanego partnera serwisowego producenta.
 - d. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/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.
 - e. 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,

Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa – 2 szt.

Zamawiający wymaga dostarczenia i instalacji zgodnie z warunkami producenta 2 szt. szafy RACK, spełniającej poniższe parametry:

Szafa serwerowa stojąca o łącznym udźwigu min. 750 kg, wysokości min. 42U oraz głębokości przystosowanej do instalacji oferowanych urządzeń.

- Szafa musi być wyposażona w przednie drzwi z zamkiem, z możliwością montażu prawostronnego lub lewostronnego.

- Szafa musi posiadać zdejmowane boczne panele z zamkami w zestawie i tylne stalowe drzwi z zamkiem.

- Szafa musi być możliwość wprowadzenia okablowania poprzez zamykany górny i dolny panel z zaślepkami w zestawie.

- W zestawie z szafą musi znajdować się panel wentylacyjny z min. 2 wentylatorami 230V.

Zarządzalny switch szkieletowy - 1 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja przełącznika szkieletowego klasy Enterprise.

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. minimum jeden zasilacz 230V AC
 - d. zakres temperatur pracy ciągłej co najmniej od -5 do +45 °C
 - e. zakres wilgotności pracy co najmniej 5% - 95%
3. Przełącznik musi zostać dostarczony z następującymi interfejsami mogącymi działać równocześnie:
 - a. 24 porty 10/100/1000M BASE-T
 - b. 16 portów 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 10G-ER
 - c. 8 portów 25G SFP28
 - d. 2 porty 40G/100G QSFP28
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 z magistralą stackującą o wydajności minimum 300Gb/
 - c. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
 - d. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
7. Zamawiający dopuszcza aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink.
8. Układ przełączający o wydajności min. 1,5 Tbps,
9. Wydajność przełączania przynajmniej 1100 Mpps,
10. Obsługa min. 64 000 adresów MAC
11. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
12. Obsługa 802.1x
13. Obsługa MACsec
14. Obsługa M-LAG
15. Obsługa protokołu BFD oraz LACP
16. Obsługa protokołu VRRP
17. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
18. Obsługa protokołów routingu OSPF, OSPFv3, IS-IS, IS-ISv6, BGP, BGPv4+, RIP, RIPng, PIM-SM, PIM-DM i SSM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
19. Obsługa protokołów związanych z obsługą ruchu typu multicast:
 - a. IGMP v1, v2 i v3
 - b. IGMP Snooping v1, v2 i v3
 - c. PIM-SM, PIM-DM, PIM-SSM
20. Przełącznik musi posiadać funkcjonalność DHCP Server
21. Ochrona przed atakami typu DoS, TCP SYN flood, UDP flood

22. 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
23. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 12 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
24. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
25. Zamawiający wymaga, aby urządzenia posiadały 24 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).
26. W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca lub autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.
27. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń.

Zarządzalny switch dostępowy – 1 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. przełącznika dostępowego 24-portowego.

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. minimum jeden zasilacz 230V AC
 - d. zakres temperatur pracy ciągłej co najmniej od -5°C do +50 °C
 - e. zakres wilgotności pracy co najmniej 5% - 95%
3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:
 - a. 24 porty 100/1000BASE-T
 - b. 4 porty 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. 4 jednostek w stosie

- c. Porty do stackowania mogą być współdzielone z portami typu uplink.
 - d. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
 - e. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
 - f. 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. 128 Gbps, wydajność przełączania przynajmniej 95 Mpps
 8. Obsługa min. 16 000 adresów MAC
 9. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
 10. Możliwość tworzenie połączeń agregowanych (link aggregation)
 11. Wsparcie dla G.8032 ERPS
 12. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
 13. Wsparcie dla mechanizmu PVST+.
 14. Obsługa protokołów routingu dynamicznego OSPFv2, OSPFv3. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
 15. Obsługa protokołów związanych z obsługą ruchu typu multicast IGMP Snooping v2 i v3
 16. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
 17. 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
 18. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 12 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
 19. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanych switchy, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
 20. Zamawiający wymaga, aby urządzenia posiadały 24 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).
 21. Usługa serwisu musi być świadczona w języku polskim.
 22. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
 23. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

Zarządzalne switche dostępne z PoE – 2 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 2 szt. przełączników dostępowych 24-portowych z PoE.

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. minimum jeden zasilacz 230V AC
 - d. zakres temperatur pracy ciągłej co najmniej od -5°C do +50 °C
 - e. zakres wilgotności pracy co najmniej 5% - 95%
3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:
 - a. 24 porty 100/1000BASE-T z obsługą PoE+ o łącznym budżecie mocy minimum 400W
 - b. 4 porty 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. 4 jednostek w stosie
 - c. Porty do stackowania mogą być współdzielone z portami typu uplink.
 - d. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
 - e. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
 - f. 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. 128 Gbps, wydajność przełączania przynajmniej 95 Mpps
8. Obsługa min. 16 000 adresów MAC
9. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
10. Możliwość tworzenie połączeń agregowanych (link aggregation)
11. Wsparcie dla G.8032 ERPS
12. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).
13. Wsparcie dla mechanizmu PVST+.
14. Obsługa protokołów routingu dynamicznego OSPFv2, OSPFv3. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
15. Obsługa protokołów związanych z obsługą ruchu typu multicast IGMP Snooping v2 i v3
16. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
17. 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
18. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 12 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
 19. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanych switchy, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
 20. Zamawiający wymaga, aby urządzenia posiadały 24 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).
 21. Usługa serwisu musi być świadczona w języku polskim.
 22. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
 23. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

Oprogramowanie typu EDR /XDR – 20 szt.

Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja oprogramowania antywirusowego. Oprogramowanie będzie musiało spełniać wymogi operacyjne i technologiczne Zamawiającego, zapewniając pełną integrację z istniejącą infrastrukturą oraz optymalizację działań związanych z cyberbezpieczeństwem. Zamówienie obejmuje dostawę licencji na 20 stanowisk (stacji roboczych, serwerów i maszyn wirtualnych) na okres do 31.12.2026.

Wymagania:

1. Administracja zdalna:
 - a. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
 - b. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
 - c. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
 - d. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
 - e. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
 - f. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
 - g. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
 - h. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
 - i. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
 - j. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

- k. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
 - l. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
2. Ochrona stacji roboczych:
- a. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
 - b. Rozwiązanie musi wspierać architekturę ARM64.
 - c. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
 - d. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
 - e. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
 - f. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
 - g. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
 - h. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
 - i. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
 - j. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
 - k. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
 - l. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
 - m. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
 - n. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
 - o. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - i. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

- ii. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - iii. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - iv. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - v. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- p. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z:
- i. zainstalowanych aplikacji
 - ii. usług systemowych
 - iii. informacji o systemie operacyjnym i sprzęcie
 - iv. aktywnych procesów i połączeń sieciowych
 - v. harmonogramu systemu operacyjnego
 - vi. pliku hosts
 - vii. sterowników.
- q. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
- r. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- s. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
- t. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- u. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook.
- v. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
- i. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - ii. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - iii. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
 - iv. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
- w. Rozwiązanie musi być wyposażone w moduł bezpiecznej przeglądarki.
- x. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
- y. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
- z. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

- aa. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
3. Ochrona serwerów:
- a. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
 - b. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
 - c. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
 - d. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
 - e. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
 - f. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
 - g. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
 - h. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
4. Wymagania dla ochrony serwerów Windows:
- a. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
 - b. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
 - c. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
 - d. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
 - e. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
 - f. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
 - g. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
 - h. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
 - i. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
5. Wymagania dla ochrony serwerów Linux:
- a. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
 - b. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

- c. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
 - d. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszzonego mikro-serwisu.
6. Ochrona urządzeń mobilnych opartych o system Android:
- a. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
 - b. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
 - c. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
 - d. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
 - e. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
 - i. usunięcie zawartości urządzenia,
 - ii. przywrócenie urządzenia do ustawień fabrycznych,
 - iii. zablokowania urządzenia,
 - iv. uruchomienie sygnału dźwiękowego,
 - v. lokalizację GPS.
 - f. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
 - g. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
 - i. nazwę aplikacji,
 - ii. nazwę pakietu,
 - iii. kategorię sklepu Google Play,
 - iv. uprawnienia aplikacji,
 - v. pochodzenie aplikacji z nieznanego źródła.
7. Szyfrowanie:
- a. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
 - b. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
 - c. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
 - d. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. Moduł XDR:
- a. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
 - b. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
 - c. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
 - d. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
 - e. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
 - f. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.

- g. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
 - h. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
 - i. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
 - j. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
 - k. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
 - l. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
 - m. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
 - n. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
 - o. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
 - p. Konsola administracyjna musi mieć możliwość tagowania obiektów.
 - q. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
9. Zamawiający wymaga licencji dla 20 stanowisk (stacji roboczych, serwerów i maszyn wirtualnych) na okres do 31.12.2026. Licencja powinna obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.
10. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

Zestaw urządzeń do magazynowania i zarządzania energią elektryczną – 1 kpl.

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa kompletnego zestawu urządzeń do konwersji, magazynowania i zarządzania energią elektryczną pozwalający na pracę wyspową, obejmującego falownik hybrydowy trójfazowy o mocy znamionowej 30 kW, wysokonapięciowy magazyn energii, szafę rack, moduł sterujący systemem bateryjnym oraz rozdzielnię elektryczną.

Zestaw musi być fabrycznie nowy, kompletny, kompatybilny ze wszystkimi elementami systemu oraz przystosowany do bezpiecznej współpracy z instalacją fotowoltaiczną i siecią elektroenergetyczną. Dostawa obejmuje wszystkie elementy niezbędne do prawidłowego montażu, podłączenia, konfiguracji i uruchomienia zestawu.

2. Zestawienie wymaganych urządzeń

Lp.	Nazwa elementu	Ilość
1	Falownik hybrydowy trójfazowy o mocy 30 kW	1 szt.
2	Moduł bateryjny wysokonapięciowy LiFePO ₄ , energia nominalna 5,12 kWh	4 szt.
3	Szafa rack do montażu modułów bateryjnych i sterownika	1 szt.
4	Moduł sterujący baterią HV, z funkcją zarządzania i zabezpieczenia klastra baterijnego	1 szt.
5	Rozdzielnia elektryczna AC/DC wraz z wymaganymi zabezpieczeniami	1 kpl.
6	Komplet przewodów zasilających, komunikacyjnych, uziemiających i elementów przyłączeniowych	1 kpl.

3. Wymagania techniczne falownika hybrydowego

1. Falownik trójfazowy, hybrydowy, przeznaczony do współpracy z instalacją fotowoltaiczną oraz wysokonapięciowym magazynem energii.
2. Znamionowa moc czynna AC: minimum 30 kW.
3. Maksymalna moc pozorna AC: minimum 33 kVA.
4. Napięcie znamionowe AC: 230/400 V, 50 Hz.
5. Maksymalna moc wejściowa instalacji PV: minimum 48 kW.
6. Maksymalne napięcie wejściowe PV: 1000 V DC.
7. Zakres napięcia MPPT obejmujący co najmniej 150–850 V DC.
8. Minimum 3 niezależne trackery MPPT.
9. Obsługa wysokonapięciowych magazynów energii z komunikacją BMS.
10. Maksymalny prąd ładowania i rozładowania baterii: minimum 75 A.
11. Obsługa pracy rezerwowej lub wyspowej.
12. Możliwość obsługi niesymetrycznych obciążeń trójfazowych.
13. Maksymalna sprawność: minimum 98%.
14. Stopień ochrony obudowy: minimum IP65.
15. Interfejsy komunikacyjne umożliwiające współpracę z systemem zarządzania baterią i monitoringiem.
16. Wbudowane zabezpieczenia wymagane przez producenta, w tym zabezpieczenia przeciwprzepięciowe oraz przed pracą wyspową.
17. Gwarancja producenta: minimum 5 lat.

4. Wymagania techniczne modułów bateryjnych

1. Technologia akumulatorów: litowo-żelazowo-fosforanowa LiFePO₄.
2. Energia nominalna pojedynczego modułu: minimum 5,12 kWh.
3. Napięcie nominalne pojedynczego modułu: około 51,2 V.
4. Pojemność znamionowa pojedynczego modułu: minimum 100 Ah.
5. Przeznaczenie do pracy w wysokonapięciowym systemie magazynowania energii.
6. Możliwość komunikacji z modułem sterującym BMS.

7. Zabezpieczenie przed przeładowaniem, nadmiernym rozładowaniem, przeciążeniem i przegrzaniem.
8. Dostarczenie kompletu przewodów zasilających i komunikacyjnych wymaganych do połączenia modułów.
9. Gwarancja i warunki eksploatacji zgodne z dokumentacją producenta.

5. Wymagania techniczne szafy rack

1. Szafa przeznaczona do montażu wysokonapięciowych modułów bateryjnych i modułu sterującego.
2. Konstrukcja dostosowana do obciążenia wynikającego z masy wszystkich zainstalowanych urządzeń.
3. Zapewnienie bezpiecznego montażu, dostępu serwisowego i prowadzenia przewodów.
4. Kompatybilność mechaniczna i elektryczna z oferowanymi modułami bateryjnymi oraz sterownikiem.
5. Dostawa kompletu elementów mocujących i montażowych.
6. Montaż zgodnie z wymaganiami producenta oraz warunkami bezpieczeństwa dla magazynów energii.

6. Wymagania techniczne modułu sterującego baterią

1. Moduł przeznaczony do zarządzania wysokonapięciowym kłosem bateryjnym.
2. Komunikacja z modułami bateryjnymi oraz falownikiem.
3. Monitorowanie parametrów pracy baterii, w tym napięcia, prądu i temperatury.
4. Realizacja funkcji zabezpieczających wymaganych przez producenta systemu.
5. Wbudowane lub współpracujące zabezpieczenia obwodu bateryjnego.
6. Dostawa kompletu przewodów zasilających, komunikacyjnych i elementów przyłączeniowych.
7. Pełna kompatybilność z oferowanymi modułami bateryjnymi i falownikiem.

7. Wymagania dotyczące rozdzielni elektrycznej

Rozdzielnia elektryczna musi być dostarczona jako kompletne urządzenie, dobrane do parametrów falownika, magazynu energii i instalacji, w której zestaw zostanie zainstalowany.

Wymagane wyposażenie, odpowiednio do przyjętego schematu instalacji, obejmuje:

1. Obudowę rozdzielnicę o stopniu ochrony dostosowanym do miejsca montażu.
2. Zabezpieczenia nadprądowe obwodów AC.
3. Zabezpieczenia przeciwprzepięciowe AC
4. Rozłączniki izolacyjne i urządzenia odłączające wymagane dla bezpiecznej obsługi serwisowej.
5. Zaciski przyłączeniowe, szyny i elementy do podłączenia przewodów ochronnych.
6. Oznaczenia obwodów, aparatów i przewodów.
7. Dokumentację techniczną, wykaz zastosowanych aparatów oraz deklaracje zgodności wymagane dla dostarczonego wyposażenia.

Parametry znamionowe aparatów, przekroje przewodów, układ ochrony przeciwporażeniowej i przepięciowej oraz stopień ochrony obudowy należy dobrać na podstawie projektu instalacji, warunków przyłączenia oraz dokumentacji producentów.

8. Wymagania dotyczące kompletności i uruchomienia

Wykonawca zapewni:

1. Dostawę wszystkich wymienionych urządzeń oraz niezbędnych akcesoriów.
2. Potwierdzenie kompatybilności falownika, baterii i modułu sterującego.
3. Dokumentację techniczną i instrukcje obsługi w języku polskim lub z tłumaczeniem na język polski.
4. Deklaracje zgodności UE i dokumenty potwierdzające spełnienie właściwych norm.
5. Schemat połączeń elektrycznych i komunikacyjnych.
6. Warunki gwarancji i dane serwisowe.

7. Możliwość prawidłowego uruchomienia i konfiguracji kompletnego zestawu zgodnie z dokumentacją producenta.

9. Rozwiązania równoważne

Jeżeli w dokumentacji zamówienia wskazano nazwę producenta lub model urządzenia, wskazanie to należy traktować jako określenie rozwiązania referencyjnego, o ile jest to zgodne z przyjętym sposobem opisu przedmiotu zamówienia. Dopuszcza się urządzenia równoważne, spełniające wszystkie wymagania techniczne, funkcjonalne, bezpieczeństwa i kompatybilności określone w niniejszym opisie.

Równoważność musi zostać wykazana przez wykonawcę za pomocą kart katalogowych, dokumentacji technicznej i innych odpowiednich dokumentów.

10. Odbiór dostawy

Podstawą odbioru będzie sprawdzenie kompletności dostawy, zgodności parametrów urządzeń z wymaganiami zamówienia oraz przekazanie wymaganej dokumentacji technicznej i gwarancyjnej.

NGFW z licencją UTM – 1 szt.

Przedmiotem zamówienia jest dostawa UTM wraz z wymaganym oprogramowaniem, licencjami, akcesoriami, dokumentacją oraz gwarancją, spełniającego minimalne wymagania techniczne i funkcjonalne określone w niniejszym OPZ.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

Wymagania:

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. Interfejs (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. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
28. 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.
29. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
30. Ochrona antyspam ma działać w oparciu o:
 - a. białe/czarne listy,
 - b. DNS RBL,
 - c. Skaner heurystyczny.
31. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
32. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

33. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
34. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
 - a. PPTP VPN,
 - b. IPSec VPN,
 - c. SSL VPN.
35. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
36. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
37. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
38. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
39. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
40. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
41. Urządzenie ma posiadać wbudowany filtr URL.
42. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
43. Administrator ma mieć możliwość dodawania własnych kategorii URL.
44. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
 - a. blokowanie dostępu do adresu URL,
 - b. zezwolenie na dostęp do adresu URL,
 - c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
45. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
46. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
47. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
48. 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.
50. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
51. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
 - a. lokalną bazę użytkowników (wewnętrzny LDAP),
 - b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
 - c. usługę katalogową Microsoft Active Directory.
52. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
53. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
 - a. SSL,
 - b. Radius,
 - c. Kerberos.
54. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
55. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
56. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

57. 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).
58. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
59. 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.
60. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
61. Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:
 - a. równoważenie względem adresu źródłowego,
 - b. równoważenie względem połączenia.
62. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
63. Urządzenie ma umożliwiać przełączenie na łączy zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).
64. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy.
65. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).
66. Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.
67. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
68. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego.
69. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
70. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
71. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
72. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
73. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
74. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
75. 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.
76. Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH)
77. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
78. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
79. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.

80. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
81. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
82. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
83. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
84. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
85. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
86. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
87. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
88. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
 - a. manualnego eksportu do pliku w dowolnym momencie czasu,
 - b. 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
89. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
90. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
91. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
92. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
93. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
94. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
95. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
96. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
97. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
98. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
99. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
100. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
101. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
102. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
103. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
104. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

105. 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).
106. Urządzenie ma posiadać usługę DNS Proxy.
107. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
108. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
109. Urządzenie musi mieć zaimplementowane Open API.
110. 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.
111. 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.
112. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
113. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
114. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB.
115. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.
116. Liczba portów Ethernet 2,5 Gbps – min. 8.
117. Liczba portów światłowodowych 1 Gbps – min. 2.
118. Liczba portów światłowodowych 10 Gbps – min. 4.
119. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
120. Urządzenie ma być wyposażone w przynajmniej jeden port konsolowy.
121. Przepustowość Firewall (1518 bajtów UDP) – minimum 10 Gbps.
122. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5 Gbps.
123. Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps.
124. Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 2.5 Gbps.
125. Liczba tuneli VPN IPSec – minimum 1 000.
126. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150.
127. Liczba tuneli typu SSL VPN (tryb portalu) – minimum 150.
128. Obsługa interfejsów 802.11q (VLAN) – minimum 128.
129. Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/kundę.
130. Urządzenie musi być wyposażone w moduł TPM.
131. Urządzenie nie ma limitu na liczbę użytkowników.
132. Liczba reguł filtrowania – minimum 16 000.
133. Liczba tras statycznego routingu – minimum 5 000.
134. Liczba tras dynamicznego routingu – minimum 10 000.
135. Uchwyty do instalacji w szafie RACK 19", wysokość urządzenia 1U.

[Sprzętowe sondy/sensory do monitorowania sieci OT – 1 kpl.](#)

Przedmiotem zamówienia jest dostawa kompletu składającego się z trzech sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (zwanym dalej system IDS).

Wymagania:

1. Oprogramowanie musi być w 100% niezależne od dostawców automatyki oraz zawierać wsparcie dla urządzeń przemysłowych wykorzystywanych przez Zamawiającego.
2. Przetwarzane dane w systemie nie mogą być przesyłane poza infrastrukturę Zamawiającego.
3. Całość rozwiązania, tj. system IDS wraz z silnikiem analitycznym oraz wszystkie sondy systemowe – zarówno sondy fizyczne, jak i wirtualne – muszą pochodzić od jednego producenta. Producent systemu IDS musi być jednocześnie producentem sond, a rozwiązanie powinno stanowić spójny, zintegrowany produkt, zaprojektowany i rozwijany jako całość.
4. System IDS musi posiadać interfejs graficzny min. w języku polskim i angielskim, który ma być dostępny przez przeglądarkę internetową. Dostęp do interfejsu musi być zabezpieczony protokołem szyfrowania TLS. Zamawiający musi mieć możliwość importu własnego certyfikatu.
5. System IDS nie może ograniczać wielkości przestrzeni dla przechowywanych logów i archiwalnego ruchu sieciowego. Musi umożliwiać ustawienie czasu przechowywania informacji o anomaliach i archiwum ruchu sieciowego.
6. System IDS musi umożliwiać konfigurowanie poziomów dostępu dla użytkowników.
7. System IDS musi umożliwiać aktualizację bazy danych, oprogramowania, podatności w trybie offline.
8. System IDS musi umożliwiać synchronizację czasu przy użyciu protokołu NTP.
9. System IDS musi zapewniać:
 - pasywne monitorowanie sieci przemysłowej Zamawiającego,
 - automatyczne tworzenie graficznej mapy urządzeń min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach.
 - szczegółową inwentaryzację urządzeń,
 - automatyczne odzwierciedlenie połączeń komunikacyjnych,
 - informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji,
 - wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST,
 - budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji,
 - obsługę LLDP, CDP, CIP, SSDP.
10. System IDS musi posiadać mechanizmy alarmujące, które będą działać w trakcie budowania modelu sieci przemysłowej w celu wykrywania zagrożeń w procesie nauki.
11. System IDS musi posiadać zaimplementowane mechanizmy wsparcia i rozumienia komend dla głównych protokołów OT i IT.
12. System IDS musi mieć możliwość dodawania nowego typu protokołu.
13. System IDS musi działać na kopii ruchu oraz musi być w 100% pasywny. Nie może generować żadnego dodatkowego ruchu w monitorowanej sieci ani mieć wpływu na komunikację w sieci przemysłowej.
14. Kopia ruchu sieciowego musi się odbywać na bazie kopii dostarczanej ze SPAN/mirror portów przełączników, lub w trybie „pass-through / in-line” przy wpięciu do linii.
15. System IDS musi umożliwiać analizę ruchu sieciowego: Packet Capture (pliki PCAP).
16. System IDS musi monitorować i klasyfikować cyberincydenty oraz zdarzenia operacyjne.
17. System IDS powinno być oparte na technologii uczenia maszynowego i umożliwiać modelowanie sieci w czasie maksymalnie 5 dni.
18. System IDS musi umożliwiać generowanie potencjalnych wektorów ataku, bazując na analizie ruchu sieciowego oraz rekomendować sposoby zwiększenia bezpieczeństwa.
19. System IDS musi umożliwiać integrację z systemami typu SIEM (np. poprzez Syslog)

20. System IDS musi zapewniać w trybie ciągłym monitoring online sieci przemysłowej z alarmowaniem w czasie rzeczywistym wykorzystując metody /techniki behawioralne.
21. System IDS musi umożliwiać sortowanie alarmów zgodnie z min.: stopniem, ważności, typie, czasie wystąpienia.
22. System IDS musi umożliwiać wysyłanie wiadomości e-mail w razie wystąpienia alarmów.
23. System IDS musi gromadzić informacje o zaistniałych alarmach min.: opis techniczny alarmu, stopień oraz ważność, rekomendacje, plik z ruchem sieciowym.
24. System IDS musi pozwalać na głęboką analizę pakietów (DPI) dla min. protokołów: MODBUS RTU, DNP3.
25. System IDS musi wspierać analizę ML/AI dla protokołów min.: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC- 61850, SRTP, BACnet.
26. System IDS musi identyfikować anomalie w ruchu sieciowym oraz incydenty w tej sieci.
27. System IDS musi obsługiwać incydenty w zakresie min.: wykrywania, rejestrowania, analizy, ustawienia priorytetu, ustawienia statusu, podejmowanie działań naprawczych, rekomendacji.
28. System IDS musi wykrywać zagrożenia min.:
 - malware/"zero-day",
 - atak DOS/DDOS,
 - atak typu ATP,
 - spyware, skanowanie sieci,
 - zagrożenia Man-in-the-Middle,
 - anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność, komend, skanowanie PLC, skanowanie urządzeń sterujących,
 - wykrywanie połączeń do innej sieci LAN/internet,
 - wykrywanie połączeń do kluczowych urządzeń wraz z prezentacją sposobu komunikacji.
29. System IDS musi pozwalać na generowanie raportów w zakresie analizy danych.
30. System IDS musi umożliwiać instalację sond programowych w środowisku Linux.
31. System IDS musi umożliwiać szyfrowaną komunikację z sondami sprzętowymi.
32. System IDS musi umożliwiać zapamiętywanie widoków graficznych skonfigurowanych przez użytkownika.
33. System IDS musi zapewniać funkcjonalność budowy oraz utrzymania Software Bill of Materials (SBOM) dla monitorowanej infrastruktury przemysłowej, realizowaną w sposób pasywny, bez ingerencji w pracę urządzeń końcowych.
34. System IDS musi mieć możliwość ukrywania urządzeń typu MULTICAST/BROADCAST.
35. System IDS musi mieć możliwość wykrywania producenta urządzenia min. pod adresie MAC.
36. System IDS musi umożliwiać eksport listy urządzeń do pliku CSV i/lub PDF z podziałem na podsieć.
37. System IDS musi umożliwiać eksport protokołów do pliku CSV i/lub PDF z informacją w której podsieci zostały one wykryte.
38. System IDS musi mieć możliwość eksportu co najmniej do pliku PCAP wybranych pakietów.
39. System IDS musi mieć możliwość zdalnej zmiany konfiguracji oraz firmware sond sprzętowych.
40. Sondy sprzętowe muszą posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej min. AES128.
41. Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.
42. Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem baterijnym do 30 minut przy zaniku zasilania z sieci.
43. Sonda sprzętowa musi wspierać: DHCP, stały adres IP.

44. Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.
45. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.
46. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.
47. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.
48. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.
49. Sonda sprzętowa musi posiadać min. jeden interfejs monitorujący RJ45 10/100Mbps pracujący w trybie Span-port. Interfejs monitorujący RJ45 nie może identyfikować się w sieci poprzez adres MAC oraz musi być pozbawiony funkcji Tx.
50. Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazaną część ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.
51. Sonda sprzętowa musi umożliwiać przekazywać do systemu IDS strumień sieciowy w formie IPFIX.
52. Wykonawca dostarczy:
 - sondy sprzętowe w liczbie 3 szt. do monitorowania sieci przemysłowej,
 - licencję wieczystą na system IDS dla nielimitowanej liczby monitorowanych urządzeń,
 - gwarancję producenta na okres 36 miesięcy.
53. Serwis producenta systemu IDS ma obejmować:
 - Dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim.
 - Dostęp do nowych wersji systemu IDS.
 - Dostęp do aktualizacji i poprawek systemu IDS.
 - Dostęp do aktualizacji oprogramowania sond sprzętowych.
 - Wymianę uszkodzonych sond sprzętowych w razie awarii.
 - Przekazanie danych kontaktowych do działu technicznego producenta systemu IDS.
 - Wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas wdrożenia i późniejszej eksploatacji.
 - Wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.
54. Wykonawca zainstaluje i zalicencjonuje oraz skonfiguruje system IDS w środowisku serwerowym wskazanym przez Zamawiającego.
55. Licencje systemowe oraz sprzęt serwerowy zapewni Zamawiający.
56. Wykonawca przeprowadzi instalację sond sprzętowych w miejscach wskazanych przez Zamawiającego. Miejsce w szafach zapewni Zamawiający a Wykonawca wykona wszystkie niezbędne połączenia pomiędzy dostarczonym sprzętem a istniejącą infrastrukturą oraz zapewni wymagane okablowanie. Instalacja sond sprzętowych nie może powodować przerw działania sieci ani wprowadzać zakłóceń do sieci.
57. Wykonawca przeprowadzi pełną konfigurację i wdrożenia systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.
58. Wykonawca przekaze Zamawiającemu wszelkie hasła, użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.
59. Dla całego powyższego zakresu dot. instalacji, konfiguracji i parametryzacji Wykonawca przeprowadzi testy sprawdzające prawidłowość jego wykonania i działania.
60. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.
61. Wykonawca przygotuje dokumentację powykonawczą opisującą wszystkie prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni kalendarzowych od dnia zrealizowania całego powyższego zakresu. Zakończenie wdrożenia i jego odbiór nastąpi po odebraniu dokumentacji powykonawczej.

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. 7.00 do 15.00,
- 2) instruktaże odbywać się będą w siedzibie Zamawiającego,

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.

Instalacja i konfiguracja dostarczonych systemów

Zamawiający wymaga aby Wykonawca przeprowadził instalację dostarczanych systemów zgodnie z poniższym opisem. W sprawach nieuregulowanych niniejszym OPZ Wykonawca ustali z Zamawiającym sposób instalacji i konfiguracji na etapie wdrożenia.

CZĘŚĆ I: INFRASTRUKTURA SIECIOWA I BEZPIECZEŃSTWO

1. Przełączniki sieciowe (CORE i Dostępowe)

1. Przełączniki Rdzeniowe (CORE): 1 zestaw w konfiguracji High Availability (HA) w szafie RACK.
2. Przełączniki Dostępowe: 2 sztuki zlokalizowane w wyznaczonych punktach dystrybucyjnych.
3. Połączenia redundantne:
 - Przełączniki CORE muszą być połączone z przełącznikami dostępowymi za pomocą zdwojonych łączy światłowodowych (SFP+ 10Gbps) w topologii gwiazdy/pierścienia zapewniającej odporność na awarię pojedynczej magistrali.
 - Wszystkie połączenia między przełącznikami a serwerami i brzegami UTM muszą być wykonane jako redundantne (LACP / Link Aggregation) zwiększające jednocześnie przepustowość.
4. Konfiguracja bezpieczeństwa na przełącznikach:

- Włączenie i konfiguracja DHCP Snooping oraz Dynamic ARP Inspection (DAI) celem ochrony przed nieautoryzowanymi serwerami DHCP i atakami typu Man-In-The-Middle.
- Włączenie standardu 802.1X oraz wsparcia dla MACsec na portach dostępowych.
- Włączenie Port Security oraz ochrony przed pętlami (STP BPDU Guard).

2. Segmentacja sieci (VLAN)

Wykonawca wyodrębni i skonfiguruje na urządzeniach sieciowych co najmniej następujące odseparowane podsieci VLAN:

- VLAN Serwery: dla maszyn wirtualnych i usług produkcyjnych,
- VLAN Klaster / Corosync: dedykowany i odizolowany ruch dedykowany dla synchronizacji klastra wirtualizacji,
- VLAN Management: do zarządzania urządzeniami IT (Out-of-Band / OOB) przeznaczony wyłącznie dla działu IT,
- VLAN OT: odizolowana sieć automatyki przemysłowej/operacyjnej (dodatkowo odizolowana fizycznie poprzez instalację oddzielnego przełącznika sieciowego),
- VLAN Biuro: dla urządzeń biurowych (drukarki, skanery, telefony VoIP),
- Inne wynikające z SZBI

3. Zabezpieczenie brzegowe i segmentacja OT

1. UTM Brzegowy (Styk z Internetem):

- Domyślna polityka: *Deny All* (blokada całego ruchu wchodzącego i wychodzącego).
- Udostępnienie wyłącznie usług wskazanych przez Zamawiającego (np. HTTPS, SMTP).
- Wdrożenie modułów bezpieczeństwa: IPS/IDS, Anty-Malware, SSL Inspection, Web Filtering.
- Dokumentacja: Wykonawca dostarczy szczegółową instrukcję operacyjną (SOP) zawierającą procedurę publikacji nowych usług oraz otwierania portów na firewallu.

CZĘŚĆ II: SERWERY, STORAGE, WIRTUALIZACJA I BACKUP

1. Architektura Serwerowa

1. Serwery Wirtualizacji (Zestaw HA):

- Wykonawca zainstaluje i skonfiguruje warstwę wirtualizacji (z obsługą klastra wysokiej dostępności HA).

2. System Kopia Zapasowej (Backup)

1. Wykonawca wdroży Serwer do wykonywania kopii zapasowych wraz z dedykowanym oprogramowaniem backupowym.
2. Architektura Backupowa (Reguła 3-2-1):
 - Kopia stopnia I: Zapisywana bezpośrednio na lokalnych szybkich dyskach serwera backupu.
 - Kopia stopnia II (Replikacja): Oprogramowanie do backupu musi pozwalać na zapis kopii bezpieczeństwa w drugiej lokalizacji (odmiejscowionej).
 - Oprogramowanie musi realizować backupy bezorkiestrowe (agentless) na poziomie hiperwizora z obsługą spójności aplikacji (VSS/Application-Consistent).

CZĘŚĆ III: HARDERING SYSTEMÓW

1. Hardening (Utwardzanie) i Zarządzanie Dostępem

1. Wykonawca zobowiązany jest do pełnego utwardzenia (hardeningu) wszystkich dostarczonych urządzeń (serwery, switchy, UTM, UPS):
 - Bezwzględny zakaz stosowania domyślnych haseł i loginów fabrycznych.

- Zablokowanie nieużywanych portów sieciowych i wyłączenie zbędnych usług.
 - Zabezpieczenie interfejsów: Wszystkie interfejsy zarządzające (SSH, WebGUI, Konsola, Telnet) muszą wymuszać szyfrowanie i uwierzytelnianie. Brak możliwości dostępu bez logowania.
 - Utworzenie indywidualnych kont imiennych dla pracowników Działu IT Zamawiającego z odpowiednimi poziomami uprawnień.
2. Stacje obsługujące obecnie SCADA: muszą zostać podłączone fizycznie do odseparowanej sieci OT, nie mogą mieć dostępu do internetu.

Przygotowanie i dostarczenie dokumentacji powykonawczej

Ramy ogólne i język dokumentacji:

- Wykonawca zobowiązany jest do sporządzenia i przekazania Zamawiającemu kompleksowej Dokumentacji Projektowej i Administratora dla całego wdrożonego środowiska (infrastruktura fizyczna, sieć LAN/OT, wirtualizacja, pamięć masowa, kopie zapasowe, usługi katalogowe AD, systemy bezpieczeństwa UTM, EDR/XDR).
- Dokumentacja musi być sporządzona w języku polskim.
- Dokumentacja musi zostać dostarczona w wersji elektronicznej w formacie przeszukiwalnym (np. nieedytowalny plik PDF z warstwą OCR umożliwiającą przeszukiwanie tekstu oraz w wersji edytowalnej, np. .docx).
- Wymóg ten dotyczy dedykowanej dokumentacji projektowo-wdrożeniowej (tzw. dokumentacji *as-built*). Standardowe instrukcje obsługi producentów sprzętu i oprogramowania stanowią jedynie załącznik i nie zastępują wymaganej Dokumentacji Projektowej.

Zakres zawartości Dokumentacji Administratora: Dokumentacja musi być opisana w sposób wyczerpujący i niebudzący wątpliwości interpretacyjnych, umożliwiający samodzielne zarządzanie i utrzymanie systemu przez dział IT Zamawiającego lub podmiot trzeci. W szczególności musi zawierać:

- Architekturę fizyczną i logiczną: Schematy połączeń kablowych (miedź/światłowod), rozmieszczenie urządzeń w szafie, schemat zasilania, topologię sieciową z uwzględnieniem podziału na VLANy, adresacji IP, routingu oraz styków sieciowych IT/OT i Internet.
- Konfigurację środowiska eksploatacyjnego: Szczegółowy opis konfiguracji urządzeń sprzętowych, systemów operacyjnych, warstwy wirtualizacji, reguł na firewallach UTM, konfiguracji switchy (802.1X, MACsec, DHCP Snooping).
- Procedury utrzymaniowe i operacyjne: Instrukcje bieżącego zarządzania, procedury wykonywania i weryfikacji kopii zapasowych, procedury aktualizacji oprogramowania (patching) oraz dedykowaną Instrukcję Dodawania Nowych Usług/Portów na UTM (SOP).
- Procedury Awaryjne i Odzyskiwania (Disaster Recovery Plan): Dokładny, krok po kroku, opis czynności niezbędnych do odtworzenia pełnej funkcjonalności każdego z elementów systemu (od zera) w przypadku awarii krytycznej, uszkodzenia sprzętu lub ataku ransomware.

Przekazanie danych dostępowych i haseł:

- Wykonawca przekaze kompletny wykaz wszystkich kont administracyjnych, loginów, haseł, kluczy szyfrujących, certyfikatów, haseł root/admin, tokenów i kodów dostępu do wszystkich dostarczonych urządzeń, systemów, licencji i interfejsów zarządzających (SSH, WebGUI, Konsola, IPMI/iDRAC/iLO).
- Wykaz ten musi gwarantować pełny i nieograniczony dostęp do zarządzania całą infrastrukturą.
- Forma przekazania danych dostępowych:

- o Forma cyfrowa (Zalecana): Zaszyfrowany plik bazy danych programu KeePass (lub równoważnego otwartego standardu, np. .kdbx) umieszczony na nośniku pendrive. Hasło główne do bazy danych zostanie przekazane Kierownikowi Projektu ze strony Zamawiającego osobnym kanałem (np. w zamkniętej kopercie lub za pomocą bezpiecznego komunikatora).
- o Forma papierowa (Zapasowa): Wydrukowana, kompletna lista haseł przekazana w nieprzezroczystej, zabezpieczonej kopercie, podpisanej na łączeniach przez reprezentanta Wykonawcy.

Niezależność technologiczna i ciągłość serwisu:

- Przekazana dokumentacja oraz dane dostępowe muszą umożliwiać przejęcie pełnej obsługi, serwisu, modyfikacji i rozwoju dostarczonego rozwiązania przez dowolny inny podmiot trzeci (świadczący usługi IT) po zakończeniu okresu gwarancji lub trwałości projektu, bez konieczności udziału Wykonawcy.

Warunek Odbioru Końcowego:

- Dostarczenie kompletnej, zweryfikowanej przez Dział IT Zamawiającego i pozbawionej błędów Dokumentacji Projektowej oraz danych dostępowych stanowi warunek konieczny do podpisania Protokołu Odbioru Końcowego bez zastrzeżeń i wypłaty wynagrodzenia.

Procedura odbioru przedmiotu zamówienia

1. Zgłoszenie gotowości do odbioru

1. Wykonawca zobowiązany jest do pisemnego (lub pocztą elektroniczną na adresy wskazane w Umowie) zgłoszenia Zamawiającemu gotowości do Odbioru Końcowego na co najmniej 3 dni robocze przed planowanym terminem zakończenia prac.
2. Wraz ze zgłoszeniem gotowości Wykonawca przekazuje Zamawiającemu wstępny komplet dokumentów odbiorowych w wersji elektronicznej do weryfikacji.

2. Wykaz dokumentów i elementów wymaganych do odbioru

Do dnia rozpoczęcia procedury odbiorowej Wykonawca musi dostarczyć Zamawiającemu:

1. Kompletną Dokumentację Projektową i Administratora (zgodnie z wymogami OPZ) – w wersji elektronicznej przeszukiwalnej oraz edytowalnej.
2. Komplet danych dostępowych (loginy, hasła, klucze szyfrujące) przekazany w zaszyfrowanej bazie danych na nośniku pendrive oraz w zabezpieczonej kopercie.
3. Protokoły pomiarowe i testowe, w tym protokół z testów systemu kopii zapasowych (scenariusz testowego odtworzenia maszyny wirtualnej z backupu).
4. Karty gwarancyjne oraz licencje (lub certyfikaty licencyjne) jeśli producent przewiduje.
5. Certyfikaty i deklaracje zgodności CE dla dostarczonych urządzeń fizycznych.

3. Sposób weryfikacji przedmiotu Umowy (Testy Odbiorowe)

Weryfikacja wykonania prac odbędzie się w obecności przedstawicieli Zamawiającego oraz Wykonawcy i obejmować będzie:

1. Inwentaryzację fizyczną i wizualną:
 - o Sprawdzenie zgodności dostarczonego sprzętu i oprogramowania z umową (numery seryjne, modele, specyfikacja).
 - o Ocena jakości montażu w szafie, ułożenia i oznaczenia okablowania, poprawności adaptacji pomieszczenia.
2. Weryfikację funkcjonalną i testy bezpieczeństwa (Odbiór Techniczny):
 - o Test zasilania awaryjnego: Fizyczne odłączenie zasilania głównego w celu weryfikacji poprawnego przełączenia na UPS.
 - o Test łączności i segmentacji (VLAN / UTM): Weryfikacja działania reguł na firewallach, separacji sieci (w tym sieci OT) oraz poprawności działania 802.1X, DHCP Snooping i logowania przez Active Directory.

- Test wirtualizacji i HA: Symulacja awarii jednego z węzłów klastra wirtualizacji/serwerów.
 - Test Backup & DR: Wykonanie próbnego odzyskania wskazanej przez Zamawiającego maszyny wirtualnej z kopii zapasowej.
3. Weryfikację kompletności dostępu:
- Testowe zalogowanie się przez Dział IT Zamawiającego do losowo wybranych urządzeń i systemów przy użyciu przekazanej bazy haseł.
4. Warunki podpisania Protokołu Odbioru
1. Jeśli w trakcie weryfikacji nie zostaną stwierdzone wady, Strony podpiszą *Protokół Odbioru Końcowego Bez Zastrzeżeń*, co stanowi podstawę do wystawienia faktury.
 2. W przypadku stwierdzenia wad lub braków (np. błędy w konfiguracji, brakujące dokumenty, usterki fizyczne):
 - Zamawiający sporządzi *Protokół Rozbieżności* ze wskazaniem wykrytych wad oraz wyznaczy Wykonawcy realny termin na ich usunięcie (nie dłuższy niż 5 dni roboczych).
 - Po usunięciu wad procedura weryfikacji zostanie powtórzona w zakresie dotyczącym zgłoszonych zastrzeżeń.