Załącznik nr.11 do SWZ

Opis Przedmiotu Zamówienia

„Dostawa i wdrożenie rozwiązań IT/OT z zakresu cyberbezpieczeństwa w ZOGKiM w Sidrze”

ZAMAWIAJĄCY :

Zakład Gospodarki Komunalnej i Mieszkaniowej w Sidrze
ul. Fabryczna 4
16-124 Sidra

Cyberbezpieczne Wodociągi

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego **Cyberbezpieczne Wodociągi** , Inwestycja C3.1.1. Cyberbezpieczeństwo - Cyber PL , infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo - Krajowy Plan Odbudowy i Zwiększania Odporności

Spis treści

Wymagania ogólne ... 4
Część 1. Dostawa sprzętu i oprogramowania IT ... 5
1. Oprogramowanie SIEM i SOAR ... 5
2. Oprogramowanie antywirusowe z EDR/XDR i MFA ... 12
3. Oprogramowanie do monitorowania infrastruktury informatycznej ... 20
4 Firewall sieciowy ... 22
5. Oprogramowanie NAC ... 27
6. Stacja robocza fizyczna z rolą stacji przesiadkowej ... 31
7. System typu NDR z oprogramowaniem HoneyPot ... 32
8. Macierz dyskowa ... 36
9. NAS ... 38
10. System wirtualizacyjny ... 41
11. System operacyjny serwerowy i licencje dostępowe ... 49
12. Serwery pod rozwiązania bezpieczeństwa ... 50
13. Serwer backupu ... 52
14. Szafa RACK ... 55
15. Zarządzalne urządzenie sieciowe szkieletowe ... 56
16. Zarządzalne urządzenie sieciowe dostępowe PoE ... 58
17. Access Point WiFi ... 59
18. Oprogramowanie do wykonywania kopii zapasowych ... 60
19. Oprogramowanie DLP ... 62
20. Oprogramowanie do zarządzania uprzywilejowanym dostępem PAM ... 63
21. Oprogramowanie typu ITSM i aktualizacji systemów operacyjnych oraz oprogramowania ... 65
22. Certyfikat SSL/TLS ... 72
23. Klucze sprzętowe U2F/FIDO2 ... 73
24. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa ... 74
25. Utrzymanie i eksploatacja urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa ... 75
26. Usługa inwentaryzacji aktywów teleinformatycznych ... 77
27. Usługa segmentacji sieci ... 78
28. Audyt cyberbezpieczeństwa sieci ... 80
Część 2. Dostawa sprzętu i oprogramowania OT ... 86
1. System IDS dedykowany sieciom OT ... 86
2. Sprzętowe sondy do monitorowania sieci OT ... 88
3. UPS ... 89
4. Agregat prądotwórczy ... 90
5. Mobilny agregat prądotwórczy ... 91

6. Wdrożenie, konfiguracja i hardening rozwiązań OT 93

Wymagania ogólne

Przedmiotem zamówienia jest dostawa nowego oprogramowania i sprzętu informatycznego oraz wdrożenie rozwiązań IT i OT w ramach projektu „***Poprawa cyberbezpieczeństwa systemu wodociągowego w Zakładzie Obsługi Gospodarki Komunalnej i Mieszkaniowej w Sidrze”***

Wymagania ogólne:

1. całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy);
2. całość sprzętu musi być fabrycznie nowa, nie używana wcześniej;
3. wszystkie dostarczone i montowane komponenty przez Wykonawcę muszą być dopuszczone do obrotu na terenie Unii Europejskiej;
4. dostarczane urządzenia muszą być pozbawione wszelkich wad;
5. urządzenia muszą być kompletne i gotowe do pracy po podłączeniu
6. wszystkie oferowane urządzenia w ramach poszczególnych typów musza być:
    a. złożone z identycznych podzespołów, sygnowanych przez ich Producenta;
    b. dostarczane w oryginalnych opakowaniach Producenta (opakowania nie mogą być otwierane od momentu wyprodukowania przez Producenta do momentu dostawy do Zamawiającego, fabryczne zamknięcie fabrycznych opakowań).
    c. objęte gwarancją dostawy sprzętu tego samego modelu/serii przez cały okres trwania projektu.
7. o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja oparte na gwarancji producenta; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu;
8. Postanowienia dotyczące nośników danych (dysków):
    a. W przypadku awarii, uszkodzenia lub wymiany dysku twardego (HDD/SSD) wchodzącego w skład dostarczonego sprzętu:
        i. Uszkodzony dysk pozostaje u Zamawiającego i nie podlega zwrotowi Wykonawcy ani producentowi.
        ii. Wykonawca zobowiązany jest do dostarczenia nowego, sprawnego dysku w miejsce uszkodzonego, bez dodatkowych kosztów dla Zamawiającego (w ramach gwarancji/serwisu).
    b. Zapis ten ma na celu zapewnienie bezpieczeństwa danych przechowywanych na nośnikach, niezależnie od ich stanu technicznego.
    c. Wykonawca uwzględnia powyższe postanowienia przy kalkulacji ceny oferty oraz przy realizacji usług serwisowych.
    d. Zamawiający zastrzega sobie prawo do samodzielnego zniszczenia lub utylizacji uszkodzonych nośników zgodnie z obowiązującymi procedurami bezpieczeństwa i ochrony danych.
9. Oprogramowanie
    a. oprogramowanie powinno posiadać gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);
10. Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części OPZ , w miejscach wskazanych przez Zamawiającego.

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części OPZ.

Część 1. Dostawa sprzętu i oprogramowania IT

1. Oprogramowanie SIEM i SOAR

Przedmiotem zamówienia jest dostawa oprogramowania do zbierania logów oraz wczesnego wykrywania, analizy i szybkiego reagowania na zagrożenia, które ma na celu automatyzację, orkiestrację i poprawę skuteczności procesów związanych z zarządzaniem incydentami bezpieczeństwa IT w organizacji.
Zamówienie obejmuje dostawę licencji wieczystej ze wsparciem technicznym do 31.12.2026.
Wymagania:

1. Gromadzenie danych
    a. Obsługuje gromadzenie danych o ruchu i danych dziennika z sensorów, terminali, urządzeń zabezpieczających (takich jak NGFW, IDPS, WAF itp.) i urządzeń sieciowych innych firm.
    b. Obsługuje dane w formatach Syslog, sysmon, netflow, metadanych i linux.
2. Wydajność platformy
    a. Obsługuje do 5 urządzeń w celu utworzenia klastra HA, w celu elastycznej rozbudowy przestrzeni dyskowej i wydajności przetwarzania danych;
    b. Dostęp do platformy możliwy poprzez adres typu IPv6 oraz IPv4
    c. Podczas wdrażania platformy obsługiwane jest używanie adresów IPv6 do konfigurowania powiązanych instancji platformy
3. Wyświetlanie pełnoekranowe
    a. Obsługa mapy rozkładu ataków, kompleksowych wyników, sytuacji podatności, sytuacji serwerów, sytuacji terminali, najnowszych zagrożeń
    b. Możliwość przeglądania statystyk i wyświetlania podziału ataków zewnętrznych na poziomie zdarzeń, 5 najpopularniejszych źródłowych adresów IP ataków, 5 najpopularniejszych lokalizacji geograficznych źródeł ataków, rozkład etapów ataku, sytuację zdarzeń ataku oraz 5 najpopularniejszych zasobów/obszarów objętych atakiem.
    c. Moduł wyświetlania pełnoekranowego, który obsługuje serwer, rozkład stanu bezpieczeństwa, TOP5 ryzykownych serwerów, TOP5 zagrożeń, tygodniowy trend ryzyka i ranking zagrożeń.
    d. Moduł wyświetlania pełnoekranowego, który obsługuje terminale, dystrybucję statusu bezpieczeństwa, TOP5 ryzykownych serwerów, TOP5 zagrożeń, tygodniowy trend ryzyka i ranking zagrożeń
    e. Moduł wyświetlania pełnoekranowego obsługujący zdarzenia, statystyki zagrożeń, najnowsze zagrożenia, najnowsze informacje o zagrożeniach, tygodniowy trend ryzyka i historyczny ranking zagrożeń
    f. Moduł wyświetlania pełnoekranowego, który obsługuje podatności hostów, dystrybucję podatności na zagrożenia, trend podatności i ranking historycznych podatności
    g. Obsługa obszarów ryzyka i wyświetlanie serwerów, punktów końcowych, zagrożeń i luk w zabezpieczeniach w ramach każdego obszaru ryzyka
    h. Obsługa przeskakiwania z pełnoekranowego wyświetlacza kompleksowej sytuacji bezpieczeństwa do innych wyświetlaczy pełnoekranowych; manualna lub automatyczna
    i. Obsługa kontroli filtrów czasowych, wybór wyświetlania informacji z dnia dzisiejszego, 7 dni i 30 dni
4. Monitorowanie sytuacji infrastruktury
    a. Obsługuje powiadamianie o alarmach oraz o zagrożeniach, informacjach alarmowych o działaniu systemu i informacjach alarmowych o licencjach w systemie.
    b. Obsługuje przegląd sytuacji bezpieczeństwa, w tym kompleksowy status ryzyka całej sieci, porównanie statusu ryzyka w tym samym okresie tygodnia, liczbę zadań i status wykonania zadania, zagrożenia i ich rozkład w tygodniu, status ryzyka i status naruszonych zasobów.

c. Obsługuje statystyki i wyświetlanie całkowitej liczby ryzykownych terminali, całkowitej liczby ryzykownych serwerów, całkowitej liczby zadań, ukończonych zadań i niedokończonych zadań
d. Obsługa niestandardowych ustawień w celu wyświetlania zagrożeń, którymi zainteresowany jest użytkownik, oraz wsparcie dla drill-down odpowiednich zdarzeń w celu przejścia do strony szczegółowej.
e. Obsługa ogólnej oceny stanu zagrożenia całej sieci i porównywanie stanu zagrożenia z jednego tygodnia w tym samym okresie czasu.
f. Obsługa statystyk i wyświetlanie 5 najważniejszych zdarzeń związanych z zagrożeniami w danym tygodniu
g. Obsługa statystyk zagrożeń i wyświetlania rozkładu na mapie
h. Obsługuje funkcję monitorowania ruchu i wykonuje statystyki, analizę i wyświetlanie informacji o danych NetFlow uzyskanych przez platformę z trendów ruchu, trendów nowych połączeń, aktywności źródłowych adresów IP i docelowych adresów IP.
i. Obsługa monitorowania całkowitego trendu ruchu i monitorowania ruchu źródłowego adresu IP / docelowego adresu IP, obsługa wyświetlania adresu IP, typu zasobu, nazwy zasobu, obszaru, ruchu uplink i downlink, nowego połączenia i innych informacji oraz obsługa rankingu TOP.
j. Obsługa zliczania liczby serwerów/terminali o różnych poziomach ryzyka zgodnie z poziomem ryzyka: krytycznym, wysokim, średnim i niskim oraz tygodniowy wykres trendu oraz TOP5
k. Obsługa statystyk trendów liczby serwerów/terminali o różnych poziomach ryzyka w ciągu tygodnia.
l. Obsługa wyświetlania statystyk TOP5 serwerów/terminali o najbardziej krytycznym ryzyku w ciągu tygodnia.
m. Obsługa rankingu TOP5 zagrożeń związanych z zasobami i obsługa statystyk ryzyka związanych z zasobami w ciągu tygodnia
n. Obsługa pulpitu monitorowania zasobów, zliczanie wszystkich zasobów/serwerów/terminali o różnych poziomach ryzyka, oraz wyświetlanie 5 najbardziej ryzykownych zasobów/serwerów/terminali.
o. Obsługa wyświetlania typu zasobu związanego z pojedynczym adresem IP, nazwy zasobu, zlokalizowanego regionu, liczby nowych połączeń, całkowitego ruchu, rozkładu ruchu i powiązanych z nim działań
p. Obsługa statystyk i wyświetlanie całkowitej liczby zasobów, całkowitej liczby serwerów/terminali/sprzętu sieciowego/sprzętu bezpieczeństwa/innego sprzętu, liczby zasobów w stanie naruszenia
q. Obsługa statystyk i wyświetlanie rozkładu typu zasobu, rozkładu źródła i systemu operacyjnego, rankingu TOP5 otwartych portów, rankingu TOP5 aplikacji oraz rankingu TOP5 dystrybucji zasobów.
r. Obsługa statystyk zagrożeń, tygodniowych statystyk zagrożeń
s. Obsługa konfigurowania danych zdarzeń, statystyk i wyświetlania rozkładu danych zagrożeń oraz informacji o zasobach dotkniętych danymi zagrożeniami
t. Obsługa statystyk luk w zabezpieczeniach, tygodniowego trendu luk w zabezpieczeniach i tygodniowej liczby luk w zabezpieczeniach
u. Obsługa statystyk obszaru ryzyka, tygodniowego trendu obszaru ryzyka i tygodniowej liczby statystyk obszaru ryzyka
v. Obsługa śledzenia źródła globalnie, obsługa śledzenia źródła poprzez IP/nazwę domeny/MD5 i musi obejmować informacje o zdarzeniach zagrożeń, analizie podatności, monitorowaniu ruchu, powiązanych danych wywiadowczych i innych powiązanych informacjach.
w. Obsługuje monitorowanie w czasie rzeczywistym użycia procesora, pamięci i dysku twardego
x. Obsługa statystyk stanu czujników, w tym całkowitej liczby czujników, liczby niedziałających czujników i liczby działających czujników,
y. Obsługa niestandardowej planszy tematycznej, wielowymiarowe wyświetlanie wykresów zasobów, zagrożeń i luk w zabezpieczeniach

5. Analiza zagrożeń
    a. Obsługa statystyk statusu wszystkich zasobów - statusu serwera, statusu terminala, statusu usługi i zagrożenia.
    b. Obsługa tygodniowych statystyk trendów zagrożeń, w tym ryzykownych serwerów, ryzykownych terminali i zagrożeń
    c. Obsługa analizy statystycznej zagrożeń, w tym etapu ataku, typu, informacji o opisie, sugestii usunięcia, informacji o zagrożeniu, informacji o dowodach i informacji o procesie. Można dostosować elementy wyświetlane w nagłówku i sortować według pól nagłówka.
    d. Obsługuje kompleksowe wyświetlanie sytuacji zagrożenia z perspektywy kompleksowej, zasobów i ataku
    e. Obsługuje oznaczanie zagrożeń i powiązanych zagrożeń, w tym rozwiązanych lub fałszywie pozytywnych.
    f. Obsługa zapytań o zagrożeniu z kombinacją wielu warunków, w tym nazwy, typu, poziomu, adresu IP, statusu itp.
    g. Obsługa zagregowanego wyświetlania i statystyk zagregowanych szczegółów zagrożeń według nazwy zagrożenia
    h. Obsługuje funkcję przechowywania pakietów informacji o dowodach i obsługuje pobieranie oryginalnego ruchu zebranego przez czujnik
    i. Obsługa pobierania oryginalnego pakietu danych
    j. Obsługa narzędzi dekodujących, informacje o zagrożeniach obsługują dekodowanie URL i Base64
    k. Obsługa bezpośredniej obsługi zagrożeń na stronie zdarzeń. Poza normalną konfiguracją polityk, można wydawać polityki bezpieczeństwa hosta, w tym blokowanie IP, kontrolę dostępu, kontrolę procesu, izolowanie plików, ponowne uruchamianie terminala, kontrolę USB itp.
    l. Obsługa analizy statystycznej serwerów/terminali zagrożeń, w tym etykiet zagrożeń, zagrożeń, poziomów ważności itp.
    m. Obsługuje powiązanie użytkowników końcowych w celu wyświetlenia najnowszego adresu IP logowania, adresu MAC i czasu ostatniego zdarzenia
    n. Obsługa uszkodzeń serwera/terminala, ocena aktualnego uszkodzenia hosta, wizualizacja zagrożeń na różnych etapach ataku i dostarczanie sugestii dotyczących usuwania zagrożeń.
    o. Obsługa perspektywy zagrożenia, relacji zagrożenia, kierunku ataku i wizualizacji zakresu wpływu.
    p. Obsługa widoku zasobu, który został podejrzany o naruszenie, oraz przeglądanie raportów dotyczących naruszeń, raportów ryzyka, powiązanych zagrożeń i informacji o lukach w zabezpieczeniach.
    q. Obsługuje statystyki monitorowania usług zagrożeń, które mogą być statystycznie filtrowane według obszaru, czasu, nazwy, poziomu i etykiety ryzyka, a także mogą być sortowane według pola nagłówka.
    r. Obsługuje szczegółowe statystyki zagrożeń, w tym serwery, obszary, opisy biznesowe, raporty o naruszeniach.
    s. Obsługa odbierania, przechowywania i wyświetlania dzienników Syslog, w tym dzienników Syslog IPv6
    t. Obsługa odbierania i przechowywania dzienników Netflow
    u. Obsługa odbierania i przechowywania metadanych
    v. Obsługa odbierania i przechowywania dziennika sysmon
    w. Obsługa odbierania i przechowywania dzienników systemu Linux
    x. Obsługa statystyk dziennika, w tym ogólnej liczby i statystyk typu dzienników Syslog, netflow, metadanych, sysmon i linux.
    y. Obsługa analizowania i wyświetlania dzienników IPv6 Netflow.
    z. Obsługa wyszukiwania zagrożeń, serwerów, usług i dzienników w języku naturalnym, języku SPL i kombinacji predefiniowanych warunków.

aa. Obsługuje zdarzenia oznaczone jako false positive i zapewnia funkcję czyszczenia, którą można ręcznie usunąć pojedyncze zagrożenia lub usunąć zagrożenia partiami

6. Analiza podatności
    a. Obsługa wyświetlania i przeglądania sytuacji podatności z perspektywy hosta, w tym: adres IP hosta, nazwa raportu podatności, czas skanowania, status podatności,
    b. Obsługa wyświetlania i przeglądania sytuacji podatności z perspektywy podatności, w tym: nazwa podatności, typ podatności, poziom podatności, liczba ustaleń
    c. Obsługa ręcznego importu raportów o podatnościach, minimum raportów w formacie .nessus z wersji 6.x i 8.x.
    d. Obsługa instalacji dodatkowych skanerów podatności w celu uzyskania raportów o podatnościach, administratorzy mogą dodawać, przeglądać, modyfikować i usuwać skanery;
    e. Obsługa wydawania zasad skanowania i konfiguracji skanowania do urządzeń skanujących podatności
    f. Obsługa okresowego zarządzania zadaniami skanowania (codziennie, co tydzień, co miesiąc), dodawanie, usuwanie, modyfikowanie, otwieranie i zamykanie zadań skanowania
7. Zarządzanie ryzykiem
    a. Wyświetlanie ogólnych informacji o ryzyku wszystkich zasobów/serwerów/usług w formie wykresów, w tym: liczba ryzykownych zasobów, liczba ważnych zagrożonych zasobów, rozkład ryzykownych serwerów, rozkład zagrożeń serwera / trend tygodniowy, rozkład podatności serwera / trend tygodniowy.
    b. Obsługuje wyświetlanie listy ryzykownych zasobów/serwerów/usług i szczegółów poszczególnych ryzykownych zasobów. Szczegóły ryzykownych zasobów obejmują trzy wymiary: raport ryzyka, podatność serwera i same zagrożenia.
    c. Obsługa eksportowania 10 000 najważniejszych zagrożeń/informacji o ryzykownych zasobach przechowywanych w systemie w formacie CSV
    d. Obsługuje funkcję oceny awarii ryzykownych serwerów i ryzykownych terminali
8. Reagowanie na incydenty
    a. Wspieranie wyznaczonej osoby odpowiedzialnej za przetwarzanie odpowiednich zagrożeń, podatności i obiektów ryzyka za pośrednictwem systemu zleceń pracy
    b. Obsługa statystycznego wyświetlania wskaźnika realizacji zleceń, całkowitej liczby zleceń, oczekujących zleceń i innych informacji.
    c. Obsługuje dodawanie powiązanych podmiotów do platformy XDR w celu scentralizowanego zarządzania, wykonywanie działań na powiązanych podmiotach,
    d. Obsługa sieciowych urządzeń zabezpieczających NGFW, IPS, WAF tego samego producenta
    e. Obsługa statystycznego wyświetlania całkowitej liczby playbooków, automatycznych playbooków i potwierdzonych playbooków oraz innych informacji.
    f. Obsługuje konfigurację warunków wyzwalania, warunków oceny dla automatycznej reakcji i działań odpowiedzi (wydawanie polityk, blokowanie adresów IP lub tworzenie zleceń pracy),
    g. Wbudowane 5 predefiniowanych playbooków, w tym miningu, wymuszeń i słabych haseł.
    h. Podczas wydawania polityki obsługuje ustawianie czasu jej działania
    i. Obsługuje dwa tryby: automatycznych playbooków i potwierdzonych playbooków, tryb potwierdzony obsługuje powiadomienia e-mail do administratora.
    j. Playbook obsługuje dopasowywanie adresów IPv4 i IPv6 oraz segmentów adresów.
    k. Gdy playbook wykonuje zadanie, które wymaga ręcznego potwierdzenia, zostanie ono zapisane na liście zadań, na które należy odpowiedzieć,
    l. Obsługa polityk dostarczanych do firewalla za pośrednictwem playbooków, muszą być sprawdzane przez agregację polityk, aby uniknąć dużej liczby podobnych polityk pojawiających się na urządzeniu firewall i wpływających na wydajność firewalla.
9. Zarządzanie raportami

a. Centralne wyświetlanie wszystkich wygenerowanych raportów, obsługa przeglądania zawartości raportów online lub eksportowanie i wyświetlanie w formacie PDF; obsługa natychmiastowego ręcznego generowania raportów o określonych wymaganiach
b. Obsługa konfiguracji zadań raportowania i regularne generowanie odpowiednich raportów zgodnie z ustalonymi warunkami, w tym raportów dziennych, tygodniowych i miesięcznych, a także raportów krótkich i szczegółowych.
c. Obsługa uruchamiania/zatrzymywania zadań raportowania w dowolnym momencie
d. Wstępnie ustawione szablony dla ogólnych raportów ryzyka, raportów ryzyka terminali, raportów ryzyka serwerów i raportów reagowania na incydenty, a także obsługa niestandardowych szablonów raportów skonfigurowanych przez użytkownika
e. Obsługa logo raportu zdefiniowanego przez użytkownika
f. Wsparcie dla statystyk i archiwizacji dokumentów i raportów

10. Intelligence Center
    a. Obsługuje odbieranie nowych informacji o zagrożeniach i obsługuje zapytania wywiadowcze na podstawie adresu IP/pliku/domeny/nazwy URL/nazwy/CVEID/etykiety zagrożenia z perspektywy poziomu zagrożenia i zakresu czasu.
    b. Po otrzymaniu wypchniętych informacji CVE, wsparcie w celu zainicjowania powiązanych zadań skanowania podatności i wysyłania zleceń pracy
    c. Obsługa wyświetlania informacji o rodzinie/grupie i obsługa powiązania z modułem śledzenia w celu generowania tagów
    d. Obsługuje co najmniej 7 typów baz danych wywiadowczych, w tym bazę danych wywiadowczych DNS, bazę danych wywiadowczych złośliwego kodu, bazę danych wywiadowczą URL, bazę danych wywiadowczą IP, bazę danych wywiadowczą podatności, bazę danych wywiadowczą wykrywania włamań i bazę danych geolokalizacyjnych.
    e. Obsługuje aktualizację offline i aktualizację online bazy danych wywiadowczych. Aktualizacja online obejmuje aktualizację ręczną i zaplanowaną.
    f. Obsługa zdefiniowanej przez użytkownika białej listy nazw domen, skutecznej dla wszystkich reguł DNS;
    g. Obsługa zdefiniowanej przez użytkownika białej listy plików, która obowiązuje dla wszystkich reguł klasy plików;
    h. Obsługa zdefiniowanej przez użytkownika konfiguracji globalnej białej listy
    i. Obsługa importu/eksportu białych list globalnych, klas DNS i klas plików jako plików CSV
    j. Obsługa zdefiniowanej przez użytkownika czarnej listy DNS, złośliwego kodu i IP
11. Zarządzanie zasobami
    a. Obsługa wsadowego importu/eksportu informacji o zasobach obszaru, usługi, serwera i terminala w postaci plików CSV.
    b. Obsługa aktywnego wykrywania i ręcznego importowania w celu wykrywania i wyświetlania zasobów w sieci prywatnej, ale nie na liście zasobów, które mogą być klasyfikowane i aktualizowane przez użytkowników
    c. Obsługa ekstrakcji odcisków palców zasobów, w tym informacji o systemie operacyjnym, otwartych portach, wdrożonych aplikacjach i wersjach, adresach MAC, producentach itp.
    d. Obsługa zaawansowanej klasyfikacji zasobów, w tym etykiet klasyfikacji zasobów w 5 głównych kategoriach i 29 podkategoriach, takich jak terminale, serwery, sprzęt sieciowy, sprzęt bezpieczeństwa, sprzęt IOT i inny sprzęt.
    e. Obsługa scentralizowanego zarządzania obszarami sieci, w tym zarządzanie konfiguracją ważności, lokalizacji i osób odpowiedzialnych.
    f. Obsługa statystycznego wyświetlania liczby terminali i serwerów w obszarze sieci.
    g. Obsługa scentralizowanego zarządzania serwerami i grupami serwerów, w tym zarządzanie konfiguracją adresu IP, obszaru, usługi, systemu operacyjnego, typu usługi itp., obsługa konfiguracji wielu segmentów sieci IP;

h. Obsługa scentralizowanego zarządzania terminalami i grupami terminali, w tym zarządzanie konfiguracją adresów IP, obszarów, systemów operacyjnych itp., obsługa konfiguracji wielu segmentów sieci IP;
i. Obsługa odbierania pakietów rozliczeniowych Radius wysyłanych przez zewnętrzne serwery uwierzytelniania, analizowanie bieżących informacji o użytkownikach i hostach online oraz wyświetlanie ich w "Statusie użytkownika".
j. Obsługa scentralizowanego zarządzania usługami i przeprowadzanie analizy zagrożeń z poziomu usługi poprzez dodawanie serwerów tego samego typu do tej samej usługi.
k. Obsługa pasywnej identyfikacji ruchu, wykrywanie i wyświetlanie zasobów sieci prywatnej, które nie znajdują się na liście konfiguracji zasobów, oraz oczekiwanie na potwierdzenie i klasyfikację przez użytkownika.
l. Obsługuje konfigurację zasobów serwerowych typu IPv6 i zasobów terminalowych oraz obsługuje identyfikację zasobów typu IPv6 za pomocą informacji Netflow.

12. Rules Engine
    a. Obsługa wykrywania skanowań, w tym skanowanie SYN, skanowanie UDP, atak skanowania adresu IP, atak skanowania portów
    b. Obsługa silnika plików, w tym wykrywanie podejrzanych plików PE (wykonywalnych), plików z niedopasowanym sufiksem i zawartością, podejrzanych plików z wieloma sufiksami, podejrzanych plików z wieloma sufiksami, plików z podejrzanym rozmiarem, plików z niedopasowanym sufiksem i zawartością oraz wrażliwych plików.
    c. Obsługa mechanizmów wykrywania HTTP, w tym HTTP Header Contain Abnormal Keywords, HTTP Response Contain X-Sinkhole, Excessive HTTP Response Errors, Suspicious HTTP Request via Tor.
    d. Obsługa mechanizmów wykrywania podejrzanych protokołów, w tym podejrzanej aktywności IRC, podejrzanej aktywności LDAP, podejrzanej aktywności NetBIOS, podejrzanej aktywności SMB i podejrzanej aktywności SSDP.
    e. Obsługa mechanizmów brute force, w tym FTP Brute Force Attack, IMAP4 Brute Force Attack, LDAP Brute Force Attack, MYSQL Brute Force Attack, POP3 Brute Force Attack, SMTP Brute Force Attack, SSH Brute Force Attack, TELNET Brute Force Attack, Weak Password Cracking, RDP Brute Force Attack, VNC Brute Force Attack i SMB Brute Force Attack.
    f. Obsługa silnika domen, w tym DNS Domain is Generated by DGA, Suspicious Amount of DNS NXDOMAIN Responses, Abnormal DNS Response, TTL in DNS Message is 0, IP Mapped Domain is in Blacklist, IP Mapped Domain is Generated by DGA, Suspicious DNS Tunnel Activity, DNS Protocol Abuse i Suspicious DNS Tunnel Data Transfer.
    g. Obsługa silnika ransomware, analiza i wykrywanie zgodnie z zachowaniem ransomware
    h. Obsługa miningu, inteligentne wykrywanie cech zachowania miningu
    i. Obsługuje silnik klasy zachowania USB, taki jak zachowanie podczas podłączania i odłączania urządzeń USB.
    j. Obsługuje blokowanie dostępu, w tym naruszenie dostępu, tworzenie złośliwych procesów Powershell, naruszenie uprawnień użytkownika do plików lub aplikacji, nieprawidłowe logowanie i naruszenie dostępu do aplikacji;
    k. Obsługuje regułę "Naruszenie dostępu do aplikacji". Użytkownicy mogą określić czarną listę / białą listę dostępu do aplikacji, konfigurując obiekt ochrony w regule, wykrywać, czy ruch ma złośliwy dostęp do określonych zasobów usługi aplikacji i generować zdarzenia zagrożeń
    l. Obsługuje wykrywanie słabych haseł dla 6 protokołów HTTP, TELNET, SMTP, POP3, IMAP i FTP, które przesyłają nazwę użytkownika i hasło w postaci zwykłego tekstu.
    m. Obsługuje ustawienia personalizacji silnika w oparciu o zebrane dzienniki zagrożeń, ustawienia wstępne: Malware, Spam, Phishing, DoS, Atak sieciowy, Skanowanie, EternalBlue, Próba ataku WebShell, RDP Remote Windows Kernel Release Reuse Vulnerability
    n. Obsługuje konfigurację analizy korelacji dzienników zagrożeń hostów
    o. Obsługuje statystyki zagrożeń oparte na polu x-forward

p. Wsparcie dla korelacji wielu zagrożeń i konfiguracji silnika kill-chain w celu odkrywania nowych informacji o zagrożeniach i dokładnej identyfikacji zagrożeń.
q. Reguła analizy korelacji klas dzienników zagrożeń sieciowych obsługuje konfigurację adresu źródłowego/docelowego IPv6.
r. Reguły analizy asocjacji klas nietypowego ruchu obsługują konfigurację segmentów sieci IP typu IPv6,

13. Zarządzanie logami
    a. Obsługa konfiguracji zaufanych źródeł logów w celu zarządzania i kontrolowania źródeł danych oraz zapewnienia bezpieczeństwa systemu.
    b. Nie ma ograniczeń co do liczby dostępnych źródeł logów
    c. Obsługuje zarządzanie i kontrolę źródeł dzienników Syslog/Netflow oraz ustawienia tworzenia kopii zapasowych i przeglądania dzienników.
    d. Obsługuje analizowanie, prezentowanie i dalszą analizę dzienników Syslog urządzeń innych firm; zapewnia predefiniowane konfiguracje analizowania dzienników i szablony dla popularnych sieciowych urządzeń zabezpieczających innych firm; obsługuje również tworzenie niestandardowych dzienników w oparciu o format konfiguracji i szablonu analizowania dziennika informacji Syslog, reguły parsowania obejmują Grok, klucz-wartość, JSON
    e. Obsługa niestandardowych pól mapowania dla dzienników innych firm
    f. Obsługa wyświetlania miejsca na dysku oraz tworzenie kopii zapasowych
    g. Obsługa przeglądania informacji o hoście, który wysyła dzienniki Sysmon
    h. Obsługuje wysyłanie dzienników Syslog odebranych przez iSource i zagrożeń wykrytych przez platformę do innych serwerów ; Obsługuje konfigurację szyfrowanego protokołu TCP i obsługuje użycie szyfrowanego protokołu TCP do odbierania i przesyłania informacji dziennika.
14. System zarządzania
    a. Obsługa wyświetlania podstawowych informacji o oprogramowaniu i sprzęcie systemu, takich jak: platforma sprzętowa, wersja oprogramowania, baza reguł, baza geograficzna, wersja bazy danych analizy zagrożeń itp.
    b. Obsługa dodawania, modyfikowania i usuwania użytkowników systemu
    c. Obsługa rozdziału uprawnień dla administratorów, operatorów i audytorów logów.
    d. Obsługa konfiguracji zaufanych hostów i kontrola praw dostępu każdego hosta do systemu XDR
    e. Obsługa konfiguracji i zarządzania wszystkimi kontaktami w systemie
    f. Obsługa rejestrowania dziennika zdarzeń i dziennika operacji samego systemu oraz obsługa ustawiania maksymalnego czasu przechowywania dziennika systemu
    g. Obsługa aktualizacji wersji offline
    h. Obsługa przeglądania licencji systemowych
    i. Obsługa serwera pocztowego, ustawień konta i odbiorcy
    j. Bramka SMS, obsługuje konfigurację modułu SMS
    k. Obsługuje ustawianie reguł alarmowych dla zagrożeń i systemów sprzętowych oraz wyzwala alarmy w postaci wiadomości e-mail, wiadomości tekstowych lub dźwięków; obsługuje wyświetlanie informacji alarmowych o zagrożeniach, działaniu systemu i wygaśnięciu licencji w interfejsie
    l. Obsługa ustawień systemowego adresu IP i serwera DNS
    m. Obsługa edycji i usuwania podłączonych urządzeń typu Sensor
    n. Obsługa monitorowania podstawowych informacji o podłączonych czujnikach, w tym adresu IP, numeru seryjnego i modelu sprzętu.
    o. Obsługa monitorowania informacji o stanie podłączonych urządzeń Sensor, w tym stanu online, ruchu w czasie rzeczywistym, wykorzystania procesora i wykorzystania dysku.
    p. Obsługa ustawień zabezpieczeń systemu, ustawień zasad logowania, ustawień zasad haseł
    q. Obsługa ustawień serwera pocztowego, konta i odbiorcy
    r. Obsługa funkcji ustawień zabezpieczeń:

s. W przypadku korzystania z domyślnego administratora systemu do logowania i hasła początkowego do urządzenia, system obsługuje funkcję wymuszania zmiany hasła początkowego;
t. Obsługuje konfigurację funkcji limitu czasu logowania. Po zalogowaniu się użytkownika do urządzenia, jeśli żadna operacja nie zostanie wykonana po upływie określonego limitu czasu, użytkownik musi ponownie zalogować się do urządzenia
u. Obsługa funkcji blokady użytkownika, jeśli użytkownik wprowadzi nieprawidłową nazwę użytkownika i hasło określoną liczbę razy. System zablokuje konto użytkownika lub adres IP zgodnie z określonym czasem blokady
v. Obsługuje konfigurację reguł haseł, z którymi muszą być zgodne hasła użytkowników;
w. Obsługa konfiguracji funkcji wymuszonej zmiany hasła dla nowych użytkowników.
x. Obsługa konfiguracji funkcji wymuszonej modyfikacji hasła. Jeśli hasło do konta użytkownika przekroczy określoną datę wygaśnięcia, system wymusi na użytkowniku użycie hasła przy ponownym logowaniu.
y. Obsługuje generowanie niezależnych reguł alarmowych dla zasobów/zdarzeń, aby spełnić zróżnicowane wymagania alarmów w różnych scenariuszach.
z. Obsługa przeglądania stanu każdego urządzenia w klastrze
aa. Obsługa przywracania ustawień fabrycznych, z wyborem czy wyczyścić wszystkie informacje konfiguracyjne, przechowywane dane, licencję

15. Zarządzanie hierarchiczne
    a. Obsługuje hierarchiczne wdrażanie zarządzania, wykorzystuje kanał kaskadowy oparty na transmisji TCP i dwukierunkowym uwierzytelnianiu SSL do realizacji połączenia między platformą wyższego poziomu a platformą niższego poziomu.
    b. Platforma wyższego poziomu obsługuje pełnoekranowe zarządzanie hierarchiczne, prezentując sytuację ryzyka całej platformy.
    c. Platforma wyższego poziomu obsługuje przełączanie do widoku innych platform, obsługuje przeglądanie ryzykownych aktywów, słabych punktów, zagrożeń i innych informacji
16. Proponowane rozwiązanie musi obsługiwać przepustowość 3 Gb/s
17. Proponowane rozwiązanie musi obsługiwać 5000 EPS
18. Licencja oprogramowania powinna być bezterminowa wraz ze wsparciem na okres do 31.12.2026.
19. Wsparcie techniczne w języku polskim

2. Oprogramowanie antywirusowe z EDR/XDR i MFA

Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja oprogramowania antywirusowego, EDR/XDR oraz MFA. 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 6 stanowisk 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 wyposażona 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 automatyczne 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 zawieszonego 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 urządzenie 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 autentykacje 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. Ochrona serwera pocztowego MS Exchange:
   a. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
   b. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
   c. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
   d. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
   e. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
   f. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
   g. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
   h. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
   i. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
   j. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
   k. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
10. Sandbox w chmurze:
   a. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
   b. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
   c. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
   d. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
   e. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
   f. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
   g. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
   h. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.

i. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
j. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
k. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
l. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    i. Czysty,
    ii. Podejrzany,
    iii. Bardzo podejrzany,
    iv. Szkodliwy.
m. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
n. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
o. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

11. Ochrona usług chmurowych:
a. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint, Teams oraz ochronę usługi Google Workspace, takie jak Gmail oraz Dysk Google.
b. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365 oraz Google Workspace.
c. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
d. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
e. Rozwiązanie musi być dostępny w języku polskim.
f. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
    i. użytkowników, otrzymujących najwięcej spamu,
    ii. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
    iii. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
    iv. kont użytkowników, które mogę być podejrzane.
g. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online, Onedrive, zespoły Teams, lokacje SharePoint, Gmail i OneDrive.
h. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
    i. jaka ilość wiadomości została przeskanowania,
    ii. wynik skanowania poszczególnej wiadomości,
    iii. czynność podjęta przez rozwiązanie.
i. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o:
    i. zagrożeniach, które zostały wykryte,
    ii. na jakim koncie zostały wykryte,
    iii. jakie zagrożenie zostało wykryte,
    iv. podjętą czynność.
j. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online, Onedrive, zespoły Teams, lokacje SharePoint, Gmail i OneDrive.
k. Rozwiązanie musi umożliwiać tworzenia reguł filtrowania w oparciu o co najmniej: DKIM, SPF, DMARC.
l. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.

m. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
n. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
    i. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
    ii. wprowadzenia białych i czarnych list adresów ochrony Exchange'a Online,
    iii. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
o. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
p. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
q. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
r. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
s. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

12. Moduł zarządzania podatnościami i aktualizacjami:
    a. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
    b. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.
    c. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych
    d. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.
    e. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:
        i. nazwę aplikacji lub systemu operacyjnego
        ii. punktacje CVSS
        iii. opis wykrytej podatności
        iv. wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta
    f. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.
    g. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
    h. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
    i. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
    j. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
    k. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
    l. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
    m. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.

n. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

13. Ochrona poprzez dwuskładnikowe uwierzytelnianie
    a. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
    b. Rozwiązanie musi wspierać system operacyjne Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11.
    c. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
    d. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.
    e. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.
    f. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.
    g. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
    h. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access.
    i. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.
    j. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
    k. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
    l. Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
    m. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
    n. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
    o. Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
    p. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego
    q. Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.
14. Zamawiający wymaga licencji dla 6 stanowisk na okres do 31.12.2026. Licencja powinna obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.

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.

3. Oprogramowanie do monitorowania infrastruktury informatycznej

Przedmiotem zamówienia jest dostawa i wdrożenie oprogramowania do monitorowania infrastruktury informatycznej. Oprogramowanie będzie musiało spełniać wymogi operacyjne i technologiczne Zamawiającego, zapewniając pełną integrację z istniejącą infrastrukturą oraz optymalizację działań związanych z monitorowaniem. Zamówienie obejmuje dostawę licencji wieczystej ze wsparciem technicznym do 31.12.2026 r.

Wymagania:

1. Architektura

   a. 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).
   b. 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.
   c. 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).
   d. 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).
2. Gromadzenie danych i monitorowanie środowiska
   a. Elastyczność odpytywania: 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).
   b. 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.
   c. 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.
   d. 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).
   e. Gotowe wsparcie dla chmur i wirtualizacji: 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).
3. Wykrywanie problemów i analiza biznesowa
   a. 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).
   b. 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.
   c. Monitorowanie usług biznesowych (SLA): Obliczanie faktycznej dostępności i przestojów dla usług biznesowych z użyciem hierarchicznych drzew zależności i wag przypisanych do składowych infrastruktury.
4. Powiadamianie i automatyzacja działań naprawczych
   a. 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).
   b. Złożone schematy eskalacji: Możliwość definiowania wielostopniowych procesów, w tym powiadomień opóźnionych, cyklicznych przypomnień do momentu rozwiązania problemu oraz powiadomień przypisanych do różnego szczebla pracowników w zależności od czasu trwania awarii.
   c. Automatyczne działania naprawcze (Auto-remediation): Możliwość zdalnego i automatycznego egzekwowania skryptów lub poleceń na urządzeniach (np. zrestartowanie usługi) bezpośrednio w odpowiedzi na wykrytą anomalię.
5. Wizualizacja i mapowanie topologii

   a. Dashboards: Możliwość personalizacji wielostronicowych kokpitów w oparciu o widżety prezentujące wykresy, statusy problemów czy usługi SLA, ze wsparciem metody przeciągnij-i-upuść.
   b. 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.
   c. Raportowanie cykliczne: Mechanizm pozwalający na generowanie i regularne (dzienne, tygodniowe, miesięczne) wysyłanie raportów z podsumowaniem stanu infrastruktury w formacie PDF bezpośrednio na skrzynki e-mail.
6. Wymagania z zakresu bezpieczeństwa (Security & Access Control)
   a. 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).
   b. Wielodostęp (Multi-tenancy) i autoryzacja: System musi oferować zaawansowany system praw i przypisywania ról opartych na odczycie/zapisie (Read/Write/Deny) lub pozwalających wyizolować widoczność elementów (np. do celów udostępnienia wglądu zewnętrznym klientom - tenants).
   c. 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.
   d. Audyt: Rejestr audytowy (Audit log) przechowujący wszystkie zmiany w konfiguracji przypisane do wprowadzającego użytkownika i adresu IP z opcją eksportu logów.
7. Automatyzacja zarządzania i wdrażania
   a. 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.
   b. 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.

4. Firewall sieciowy

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 2 szt. zapory sieciowej z pakietem bezpieczeństwa UTM pracujących w klastrze Active-Passive, które zapewnia zaawansowaną ochronę w infrastrukturze informatycznej zamawiającego. Zamówienie obejmuje zarówno dostawę urządzeń fizycznych firewall jak i licencje na oprogramowanie UTM na okres minimum do 31.12.2026.
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. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP,

pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.

7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
27. Urządzenie ma umożliwiać zastosowanie skanera antywirusowego dostarczonego przez producenta innego niż producent rozwiązania.
28. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
29. 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.
30. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).

31. Ochrona antyspam ma działać w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,
    c. Skaner heurystyczny.
32. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
33. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
34. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
35. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN.
36. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
37. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
38. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
39. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
40. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
41. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
42. Urządzenie ma posiadać wbudowany filtr URL.
43. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
44. Administrator ma mieć możliwość dodawania własnych kategorii URL.
45. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
    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.
46. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
47. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
48. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
49. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
50. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
51. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
52. 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.
53. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
54. 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.

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

81. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
82. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
83. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
84. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
85. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
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 pochodzących 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 posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
102. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
103. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
104. 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).
105. Urządzenie ma posiadać usługę DNS Proxy.
106. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
107. Urządzenie musi mieć zaimplementowane Open API

108. 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.
109. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
110. 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.
111. Urządzenie ma być objęte do 31.12.2026 gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
112. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
113. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
114. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
115. Liczba portów Ethernet 2,5Gbps – min. 8.
116. Liczba portów światłowodowych 1Gbps – min. 1.
117. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
118. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
119. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
120. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
121. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
122. Maksymalna liczba tuneli VPN IPSec – minimum 100.
123. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
124. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
125. Obsługa interfejsów 802.11q (VLAN) – minimum 128
126. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
127. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
128. Urządzenie nie ma limitu na liczbę użytkowników.
129. Liczba reguł filtrowania – minimum 8 192.
130. Liczba tras statycznego routingu – minimum 512.
131. Liczba tras dynamicznego routingu – minimum 10 000.
132. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
133. Urządzenie musi być wyposażone w moduł TPM.

5. Oprogramowanie NAC

Przedmiotem zamówienia jest dostawa oprogramowania klasy NAC – Network Access Control, przeznaczonego do centralnego zarządzania dostępem użytkowników i urządzeń końcowych do sieci przewodowej, bezprzewodowej oraz połączeń zdalnych.

Zamówienie obejmuje dostawę licencji bezterminowej dla minimum 20 urządzeń końcowych jednocześnie poprawnie uwierzytelnionych i zalogowanych do sieci, przeznaczonej do uruchomienia w środowisku maszyny wirtualnej, wraz z dostępem do aktualizacji oraz wsparciem technicznym przez okres do 31.12.2026.

Wymagania:

1. Oprogramowanie musi posiadać interfejs administracyjny dostępny co najmniej w języku polskim.
2. Zarządzanie systemem musi odbywać się centralnie z wykorzystaniem graficznego interfejsu dostępnego przez przeglądarkę internetową.

3. Oprogramowanie musi być dostarczone jako rozwiązanie przeznaczone do instalacji w środowisku wirtualnym.
4. Oprogramowanie musi umożliwiać instalację i prawidłowe działanie w środowisku wirtualizacyjnym klasy Proxmox VE lub równoważnym.
5. Wykonawca musi dostarczyć obraz maszyny wirtualnej lub pliki instalacyjne umożliwiające uruchomienie systemu w środowisku Zamawiającego.
6. Licencja musi umożliwiać obsługę minimum 20 urządzeń końcowych jednocześnie poprawnie uwierzytelnionych i zalogowanych do sieci.
7. Do limitu licencyjnego mogą być zaliczane w szczególności komputery, laptopy, urządzenia mobilne, drukarki, telefony VoIP, kamery IP, urządzenia IoT oraz inne urządzenia podlegające kontroli dostępu do sieci.
8. Licencja musi obejmować wszystkie wymagane funkcjonalności systemu bez konieczności zakupu odrębnych licencji na podstawowe moduły kontroli dostępu, profilowania urządzeń, dostępu gościnnego, zarządzania adresacją IP i integracji z usługami katalogowymi.
9. Oprogramowanie musi umożliwiać kontrolowanie dostępu użytkowników i urządzeń końcowych do sieci przewodowej i bezprzewodowej.
10. Oprogramowanie musi umożliwiać kontrolowanie urządzeń uzyskujących dostęp do zasobów sieciowych za pośrednictwem połączeń VPN.
11. Oprogramowanie musi posiadać wbudowaną funkcjonalność serwera RADIUS, umożliwiającą realizację uwierzytelniania, autoryzacji i rozliczania dostępu do sieci.
12. Oprogramowanie musi obsługiwać standard IEEE 802.1X dla sieci przewodowych oraz bezprzewodowych.
13. Oprogramowanie musi umożliwiać uwierzytelnianie urządzeń niewspierających standardu 802.1X na podstawie adresu MAC, w tym z wykorzystaniem mechanizmu MAB – MAC Authentication Bypass.
14. Oprogramowanie musi umożliwiać stosowanie mechanizmu 802.1X z awaryjnym uwierzytelnianiem urządzeń na podstawie adresu MAC.
15. Oprogramowanie musi obsługiwać uwierzytelnianie z wykorzystaniem co najmniej protokołów PEAP oraz EAP-TLS.
16. Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników przy użyciu loginu i hasła, certyfikatu cyfrowego lub danych urządzenia końcowego.
17. Oprogramowanie musi obsługiwać komunikację RADIUS Authentication, RADIUS Accounting oraz mechanizm CoA – Change of Authorization.
18. Oprogramowanie musi umożliwiać wymuszenie ponownej autoryzacji, odłączenie urządzenia lub zmianę przydzielonego poziomu dostępu bez konieczności ręcznego konfigurowania portu przełącznika.
19. Oprogramowanie musi umożliwiać tworzenie centralnych polityk dostępu do sieci.
20. Polityki dostępu muszą umożliwiać podejmowanie decyzji co najmniej na podstawie:
    a) tożsamości użytkownika,
    b) grupy użytkownika,
    c) urządzenia końcowego,
    d) adresu MAC urządzenia,
    e) rodzaju urządzenia,
    f) systemu operacyjnego,
    g) urządzenia sieciowego, za pośrednictwem którego realizowane jest połączenie,
    h) portu przełącznika lub punktu dostępowego,
    i) lokalizacji lub segmentu sieci,
    j) dnia i godziny połączenia,
    k) wyniku uwierzytelnienia,
    l) poziomu zgodności urządzenia z wymaganiami bezpieczeństwa.
21. Oprogramowanie musi umożliwiać dynamiczne przydzielanie urządzeń i użytkowników do odpowiednich

sieci VLAN na podstawie zdefiniowanych polityk.

22. Oprogramowanie musi umożliwiać skierowanie urządzenia do sieci produkcyjnej, sieci gościnnej, sieci rejestracyjnej, sieci izolowanej lub sieci kwarantanny.
23. Oprogramowanie musi umożliwiać całkowitą odmowę dostępu do sieci urządzeniom lub użytkownikom niespełniającym ustalonych warunków.
24. Oprogramowanie musi współpracować z przełącznikami sieciowymi i punktami dostępowymi różnych producentów, wykorzystującymi otwarte standardy 802.1X, RADIUS, CoA oraz SNMP.
25. Oprogramowanie nie może wymagać stosowania przełączników i punktów dostępowych pochodzących wyłącznie od producenta systemu NAC.
26. Oprogramowanie musi umożliwiać integrację z usługą katalogową Microsoft Active Directory.
27. Oprogramowanie musi umożliwiać integrację z usługami katalogowymi zgodnymi z protokołem LDAP.
28. Oprogramowanie musi umożliwiać pobieranie informacji o użytkownikach i urządzeniach z zewnętrznych źródeł, takich jak Active Directory, LDAP, bazy SQL lub zewnętrzne serwery RADIUS.
29. Integracja z usługą katalogową musi umożliwiać wykorzystywanie kont, grup i innych atrybutów użytkowników podczas tworzenia polityk dostępu.
30. Oprogramowanie musi umożliwiać synchronizację kont administracyjnych, tożsamości użytkowników i urządzeń końcowych z zewnętrznymi źródłami danych.
31. Oprogramowanie musi posiadać mechanizmy zarządzania certyfikatami cyfrowymi.
32. Oprogramowanie musi umożliwiać wykorzystanie wewnętrznego urzędu certyfikacji.
33. Oprogramowanie musi umożliwiać integrację z zewnętrznym urzędem certyfikacji.
34. Oprogramowanie musi umożliwiać wygenerowanie żądania podpisania certyfikatu CSR w celu wykorzystania certyfikatu wystawionego przez zewnętrzny urząd certyfikacji.
35. Oprogramowanie musi na bieżąco wykrywać urządzenia końcowe podłączone do sieci.
36. Oprogramowanie musi umożliwiać identyfikację urządzeń sieciowych, do których podłączone są urządzenia końcowe.
37. Oprogramowanie musi umożliwiać ustalenie co najmniej adresu IP, adresu MAC, rodzaju urządzenia, producenta, systemu operacyjnego oraz miejsca podłączenia urządzenia do sieci, o ile dane te są możliwe do uzyskania.
38. Oprogramowanie musi umożliwiać automatyczne profilowanie i klasyfikowanie urządzeń końcowych.
39. Profilowanie urządzeń musi umożliwiać wykorzystanie wielu metod identyfikacji, w tym co najmniej informacji pochodzących z DHCP, DNS, RADIUS, HTTP/HTTPS lub aktywnego rozpoznawania urządzeń.
40. Oprogramowanie musi umożliwiać klasyfikację urządzeń co najmniej według typu urządzenia, systemu operacyjnego oraz producenta.
41. Oprogramowanie musi umożliwiać identyfikację między innymi komputerów, urządzeń mobilnych, drukarek, telefonów, kamer, urządzeń sieciowych oraz urządzeń IoT.
42. Oprogramowanie musi posiadać graficzną mapę powiązań urządzeń końcowych i urządzeń sieciowych.
43. Mapa musi umożliwiać sprawdzenie, które urządzenia są podłączone do sieci oraz za pośrednictwem którego urządzenia sieciowego realizowane jest połączenie.
44. Oprogramowanie musi posiadać moduł zarządzania adresacją IP – IPAM.
45. Moduł IPAM musi umożliwiać przegląd wykorzystania adresów IP oraz powiązanie adresu IP z urządzeniem lub użytkownikiem.
46. Oprogramowanie musi umożliwiać wykrywanie kolizji adresów IP.
47. Oprogramowanie musi umożliwiać wykrywanie urządzeń nieznanych, niezgodnych z polityką lub błędnie skonfigurowanych.
48. Oprogramowanie musi umożliwiać wykrywanie zdarzeń takich jak:
    a) klonowanie adresu MAC,
    b) klonowanie adresu IP,
    c) skanowanie portów,

d) użycie nieprawidłowej bramy sieciowej,
e) pojawienie się nieautoryzowanego urządzenia,
f) naruszenie zdefiniowanej polityki dostępu.

49. Oprogramowanie musi umożliwiać automatyczne odłączenie lub skierowanie do kwarantanny urządzenia, dla którego wykryto zagrożenie albo niezgodność z polityką bezpieczeństwa.
50. Oprogramowanie musi umożliwiać zapewnienie dostępu gościnnego do sieci.
51. Oprogramowanie musi umożliwiać tworzenie kont gościnnych obowiązujących przez określony czas.
52. Oprogramowanie musi umożliwiać rejestrację prywatnych urządzeń użytkowników w modelu BYOD.
53. Oprogramowanie musi posiadać wbudowany portal uwierzytelniający typu Captive Portal lub umożliwiać współpracę z zewnętrznym Captive Portalem.
54. Portal gościnny musi umożliwiać przydzielenie użytkownikowi ograniczonego dostępu do wskazanych zasobów sieciowych lub Internetu.
55. Oprogramowanie musi umożliwiać ograniczenie czasu obowiązywania dostępu gościnnego.
56. Oprogramowanie musi umożliwiać pozyskiwanie dodatkowych informacji o stanie bezpieczeństwa urządzenia końcowego za pomocą dedykowanego komponentu instalowanego na urządzeniu lub rozwiązania równoważnego.
57. Mechanizm oceny stanu urządzenia musi umożliwiać co najmniej sprawdzenie, czy urządzenie posiada wymagane oprogramowanie ochronne lub inne elementy wskazane przez administratora jako istotne dla bezpieczeństwa.
58. Oprogramowanie musi umożliwiać uzależnienie dostępu do sieci od wyniku oceny stanu bezpieczeństwa urządzenia.
59. Instalacja dodatkowego komponentu na urządzeniach końcowych nie może być wymagana do realizowania podstawowej autoryzacji 802.1X lub MAB.
60. Oprogramowanie musi umożliwiać dwukierunkową integrację z zewnętrznymi systemami bezpieczeństwa, w szczególności systemami klasy Firewall, UTM, MDM, EDR lub SIEM.
61. Integracja musi umożliwiać automatyczne wykonanie reakcji, takiej jak odłączenie albo odizolowanie urządzenia, po otrzymaniu informacji o wykrytym zagrożeniu.
62. Oprogramowanie musi umożliwiać monitorowanie urządzeń sieciowych z wykorzystaniem protokołu SNMP.
63. Monitoring urządzeń sieciowych musi umożliwiać sprawdzenie co najmniej dostępności urządzenia, jego obciążenia oraz wykorzystania procesora i pamięci, o ile urządzenie udostępnia takie informacje.
64. Oprogramowanie musi umożliwiać przegląd informacji dotyczących przebiegu procesu autoryzacji urządzeń i użytkowników.
65. Oprogramowanie musi rejestrować zdarzenia dotyczące poprawnych i niepoprawnych prób uzyskania dostępu do sieci.
66. Oprogramowanie musi umożliwiać wyszukiwanie urządzeń i użytkowników na podstawie dostępnych atrybutów.
67. Oprogramowanie musi umożliwiać centralne zarządzanie podsieciami, sieciami VLAN, sieciami bezprzewodowymi oraz urządzeniami sieciowymi.
68. Oprogramowanie musi umożliwiać działanie w konfiguracji wysokiej dostępności, bez konieczności dostarczania takiej konfiguracji w ramach niniejszej pozycji.
69. Wszystkie funkcjonalności wskazane w opisie muszą być dostępne w ramach dostarczonej licencji lub wymaganych komponentów dostarczonych bez dodatkowych opłat licencyjnych.
70. Zamawiający wymaga dostarczenia licencji bezterminowej.
71. Licencja musi obejmować minimum 20 urządzeń końcowych jednocześnie poprawnie uwierzytelnionych i zalogowanych do sieci.
72. Licencja nie może wygasać po zakończeniu okresu wsparcia technicznego.
73. Zakończenie okresu wsparcia nie może powodować wyłączenia systemu ani utraty skonfigurowanych

polityk dostępu.

74. Okres wsparcia technicznego musi do 31.12.2026.

6. Stacja robocza fizyczna z rolą stacji przesiadkowej

Przedmiotem zamówienia jest dostawa 2 szt. mobilnych stacji roboczych.
Wymagania:

1. Procesor: minimum 6 rdzeni i 12 wątków, osiągający wynik nie mniejszy niż 19 500 punkty w teście PassMark CPU Mark (Average CPU Mark), według wyników opublikowanych na stronie www.cpubenchmark.net na 30 dni przed publikacją postępowania.
2. Pamięć RAM: minimum 16 GB DDR5, z możliwością rozbudowy.
3. Dysk twardy: SSD NVMe o pojemności minimum 512 GB.
4. Wyświetlacz: matryca IPS o przekątnej 16", rozdzielczość minimum 1920 × 1200 pikseli (WUXGA), powłoka antyrefleksyjna.
5. Karta graficzna: zintegrowana, obsługująca rozdzielczość ekranu oraz zewnętrzne monitory.
6. Łączność bezprzewodowa: Wi-Fi 6E lub nowsze, Bluetooth minimum 5.3.
7. Modem komórkowy: wbudowany modem 4G LTE umożliwiający korzystanie z mobilnego Internetu za pomocą karty SIM, fabrycznie zainstalowany i gotowy do pracy.
8. Interfejsy: minimum 2 × USB-A, 2 × USB-C, HDMI, RJ-45 (Gigabit Ethernet), złącze słuchawkowo-mikrofonowe.
9. Klawiatura: pełnowymiarowa, z wydzielonym blokiem numerycznym.
10. Multimedia: zintegrowana kamera internetowa, mikrofon i głośniki.
11. Bezpieczeństwo: sprzętowy moduł TPM 2.0, możliwość zabezpieczenia dostępu do BIOS/UEFI hasłem.
12. System operacyjny: Microsoft Windows 11 Pro 64-bit, w polskiej wersji językowej, fabrycznie zainstalowany i aktywowany, lub rozwiązanie równoważne zapewniające wymaganą kompatybilność ze środowiskiem Zamawiającego. Za system równoważny Zamawiający uzna system operacyjny spełniający łącznie następujące wymagania:
    a. Architektura 64-bitowa, interfejs użytkownika w języku polskim.
    b. Możliwość dołączenia komputera do domeny Microsoft Active Directory, uwierzytelniania użytkowników domenowych oraz obsługi zasad grupowych (GPO).
    c. Pełna kompatybilność z oprogramowaniem użytkowanym przez Zamawiającego, przeznaczonym dla środowiska Windows 11 Pro.
    d. Obsługa szyfrowania dysków, sprzętowego modułu TPM 2.0 oraz zdalnego pulpitu.
    e. Możliwość centralnego zarządzania komputerem, kontami użytkowników i politykami bezpieczeństwa.
    f. Zapewnienie automatycznych aktualizacji systemu i poprawek bezpieczeństwa.
    g. Licencja umożliwiająca bezterminowe użytkowanie systemu w środowisku organizacyjnym Zamawiającego, bez dodatkowych opłat abonamentowych.
13. System musi być fabrycznie zainstalowany, aktywowany i gotowy do użytkowania, bez konieczności zakupu dodatkowego oprogramowania w celu spełnienia powyższych wymagań.
14. Zasilanie: akumulator litowo-jonowy, zasilacz sieciowy dostarczony w komplecie.
15. Stan urządzenia: sprzęt fabrycznie nowy, kompletny, nieużywany, pochodzący z oficjalnego kanału dystrybucji producenta.

7. System typu NDR z oprogramowaniem HoneyPot

Dostawa urządzenia klasy NDR wraz z oprogramowaniem HoneyPot.
Wymagania:

1. System NDR musi posiadać możliwość integracji z dowolnym systemem bezpieczeństwa, za pomocą linii komend. Musi istnieć możliwość uruchomiania dowolnego polecenia na systemie zewnętrznym, wraz z jego parametryzacją dynamiczna (np. adres IP atakującego)
2. Elementy systemu bezpieczeństwa
   a. Wysokość 1U do montażu w szafie rack.
   b. Posiadać co najmniej dwa porty USB
   c. Urządzenie musi posiadać dedykowany port do zarządzania
   d. Urządzenie musi posiadać minimum interfejsów: 2x SFP+, 8x SFP, 8x GE
   e. Musi obsługiwać co najmniej 1T przestrzeni dyskowej SSD.
   f. Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń
   g. Proponowane rozwiązanie musi obsługiwać minimum 750 tys . jednoczesnych sesji.
   h. Proponowane rozwiązanie musi obsługiwać 25000 nowych sesji /s w ruchu HTTP.
3. Usługi sieciowe
   a. Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta.
   b. Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń
   c. Musi posiadać możliwość rozwiązywania wiadomości przez protokół MPLS, VXLAN oraz QinQ i wykrywania zagrożeń w tych wiadomościach.
   d. System musi posiadać możliwość deszyfrowania ruchu kierowanego na/wracającego z kluczowych serwerów. Funkcjonalność musi być realizowana na tej samej platformie co pozostałe elementy systemu
4. Kontrola aplikacji
   a. Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimediów itp.
   b. Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android.
   c. Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje.
5. Wykrywanie zagrożeń
   a. Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń.
   b. Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow zarówno dla IPv4 jak i IPv6
   c. Rozwiązanie powinno obsługiwać ochronę przez atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA
   d. Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp.
   e. Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku.
   f. Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS.
   g. Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS.

h. Rozwiązanie musi mieć opcję przechwytywania pakietów
i. Rozwiązanie musi umieć wykrywa reverse-shell
j. Rozwiązanie potrafi zdefiniować odpowiednie treshholdy chroniące przed atakami Flood, bazując na parametrach dostarczonego ruchu
k. System musi mapować wykryte zagrożenia na framework MITRE ATT&CK

6. Skanowanie antywirusowe
   a. Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur.
   b. Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP.
   c. Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach
   d. Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików
7. Wykrywanie botnetów C&C
   a. Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C.
   b. Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C
   c. Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen.
   d. Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS.
   e. Rozwiązanie musi wspierać właczenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA.
   f. Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS.
8. Sandbox w chmurze
   a. Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanych zagrożeń
   b. Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy.
   c. Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP.
   d. Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF oraz skrypty
   e. Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików.
   f. Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznane zagrożenie.
9. Wykrywanie spamu
   a. Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym
   b. Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości.
   c. Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3
   d. Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.
10. Dodatkowe funkcje ochrony
    a. Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp.
    b. Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP
    c. Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu.

   d. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop
11. Web Attack Detection
   a. System NDR musi posiadać wbudowany w siebie dwukierunkowy moduł ochrony aplikacji webowych (WAF)
   b. Moduł WAF musi posiadać co najmniej 1200 wbudowanych reguł
   c. Reguły muszą być podzielona na kategorie, co najmniej: anomalie HTTP, Injection, XSS, Vulnerabilities, Malware, wyciek informacji, kontrola dostępu
   d. System za pomocą panelu WEBUI musi umożliwiać tworzenie własnych sygnatur dla modułu WAF
   e. System musi pozwalać na selektywne włączanie lub wyłączanie poszczególnych reguł modułu WAF. Niedopuszczalnym jest, by moduł włączany lub wyłączany jako całość.
   f. System musi pozwalać na dodawanie adresów źródłowych i docelowych do białej listy modułu WAF
12. Inteligentne funkcje bezpieczeństwa
   a. Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki.
   b. Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym.
   c. Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp.
   d. Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania
   e. Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut.
   f. Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów.
   g. Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS
   h. Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanych aplikacji
   i. Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym
   j. Rozwiązanie musi zapewniać analizę kryminalistyczną , w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń.
   k. Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia
   l. Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta
   m. Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd.
   n. Rozwiązanie musi obsługiwać przechwytywanie pakietów online
   o. Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania
   p. Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych
   q. Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę

r. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dektop, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalność funkcji śledzenia zagrożeń.

13. Widoczność ryzyka/zagrożeń
    a. Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego.
    b. Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów, w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch.
    c. Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu.
    d. Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp.
    e. Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni.
    f. Rozwiązanie musi wspierać wskazanie ścieżki ataku.
14. Analiza i odpowiedzi na incydenty
    a. Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury
    b. Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach.
    c. Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie.
    d. Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania.
    e. Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpowiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail)
15. Administracja
    a. Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI)
    b. Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli
    c. Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło
    d. Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.
    e. Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych
    f. Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny
    g. Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń
16. Logowanie i raportowanie
    a. Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP.
    b. Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na dysku, nowych połączeń itp.
    c. Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS.
    d. Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń.
    e. Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje

f. Wstępnie zdefiniowane zadania raportowania
g. Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni.
h. Rozwiązanie musi wspierać restAPI

17. Gwarancja producenta min. 12 miesięcy na dostarczone elementy systemu
18. Licencje wieczyste na wszystkie funkcje bezpieczeństwa producentów lub na okres minimum do 31.12.2026 (IPS, AV, AS, WAF, Cloud-Sandbox, IP Reputation, Botnet C&C)
19. Wsparcie techniczne dostawcy rozwiązań w języku polskim

8. Macierz dyskowa

Przedmiotem zamówienia jest macierz blokowa do zadań produkcyjnych.
Wymagania:

1. Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowana macierz nie może przekroczyć rozmiaru 2U. Oferowana obudowa musi umożliwiać instalację min 25 dysków.
2. Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active-active. Akceptowalna architektura to symmetric active-active, to znaczy pracę kontrolerów w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery nie mogą pracować w trybie active-passive.
3. Oferowane urządzenie musi być przystosowane do zasilania z sieci AC oraz wyposażone w kable zasilające PDU. Macierz musi być wyposażona w zdublowany, redundantny system zasilania, umożliwiający prawidłową, nieprzerwaną pracę urządzenia w przypadku awarii dowolnego pojedynczego źródła zasilania.
4. Surowa przestrzeń dyskowa (RAW) zbudowana tylko i wyłącznie za pomocą dysków SSD SAS musi wynosić min. 30 TB. Przestrzeń użytkowa musi być zbudowana z RAID 6 z 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności 1 dysku. Ze względów wydajnościowych oraz niezawodnościowych rozmiar pojedynczego dysku nie może być większy niż 4 TB. Dyski muszą być wyposażone w podwójne interfejsy.
5. Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.
6. Rozbudowa oferowanej macierzy, do co najmniej 80 szt dysków SSD SAS, bez wymiany kontrolerów macierzowych oraz bez rozbudowy o dodatkowe kontrolery, tylko poprzez dodawanie półek i dysków SSD SAS. Macierz nie może obsługiwać dysków HDD.
7. Co najmniej 64GB pamięci cache na całą macierz (dwa kontrolery). Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć.
8. Razem kontrolery muszą udostępnić minimum 4 porty optyczne 10Gb Eth z modułami optycznymi SFP+ Multimode, 8 portów miedzianych 1Gb Eth oraz 8 portów FC 16G z modułami optycznymi Multimode.
9. Macierz musi posiadać wbudowane min 4 porty SAS 12Gb/s do podłączenia półek dyskowych.
10. Wymagane wsparcie dla FC, iSCSI.
11. Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków bez utraty danych.
12. Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu

skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Macierz musi wspierać nie mniej niż 1024 LUNów. Wymagana możliwość tworzenia grup wolumenów. Max liczba LUNów w grupie wolumenów nie może być mniejsza niż 100. Wymagane dostarczenie w/w funkcjonalności na zainstalowaną przestrzeń dyskową.

13. Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy w tym monitorowanie wydajności obiektów takich jak:
    a. cała macierz
    b. kontrolery
    c. porty front-end
    d. dyski
    e. LUNy
    f. Hosty

    Jeżeli do obsługi tych funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
14. Wymagane jest stałe monitorowanie stanu macierzy pod kątem parametrów takich jak:
    a. operacje wejścia/wyjścia IOPS
    b. przepustowość (KB/s lub MB/s)
    c. czas odpowiedzi (latency)

    Jeżeli do obsługi tych funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
15. Wymagana możliwość monitorowania stanu żywotności dysków SSD SAS. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
16. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
17. Wymagana możliwość konfigurowania zasobów macierzy. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
18. Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych. Snapshoty muszą być wykonywanie w technologii ROW (Redirect On Write). Macierz musi obsługiwać min 2000 snapshotów. Wymagane wsparcie dla snapshotów kaskadowych. Wymagana możliwość tworzenia harmonogramu wykonywania snapshotów oraz zabezpieczenia migawek przed modyfikacją lub usunięciem pod kątem szybkiego przywrócenia danych w przypadku ataku ransomware. Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model macierzy.
19. Tworzenie na żądanie kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z wolumenu źródłowego na docelowy oraz resynchronizację danych z wolumenu docelowego na źródłowy. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
20. Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybie asynchronicznym oraz synchronicznym przy wykorzystaniu portów FC lub IP. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.
21. Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage Metro Cluster). Macierz musi dostarczać funkcjonalność klastra klasy "wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform oprogramowania i sprzętowych z wykorzystaniem synchronicznej replikacji danych po protokole FC lub IP pomiędzy 2 macierzami. Pod użytym pojęciem "wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie

bezprzerwowego działania środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy (macierz preferowana) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodujących dla danego środowiska brak dostępu do zasobów macierzy preferowanej. Funkcjonalność klastra "wysokiej dostępności" pozwala na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy preferowanej na niepreferowaną w przypadku awarii macierzy preferowanej (tzw. automated failover). Wymagany jest również automatyczny failover z macierzy niepreferowanej na preferowaną. Dopuszczalne jest zastosowanie tzw arbitra (serwer quorum). Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.

22. Macierz musi posiadać możliwość zapewnienia ciągłości biznesu na oczekiwanym poziomie usług (QoS) poprzez definicję polityk QoS w oparciu o maksymalne progi wydajności IOPS i MB/s. Musi istnieć możliwość określenia polityk QoS na poziomie wolumenów. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
23. Macierz musi oferować wsparcie dla zachowania integralności danych na całej ścieżce transferu (ang. End-to-End) zgodnego ze standardem/specyfikacją T10 PI.
24. Wsparcie, dla co najmniej Microsoft Server Windows 2016/2019/2022/2025, VMware 6.x/7.x, Linux RedHat 7.x/8.x, CentOS 7.x/8.x
25. Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.
26. Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania.
27. Macierz musi umożliwiać zdalne zarządzanie.
28. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.
29. Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta oferowanej macierzy, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.
30. Wymagana gwarancja na 24 miesiące w trybie 9x5 NBD. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
31. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.

9. NAS

Przedmiotem zamówienia jest serwer typu NAS do realizacji kopii zapasowych wraz z funkcjonalnością deduplikacji.

Wymagania:

1. Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowany deduplikator nie może przekroczyć rozmiaru 2U. Oferowana obudowa musi umożliwiać instalację min 12 dysków 3.5”.
2. Deduplikator musi być wyposażony w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler.
3. Oferowany model deduplikatora musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu co najmniej 5 TB/h (dane podawane przez producenta). Dodatkowo wymagana zagregowana wydajność backupu przy zastosowaniu deduplikacji na źródle co najmniej 15 TB/h (dane podawane przez producenta).
4. Surowa przestrzeń dyskowa (RAW) stworzona w oparciu o dyski NL SAS musi wynosić min. 64TB. Dyski muszą być skonfigurowane w RAID 6 z min. 1 dyskiem hot-spare lub przestrzenią hot-spare równą

pojemności min. 1 dysku. Dodatkowo wymagane jest zastosowanie co najmniej 4 dysków SSD SAS o łącznej pojemności RAW min. 3,8TB jako cache pod zapis backupu.

5. Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej tolerującej jednoczesną awarię 2 dysków bez utraty danych.
6. Wymagana możliwość rozbudowy przestrzeni użytkowej poprzez instalację dysków i półek dyskowych oraz dodanie licencji (jeśli będzie wymagana) do min 300 TB.
7. Co najmniej 256GB pamięci cache na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania.
8. Urządzenie musi posiadać minimum:
    a. 8 portów RJ45 Ethernet 1 Gb/s oraz 4 porty SFP+ Ethernet 10 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS, NFS.
    b. Wszystkie porty SFP+ wyposażone we wkładki optyczne MM.
9. Wymagana możliwość agregowania portów (bond port).
10. Wymagane wsparcie dla NFS, CIFS.
11. Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak:
    a. cały deduplikator
    b. kontrolery
    c. CPU
    d. porty front-end
    e. porty logiczne
    f. dyski
    g. file systemy

    Jeżeli do obsługi tych funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
12. Wymagane jest stałe monitorowanie stanu deduplikatora pod kątem parametrów takich jak:
    a. operacje wejścia/wyjścia IOPS
    b. przepustowość (KB/s lub MB/s)
    c. czas odpowiedzi (latency)
    d. średnie użycie (w % dla CPU)

    Jeżeli do obsługi tych funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
13. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
14. Wymagany dostęp do informacji o wykorzystanej fizycznej przestrzeni oraz aktualnym współczynniku redukcji danych. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
15. Wymagane wsparcie dla Multi-factor authentication. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
16. Wymagana możliwość definiowania polityk logowania. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
17. Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

18. Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
19. Musi być oficjalne wsparcie producenta dla oferowanego deduplikatora maksymalnego stopnia redukcji danych co najmniej 65:1.
20. Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
21. Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
22. Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system'ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.
23. Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM) na poziomie całego file system'u. Dostarczenie licencji na tą funkcjonalność jest wymagane na tym etapie postępowania.
24. Urządzenie musi umożliwiać replikację danych do drugiego urządzenia w ramach tej samej rodziny oferowanego deduplikatora. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję. Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.
25. Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00). Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.
26. Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veeam Backup&Replication.
27. Deduplikator musi posiadać możliwość upgrade'u firmware-u kontrolerów bez przerywania dostępu do danych.
28. Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączania.
29. Urządzenie musi umożliwiać zdalne zarządzanie.
30. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.
31. Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta oferowanego deduplikatora, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.
32. Wymagana gwarancja na 24 miesiące w trybie 9x5 NBD. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
33. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.

10. System wirtualizacyjny

Przedmiotem zamówienia jest dostawa, instalacja i wdrożenie platformy wirtualizacyjnej.
Wymagania:

1. Oferowane rozwiązanie musi zapewniać kompletną platformę wirtualizacyjną obejmującą:
   a. wirtualizację mocy obliczeniowej,
   b. wysoką dostępność maszyn wirtualnych,
   c. mechanizmy migracji maszyn wirtualnych,
   d. centralne zarządzanie środowiskiem wirtualnym,
   e. integrację z systemami wykonywania kopii zapasowych,
   f. możliwość realizacji funkcji wirtualizacji sieciowej SDN,
   g. możliwość realizacji funkcji programowo definiowanej pamięci masowej SDS.
2. Zamawiający dopuszcza realizację wymaganych funkcjonalności:
   a. w ramach jednego produktu,
   b. w ramach systemu operacyjnego hosta,
   c. za pomocą zestawu wzajemnie interoperacyjnych komponentów programowych,
   d. z wykorzystaniem dodatkowych komponentów SDS, SDN, zarządzania, backupu lub bezpieczeństwa pochodzących od tego samego lub różnych producentów.
3. Zamawiający nie wymaga, aby wszystkie funkcjonalności platformy wirtualizacyjnej, SDS i SDN były zawarte w jednej edycji systemu operacyjnego hosta.
4. Zamawiający nie wymaga zastosowania określonej edycji systemu operacyjnego, w szczególności nie wymaga zastosowania edycji zapewniającej nieograniczone prawa do uruchamiania wirtualnych instancji systemu operacyjnego.
5. Jeżeli dla realizacji którejkolwiek z wymaganych funkcjonalności konieczny jest odrębny komponent, system operacyjny, licencja, subskrypcja lub oprogramowanie dodatkowe, Wykonawca zobowiązany jest dostarczyć wszystkie elementy wymagane do prawidłowego działania zaoferowanej konfiguracji.
6. Poszczególne komponenty rozwiązania muszą być wzajemnie kompatybilne oraz wspierane w zaoferowanej konfiguracji przez ich producentów.
7. W przypadku wykorzystania komponentów różnych producentów Wykonawca odpowiada za prawidłową integrację całego rozwiązania i nie może przenosić na Zamawiającego obowiązku ustalania, który producent odpowiada za występujący problem integracyjny.
8. Oferowana warstwa wirtualizacji musi być rozwiązaniem klasy bare-metal/type-1, w którym hypervisor korzysta bezpośrednio z mechanizmów wirtualizacji sprzętowej serwera.
9. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi umożliwiać obsługę serwera wyposażonego w co najmniej:
   a. 512 logicznych procesorów/wątków procesora,
   b. 12 TB fizycznej pamięci RAM.
10. Oprogramowanie do wirtualizacji musi umożliwiać skonfigurowanie pojedynczej maszyny wirtualnej posiadającej od 1 do co najmniej 128 procesorów wirtualnych.
11. Oprogramowanie do wirtualizacji musi umożliwiać skonfigurowanie pojedynczej maszyny wirtualnej posiadającej co najmniej 6 TB pamięci operacyjnej RAM.
12. Oprogramowanie do wirtualizacji musi umożliwiać skonfigurowanie pojedynczej maszyny wirtualnej posiadającej co najmniej 8 wirtualnych kart sieciowych.
13. Dla maszyn wirtualnych i systemów operacyjnych wymagających komunikacji szeregowej rozwiązanie musi umożliwiać realizację co najmniej dwóch logicznych kanałów komunikacji szeregowej, z wykorzystaniem wirtualnych portów COM, named pipe lub mechanizmu równoważnego, o ile stosowany typ/generacja maszyny wirtualnej wspiera taką funkcjonalność.
14. Rozwiązanie musi umożliwiać uruchamianie jako systemy gościnne co najmniej systemów z rodzin:
   a. Microsoft Windows Server,
   b. Microsoft Windows,
   c. Red Hat Enterprise Linux,

   d. SUSE Linux Enterprise Server,
   e. Debian,
   f. Ubuntu,
   g. Oracle Linux,
   h. CentOS lub kompatybilnych dystrybucji Linux,
   i. FreeBSD.
15. Wymagane jest wsparcie dla aktualnie wspieranych przez producenta platformy wirtualizacyjnej wersji systemów gościnnych, w tym co najmniej Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025 oraz Windows 10 i Windows 11.
16. Rozwiązanie powinno umożliwiać techniczne uruchamianie starszych systemów operacyjnych, w szczególności Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows 7, Windows 8.1, RHEL 5/6/7 i SLES 11/12, jeżeli dana wersja platformy wirtualizacyjnej zapewnia taką kompatybilność. Wymaganie to nie oznacza obowiązku zapewnienia przez producenta platformy wsparcia serwisowego dla systemów operacyjnych, których cykl życia został zakończony przez ich producentów.
17. Rozwiązanie musi posiadać mechanizm dynamicznego zarządzania pamięcią operacyjną maszyn wirtualnych umożliwiający co najmniej:
   a. określenie pamięci początkowej,
   b. określenie pamięci minimalnej,
   c. określenie pamięci maksymalnej,
   d. dynamiczne zwiększanie lub odzyskiwanie pamięci w zależności od zapotrzebowania maszyny wirtualnej, dla systemów gościnnych wspierających tę funkcjonalność.
18. Zamawiający nie wymaga stosowania mechanizmu, którego działanie polega na trwałym przydzielaniu maszynom wirtualnym większej ilości rzeczywiście wykorzystywanej pamięci RAM niż dostępna fizycznie w serwerze.
19. Rozwiązanie musi umożliwiać tworzenie wirtualnych dysków wykorzystujących mechanizm dynamicznej alokacji przestrzeni, pozwalający zadeklarować maszynie wirtualnej większą maksymalną pojemność dysku niż przestrzeń fizycznie zajęta przez dany dysk w chwili jego utworzenia.
20. Rozwiązanie musi zapewniać możliwość wykorzystania sprzętowego wsparcia procesora dla wirtualizacji zagnieżdżonej i umożliwiać uruchomienie warstwy wirtualizacyjnej wewnątrz odpowiednio skonfigurowanej maszyny wirtualnej.
21. Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi, EDR/XDR oraz innymi systemami bezpieczeństwa firm trzecich. Integracja może być realizowana na poziomie hosta, systemu gościnnego, systemu zarządzającego, poprzez API, rozszerzenia, agenta lub inny mechanizm wspierany przez producentów współpracujących rozwiązań.
22. Nie wymaga się bezagentowego skanowania antywirusowego realizowanego bezpośrednio przez hypervisor.
23. Rozwiązanie musi zapewniać możliwość zdalnego i lokalnego zarządzania hostami fizycznymi poprzez bezpieczne, uwierzytelnione i szyfrowane kanały administracyjne.
24. Rozwiązanie musi umożliwiać nadawanie praw administracyjnych nazwanym użytkownikom lub grupom użytkowników bez konieczności udostępniania wspólnego konta Administrator/root.
25. System musi umożliwiać integrację uwierzytelniania i autoryzacji administratorów co najmniej z usługą katalogową Microsoft Active Directory lub równoważną usługą katalogową.
26. Oprogramowanie do wirtualizacji musi umożliwiać:
   a. eksport maszyny wirtualnej,
   b. import maszyny wirtualnej,
   c. kopiowanie lub klonowanie maszyny wirtualnej, bez konieczności ręcznego odtwarzania jej konfiguracji sprzętowej.
27. Rozwiązanie musi umożliwiać wykonywanie punktów kontrolnych/migawek działających maszyn wirtualnych.
28. Mechanizm punktów kontrolnych musi umożliwiać co najmniej:
   a. wykonanie punktu kontrolnego z zachowaniem konfiguracji i stanu dysków,

   b. dla odpowiednich typów punktów kontrolnych – zachowanie bieżącego stanu pamięci maszyny,
   c. wykonywanie punktów kontrolnych zgodnych z mechanizmami VSS lub równoważnymi mechanizmami spójności aplikacyjnej dla systemów gościnnych, które je wspierają.
29. Punkty kontrolne nie mogą być traktowane jako jedyny mechanizm wykonywania kopii zapasowych.
30. Rozwiązanie musi umożliwiać zmianę zasobów przydzielonych do działającej maszyny wirtualnej bez jej wyłączania, co najmniej w zakresie:
   a. zwiększenia pojemności wspieranego wirtualnego dysku,
   b. dynamicznej zmiany lub dodania pamięci RAM dla systemów gościnnych i konfiguracji wspierających tę funkcjonalność.
31. Rozwiązanie musi umożliwiać integrację z mechanizmami automatycznego wdrażania systemów operacyjnych hostów fizycznych wykorzystującymi rozruch sieciowy PXE lub mechanizm równoważny.
32. Funkcja wdrażania systemów hostów poprzez PXE może być realizowana przez odrębny komponent zarządzający lub wdrożeniowy i nie musi stanowić funkcjonalności samego hypervisora.
33. System musi wspierać mechanizmy sprzętowej akceleracji urządzeń I/O, w tym co najmniej SR-IOV dla zgodnych urządzeń sieciowych.
34. Rozwiązanie musi umożliwiać bezpośrednie przypisanie kompatybilnego urządzenia PCIe do maszyny wirtualnej lub wykorzystanie sprzętowego mechanizmu partycjonowania urządzenia, jeżeli funkcjonalność taka jest wspierana przez dane urządzenie, platformę sprzętową i hypervisor.
35. Nie wymaga się możliwości logicznego podziału każdego dowolnego urządzenia PCIe pomiędzy wiele maszyn wirtualnych.
36. System musi posiadać funkcjonalność wirtualnego przełącznika Ethernet umożliwiającego:
   a. tworzenie sieci wewnętrznych dla maszyn działających na jednym hoście,
   b. komunikację maszyn wirtualnych z siecią fizyczną,
   c. separację wybranych sieci maszyn wirtualnych.
37. Pojedynczy host musi umożliwiać obsługę co najmniej 4000 logicznych portów lub połączeń wirtualnych przełączników albo nie posiadać programowego ograniczenia niższego niż wskazana wartość.
38. Rozwiązanie musi umożliwiać wykorzystanie co najmniej dwóch fizycznych interfejsów sieciowych w celu zapewnienia redundancji połączenia hosta.
39. Redundancja może być realizowana przez:
   a. teaming kart sieciowych,
   b. Switch Embedded Teaming,
   c. bonding,
   d. LACP,
   e. rozwiązanie równoważne.
40. Awaria pojedynczego fizycznego interfejsu sieciowego wykorzystywanego w układzie redundantnym nie może powodować trwałej utraty komunikacji maszyn wirtualnych, jeżeli pozostała ścieżka jest sprawna.
41. Wirtualny przełącznik musi obsługiwać VLAN zgodny z IEEE 802.1Q lub rozwiązanie równoważne zapewniające logiczną separację sieci w warstwie drugiej.
42. Kontrola komunikacji pomiędzy odseparowanymi segmentami sieci w warstwie trzeciej musi być realizowana przez routing, ACL, firewall, mechanizmy SDN lub rozwiązanie równoważne.
43. Rozwiązanie musi umożliwiać wykorzystanie interfejsów sieciowych o przepustowości co najmniej 10 Gb/s.
44. Rozwiązanie musi umożliwiać wykorzystanie wielu fizycznych interfejsów lub ścieżek sieciowych w celu zwiększenia dostępnej przepustowości i/lub zapewnienia redundancji transmisji.
45. Mechanizmy migracji maszyn wirtualnych muszą umożliwiać wykorzystanie sieci co najmniej 10 GbE oraz, jeżeli zastosowana konfiguracja to wspiera, więcej niż jednej ścieżki sieciowej.
46. Rozwiązanie musi umożliwiać utworzenie wydzielonej logicznie lub fizycznie sieci przeznaczonej dla migracji maszyn wirtualnych.
47. Oprogramowanie do wirtualizacji musi umożliwiać przełączenie komunikacji na dostępną ścieżkę sieciową w przypadku awarii jednego z interfejsów lub połączeń wykorzystywanych w konfiguracji redundantnej.

48. Oprogramowanie do wirtualizacji musi współpracować z zewnętrzną współdzieloną pamięcią masową klasy SAN lub rozwiązaniem równoważnym.
49. Rozwiązanie musi umożliwiać wykorzystanie co najmniej jednego z powszechnie stosowanych protokołów lub technologii współdzielonej pamięci masowej, takich jak:
    a. Fibre Channel,
    b. iSCSI,
    c. SMB 3.x,
    d. NFS – jeżeli wspierany przez zaoferowaną platformę,
    e. rozwiązanie równoważne zapewniające współdzielenie przestrzeni przez hosty klastra.
50. W przypadku zastosowania pamięci masowej SAN rozwiązanie musi umożliwiać konfigurację redundantnych ścieżek dostępu do pamięci masowej z wykorzystaniem MPIO lub mechanizmu równoważnego.
51. Awaria pojedynczej ścieżki do współdzielonej pamięci masowej nie może powodować trwałej utraty dostępu do danych, jeżeli dostępna jest druga sprawna ścieżka.
52. Oprogramowanie do wirtualizacji musi zapewniać możliwość utworzenia pojedynczego wirtualnego dysku maszyny wirtualnej o maksymalnym rozmiarze co najmniej 62 TB.
53. Rozwiązanie musi obsługiwać mechanizmy jakości usług dla operacji wejścia/wyjścia pamięci masowej lub mechanizmy pozwalające ograniczać, kontrolować albo priorytetyzować operacje I/O pomiędzy wybranymi maszynami wirtualnymi.
54. Rozwiązanie musi umożliwiać przenoszenie działających maszyn wirtualnych pomiędzy serwerami fizycznymi z zachowaniem ciągłości ich pracy.
55. Migracja działającej maszyny wirtualnej nie może wymagać jej wyłączenia.
56. Rozwiązanie musi umożliwiać migrację maszyn pomiędzy węzłami tego samego klastra.
57. Jeżeli architektura zaoferowanego rozwiązania na to pozwala, rozwiązanie musi umożliwiać również migrację pomiędzy hostami lub klastrami niewchodzącymi w skład tego samego klastra HA.
58. System musi umożliwiać migrację konfiguracji i przestrzeni dyskowej maszyny wirtualnej pomiędzy obsługiwanymi zasobami pamięci masowej.
59. Oferowane rozwiązanie musi zapewniać mechanizm klastrowy wysokiej dostępności dla maszyn wirtualnych.
60. Awaria pojedynczego węzła klastra nie może powodować trwałej utraty dostępności maszyn wirtualnych przypisanych do mechanizmu HA, jeżeli pozostałe węzły klastra posiadają wystarczające zasoby do ich uruchomienia.
61. W przypadku awarii serwera fizycznego system musi automatycznie wykryć jego niedostępność i podjąć decyzję o uruchomieniu chronionych maszyn wirtualnych na innym dostępnym węźle klastra.
62. Proces przywrócenia działania maszyn po awarii hosta nie może wymagać ręcznego odtwarzania konfiguracji maszyn wirtualnych.
63. Rozwiązanie musi posiadać mechanizmy quorum, witness lub rozwiązanie równoważne pozwalające ograniczać ryzyko wystąpienia sytuacji typu split-brain.
64. Architektura musi umożliwiać zastosowanie redundantnych ścieżek komunikacji pomiędzy węzłami klastra.
65. Utrata pojedynczego połączenia sieciowego nie może być automatycznie interpretowana jako całkowita awaria węzła, jeżeli dostępna jest inna skonfigurowana ścieżka komunikacyjna.
66. System musi posiadać mechanizm monitorowania stanu węzłów klastra oraz regularnej wymiany informacji o ich stanie.
67. Rozwiązanie musi umożliwiać przeprowadzanie planowanych prac serwisowych na pojedynczym węźle klastra poprzez przeniesienie działających maszyn wirtualnych na inne węzły.
68. System musi umożliwiać sekwencyjną/rolling aktualizację węzłów klastra, obejmującą co najmniej:
    a. przeniesienie działających maszyn wirtualnych z aktualizowanego węzła,
    b. wprowadzenie węzła w tryb serwisowy,
    c. instalację aktualizacji,
    d. ponowne uruchomienie węzła, jeśli jest wymagane,

e. przywrócenie go do pracy w klastrze.

69. Aktualizacja pojedynczego hosta nie może wymagać jednoczesnego wyłączania wszystkich maszyn wirtualnych w klastrze, o ile pozostałe węzły posiadają zasoby pozwalające na ich czasowe uruchomienie.
70. Rozwiązanie musi umożliwiać automatyczne lub oparte o polityki równoważenie obciążenia pomiędzy hostami wirtualizacyjnymi na podstawie co najmniej wykorzystania procesora i pamięci RAM.
71. Mechanizm równoważenia obciążenia musi umożliwiać wykorzystanie migracji działających maszyn wirtualnych do innego węzła w sytuacji przekroczenia zdefiniowanych progów lub stwierdzenia nierównomiernego wykorzystania zasobów.
72. Dopuszcza się realizację automatycznego równoważenia obciążenia za pomocą odrębnego komponentu zarządzającego współpracującego z hypervisorem.
73. Nie wymaga się mechanizmu predykcyjnego automatycznie migrującego maszyny na podstawie przewidywanej przez producenta sprzętu przyszłej awarii komponentu fizycznego.
74. Dopuszcza się dodatkowo integrację systemu wirtualizacyjnego z systemami monitoringu sprzętu umożliwiającymi podejmowanie działań prewencyjnych.
75. Rozwiązanie musi umożliwiać stosowanie szyfrowania danych przechowywanych przez maszyny wirtualne.
76. Funkcjonalność szyfrowania może być realizowana:
    a. przez mechanizm systemu gościnnego,
    b. poprzez szyfrowanie wirtualnego dysku,
    c. poprzez szyfrowanie warstwy pamięci masowej,
    d. poprzez mechanizm hypervisora,
    e. za pomocą odrębnego rozwiązania szyfrującego.
77. Zamawiający nie wymaga zastosowania mechanizmu szyfrowania dostępnego wyłącznie w jednej, konkretnej edycji systemu operacyjnego hosta.
78. Rozwiązanie musi umożliwiać wykorzystanie mechanizmu TPM/vTPM lub rozwiązania równoważnego dla maszyn wirtualnych, jeżeli jest on wspierany przez zaoferowaną platformę i system gościnny.
79. Rozwiązanie nie może uniemożliwiać stosowania w maszynach wirtualnych:
    a. uwierzytelniania wieloskładnikowego,
    b. certyfikatów użytkowników i urządzeń,
    c. kart inteligentnych Smart Card,
    d. innych sprzętowych lub programowych mechanizmów uwierzytelnienia wspieranych przez system gościnny.
80. Jeżeli dostęp administracyjny realizowany jest poprzez sieć, wykorzystywane protokoły administracyjne muszą zapewniać możliwość szyfrowania komunikacji.
81. System musi zapewniać mechanizmy kontroli uprawnień administratorów.
82. Rozwiązanie musi umożliwiać rejestrowanie zdarzeń administracyjnych i operacyjnych niezbędnych do audytu działania środowiska.
83. Rozwiązanie musi posiadać centralną konsolę graficzną umożliwiającą zarządzanie co najmniej:
    a. hostami wirtualizacyjnymi,
    b. maszynami wirtualnymi,
    c. klastrami wysokiej dostępności,
    d. konfiguracją sieciową hostów i maszyn wirtualnych,
    e. przestrzenią dyskową dostępną dla środowiska wirtualnego.
84. Centralna konsola może być zainstalowana:
    a. na serwerze fizycznym,
    b. na maszynie wirtualnej,
    c. jako usługa zarządzająca współpracująca z oferowanym środowiskiem.
85. Co najmniej podstawowe funkcje centralnej konsoli zarządzającej muszą być dostępne poprzez przeglądarkę internetową lub dedykowaną aplikację administracyjną.
86. W przypadku wykorzystania konsoli przeglądarkowej komunikacja musi być chroniona przy użyciu protokołu HTTPS/TLS.

87. Dostarczone licencje systemu zarządzającego muszą obejmować wszystkie hosty fizyczne dostarczane w ramach przedmiotowego zamówienia.
88. Nie dopuszcza się sytuacji, w której do zarządzania którymkolwiek z dostarczonych hostów konieczne jest dokupienie przez Zamawiającego dodatkowej licencji nieujętej w ofercie.
89. Rozwiązanie musi zapewniać bieżące monitorowanie co najmniej:
    a. stanu hostów,
    b. stanu maszyn wirtualnych,
    c. wykorzystania CPU,
    d. wykorzystania pamięci RAM,
    e. wykorzystania pamięci masowej,
    f. stanu podstawowych interfejsów sieciowych.
90. Informacje dotyczące bieżącego stanu środowiska muszą być możliwe do odświeżania w czasie zbliżonym do rzeczywistego.
91. Rozwiązanie musi umożliwiać wykonywanie czynności administracyjnych za pomocą interfejsu graficznego oraz co najmniej jednego interfejsu automatyzacji, np. PowerShell, REST API, CLI lub rozwiązania równoważnego.
92. Oferowane rozwiązanie musi zapewniać możliwość budowy programowo definiowanej warstwy pamięci masowej – SDS – wykorzystującej lokalne nośniki danych zainstalowane w serwerach fizycznych.
93. Warstwa SDS może być realizowana:
    a. przez system operacyjny hosta,
    b. jako osobne oprogramowanie zainstalowane na hostach,
    c. jako wysokodostępne komponenty programowe lub wirtualne,
    d. przez rozwiązanie firmy trzeciej współpracujące z zaoferowanym hypervisorem.
94. Zamawiający nie wymaga, aby warstwa SDS była wbudowaną funkcją określonej edycji systemu operacyjnego hosta.
95. Jeżeli realizacja funkcjonalności SDS wymaga dodatkowych licencji, komponentów programowych lub maszyn systemowych, wszystkie takie elementy muszą zostać dostarczone przez Wykonawcę.
96. Rozwiązanie SDS musi umożliwiać utworzenie wspólnej przestrzeni dyskowej z wykorzystaniem lokalnych dysków/nośników zainstalowanych w serwerach fizycznych.
97. Rozwiązanie musi obsługiwać konfiguracje wykorzystujące:
    a. dyski SSD/NVMe,
    b. konfiguracje hybrydowe wykorzystujące SSD/NVMe oraz HDD, jeżeli producent rozwiązania wspiera taką konfigurację,
    c. konfiguracje all-flash.
98. Rozwiązanie musi posiadać mechanizmy optymalizacji wydajności operacji odczytu i zapisu.
99. Rozwiązanie SDS musi być wspierane do pracy z oferowaną platformą wirtualizacyjną.
100. Przestrzeń SDS musi być dostępna jako współdzielony zasób pozwalający na realizację wysokiej dostępności i migracji maszyn wirtualnych pomiędzy hostami, zgodnie z architekturą zaoferowanego rozwiązania.
101. Konfiguracja SDS nie może uniemożliwiać wykorzystania wymaganych funkcji:
    a. klastra HA,
    b. migracji działających maszyn wirtualnych,
    c. backupu,
    d. monitorowania środowiska.
102. Zarządzanie SDS musi być możliwe z centralnego systemu zarządzania platformą lub z dedykowanej konsoli administracyjnej SDS.
103. Rozwiązanie musi umożliwiać rozbudowę warstwy SDS poprzez:
    a. dodawanie kolejnych nośników do istniejących serwerów,
    b. dodawanie kolejnych serwerów/węzłów.
104. Minimalna liczba obsługiwanych węzłów musi obejmować co najmniej liczbę serwerów dostarczanych w ramach niniejszego postępowania.

105. Rozwiązanie musi zapewniać możliwość późniejszej rozbudowy o co najmniej dwa dodatkowe węzły ponad konfigurację dostarczaną w ramach niniejszego postępowania, bez konieczności wymiany istniejącej platformy SDS.
106. Rozwiązanie SDS musi umożliwiać przechowywanie wirtualnych dysków maszyn wirtualnych o rozmiarze co najmniej 32 TB.
107. Rozwiązanie SDS musi zapewniać wysoką dostępność danych i odporność co najmniej na awarię pojedynczego nośnika.
108. Dla konfiguracji posiadającej odpowiednią liczbę węzłów i nośników rozwiązanie musi umożliwiać ochronę przed awarią całego pojedynczego serwera/węzła.
109. Awaria pojedynczego nośnika lub węzła objętego skonfigurowanym poziomem redundancji nie może powodować utraty danych.
110. Rozwiązanie musi posiadać mechanizmy automatycznego odbudowywania wymaganej redundancji danych po awarii i wymianie komponentu lub po dodaniu nowej przestrzeni.
111. Rozwiązanie musi umożliwiać co najmniej dwa poziomy odporności danych odpowiednie dla różnych klas obciążeń.
112. Dopuszcza się wykorzystanie:
    a. mirroringu,
    b. dwu- lub trzykopiowej redundancji,
    c. pojedynczej parzystości,
    d. podwójnej parzystości,
    e. erasure coding,
    f. innych równoważnych mechanizmów.
113. Rozwiązanie musi umożliwiać zastosowanie mechanizmu ochrony danych przed utratą integralności, np. za pomocą sum kontrolnych bloków, mechanizmów integralności systemu plików lub równoważnego rozwiązania.
114. Rozwiązanie SDS nie może wymagać zastosowania serwerów wyłącznie jednego określonego producenta, chyba że rozwiązanie jest dostarczane jako certyfikowane zintegrowane urządzenie/appliance.
115. Rozwiązanie musi udostępniać przestrzeń dyskową platformie wirtualizacyjnej.
116. Jeżeli architektura rozwiązania to umożliwia, warstwa SDS powinna umożliwiać udostępnienie przestrzeni również innym systemom fizycznym lub wirtualnym z wykorzystaniem co najmniej jednego standardowego protokołu pamięci masowej, np.:
    a. iSCSI,
    b. SMB 3.x,
    c. NFS,
    d. Fibre Channel,
    e. NVMe-oF,
    f. protokołu równoważnego.
117. Licencje SDS muszą obejmować:
    a. wszystkie serwery objęte rozwiązaniem,
    b. całą pojemność dostarczoną w ramach zamówienia,
    c. wszystkie maszyny wirtualne korzystające z dostarczonego zasobu SDS.
118. Dopuszcza się licencjonowanie:
    a. per-host,
    b. per-core,
    c. per-socket,
    d. per-VM,
    e. inne stosowane przez producenta.
119. Niezależnie od modelu licencjonowania Zamawiający nie może być zobowiązany do zakupu dodatkowych licencji w celu wykorzystania całości dostarczonej pojemności i funkcjonalności opisanych w OPZ.

120. Oferowane rozwiązanie musi umożliwiać utworzenie wspólnego środowiska obejmującego:
    a. zasoby obliczeniowe,
    b. zasoby pamięci masowej,
    c. sieć serwerową i wirtualną,
    d. mechanizmy wysokiej dostępności.
121. Wirtualizacja mocy obliczeniowej musi umożliwiać połączenie dostarczonych serwerów w klaster zapewniający:
    a. migrację działających maszyn wirtualnych pomiędzy hostami,
    b. automatyczne ponowne uruchomienie chronionych maszyn po awarii hosta,
    c. wykonywanie planowanych prac serwisowych na pojedynczym węźle bez konieczności wyłączenia całego środowiska.
122. Rozwiązanie musi umożliwiać rozbudowę platformy poprzez dodawanie kolejnych zgodnych serwerów bez konieczności wymiany całego istniejącego środowiska.
123. Wykonawca musi dostarczyć dla każdego serwera wszystkie licencje niezbędne do wykorzystania wymaganych w OPZ funkcjonalności wirtualizacyjnych, zarządzających, sieciowych i pamięci masowej zgodnie z zaoferowaną architekturą.
124. Wykonawca zobowiązany jest dostarczyć komplet praw licencyjnych niezbędnych do legalnego uruchomienia i eksploatacji wszystkich komponentów rozwiązania w konfiguracji objętej ofertą.
125. Zamawiający nie wymaga stosowania jednej konkretnej edycji systemu operacyjnego hosta.
126. Zamawiający dopuszcza rozwiązania, w których uprawnienia do uruchamiania systemów operacyjnych w maszynach wirtualnych są licencjonowane oddzielnie od samej funkcji hypervisora.
127. Jeżeli producent systemu operacyjnego stosuje model licencjonowania oparty o fizyczne rdzenie procesorów, Wykonawca musi objąć licencjami wymaganą liczbę fizycznych rdzeni zgodnie z aktualnymi zasadami licencyjnymi producenta.
128. Jeżeli dla uzyskania prawa do uruchomienia wymaganej liczby wirtualnych instancji systemu operacyjnego dopuszczalne jest wielokrotne licencjonowanie tych samych rdzeni fizycznych, tzw. stacking licencji, Zamawiający dopuszcza taki sposób licencjonowania.
129. Licencjonowanie warstwy wirtualizacyjnej nie może wprowadzać technicznego ograniczenia liczby uruchamianych maszyn wirtualnych poniżej możliwości sprzętowych dostarczonych serwerów.
130. Ograniczenia wynikające z praw licencyjnych systemów operacyjnych uruchamianych wewnątrz maszyn wirtualnych nie są traktowane jako techniczne ograniczenie hypervisora.
131. Wszystkie oferowane licencje muszą:
    a. pochodzić z legalnego kanału dystrybucji producenta lub jego autoryzowanego partnera,
    b. posiadać prawo do wykorzystania na terytorium Rzeczypospolitej Polskiej lub Europejskiego Obszaru Gospodarczego, zgodnie z warunkami producenta i obowiązującymi przepisami,
    c. zostać prawidłowo przypisane Zamawiającemu,
    d. posiadać dokumentację umożliwiającą potwierdzenie legalności ich pochodzenia.
132. Zamawiający wymaga licencji wieczystej lub licencji OEM.
133. Wszystkie zaoferowane komponenty muszą posiadać wsparcie producenta lub autoryzowanego kanału wsparcia przez okres wymagany w pozostałej części OPZ/SWZ.
134. Wszystkie dostarczone serwery, karty sieciowe, kontrolery dyskowe, HBA, nośniki danych oraz pozostałe komponenty mające wpływ na funkcjonowanie platformy muszą być zgodne z wymaganiami sprzętowymi zastosowanej platformy wirtualizacyjnej.
135. Dostarczona platforma musi umożliwiać wirtualizację wszystkich serwerów dostarczanych w ramach niniejszego postępowania.
136. Dostarczone licencje i komponenty muszą umożliwiać wykorzystanie wszystkich obowiązkowych funkcjonalności opisanych w niniejszym OPZ.

11. System operacyjny serwerowy i licencje dostępowe

Przedmiotem zamówienia jest dostarczenie licencji na serwerowy system operacyjny wspierający rozwiązanie do cyberbezpieczeństwa (najnowsza wersja dostępna w dniu składania ofert) na cztery maszyny wirtualne w ilości pokrywającej zapotrzebowanie na wszystkie fizyczne rdzenie procesorów w serwerach pod rozwiązania bezpieczeństwa oraz z licencjami dostępowymi na 6 użytkowników.
Wymagania dotyczące rozwiązania – oprogramowanie musi spełniać co najmniej wymagania:

1. Oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzinowego użytkowanego aktualnie przez Zamawiającego oraz pełną współpracę z ActiveDirectory. Licencja zostanie wykorzystana do uruchomienia oprogramowania na serwerze zakupionym w ramach niniejszego postępowania.
2. Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.
3. Licencja bez ograniczeń czasowych.
4. Instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym;
5. Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych);
6. Wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB;
7. 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;
8. Praca w roli klienta domeny Microsoft Active Directory;
9. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory;
10. 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);
11. Zawarta możliwość uruchomienia roli serwera DNS;
12. Możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
13. Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP);
14. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
15. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
16. Zawarta możliwość uruchomienia roli serwera stron WWW;
17. Zawarta funkcjonalność szyfrowania dysków;
18. Dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera;
19. W ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego;
20. 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);
21. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
22. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
23. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
24. Obsługa zdalnego pulpitu;
25. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
26. Obsługa PowerShell 4.0;

27. Obsługa WiFi i Bluetooth;
28. Możliwość współdzielenia zasobów GPU między hostami;

12. Serwery pod rozwiązania bezpieczeństwa

Przedmiotem zamówienia są 2 szt. serwerów przeznaczonych do zbudowania klastra wirtualizacji wysokiej dostępności, współpracującego z macierzą dyskową.
Wymagania:

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków 3,5”.
2. Serwer wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
3. Serwer musi być dostarczony 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. Zainstalowane dwa procesory min. 16-rdzeniowe o taktowaniu min. 2.8GHz (base frequency) umożliwiające osiągnięcie w teście SPECrate2017_fp_base wyniku min. 500 pkt. w konfiguracji dla dwóch procesorów. Wynik należy dołączyć do oferty.
7. Pamięć RAM min. 256 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. Zabezpieczenie pamięci:
    a. Memory mirroring
    b. ECC
    c. patrol scrubbing
    d. SDDC
    e. memory thermal throttling
    f. ADDDC-SR
    g. PPR
    h. Memory SMBus hang recovery.
10. Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200.
11. 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.
12. Minimum 3 aktywne sloty PCI-E 5.0 x16.
13. 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,
    d. minimum 2 porty FC 16Gb/s wraz z odpowiednimi wkładkami optycznymi.
14. Zainstalowane 2 dyski serwerowe SSD SATA Read-Intensive o pojemności min. 480GB każdy.
15. Zainstalowane 5 dysków serwerowych HDD SATA o pojemności min. 8 TB każdy.
16. 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.

17. Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo.
18. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).
19. 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.
20. Bezpieczeństwo:
    a. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
    b. Moduł TPM 2.0.
21. 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.
22. 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.
23. Wraz z serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:
    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. dalne 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.

24. Zgodność z normą ISO 9001, ISO 14001 lub równoważne.
25. Serwer musi posiadać deklarację CE.
26. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
27. 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.
28. 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 24-miesięcznym okresem gwarancji w trybie On-Site z gwarantowanym czasem reakcji najpóźniej Next Business Day od momentu zgłoszenia usterki.
    c. Zamawiający dopuszcza realizację gwarancji przez autoryzowanego partnera serwisowego producenta.
    d. 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.
    e. 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.
    f. 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.
    g. 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.

13. Serwer backupu

Przedmiotem zamówienia jest serwer przeznaczony do wykonywania kopii zapasowych.
Wymagania:

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków 3,5”.
2. Serwer wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
3. Serwer musi być dostarczony 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 dla dwóch procesorów. Wynik należy dołączyć do oferty.
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. Zabezpieczenie pamięci:
    a. Memory mirroring
    b. ECC
    c. patrol scrubbing
    d. SDDC
    e. memory thermal throttling
    f. ADDDC-SR
    g. PPR
    h. Memory SMBus hang recovery.
10. Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200.
11. 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.
12. Minimum 3 aktywne sloty PCI-E 5.0 x16.
13. Zainstalowane i w pełni funkcjonalne interfejsy sieciowe:
    a. minimum 1 x RJ-45 Ethernet management port,
    b. minimum 4 porty 10Gb/s Ethernet w standardzie SFP+ wraz z odpowiednimi wkładkami optycznymi SFP+ Multimode.
14. Zainstalowane 2 dyski serwerowe SSD SATA Read-Intensive o pojemności min. 480GB każdy.
15. Zainstalowane 5 dysków serwerowych HDD SATA o pojemności min. 16 TB każdy.
16. 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.
17. Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo.
18. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).
19. 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.
20. Bezpieczeństwo:
    a. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
    b. Moduł TPM 2.0.
21. 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.
22. 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.

23. Wraz z serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:
    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. dalne 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.
24. Zgodność z normą ISO 9001, ISO 14001 lub równoważnymi.
25. Serwer musi posiadać deklarację CE.
26. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
27. 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.
28. 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 24-miesięcznym okresem gwarancji w trybie On-Site z gwarantowanym czasem reakcji najpóźniej Next Business Day od momentu zgłoszenia usterki.
    c. Zamawiający dopuszcza realizację gwarancji przez autoryzowanego partnera serwisowego producenta.
    d. 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.
    e. 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.
    f. 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.

g. 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.

14. Szafa RACK

W ramach postępowania należy dostarczyć szafę rack 42U o wymiarach minimum 800x1200 mm jako kompletny, fabrycznie zintegrowany system samowystarczalnej mikroserwerowni typu All-In-One (Data Center w jednej szafie). System musi zapewniać izolowane środowisko pracy dla urządzeń IT, wyposażone w zintegrowany system chłodzenia precyzyjnego o mocy minimum 4 kW, system zasilania gwarantowanego UPS o mocy min. 5,4 kW / 6 kVA, inteligentną rozdzielnię elektryczną oraz zaawansowany system monitoringu i zarządzania DCIM.
Wewnątrz szafy 42U o wymiarach ramy 800x1200x2000 mm (szer. x gł. x wys.) muszą znajdować się następujące komponenty i wyposażenie standardowe:

1. Konstrukcja szafy i izolacja termiczna:
   a. Zamknięta obudowa z uszczelnionym obiegiem zimnego i gorącego korytarza wewnątrz szafy.
   b. Drzwi przednie przeszklone (szkło hartowane, przegroda próżniowa/dwuszybowa) zamykane na klucz.
   c. Drzwi tylne wyposażone w elektrozamek odblokowywany cyfrowo – kod
   d. Dwa pionowe grzebieniowe organizatory kabli (szerokość/głębokość min. 95 mm, wysokość 42U) po obu stronach szafy.
   e. Przepusty szczotkowe w dachu i podłodze szafy do bezpyłowego wprowadzania okablowania.
   f. Zestaw zaślepek pełnych 1U (tworzywo ABS, montaż beznarzędziowy) oraz zaślepek szczotkowych 1U do zachowania szczelności układu.
   g. Półki stałe RACK (nośność min. 120 kg, głębokość min. 750 mm) – min. 3 sztuki.
2. System oświetlenia i sygnalizacji:
   a. Dwie pionowe dekoracyjno-sygnalizacyjne listwy LED w kolorze niebieskim z przodu szafy.
   b. Automatyczne oświetlenie robocze LED (białe) aktywowane otwarciem drzwi (przód i tył).
3. Klimatyzacja precyzyjna (Moc 4 kW):
   a. Zintegrowany, zmiennoprzepływowy (inwerterowy) moduł klimatyzacji precyzyjnej typu DX o mocy chłodniczej min. 4 kW montowany w obudowie rack.
   b. Wykorzystanie ekologicznego czynnika chłodniczego oraz automatyczna regulacja wydajności zapewniająca wskaźnik efektywności PUE < 1,25.
   c. System wentylacji awaryjnej i wymuszenia bezwładnościowego
   d. Awaryjny dachowy moduł wentylatorów ze szczelnymi żaluzjami grawitacyjnymi.
   e. Inteligentny moduł automatycznego uchylania/otwierania drzwi szafy po przekroczeniu krytycznej temperatury – tylne lub przednie drzwi lub oba na raz powinny się automatycznie otworzyć.
4. Zasilanie gwarantowane (UPS) i Dystrybucja Energii:
   a. Rackowy zasilacz UPS o mocy wyjściowej min. 6 kVA / 5,4 kW wraz z zestawem Battery Pack na min 5 min podtrzymania dla max mocy 4kW.
   b. Zintegrowana prefabrykowana rozdzielnica elektryczna zapewniająca rozdział zasilania podstawowego oraz gwarantowanego UPS wraz z modułem obejścia serwisowego UPSa.

   c. Dwie pionowe listwy zasilające rPDU montowane w strefie serwerowej wyposażone w gniazda min. 16 x C13 + 4xC19.
   d. Hardware'owy system monitoringu linii elektrycznych w rozdzielni głównej – badanie na poziomie obwodów odgałęźnych (prąd, napięcie, częstotliwość, zużycie energii).
5. Po zamontowaniu i zintegrowaniu wszystkich w/w modułów, szafa musi oferować nie mniej niż 22U wolnej przestrzeni montażowej na urządzenia IT zamawiającego.
6. Szafa 42U musi być dostarczona wraz z autonomicznym, pełnofunkcyjnym systemem DCIM realizującym ciągły monitoring i sterowanie pracą całego rozwiązania:
   a. Wbudowany w drzwi lub profil szafy dotykowy ekran LCD (przekątna min. 7" z systemem Android) umożliwiający bezpośrednią weryfikację parametrów środowiskowych, stanu klimatyzacji, obciążenia UPS i stanu rozdzielnicy bez konieczności otwierania szafy.
   b. Wizualizacja graficzna stanu pracy w czasie rzeczywistym.
   c. Pomiary parametrów zasilania: napięcie, prąd, częstotliwość, moc czynna/bierna, zużycie energii (kWh) z rozbiciem na sekcje i gałęzie rPDU.
   d. Pomiary środowiskowe: temperatura i wilgotność w strefie zimnej i gorącej.
   e. Sygnalizacja stanu drzwi (zamknięte/otwarte/wymuszenie), stanu pracy wentylatorów awaryjnych i modułów chłodzenia.
   f. Błyskawiczne powiadamianie zdarzeniowe i alarmowe za pośrednictwem wiadomości SMS oraz wiadomości e-mail
   g. Interfejs sieciowy (Web / HTML5) dostępny z poziomu przeglądarki internetowej.
   h. Dedykowane aplikacje mobilne (Android oraz iOS) do bezobsługowego i zdalnego nadzoru nad parametrami pracy mikro-serwerowni w trybie 24/7.
   i. Fabryczny pakiet licencyjny na monitoring min. 50 węzłów/urządzeń IT (serwery, przełączniki, rejestratory) w ramach dostarczonego oprogramowania. Monitorowanie podstawowych parametrów pracy urządzeń IT udostępnionych przez producenta.

15. Zarządzalne urządzenie sieciowe szkieletowe

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.

16. Zarządzalne urządzenie sieciowe dostępowe PoE

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

17. Access Point WiFi

Przedmiotem zamówienia jest dostawa 4 sztuk punktu dostępowego sieci bezprzewodowej WiFi, przystosowanych do zasilania w standardzie PoE, spełniających wymagania techniczne i funkcjonalności określone przez Zamawiającego

Wymagania:

1. Punkt dostępowy musi być dedykowanym urządzeniem sieciowym przystosowanym do zamontowania na suficie i na ścianie. Wymagane dostarczenie z zestawu montażowego. System operacyjny (firmware) musi być dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej. Oprogramowanie do pracy w trybie tzw „lekkiego AP”, możliwość pracy jako tzw “grubego AP (FAT AP)” oraz możliwość pracy w trybie Cloud.
2. Wymagane parametry fizyczne:
    a. możliwość montażu na suficie oraz ścianie (wraz z urządzeniem należy dostarczyć elementy do montowania)
    b. wysokość maksymalna 5 cm
    c. możliwość zasilania przez zasilacz DC
    d. zakres temperatur pracy ciągłej co najmniej 0°C – +50°C
    e. zakres wilgotności pracy co najmniej 5% - 95%
    f. maksymalny pobór mocy nie większy niż 22W
3. Punkt dostępowy musi posiadać:
    a. minimum 1 port 100/1000/2500/5000Mbit BaseT PoE zgodny ze standardem minimum 802.3af/at
    b. minimum 1 port 100/1000Mbit BaseT
    c. minimum 1 port USB
4. Obsługiwane standardy radiowe: 802.11a/b/g/n/ac/ax/be, jednoczesna obsługa minimum 10 SSID
5. Wbudowane anteny minimum 4dBi dla 2,4GHz, 5dBi dla 5GHz oraz 5dBi dla 6GHz z pracą w standardzie minimum MIMO: 2.4GHz: 2x2, 5GHz: 2x2, 6GHz: 4x4
6. Wsparcie dla standardów/funkcjonalności bezpieczeństwa: WPA2-802.1x, WPA2-PSK, WPA2-PPSK, WPA3-SAE, WPA3-802.1x, IP Source Guard (IPSG)
7. Wsparcie dla roamingu zgodnego z 802.11k, 802.11v, 802.11r
8. Wydajność minimum 13Gbps w tym minimum 600Mbps dla 2.4GHz, 1,4Gbps dla 5GHz oraz 11Gbps dla 6GHz
9. Możliwość zarządzania poprzez:
    a. Kontroler tego samego producenta
    b. SSHv2
    c. Usługę w Internecie, świadczoną przez producenta sprzętu.
10. Urządzenie musi posiadać standard bezpieczeństwa EN62368-1

11. Tunel CAPWAP dla komunikacji z kontrolerem muszą być zaszyfrowane celem ochrony przed możliwością podsłuchania transmisji w sieci kablowej
12. Wsparcie dla protokołów i standardów:
    a. 802.11e
    b. 802.11i
    c. 802.11d
    d. 802.11h
    e. 802.11w
    f. LLDP
    g. DTLS encryption
    h. A-MPDU i A-MSDU
13. Obsługa NTP lub SNTP
14. 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
15. 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.
16. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski
17. Zamawiający wymaga, aby urządzenia posiadały 24-miesięczny serwis gwarancyjny świadczony przez producenta lub Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
18. W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.
19. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.

18. Oprogramowanie do wykonywania kopii zapasowych

Przedmiotem zamówienia jest oprogramowanie na licencji wieczystej do tworzenia kopii zapasowych i odzyskiwania danych dla min. 6 stacji roboczych oraz min. 5 maszyn wirtualnych. System powinien zapewniać automatyczną ochronę danych, elastyczność konfiguracji oraz możliwość szybkiego odzyskiwania danych w przypadku awarii. Wymagania:

1. Wsparcie dla różnych środowisk:
    a. Obsługa systemów operacyjnych: Windows 7, 8, 10, 11 oraz Windows Server 2012 R2, 2016, 2019, 2022 oraz 2025.
    b. Obsługa systemów Linux: CentOS, Red Hat Enterprise Linux (RHEL), Ubuntu, Debian, SUSE Linux Enterprise Server, Rocky Linux, Oracle Linux.
    c. Obsługa wirtualizacji: zgodność z maszynami wirtualnymi działającymi na Microsoft Hyper-V, VMware vSphere, Proxmox VE, OpenStack, Oracle Linux Virtualization Manager.

2. Metody tworzenia kopii zapasowych:
    a. Możliwość wykonywania pełnych, przyrostowych oraz różnicowych kopii zapasowych.
    b. Obsługa kopii zapasowych na poziomie plików oraz całych maszyn (bare-metal backup).
    c. Obsługa backupu dla baz danych takich jak Microsoft SQL Server, MySQL, PostgreSQL, MariaDB oraz Oracle Database.
    d. Możliwość wykonywania backupu NAS oraz zasobów współdzielonych.
3. Automatyzacja i harmonogramowanie:
    a. Możliwość tworzenia harmonogramów backupów z opcją codziennego, tygodniowego, miesięcznego wykonywania kopii zapasowych.
    b. Obsługa polityki retencji (krótkoterminowej i długoterminowej) z możliwością definiowania liczby przechowywanych kopii.
4. Szybkie odzyskiwanie danych:
    a. Możliwość pełnego przywracania systemu oraz przywracania pojedynczych plików i folderów.
    b. Funkcja natychmiastowego przywracania maszyn wirtualnych (RTO < 15 sekund).
    c. Możliwość odzyskiwania baz danych do określonego punktu w czasie (point-in-time recovery).
5. Bezpieczeństwo danych:
    a. Szyfrowanie danych w trakcie przesyłania oraz przechowywania (AES-256).
    b. Obsługa zabezpieczeń przed ransomware (np. poprzez mechanizmy wykrywania anomalii i ochronę przed nadpisaniem).
    c. Możliwość tworzenia kopii zapasowych na nośnikach taśmowych oraz w chmurze (AWS S3, Azure Blob, Ceph S3, Wasabi).
6. Wydajność i optymalizacja:
    a. Obsługa technologii deduplikacji i kompresji danych w celu oszczędności miejsca.
    b. Obsługa wielowątkowej transmisji danych.
    c. Wsparcie dla technologii Changed Block Tracking (CBT) dla szybkiego backupu przyrostowego.
7. Przechowywanie danych:
    a. Możliwość zapisu kopii zapasowych na lokalnym serwerze, sieciowym NAS, SAN oraz w chmurze.
    b. Możliwość wykonywania kopii na nośniki taśmowe (bibliotekę taśmową).
8. Wymagania sieciowe:
    a. Obsługa LAN-Free Transmission dla zmniejszenia obciążenia sieci.
    b. Możliwość konfiguracji limitu pasma wykorzystywanego przez backup.
    c. Wsparcie dla protokołów CIFS, NFS, iSCSI.
9. Interfejs użytkownika:
    a. Intuicyjny panel zarządzania dostępny przez przeglądarkę internetową.
    b. Możliwość zarządzania poprzez CLI oraz API.
    c. Powiadomienia e-mail i raporty o stanie backupu oraz ewentualnych błędach.
10. Funkcje monitorowania:
    a. Monitorowanie statusu backupów, zajętości przestrzeni dyskowej oraz obciążenia systemu.
    b. Możliwość generowania raportów i logów z wykonywanych operacji.
11. Wymagania dotyczące wsparcia technicznego:
    a. Gwarancja i wsparcie techniczne przez okres min. do 31.12.2026.
    b. Możliwość uzyskania pomocy technicznej w języku polskim.
    c. Aktualizacje oprogramowania w okresie gwarancyjnym.
12. Dodatkowe wymagania:
    a. Oprogramowanie powinno umożliwiać bezagentowy backup maszyn wirtualnych z oprogramowania wirtualizacyjnego dostarczonego w ramach tego postępowania.
    b. Możliwość migracji danych pomiędzy różnymi środowiskami wirtualizacji (V2V oraz V2C/C2V).
    c. Wsparcie dla funkcji automatycznego failover i failback w przypadku awarii systemu.
    d. Wsparcie dla testowego odtwarzania backupu w celu weryfikacji integralności danych.
13. Wykonawca zobowiązany jest do dostarczenia pełnej dokumentacji technicznej w języku polskim lub angielskim, w tym instrukcji instalacji, konfiguracji oraz obsługi oprogramowania.

19. Oprogramowanie DLP

Przedmiotem zamówienia jest zakup oprogramowania DLP. Zamówienie obejmuje dostawę licencji wieczystej dla 6 użytkowników ze wsparciem technicznym do 31.12.2026.
Wymagania:

1. System operacyjny:
    a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
    b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
    c. MacOS 12 lub nowszy.
2. Serwer administracyjny musi obsługiwać instalację na systemach:
    a. Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych:
    a. MS SQL Server 2016 lub nowsze,
    b. MS SQL Express,
    c. AzureSQL S3 lub nowsze.
4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
11. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.

24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
27. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
28. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
29. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
30. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
31. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
32. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
33. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
34. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach
35. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)
36. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych.
37. Licencja oprogramowania powinna być bezterminowa na 6 użytkowników wraz ze wsparciem na okres do 31.12.2026.
38. Wsparcie techniczne dystrybutora rozwiązań w języku polskim
39. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta.

20. Oprogramowanie do zarządzania uprzywilejowanym dostępem PAM

Wymagania:

1. System PAM musi być rozwiązaniem bezagentowym tj. umożliwiającym nawiązywanie sesji z wykorzystaniem serwerów proxy bez potrzeby instalacji oprogramowania (agenta) na systemie, do którego będzie nawiązywana sesja, umożliwiającym uwierzytelnianie wieloskładnikowe i obsługujące wiele platform i systemów operacyjnych. System PAM ma zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego m.in. routery, przełączniki, zapory sieciowe, aplikacje, bazy danych itp.
2. System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze Hyper-V lub VMware . Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizująca wszystkie funkcjonalności systemu.
3. System PAM musi zostać dostarczony z kompletem licencji dla co najmniej 5 administratorów, którzy będą korzystali z Systemu PAM, minimum dla następującej liczby funkcjonalności:
   a. Ochrona kont uprzywilejowanych,
   b. Ochrona kluczy SSH,
   c. Zarządzanie i monitorowanie sesji uprzywilejowanych,
   d. Rejestrowanie sesji uprzywilejowanych

   e. Raportowanie wykorzystania kont uprzywilejowanych,
4. Dostarczone licencje na System PAM do ochrony kont uprzywilejowanych nie mogą mieć ograniczeń czasowych. Dostarczone licencje będą udzielone bezterminowo.
5. Dostarczone licencje na system PAM nie mogą w żaden sposób limitować ilości chronionych systemów docelowych.
6. System PAM musi zapewniać możliwość zarządzania (w szczególności):
   a. Użytkownikami na systemach operacyjnych: Windows, Unix/Linux,
   b. Kontami domenowymi: MS Active Directory,
   c. Kontami lokalnymi: VMware ESX/ESXi,
   d. Kontami na urządzeniach m.in.: Cisco, Aruba, Alcatel, CheckPoint, Fortigate, Huawei, IBM AIX, Brocade,
   e. Kontami baz danych: Microsoft SQL, Oracle, MySQL, PostgreSQL
   f. Kontami do zarządzania i monitorowania serwerów: m.in. iLO, iDRAC,
   g. Kontami aplikacji webowych: Facebook, Google, Twitter, Linkedin, Instagram, Openstack, AWS
   h. Kontami w innych nie wymienionych systemach/urządzeniach do których dostęp odbywa się po protokołach: SSH, RDP,VNC, TELNET, HTTP/HTTPS.
7. System PAM musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP,VNC, TELNET, HTTP/HTTPS.
8. System PAM musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami:
   a. przeglądarka internetowa,
   b. klient RDP,
   c. klient protokołu SSH/Telnet (np. putty).
9. System PAM musi wspierać minimum następujące mechanizmy uwierzytelniania: LDAP, RADIUS, Tacacs, Active Directory, OpenID.
10. System PAM powinien zapewniać możliwość dwuskładnikowego uwierzytelniania.
11. System PAM musi obsługiwać monitorowanie i ochronę nawet kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez wiele lub jedno konto uprzywilejowane.
12. System PAM musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd do haseł uprzywilejowanych.
13. System PAM musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP.
14. System PAM musi posiadać log dla wszystkich zdarzeń systemowych.
15. System PAM musi umożliwiać wskazanie kont użytkowników, które realizowały logowanie do
16. stacji/serwera.
17. System PAM musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów.
18. System PAM musi umożliwiać raportowanie wszystkich logowań do systemu.
19. System PAM musi umożliwiać raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego.
20. Rozwiązanie musi posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych.
21. System PAM musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów.
22. System PAM musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką m.in.:

   a. umożliwiać zdefiniowanie wymagań na: długość hasła, znaki w haśle (małe i duże litery, cyfry, znaki specjalne),
   b. generować automatycznie hasła kont systemów docelowych w sposób pseudo losowy,
   c. generować unikalne hasła dla konta systemów docelowych,
   d. wymuszać automatyczną zmianę hasła po jego podglądzie
23. System PAM musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.
24. System PAM musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym (audyt poleceń).
25. Audyt poleceń musi umożliwiać podjęcie co najmniej akcji, zablokuj polecenie i rozłącz sesję po wykryciu audytowanego polecenia a także automatyczne umieszczenie na liście blokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie.
26. System PAM musi umożliwiać nagrywanie sesji wraz z podglądem sesji aktywnej oraz możliwość jej przerwania.
27. Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego.
28. System PAM musi rejestrować znaki wprowadzone z klawiatury przez użytkownika co najmniej dla sesji SSH i RDP oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych.
29. System PAM musi umożliwiać odtworzenie zarejestrowanych nagrań sesji.
30. Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie producenta na terenie Polski.
31. System PAM musi być kompletny i pozwalać na uruchomienie minimum następujących funkcjonalności:
   a. zarządzać kontami uprzywilejowanymi w ramach organizacji,
   b. monitorować wykorzystanie kont uprzywilejowanych,
   c. nagrywać i archiwizować sesje zdalne,
   d. gwarantować skalowalność rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług,
32. System PAM musi umożliwiać personalizację wyglądu aplikacji co najmniej po przez umieszczenie logo zamawiającego w głównym oknie aplikacji.

21. Oprogramowanie typu ITSM

Przedmiotem zamówienia jest dostawa oprogramowania do zarządzania zasobami IT. Zamówienie obejmuje dostawę licencji wieczystej na 6 stanowisk ze wsparciem technicznym do 31.12.2026.
Wymagania:

1. Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
2. Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.
3. Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
4. Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
5. Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.
6. Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.

7. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.
8. Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.
9. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
10. Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
11. Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
12. Oprogramowanie musi współpracować z serwerem MSSQL Server 2008R2-2019
13. Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
14. Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych .
15. Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty.
16. Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (*.exe), plików bibliotek współdzielonych (*.dll), plików sterowników (*.sys) oraz pakietów instalacyjnych oprogramowania (*.msi).
17. Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
18. Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).
19. Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
20. Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).
21. Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
22. Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
23. Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
24. Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
25. Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
26. Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
27. Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.

28. Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu, obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu).
29. Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.
30. Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
31. Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.
32. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.
33. Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
34. Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
35. Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
36. Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417
37. Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
38. Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.
39. Oprogramowanie musi umożliwiać analizę sprzętową:
    a. płyty głównej w zakresie model, producent, nr. Seryjny,
    b. CPU w zakresie nazwy, modelu, producenta, częstotliwości,
    c. HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci,
    d. RAM w zakresie wielkości pamięci,
    e. karty sieciowej w zakresie model, adres IP, adres MAC,
    f. karty graficznej w zakresie model.
40. Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
41. Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
42. Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.
43. Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
44. Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
45. Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
46. Oprogramowanie musi umożliwiać odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji)
47. Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB

48. Oprogramowanie musi umożliwiać integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag)
49. Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).
50. Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
51. Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
52. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
53. Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
54. Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
55. Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
56. Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
57. Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
58. Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
59. Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.
60. Oprogramowanie musi posiadać wbudowaną bazę sygnatur aplikacji (produktów) wraz z możliwością automatycznej aktualizacji wzorców ze strony Producenta oprogramowania
61. Oprogramowanie musi umożliwiać zdefiniowanie własnych sygnatur aplikacji (produktów) wykorzystywanych
    w procesie automatycznego audytu licencji (rozliczenie ilościowe).
62. Oprogramowanie musi umożliwiać wykonanie audytu licencji tj. systemowego porównania zidentyfikowanego na stanowiskach komputerowych oprogramowania (produktów) z zakupionymi licencjami wprowadzonymi do systemu jako odpowiednie obiekty. Mechanizm audytu musi umożliwiać rozliczenie licencji z wykorzystaniem mechanizmów downgrade, upgrade.
63. Oprogramowanie musi umożliwiać zapis historii wykonywanych audytów licencji.
64. Oprogramowanie musi umożliwiać tworzenie bazy licencji systemowo/programowych i przypisywanie ich do stanowisk komputerowych oraz użytkowników.
65. Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
66. Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
67. Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
68. Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
69. Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.

70. Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
71. Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
72. Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
73. Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
74. Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
75. Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
76. Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
77. Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
78. Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
79. Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
80. Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.
81. Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.
82. Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg, *.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
83. Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
84. Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
85. Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.
86. Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.
87. Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
88. Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).
89. Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
90. Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.

91. Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.
92. Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.
93. Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.
94. Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis:
    a. Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0)
    b. Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0)
    Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi
    c. Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y.
    d. Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego.
    e. W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.
95. Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)
96. Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji
97. Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika
98. Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)
99. Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)
100. Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)
101. Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)
102. Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.
103. Oprogramowanie musi umożliwiać tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
104. Oprogramowanie musi umożliwiać globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
105. Oprogramowanie musi umożliwiać definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.

106. Oprogramowanie Agenta musi umożliwiać kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
107. Mechanizm archiwizacji danych musi być realizowany przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
108. Oprogramowanie musi umożliwiać definiowanie cyklu archiwizacji.
109. Oprogramowanie musi umożliwiać automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.
110. Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o kopiowaniu z/do urządzeń zewnętrznych typu: Pendrive USB, dysk zewnętrzny.
111. Oprogramowanie musi posiadać raport w zakresie rejestracji informacji na temat użytkownika, który kopiował i/lub uruchamiał napęd, kiedy miało miejsce zdarzenie i jakie dokumenty zostały skopiowane.
112. Oprogramowanie musi umożliwiać blokadę oraz autoryzację wybranych urządzeń USB w obrębie klasy USBStorage.
113. Oprogramowanie musi umożliwiać włączenie trybu ReadOnly dla klasy USBStorage
114. Oprogramowanie musi umożliwiać całkowitą blokadę klasy FDD/CD/DVD
115. Oprogramowanie musi umożliwiać zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
116. Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
117. Oprogramowanie musi umożliwiać analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
118. Oprogramowanie musi umożliwiać analizę efektywności pracy użytkowników na poszczególnych aplikacjach
119. Oprogramowanie musi umożliwiać blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
120. Oprogramowanie musi umożliwiać tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
121. Oprogramowanie musi umożliwiać podział stron na dozwolone i zabronione.
122. Oprogramowanie musi umożliwiać wydruki tabelaryczne oraz graficzne (wykresy aktywności).
123. Oprogramowanie musi umożliwiać okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
124. Oprogramowanie musi umożliwiać rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
125. Oprogramowanie musi umożliwiać odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
126. Oprogramowanie musi umożliwiać analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).
127. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
128. Oprogramowanie musi umożliwiać monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków musi odbywać się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.
129. Oprogramowanie po zainstalowaniu musi przesyłać do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.

130. Oprogramowanie musi posiadać możliwość definicji kosztów wydruku dla poszczególnych urządzeń drukujących (podział kosztu na mono/kolor).
131. Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony
132. Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.
133. Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
134. Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
135. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
136. Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
137. Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
138. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.
139. Zamawiający wymaga udostępnienia oprogramowania spełniającego wymagania w licencji wieczystej.
140. W okresie trwania umowy wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.
141. Obsługa serwisowa musi być realizowana przez Producenta oprogramowania, w dni robocze w godzinach 8-16 w języku polskim, zgodnie z poniższymi parametrami:
142. Dostarczone licencje na oprogramowanie muszą objąć co najmniej 6 stanowisk komputerowych z systemem klasy Microsoft Windows. Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 1 licencji dostępowych do konsoli zarządzającej.
143. Zamawiający wymaga wsparcia dedykowanego konsultanta technicznego w wymiarze 50 godzin dla okresu trwania umowy.
144. W przypadku wątpliwości zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu.

22. Certyfikat SSL/TLS

Przedmiotem zamówienia jest dostawa certyfikatu SSL/TLS typu Multi-Domain lub równoważnego, przeznaczonego do zabezpieczenia transmisji HTTPS dla publicznych serwisów internetowych Zamawiającego.
Wymagania:

1. Certyfikat musi pochodzić od publicznie zaufanego centrum certyfikacji, którego certyfikaty są domyślnie rozpoznawane przez popularne przeglądarki internetowe oraz systemy operacyjne.
2. Wykonawca nie może dostarczyć certyfikatu samopodpisanego ani certyfikatu wystawionego przez wewnętrzne, prywatne centrum certyfikacji, które nie jest publicznie zaufane.
3. Certyfikat musi być certyfikatem SSL/TLS typu Multi-Domain, SAN/UCC lub równoważnym, umożliwiającym zabezpieczenie wielu nazw DNS w ramach jednego certyfikatu albo równoważnego pakietu certyfikatów.
4. Certyfikat musi być wystawiony zgodnie z aktualnymi wymaganiami branżowymi dla publicznych certyfikatów SSL/TLS, w tym zgodnie z zasadami obowiązującymi centra certyfikacji i przeglądarki

internetowe.

5. Certyfikat musi wykorzystywać algorytmy kryptograficzne akceptowane przez aktualne wersje popularnych przeglądarek internetowych.
6. Certyfikat musi wspierać klucz publiczny RSA o długości minimum 2048 bitów lub klucz ECC o równoważnym poziomie bezpieczeństwa.
7. Certyfikat musi być podpisany algorytmem skrótu z rodziny SHA-2 lub nowszym, akceptowanym przez publiczne centra certyfikacji.
8. Certyfikat musi umożliwiać wykorzystanie z protokołem TLS 1.2 oraz TLS 1.3, o ile konfiguracja serwera Zamawiającego obsługuje te protokoły.
9. Certyfikat musi być dostarczony wraz z kompletnym łańcuchem certyfikacji, w tym certyfikatami pośrednimi wymaganymi do prawidłowej walidacji przez przeglądarki internetowe.
10. Certyfikat musi umożliwiać instalację na typowych serwerach WWW, serwerach aplikacyjnych, urządzeniach sieciowych lub systemach bezpieczeństwa obsługujących standardowe certyfikaty SSL/TLS.
11. Wykonawca musi zapewnić obsługę certyfikatu SSL/TLS przez okres minimum 12 miesięcy.
12. Wykonawca musi wskazać Zamawiającemu wymagany sposób potwierdzenia kontroli nad domeną, np. poprzez wiadomość e-mail, rekord DNS, plik umieszczony w serwisie WWW lub inny mechanizm dopuszczony przez centrum certyfikacji.
13. Wykonawca nie może przechowywać klucza prywatnego Zamawiającego bez jego wyraźnej zgody.
14. Jeżeli klucz prywatny lub plik PFX/P12 zostanie wygenerowany przez Wykonawcę na potrzeby instalacji, musi zostać przekazany Zamawiającemu w sposób bezpieczny, z hasłem przekazanym oddzielnym kanałem komunikacji.
15. Wykonawca musi przekazać Zamawiającemu komplet plików certyfikatu oraz instrukcję instalacji albo przeprowadzić instalację, jeżeli zakres wdrożenia będzie obejmował taką czynność.
16. Certyfikat musi być akceptowany przez aktualne wersje popularnych przeglądarek internetowych, co najmniej Microsoft Edge, Google Chrome, Mozilla Firefox, Safari oraz przeglądarki mobilne systemów Android i iOS.
17. Certyfikat musi być możliwy do wykorzystania na typowych serwerach WWW i aplikacyjnych obsługujących certyfikaty SSL/TLS.
18. Certyfikat musi umożliwiać zabezpieczenie transmisji HTTPS dla serwisów internetowych Zamawiającego.
19. Wykonawca musi przekazać Zamawiającemu informacje niezbędne do zarządzania certyfikatem, w tym datę wystawienia, datę końca ważności, listę objętych nazw DNS oraz nazwę wystawcy certyfikatu.
20. Wykonawca musi przekazać Zamawiającemu procedurę odnowienia, ponownego wystawienia i unieważnienia certyfikatu.
21. Wykonawca musi dostarczyć dokument lub potwierdzenie wystawienia certyfikatu SSL/TLS.
22. Wykonawca musi dostarczyć datę rozpoczęcia i zakończenia ważności aktualnie wystawionego certyfikatu.
23. Wykonawca musi dostarczyć instrukcję instalacji certyfikatu lub podstawowe wytyczne instalacyjne dla
24. Wykonawca musi dostarczyć komplet plików certyfikatu w formacie wymaganym przez Zamawiającego, o ile format ten jest obsługiwany przez centrum certyfikacji i możliwy do wygenerowania na podstawie przekazanych danych.

23. Klucze sprzętowe U2F/FIDO2

Przedmiotem zamówienia jest dostawa 6 sztuk sprzętowego tokena uwierzytelniającego standard U2F/FIDO2, wyposażonych w interfejs USB-A oraz obsługę komunikacji NFC, kompatybilnych z rozwiązaniami klasy MFA, spełniających wymagania techniczne określone w dokumentacji postępowania.
Wymagania dotyczące rozwiązania:

1. Rozwiązanie sprzętowe skutecznie chroniące m.in. przed phishingiem.
2. Posiada wsparcie dla platform: Microsoft Windows, Mac OS, Linux, Chrome OS.
3. Umożliwia współpracę z mobilnymi systemami operacyjnymi iOS oraz Android.
4. Jest kompatybilny z przeglądarkami: Chrome, Edge, Opera, Safari, Firefox.

5. Jest kompatybilny z serwisami: Google, Microsoft, Twitter, Facebook, Instagram, Gmail, Google Drive i YouTube.
6. Posiada możliwość potwierdzenia logowania dotknięciem przycisku - obowiązkowa interakcja użytkownika podczas logowania.
7. Posiada wsparcie dla PKCS#11.
8. Obsługuje algorytmy kryptograficzne: RSA 2048, RSA 4096 (PGP), ECC p256, ECC p384.
9. Jest odporny na zgniecenie.
10. Posiada klasę szczelności IP68.
11. Nie wymaga baterii.
12. Nie wymaga połączenia internetowego.
13. Nie jest typem pendrive, czyli nie posiada miejsca do przechowywania danych: pliki, katalogi.
14. Nie działa po Bluetooth.
15. Posiada możliwość wygrawerowania loga/kodu.
16. Jest tak fizycznie skonstruowany, by uniemożliwić jego rozłożenie na części i ponowne złożenie.
17. Nie obsługuje logowania za pomocą biometrii.
18. Umożliwia przechowywanie na nim kodów OTP, zamiast np: w aplikacji mobilnej.
19. Posiada specjalne oczko umożliwiające zawieszenie urządzenia.
20. Klucz sprzętowy do dwupoziomowego uwierzytelnienia, który posiada certyfikację U2F i FIDO2.
21. Posiada NFC, by można było zdalnie przekazać kod do urządzenia mobilnego.
22. Złącze na USB A.
23. Klucz jest zasilany tylko z portu USB lub wyzwala tag NFC po przyłożeniu do urządzenia mobilnego.
24. Klucz wyzwala tag NFC (kod FIDO/FIDO2 w aplikacji mobilnej) po przyłożeniu do urządzenia mobilnego.
25. Klucz jest tak zabezpieczony przez producenta, że nie ma możliwości wykonania jego kopii na inny klucz czy też dokonania manipulacji w obrębie jego oprogramowania.
26. Oprogramowanie do zarządzania kluczem jest udostępnione do pobrania ze strony producenta.
27. Klucz sprzętowy posiada oprócz U2F i FIDO2 również inne możliwości logowania czy obsługi szyfrowania, jak: smart card, Open PGP, OTP, kody zdarzeniowe i czasowe TOTP/HOTP, statyczne hasło oraz Challenge-Response.
28. Klucz posiada możliwość zaprogramowania dwóch dodatkowych portów o dodatkowe funkcje:
    a. OTP (przechowywanie kodów na kluczu sprzętowym do odczytu za pomocą darmowej aplikacji producenta)
    b. kody zdarzeniowe i czasowe TOTP/HOTP (przechowywanie kodów na kluczu sprzętowym do odczytu za pomocą darmowej aplikacji producenta)
    c. statyczne hasło
    d. Challenge-Response
29. Dostępność oprogramowania/bibliotek/API na stronie producenta na zasadzie open source, w celu integracji z niestandardowymi aplikacjami.

24. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa

Przedmiotem zamówienia jest wykonanie usługi wdrożenia urządzeń, oprogramowania oraz rozwiązań z zakresu bezpieczeństwa IT dostarczanych lub uruchamianych w ramach niniejszego zamówienia.
Wymagania:

1. Usługa obejmuje przygotowanie środowiska, instalację, konfigurację, integrację, hardening, testy, uruchomienie produkcyjne oraz przekazanie dokumentacji powykonawczej dla rozwiązań bezpieczeństwa wdrażanych u Zamawiającego.
2. Zakres wdrożenia dotyczy rozwiązań wskazanych w OPZ, w szczególności systemów i komponentów bezpieczeństwa IT, systemów monitorowania, wykrywania zagrożeń, kontroli dostępu, ochrony danych, analizy zdarzeń, kopii zapasowych oraz infrastruktury technicznej niezbędnej do ich działania, o ile dany

element został objęty zakresem dostawy.

3. Wykonawca przeprowadzi analizę przedwdrożeniową obejmującą co najmniej identyfikację środowiska IT, zależności pomiędzy systemami, wymaganych integracji, ograniczeń technicznych oraz ryzyk wdrożeniowych.
4. Wykonawca uzgodni z Zamawiającym zakres danych wejściowych, adresację sieciową, konta techniczne, wymagane dostępy, okna serwisowe oraz osoby odpowiedzialne po stronie Zamawiającego.
5. Wykonawca zainstaluje i skonfiguruje dostarczone rozwiązania zgodnie z dokumentacją producenta, dobrymi praktykami bezpieczeństwa oraz wymaganiami Zamawiającego.
6. Wykonawca skonfiguruje podstawowe parametry działania wdrażanych rozwiązań, w szczególności adresację, interfejsy, role użytkowników, konta administracyjne, repozytoria, integracje, polityki, reguły, harmonogramy oraz mechanizmy powiadomień, jeżeli mają zastosowanie do danego rozwiązania.
7. Wykonawca zapewni integrację wdrażanych rozwiązań z istniejącą infrastrukturą Zamawiającego, w tym z usługami katalogowymi, systemami logowania, systemami kopii zapasowych, urządzeniami sieciowymi, serwerami, stacjami roboczymi oraz elementami OT/ICS, w zakresie wymaganym do uruchomienia funkcji opisanych w OPZ.
8. W przypadku rozwiązań open source Wykonawca odpowiada za prawidłową instalację, konfigurację, podstawowe zabezpieczenie, uruchomienie oraz przekazanie Zamawiającemu dokumentacji umożliwiającej dalszą eksploatację systemu.
9. Wykonawca nie może pozostawić w środowisku Zamawiającego domyślnych haseł, nieudokumentowanych kont serwisowych ani nieuzgodnionych mechanizmów zdalnego dostępu.
10. Wykonawca przeprowadzi podstawowy hardening wdrażanych rozwiązań, obejmujący co najmniej zmianę domyślnych haseł, ograniczenie dostępu administracyjnego, konfigurację ról i uprawnień, włączenie szyfrowanej komunikacji tam, gdzie jest to wspierane, oraz wyłączenie zbędnych usług.
11. Wykonawca skonfiguruje mechanizmy rejestrowania zdarzeń administracyjnych i bezpieczeństwa, o ile są dostępne w danym rozwiązaniu.
12. Wykonawca skonfiguruje mechanizmy tworzenia kopii zapasowej konfiguracji wdrażanych rozwiązań lub przekaże Zamawiającemu procedurę wykonywania takiej kopii.
13. Po zakończeniu konfiguracji Wykonawca przeprowadzi testy funkcjonalne potwierdzające poprawność działania wdrożonych rozwiązań.
14. Testy muszą obejmować co najmniej weryfikację dostępu administracyjnego, poprawności konfiguracji, działania podstawowych funkcji systemu, komunikacji sieciowej, generowania alertów lub raportów, jeżeli dotyczy, oraz integracji z innymi systemami.
15. Wykonawca dostarczy dokumentację powykonawczą w języku polskim w formie elektronicznej.
16. Dokumentacja musi zawierać co najmniej opis zainstalowanych komponentów, wersji oprogramowania, konfiguracji sieciowej, kont administracyjnych i ról, integracji, polityk, reguł, harmonogramów, kopii konfiguracji oraz procedur podstawowej eksploatacji.
17. Wykonawca przekaże Zamawiającemu dane dostępowe do wdrożonych systemów w sposób bezpieczny, odrębny od głównej dokumentacji.
18. Wykonawca przeprowadzi instruktaż administracyjny dla wskazanych pracowników Zamawiającego, obejmujący podstawową obsługę wdrożonych rozwiązań, sposób odczytywania alertów i raportów, wykonywanie podstawowych czynności eksploatacyjnych oraz zgłaszanie problemów.
19. Wykonawca jest zobowiązany do usunięcia błędów konfiguracyjnych ujawnionych podczas odbioru wdrożenia bez dodatkowego wynagrodzenia, o ile wynikają one z prac wykonanych przez Wykonawcę.
20. Wdrożenie musi zakończyć się przekazaniem kompletnego, działającego i udokumentowanego rozwiązania gotowego do eksploatacji przez Zamawiającego.

25. Utrzymanie i eksploatacja urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa

Przedmiotem zamówienia jest świadczenie usługi utrzymania i eksploatacji urządzeń, oprogramowania oraz

rozwiązań z zakresu bezpieczeństwa IT, w tym również rozwiązań typu open source, wdrożonych lub dostarczonych w ramach projektu.

Wymagania:

1. Usługa ma zapewnić ciągłość operacyjną, poprawność działania, bezpieczeństwo konfiguracji oraz bieżące wsparcie techniczne dla administratorów Zamawiającego w okresie do 31.12.2026.
2. Usługa nie obejmuje całodobowego monitoringu SOC/MDR, stałego administrowania wszystkimi systemami Zamawiającego, zakupu nowych licencji, zakupu nowego sprzętu ani rozwoju funkcjonalnego wykraczającego poza zakres wdrożonych rozwiązań, chyba że OPZ lub umowa stanowią inaczej.
3. Wykonawca zapewni wsparcie eksploatacyjne dla wdrożonych rozwiązań bezpieczeństwa IT, obejmujące co najmniej pomoc w analizie problemów, weryfikację działania usług, wsparcie konfiguracji, kontrolę poprawności integracji oraz konsultacje techniczne.
4. Wykonawca będzie wspierał Zamawiającego w utrzymaniu poprawności działania rozwiązań takich jak systemy monitorowania, wykrywania zagrożeń, logowania i analizy zdarzeń, ochrony punktów końcowych, kontroli dostępu, kopii zapasowych, wirtualizacji, rozwiązań OT oraz innych elementów bezpieczeństwa objętych projektem.
5. Wykonawca zapewni możliwość zgłaszania problemów technicznych w dni robocze w godzinach 8:00-16:00, co najmniej za pośrednictwem poczty elektronicznej lub systemu zgłoszeniowego.
6. Usługa będzie świadczona zdalnie, a prace w siedzibie Zamawiającego będą realizowane w przypadkach, w których zdalne rozwiązanie problemu nie będzie możliwe lub będzie niewystarczające.
7. W ramach usługi Wykonawca zapewni pakiet minimum 100 roboczogodzin wsparcia eksperckiego do wykorzystania przez Zamawiającego w okresie obowiązywania usługi.
8. Pakiet godzin może być wykorzystany na konsultacje, analizę problemów, drobne zmiany konfiguracyjne, wsparcie aktualizacji, korektę reguł, analizę alertów, przygotowanie raportów technicznych oraz wsparcie powdrożeniowe.
9. Wykonawca będzie prowadził ewidencję wykorzystania godzin i na żądanie Zamawiającego przekaże zestawienie wykonanych prac.
10. Prace przekraczające zakres pakietu godzin lub wymagające zakupu dodatkowych licencji, subskrypcji, sprzętu albo usług producenta wymagają odrębnej akceptacji Zamawiającego.
11. Wykonawca będzie wspierał Zamawiającego w planowaniu i wykonywaniu aktualizacji oprogramowania, poprawek bezpieczeństwa, aktualizacji baz sygnatur, parserów, reguł, szablonów oraz innych komponentów utrzymaniowych, o ile są one dostępne dla danego rozwiązania i objęte posiadanymi licencjami lub subskrypcjami.
12. Przed wykonaniem istotnej zmiany lub aktualizacji Wykonawca musi uzgodnić z Zamawiającym termin prac, zakres zmian, ryzyka oraz sposób przywrócenia poprzedniej konfiguracji.
13. Wykonawca będzie wspierał Zamawiającego w okresowej weryfikacji konfiguracji wdrożonych rozwiązań pod kątem zgodności z dokumentacją powykonawczą i dobrymi praktykami bezpieczeństwa.
14. W przypadku stwierdzenia nieprawidłowości Wykonawca wskaże rekomendowane działania naprawcze oraz, po akceptacji Zamawiającego, wykona uzgodnione korekty w ramach dostępnego pakietu godzin.
15. Wykonawca będzie wykonywał okresowe przeglądy stanu wdrożonych rozwiązań bezpieczeństwa, nie rzadziej niż raz na kwartał.
16. Przegląd powinien obejmować co najmniej weryfikację dostępności systemów, stanu usług, stanu integracji, poprawności zbierania danych, aktualności komponentów, wykorzystania zasobów oraz występowania błędów krytycznych.
17. Po każdym przeglądzie Wykonawca przygotuje krótką informację dla Zamawiającego zawierającą wykryte problemy, rekomendowane działania oraz status wykonanych prac.
18. W przypadku systemów generujących alerty bezpieczeństwa Wykonawca będzie wspierał Zamawiającego w dostrajaniu reguł i ograniczaniu liczby fałszywych alarmów, bez obniżania skuteczności wykrywania zagrożeń.
19. Wykonawca zapewni przyjmowanie zgłoszeń dotyczących problemów z działaniem wdrożonych rozwiązań oraz problemów związanych z ich konfiguracją i eksploatacją.
20. Wykonawca rozpocznie analizę zgłoszeń krytycznych nie później niż w następnym dniu roboczym od

otrzymania zgłoszenia.

21. Wykonawca rozpocznie analizę zgłoszeń niekrytycznych nie później niż w terminie 3 dni roboczych od otrzymania zgłoszenia.
22. W ramach wsparcia incydentowego Wykonawca pomoże Zamawiającemu w analizie alertów, logów, zdarzeń systemowych i konfiguracji wdrożonych rozwiązań, przygotowaniu rekomendacji działań naprawczych oraz weryfikacji skutków wykonanych działań.
23. Usługa wsparcia incydentowego nie oznacza przejęcia odpowiedzialności za prowadzenie całego procesu obsługi incydentu po stronie Zamawiającego ani świadczenia całodobowego centrum monitorowania bezpieczeństwa.
24. Wykonawca będzie aktualizował dokumentację powykonawczą w zakresie zmian konfiguracyjnych wykonanych w ramach usługi utrzymania, jeżeli zmiany te wpływają na sposób działania systemu.
25. Wykonawca będzie przekazywał Zamawiającemu raporty okresowe z wykonanych czynności utrzymaniowych nie rzadziej niż raz na kwartał.
26. Raport musi zawierać co najmniej listę zgłoszeń, wykonanych czynności, wykorzystanych godzin, wykrytych problemów, rekomendacji oraz informacji o planowanych pracach utrzymaniowych.
27. Wykonawca zapewni bieżące konsultacje dla administratorów Zamawiającego w zakresie eksploatacji wdrożonych rozwiązań bezpieczeństwa.
28. Wszystkie działania utrzymaniowe muszą być wykonywane z zachowaniem poufności, integralności i dostępności danych oraz z poszanowaniem wymagań bezpieczeństwa środowisk IT i OT.
29. Wykonawca nie może wykonywać zmian w środowisku produkcyjnym bez wiedzy i akceptacji Zamawiającego.
30. Wykonawca musi stosować zasadę minimalnych uprawnień oraz uzgodnione z Zamawiającym mechanizmy dostępu zdalnego.
31. Po zakończeniu okresu świadczenia usługi Wykonawca przekaże Zamawiającemu końcowe zestawienie wykonanych prac, wykorzystanych godzin oraz rekomendacji dotyczących dalszego utrzymania środowiska.

26. Usługa inwentaryzacji aktywów teleinformatycznych

Cel usługi: Automatyzacja procesu identyfikacji i ewidencji zasobów w celu stworzenia rzetelnego Rejestru Aktywów.

Wymagania szczegółowe:

1. Automatyczne wykrywanie (Discovery): Wykonawca skonfiguruje system do automatycznego skanowania sieci Zamawiającego w celu identyfikacji wszystkich urządzeń końcowych, serwerów, urządzeń sieciowych oraz komponentów automatyki przemysłowej (OT/ICS).
2. Zakres inwentaryzacji sprzętowej: Usługa musi obejmować zebranie danych o modelach urządzeń, numerach seryjnych, parametrach procesorów, pamięci RAM, dysków oraz adresacji IP/MAC dla całej infrastruktury objętej projektem.
3. Inwentaryzacja oprogramowania: Wykonawca wdroży mechanizm zbierający informacje o zainstalowanych systemach operacyjnych (serwerowych i klienckich) oraz aplikacjach wraz z ich wersjami.
4. Zarządzanie licencjami: Konfiguracja modułu do śledzenia wykorzystania posiadanych licencji (m.in. licencji CAL, licencji serwerowych oraz oprogramowania EDR) w celu zapewnienia zgodności licencyjnej.
5. Klasyfikacja aktywów: Integracja wyników inwentaryzacji z opracowaną w SZBI klasyfikacją informacji pod kątem poufności, integralności i dostępności.
6. Raportowanie: Przygotowanie dedykowanych raportów inwentaryzacyjnych w formatach edytowalnych, umożliwiających bezpośredni eksport danych do centralnego Rejestru Aktywów Informacyjnych.

27. Usługa segmentacji sieci

Przedmiotem zamówienia jest kompleksowa usługa analizy, zaprojektowania, wdrożenia i przetestowania segmentacji sieci Zamawiającego, obejmującej środowiska IT oraz połączenia pomiędzy środowiskami IT, OT, ICS i IIoT.

Zakres usługi obejmuje:

1. Analizę istniejącej architektury sieciowej, w szczególności:
    - topologii fizycznej i logicznej;
    - wykorzystywanej adresacji IP;
    - istniejących sieci VLAN;
    - routingu;
    - reguł zapory sieciowej;
    - list kontroli dostępu;
    - połączeń pomiędzy środowiskami IT, OT, ICS i IIoT;
    - sposobów dostępu administracyjnego i zdalnego.
2. Wykorzystanie wyników inwentaryzacji aktywów teleinformatycznych wykonanej w ramach odrębnej pozycji zamówienia.
3. Identyfikację urządzeń, systemów i usług wymagających odseparowania ze względu na:
    - pełnioną funkcję;
    - poziom krytyczności;
    - rodzaj przetwarzanych informacji;
    - wymagany poziom dostępu;
    - przynależność do środowiska IT, OT, ICS albo IIoT.
4. Opracowanie projektu docelowej segmentacji sieci obejmującego co najmniej następujące strefy, o ile występują w środowisku Zamawiającego:
    - strefę użytkowników;
    - strefę administracyjną;
    - strefę serwerową;
    - strefę systemów bezpieczeństwa;
    - strefę wykonywania i przechowywania kopii zapasowych;
    - strefę zarządzania urządzeniami;
    - strefę urządzeń sieciowych;
    - strefę sieci bezprzewodowej dla pracowników;
    - strefę sieci bezprzewodowej dla gości;
    - strefę urządzeń drukujących i wielofunkcyjnych;
    - strefę urządzeń IoT i IIoT;
    - strefę OT i ICS;
    - strefę DMZ;
    - strefę dostępu zdalnego;
    - strefę kwarantanny dla urządzeń niespełniających wymagań bezpieczeństwa.
5. Opracowanie planu adresacji IP oraz przypisania sieci VLAN do poszczególnych stref bezpieczeństwa.
6. Opracowanie macierzy dozwolonej komunikacji pomiędzy strefami, zawierającej co najmniej:
    - strefę źródłową;
    - strefę docelową;
    - źródłowe i docelowe adresy lub grupy urządzeń;
    - wymagane protokoły i porty;
    - uzasadnienie biznesowe komunikacji;
    - sposób kontroli ruchu;
    - decyzję o dopuszczeniu albo zablokowaniu komunikacji.

7. Przyjęcie zasady domyślnego blokowania komunikacji pomiędzy strefami, z dopuszczeniem wyłącznie połączeń niezbędnych do prawidłowego działania systemów i procesów Zamawiającego.
8. Przygotowanie planu wdrożenia segmentacji obejmującego:
    - kolejność wykonywania zmian;
    - wymagane okna serwisowe;
    - ocenę ryzyka zmian;
    - sposób weryfikacji działania usług;
    - plan przywrócenia konfiguracji poprzedniej w przypadku niepowodzenia.
9. Wykonanie kopii zapasowych konfiguracji urządzeń sieciowych i bezpieczeństwa przed rozpoczęciem zmian.
10. Konfigurację, w zakresie obsługiwanym przez urządzenia Zamawiającego:
    - sieci VLAN;
    - portów dostępowych i trunk;
    - interfejsów warstwy trzeciej;
    - routingu pomiędzy sieciami;
    - list ACL;
    - stref bezpieczeństwa i reguł zapory sieciowej;
    - izolacji portów;
    - sieci gościnnej;
    - sieci kwarantanny;
    - odrębnej sieci zarządzającej;
    - mechanizmów zabezpieczających przed nieautoryzowaną komunikacją pomiędzy segmentami.
11. Konfigurację segmentacji na przełączniku, firewallu i punkcie dostępowym dostarczanych w ramach zamówienia oraz na innych urządzeniach wskazanych przez Zamawiającego, o ile ich funkcjonalność i stan wsparcia umożliwiają bezpieczne wykonanie konfiguracji.
12. Integrację segmentacji z systemem NAC poprzez:
    - dynamiczne przypisywanie urządzeń lub użytkowników do sieci VLAN;
    - przypisywanie urządzeń niespełniających polityki do strefy kwarantanny;
    - obsługę uwierzytelniania IEEE 802.1X;
    - obsługę urządzeń niewspierających IEEE 802.1X za pomocą uwierzytelniania opartego na adresie MAC.
13. Zapewnienie, że dostęp administracyjny do urządzeń sieciowych, serwerów i systemów bezpieczeństwa będzie możliwy wyłącznie z wydzielonej sieci zarządzającej lub za pośrednictwem stacji przesiadkowej.
14. Ograniczenie bezpośredniej komunikacji pomiędzy środowiskami IT i OT wyłącznie do połączeń wynikających z zatwierdzonej macierzy komunikacji.
15. Wprowadzenie zmian w środowiskach OT, ICS i IIoT wyłącznie:
    - po wcześniejszym uzgodnieniu zakresu z Zamawiającym;
    - po ocenie wpływu zmian na proces technologiczny;
    - w uzgodnionym oknie serwisowym;
    - pod nadzorem osoby odpowiedzialnej za środowisko OT;
    - z przygotowanym planem wycofania zmian.
16. Przeprowadzenie testów poprawności wdrożonej segmentacji obejmujących co najmniej:
    - test komunikacji dozwolonej;
    - test blokowania komunikacji niedozwolonej;
    - test dostępu do usług serwerowych;
    - test dostępu administracyjnego;

- test izolacji sieci gościnnej;
- test działania sieci kwarantanny;
- test komunikacji pomiędzy IT i OT;
- test działania usług po wprowadzeniu zmian.

17. Usunięcie albo wyłączenie nieużywanych reguł komunikacyjnych, tras, sieci VLAN i portów wyłącznie po uzyskaniu zgody Zamawiającego.
18. Przekazanie Zamawiającemu wszystkich haseł, danych dostępowych oraz kopii konfiguracji zmodyfikowanych urządzeń.
19. Sporządzenie dokumentacji powykonawczej zawierającej co najmniej:
    - opis stanu przed wdrożeniem;
    - opis docelowej architektury;
    - schemat logiczny sieci;
    - zestawienie sieci VLAN i adresacji;
    - macierz komunikacji;
    - zestawienie skonfigurowanych reguł;
    - wykaz wykonanych zmian;
    - wyniki testów;
    - kopie konfiguracji urządzeń;
    - zalecenia dotyczące dalszego rozwoju segmentacji.
20. Przekazanie dokumentacji powykonawczej w formacie PDF oraz w wersji edytowalnej w terminie do 14 dni od zakończenia wdrożenia.
21. Wszystkie zmiany konfiguracyjne muszą być realizowane w siedzibie i pod nadzorem Zamawiającego. Prace nie mogą powodować nieuzgodnionych przerw w funkcjonowaniu sieci ani procesów technologicznych.

28. Audyt cyberbezpieczeństwa sieci

Przedmiotem zamówienia jest wykonanie technicznego audytu cyberbezpieczeństwa infrastruktury sieciowej Zamawiającego, obejmującego środowiska IT oraz połączenia i elementy infrastruktury OT, ICS i IIoT.
Audyt powinien zostać wykonany po zakończeniu wdrożenia głównych rozwiązań technicznych i segmentacji sieci, tak aby umożliwić ocenę stanu powdrożeniowego.
Zakres usługi obejmuje:

1. Uzgodnienie z Zamawiającym:
    - zakresu adresacji sieciowej;
    - lokalizacji objętych audytem;
    - systemów i urządzeń podlegających ocenie;
    - dopuszczalnych metod badania;
    - terminów i okien serwisowych;
    - ograniczeń obowiązujących w środowisku OT, ICS i IIoT;
    - osób odpowiedzialnych za poszczególne obszary infrastruktury.
2. Analizę dokumentacji dotyczącej:
    - architektury fizycznej i logicznej sieci;
    - adresacji IP;
    - sieci VLAN;
    - stref bezpieczeństwa;
    - reguł zapory sieciowej;
    - list kontroli dostępu;
    - sposobu dostępu administracyjnego;

- połączeń zdalnych;
- połączeń pomiędzy środowiskami IT i OT;
- wyników inwentaryzacji aktywów;
- dokumentacji wykonanej w ramach usługi segmentacji sieci.

3. Weryfikację zgodności stanu faktycznego z dokumentacją powykonawczą, w szczególności:
   - istniejących segmentów sieci;
   - skonfigurowanych sieci VLAN;
   - routingu;
   - stref bezpieczeństwa;
   - reguł komunikacji;
   - punktów styku sieci IT i OT;
   - połączeń z Internetem i sieciami zewnętrznymi;
   - urządzeń realizujących dostęp zdalny.
4. Audyt konfiguracji urządzeń sieciowych i bezpieczeństwa, obejmujący co najmniej:
   - przełączniki;
   - routery;
   - urządzenia firewall;
   - punkty dostępowe WiFi;
   - system NAC;
   - urządzenia i bramy znajdujące się na styku IT i OT;
   - urządzenia dostępu zdalnego;
   - urządzenia sieci przemysłowej, o ile ich konfiguracja może zostać bezpiecznie udostępniona.
5. Weryfikację konfiguracji urządzeń pod kątem:
   - stosowania bezpiecznych protokołów zarządzania;
   - wyłączenia usług nieużywanych;
   - wyłączenia protokołów przestarzałych i nieszyfrowanych;
   - właściwego ograniczenia dostępu administracyjnego;
   - stosowania indywidualnych kont administratorów;
   - integracji z centralnymi usługami uwierzytelniania;
   - stosowania odpowiednich mechanizmów uwierzytelniania;
   - rejestrowania działań administracyjnych;
   - synchronizacji czasu;
   - przekazywania logów do systemu SIEM;
   - aktualności wersji firmware i oprogramowania;
   - zabezpieczenia kopii konfiguracji.
6. Weryfikację segmentacji sieci, obejmującą:
   - prawidłowość podziału na strefy;
   - oddzielenie sieci użytkowników od sieci serwerowej;
   - oddzielenie sieci administracyjnej;
   - oddzielenie systemu backupowego;
   - oddzielenie urządzeń bezpieczeństwa;
   - oddzielenie sieci gościnnej;
   - oddzielenie urządzeń IoT i IIoT;
   - oddzielenie środowiska OT i ICS;
   - ograniczenie komunikacji pomiędzy strefami;
   - funkcjonowanie strefy kwarantanny;
   - zgodność reguł komunikacji z zatwierdzoną macierzą przepływów.
7. Weryfikację, czy pomiędzy strefami stosowana jest zasada:

- domyślnego blokowania komunikacji;
- dopuszczania wyłącznie wymaganych połączeń;
- ograniczania ruchu do niezbędnych adresów, protokołów i portów;
- dokumentowania uzasadnienia dla dopuszczonej komunikacji.

8. Weryfikację bezpieczeństwa dostępu do sieci, obejmującą:
   - stosowanie IEEE 802.1X;
   - współpracę przełączników i punktów dostępowych z systemem NAC;
   - uwierzytelnianie urządzeń nieobsługujących IEEE 802.1X;
   - dynamiczne przypisywanie sieci VLAN;
   - funkcjonowanie sieci kwarantanny;
   - zabezpieczenia portów przełączników;
   - wykrywanie nieautoryzowanych urządzeń;
   - obsługę nieudanych prób uwierzytelnienia.
9. Audyt bezpieczeństwa sieci bezprzewodowej, obejmujący:
   - wykorzystywane standardy szyfrowania;
   - stosowanie WPA3-Enterprise;
   - integrację z serwerem RADIUS;
   - stosowanie IEEE 802.1X;
   - oddzielenie sieci pracowników i gości;
   - izolację klientów;
   - dostęp sieci gościnnej do zasobów wewnętrznych;
   - wykrywanie nieautoryzowanych punktów dostępowych;
   - bezpieczeństwo zarządzania punktem dostępowym.
10. Audyt styku środowisk IT i OT, obejmujący:
    - identyfikację wszystkich połączeń pomiędzy IT i OT;
    - ocenę zasadności każdego połączenia;
    - weryfikację kontroli ruchu;
    - ocenę dostępu administracyjnego do środowiska OT;
    - ocenę dostępu dostawców i serwisantów;
    - weryfikację mechanizmów rejestrowania sesji;
    - ocenę stosowania stacji przesiadkowej;
    - identyfikację bezpośrednich połączeń omijających zabezpieczenia;
    - ocenę separacji krytycznych urządzeń technologicznych.
11. Identyfikację urządzeń i usług dostępnych w sieci poprzez bezpieczne metody, obejmujące:
    - analizę tabel urządzeń sieciowych;
    - analizę logów;
    - analizę danych z systemu monitorowania;
    - analizę danych z NAC;
    - kontrolowane skanowanie środowiska IT;
    - pasywną analizę środowiska OT;
    - porównanie wyników z rejestrem aktywów.
12. Przeprowadzenie kontrolowanego skanowania podatności środowiska IT, obejmującego co najmniej:
    - serwery;
    - urządzenia sieciowe;
    - urządzenia bezpieczeństwa;
    - systemy zarządzające;
    - wybrane stacje administracyjne;
    - usługi dostępne z sieci wewnętrznej;

- usługi publicznie dostępne, jeżeli należą do Zamawiającego.

13. Skanowanie podatności musi zostać wykonane:
    - w uzgodnionym zakresie adresów;
    - za pomocą aktualnych baz podatności;
    - z ograniczeniem wpływu na działanie systemów;
    - w uzgodnionym oknie czasowym;
    - bez prowadzenia ataków powodujących utratę dostępności;
    - bez trwałej zmiany konfiguracji badanego urządzenia.
14. W środowisku OT, ICS i IIoT podstawowymi metodami badania muszą być:
    - analiza dokumentacji;
    - analiza konfiguracji;
    - analiza danych z systemów monitorowania;
    - analiza logów;
    - pasywna obserwacja komunikacji;
    - wywiady z osobami odpowiedzialnymi;
    - fizyczna identyfikacja urządzeń.
15. Aktywne skanowanie urządzeń OT, ICS i IIoT może zostać wykonane wyłącznie:
    - po przedstawieniu szczegółowych parametrów badania;
    - po ocenie ryzyka dla procesu technologicznego;
    - po uzyskaniu pisemnej zgody Zamawiającego;
    - w uzgodnionym oknie serwisowym;
    - pod nadzorem osoby odpowiedzialnej za środowisko OT.
16. W ramach audytu nie wolno wykonywać w środowisku OT działań mogących:
    - zatrzymać urządzenie;
    - zmienić jego konfigurację;
    - spowodować restart;
    - zakłócić proces technologiczny;
    - doprowadzić do utraty danych;
    - wpłynąć na bezpieczeństwo ludzi lub infrastruktury;
    - wykorzystać podatność w sposób mogący naruszyć ciągłość działania.
17. Weryfikację bezpieczeństwa usług administracyjnych, w tym:
    - SSH;
    - HTTPS;
    - RDP;
    - VPN;
    - SNMP;
    - interfejsów zarządzających urządzeń;
    - dostępu do konsol systemów wirtualizacyjnych;
    - dostępu do systemu backupowego;
    - dostępu do systemów SIEM, SOAR i NAC.
18. Weryfikację mechanizmów ochrony przed typowymi zagrożeniami sieciowymi, obejmującą w szczególności:
    - podszywanie się pod adresy IP i MAC;
    - nieautoryzowane serwery DHCP;
    - ataki na protokół ARP;
    - pętle sieciowe;
    - nieautoryzowane podłączenie urządzeń;
    - niekontrolowany ruch pomiędzy sieciami VLAN;

- przejęcie lub nadużycie kont administracyjnych;
- wykorzystanie niezabezpieczonych usług zarządzania.

19. Weryfikację logowania i monitorowania zdarzeń, obejmującą:
    - kompletność źródeł logów;
    - synchronizację czasu;
    - przekazywanie logów do SIEM;
    - rejestrowanie prób uwierzytelnienia;
    - rejestrowanie zmian konfiguracji;
    - rejestrowanie dostępu administracyjnego;
    - rejestrowanie ruchu pomiędzy krytycznymi strefami;
    - właściwy czas przechowywania logów;
    - możliwość powiązania zdarzenia z użytkownikiem lub urządzeniem.
20. Przeprowadzenie testów weryfikujących wybrane mechanizmy bezpieczeństwa, obejmujących co najmniej:
    - próbę komunikacji pomiędzy odseparowanymi strefami;
    - próbę dostępu do sieci przez nieuwierzytelnione urządzenie;
    - weryfikację przypisania urządzenia do kwarantanny;
    - próbę dostępu administracyjnego spoza wydzielonej sieci;
    - test izolacji sieci gościnnej;
    - test blokowania nieautoryzowanej komunikacji pomiędzy IT i OT;
    - weryfikację generowania zdarzeń w systemie SIEM.
21. Testy nie mogą obejmować:
    - ataków typu denial of service;
    - celowego uszkadzania danych;
    - trwałego przejmowania kont;
    - instalacji trwałego złośliwego oprogramowania;
    - nieuzgodnionych prób socjotechnicznych;
    - działań poza zakresem pisemnie zatwierdzonym przez Zamawiającego.
22. Klasyfikację wykrytych nieprawidłowości co najmniej według poziomów:
    - krytyczny;
    - wysoki;
    - średni;
    - niski;
    - informacyjny.
23. Dla każdej nieprawidłowości Wykonawca musi podać:
    - nazwę i opis;
    - dotknięte aktywa;
    - dowody potwierdzające występowanie;
    - możliwe skutki;
    - prawdopodobieństwo wykorzystania;
    - poziom ryzyka;
    - zalecane działanie naprawcze;
    - priorytet i proponowany termin usunięcia;
    - odniesienie do powszechnie stosowanej klasyfikacji podatności, jeżeli ma zastosowanie.
24. W przypadku wykrycia podatności krytycznej albo aktywnego zagrożenia Wykonawca musi:
    - niezwłocznie poinformować wskazanego przedstawiciela Zamawiającego;
    - przekazać podstawowe informacje o zagrożeniu;
    - wskazać tymczasowe działania ograniczające ryzyko;

- nie czekać z informacją do przekazania raportu końcowego.

25. Sporządzenie raportu technicznego zawierającego co najmniej:
    - zakres i metodykę audytu;
    - ograniczenia przeprowadzonych prac;
    - opis badanego środowiska;
    - wykaz wykorzystanych narzędzi;
    - wykaz zidentyfikowanych podatności i nieprawidłowości;
    - dowody techniczne;
    - klasyfikację ryzyka;
    - rekomendacje naprawcze;
    - proponowany harmonogram usuwania nieprawidłowości;
    - ocenę segmentacji sieci;
    - ocenę bezpieczeństwa styku IT i OT;
    - ocenę dostępu administracyjnego i zdalnego;
    - ocenę mechanizmów monitorowania i rejestrowania.
26. Sporządzenie streszczenia zarządczego zawierającego:
    - ogólną ocenę poziomu bezpieczeństwa sieci;
    - najważniejsze ryzyka;
    - wykaz ustaleń krytycznych i wysokich;
    - wpływ ustaleń na ciągłość działania;
    - priorytety działań naprawczych;
    - rekomendacje krótkoterminowe i długoterminowe.
27. Przekazanie raportu:
    - w formacie PDF;
    - w formacie edytowalnym;
    - wraz z tabelą ustaleń w formacie XLSX lub CSV;
    - w sposób zaszyfrowany albo na zaszyfrowanym nośniku.
28. Przeprowadzenie spotkania podsumowującego, podczas którego Wykonawca:
    - przedstawi najważniejsze ustalenia;
    - omówi ryzyka;
    - wyjaśni zalecenia;
    - odpowie na pytania Zamawiającego;
    - uzgodni priorytety działań naprawczych.
29. W ramach odbioru Wykonawca poprawi:
    - błędy merytoryczne;
    - niezgodności pomiędzy raportem a materiałem dowodowym;
    - niejasne lub niewykonalne rekomendacje;
    - braki formalne wskazane przez Zamawiającego.
30. Audyt zostanie uznany za wykonany po:
    - przekazaniu wszystkich wymaganych raportów i załączników;
    - przeprowadzeniu spotkania podsumowującego;
    - uwzględnieniu uzasadnionych uwag Zamawiającego;
    - podpisaniu protokołu odbioru.
31. Wykonawca oraz osoby wykonujące audyt muszą:
    - zachować poufność informacji;
    - stosować bezpieczne metody przechowywania materiałów;
    - nie przekazywać danych do zewnętrznych usług bez zgody Zamawiającego;
    - usunąć robocze kopie danych po zakończeniu odbioru;

- przekazać oświadczenie o usunięciu danych.

32. Audyt powinien zostać wykonany przez osobę posiadającą doświadczenie w technicznych audytach sieci IT, a w części dotyczącej OT – doświadczenie w ocenie bezpieczeństwa środowisk przemysłowych lub technologicznych.
33. Audyt musi zostać przeprowadzony przez inną osobę niż osoba bezpośrednio konfigurująca oceniane urządzenia.

Część 2. Dostawa sprzętu i oprogramowania OT

1. System IDS dedykowany dla sieci OT

Przedmiotem zamówienia jest dostawa 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 rządzeń 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/BORADCAST.
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. Wykonawca dostarczy:
    - licencję wieczystą na system IDS dla nielimitowanej liczby monitorowanych urządzeń,

- gwarancję producenta na okres 24 miesiące.

41. 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.
    - 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.
42. Wykonawca zainstaluje i za licencjonuje oraz skonfiguruje system IDS w środowisku serwerowym wskazanym przez Zamawiającego.
43. Licencje systemowe oraz sprzęt serwerowy zapewnia Wykonawca w ramach serwera pod system wirtualizacji.
44. Wykonawca przeprowadzi pełną konfigurację i wdrożenia systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.
45. Wykonawca przekaże Zamawiającemu wszelkie hasła, użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.
46. Dla całego powyższego zakresu dot. instalacji, konfiguracji i parametryzacji Wykonawca przeprowadzi testy sprawdzające prawidłowość jego wykonania i działania.
47. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.
48. 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.

2. Sprzętowe sondy do monitorowania sieci OT

Przedmiotem zamówienia jest dostawa trzech sond sprzętowych.
Wymagania:

1. 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.
2. Sondy sprzętowe muszą posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej min. AES128.
3. Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.
4. Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem bateryjnym do 30 minut przy zaniku zasilania z sieci.
5. Sonda sprzętowa musi wspierać: DHCP, stały adres IP.
6. Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.
7. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.
8. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.
9. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.
10. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.
11. 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.

12. Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazaną część ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.
13. Sonda sprzętowa musi umożliwiać przekazywać do systemu IDS strumień sieciowy w formacie IPFIX.
14. Wykonawca dostarczy:
    - sondy sprzętowe w liczbie 3 szt. do monitorowania sieci przemysłowej,
    - gwarancję producenta na okres 24 miesięcy.
15. Serwis producenta ma obejmować:
    - Dostęp do aktualizacji oprogramowania sond sprzętowych.
    - Wymianę uszkodzonych sond sprzętowych w razie awarii.
    - Przekazanie danych kontaktowych do działu technicznego producenta.
    - Wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.
16. 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.
17. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.
18. 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.

3. UPS

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 3 szt. UPS.
Wymagania:

1. MOC min. 1500VA/1500W
2. Obudowa Rack o wysokości max. 2U
3. Topologia Line-interactive
4. Kształt napięcia w trybie bateryjnym: Czyste napięcie sinusoidalne
5. Czas przełączania do 4ms
6. Czas ładowania akumulatorów do 3 godzin
7. Możliwość podłączenia dodatkowych modułów bateryjnych
8. Czas podtrzymania UPSa dla obciążenia 900 W minimum 14 min. przy wykorzystaniu przestrzeni w szafie rack max. 2U dla UPSa i modułów bateryjnych łącznie.
9. Możliwość rozbudowy systemu do uzyskania podtrzymania min. 12 godzin dla w/w obciążenia
10. Ilość gniazd wyjściowych C13: co najmniej 10
11. UPS musi posiadać wydzieloną grupę gniazd dla obciążeń kluczowych/krytycznych oraz dla pozostałych obciążeń .
12. Porty komunikacyjne: USB/RS232/EPO/Dry contact
13. Komunikacja po protokole SNMP oraz http
14. Oprogramowanie w języku polskim do zarządzania UPSem z możliwością monitorowania zużycia energii oraz współpracy ze środowiskiem VMware ESXi 8.0 U2
15. Rozproszenie ciepła online do 75 BTU/h
16. Gwarancja min. 24 miesiące
17. Urządzenie i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego UPSa, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

4. Agregat prądotwórczy

Przedmiotem zamówienia jest agregat prądotwórczy o minimalnej mocy znamionowej 65 kVA (52 kW) - 1 sztuka

1. Wymagania ogólne
   - Agregat wykonany zgodnie z obowiązującymi normami i dyrektywami, w szczególności: 2006/42/WE, 2014/35/UE, 2014/30/UE, 2000/14/WE, 2005/88/WE, PN-EN ISO 8528-13:2016, PN-EN 60204-1 oraz ISO 8528-1.
   - Agregat fabrycznie nowy, trójfazowy, 400/230 V, 50 Hz, cosϕ = 0,8.
   - Paliwo: olej napędowy.
   - Agregat w wykonaniu wyciszonym, obudowanym i przystosowanym do pracy na zewnątrz.
   - Stalowa rama, wibroizolatory i zintegrowany zbiornik paliwa.
   - Poziom ciśnienia akustycznego z odległości 7 m: nie więcej niż 62 dB(A).
   - Maksymalne wymiary agregatu w obudowie: 2700 x 1000 x 1190 mm.
   - Masa bez paliwa: nie więcej niż 1200 kg.
2. Parametry elektryczne
   - Moc znamionowa PRP minimum 65 kVA / 52 kW.
   - Moc maksymalna ESP minimum 71 kVA / 57 kW.
   - Prąd znamionowy minimum 93 A.
   - Napięcie 400/230 V, częstotliwość 50 Hz.
   - Wyłącznik główny minimum 100 A, 3-biegunowy.
3. Silnik
   - Silnik wysokoprężny, 4-cylindrowy.
   - Pojemność skokowa minimum 3760 cm^3.
   - Wtrysk bezpośredni paliwa.
   - Prędkość obrotowa 1500 obr./min.
   - Elektroniczna regulacja obrotów, klasa regulacji G3.
   - Instalacja elektryczna 12 V.
   - Grzałka bloku silnika z termostatem i pompką cyrkulacyjną.
   - Akumulatory rozruchowe i automatyczna ładowarka akumulatorów.
4. Zbiornik paliwa i obudowa
   - Zintegrowany zbiornik paliwa z tworzywa sztucznego o pojemności minimum 160 l.
   - Obudowa wyciszona z kulisami dźwiękochłonnymi.
   - Kompensator wydechu i tłumik.
   - Wibroizolatory pomiędzy zespołem napędowym a ramą.
   - Punkty umożliwiające bezpieczny transport i podnoszenie agregatu.
5. Prądnica
   - Prądnica synchroniczna, bezszczotkowa, samowzbudna.
   - Napięcie 400 V.
   - Elektroniczny regulator napięcia AVR, dokładność regulacji ±1%.
   - Klasa izolacji H.
   - Stopień ochrony IP23.
   - Uzwojenia wykonane w 100% z miedzi.
   - Poskok uzwojenia 2/3.
   - Zawartość harmonicznych THC poniżej 5%.
   - Podtrzymanie prądu zwarciowego 300% prądu znamionowego przez 10 s.
6. Sterownik i wyposażenie elektryczne
   - Sterownik mikroprocesorowy z wyświetlaczem graficznym LCD i menu w języku polskim.

- Tryby pracy OFF / MAN / AUT oraz funkcja automatycznego startu po zaniku napięcia (AMF).
- Współpraca z układem SZR.
- Pomiar napięć, prądów i mocy oraz kontrola podstawowych parametrów silnika.
- Historia zdarzeń i licznik godzin pracy.
- Wbudowany port RS485, obsługa protokołu Modbus oraz możliwość programowania przez Wi-Fi.
- Stopień ochrony panelu sterownika od frontu minimum IP65.
- Przycisk zatrzymania awaryjnego.
- Czujniki ciśnienia oleju, temperatury silnika i poziomu paliwa.

7. Zakres dostawy
   - Dostawa fabrycznie nowego, kompletnego agregatu prądotwórczego do miejsca wskazanego przez Zamawiającego.
   - Przekazanie instrukcji obsługi i dokumentacji urządzenia w języku polskim.
   - Przekazanie karty gwarancyjnej.
   - Szkolenie wskazanych przez Zamawiającego osób z zakresu podstawowej obsługi agregatu.
   - Gwarancja minimum 24 miesiące.

5. Mobilny agregat prądotwórczy

Przedmiotem zamówienia jest mobilny agregat prądotwórczy na przyczepie o minimalnej mocy znamionowej PRP 52 kVA (42 kW) - 1 sztuka.

Wymagania:

1. Agregat wykonany zgodnie z obowiązującymi normami i w szczególności: 2006/42/WE, 2014/35/UE, 2014/30/UE, 2000/14/WE, 2005/88/WE, PN-EN ISO 8528-13:2016 oraz PN-EN 60204-1.
2. Agregat trójfazowy 400/230 V, 50 Hz, w wykonaniu wyciszonym i obudowanym, fabrycznie nowy.
3. Stalowa rama z wzmocnionymi punktami transportowymi oraz wibroizolatorami.
4. Obudowa galwanizowana o grubości minimum 2 mm, wyposażona w kulisy dźwiękochłonne i dostęp serwisowy.
5. Masa agregatu bez paliwa: nie więcej niż 980 kg.
6. Maksymalne wymiary obudowy agregatu: 2080 x 950 x 1130 mm.
7. Ciśnienie akustyczne w odległości 7 m: nie więcej niż 68 dB(A).
8. Gwarantowany poziom mocy akustycznej: nie więcej niż 91 dB(A).
9. Moc znamionowa PRP: minimum 52 kVA / 42 kW.
10. Moc maksymalna ESP: minimum 57 kVA / 46 kW.
11. Prąd znamionowy: minimum 75 A.
12. Współczynnik mocy cos ϕ = 0,8.
13. Napięcie znamionowe 400/230 V, częstotliwość 50 Hz.
14. Silnik wysokoprężny, chłodzony cieczą, spełniający wymagania emisji spalin Stage V.
    a. 4 cylindry, pojemność skokowa minimum 3600 cm^3.
    b. Prędkość obrotowa 1500 obr./min.
    c. Układ paliwowy ECU - Common Rail oraz elektroniczna regulacja obrotów ECU.
    d. Klasa regulacji obrotów G3.
    e. Napięcie instalacji 12 V.
15. Grzałka powietrza dolotowego
16. Świece żarowe.
17. Akumulator rozruchowy z wyłącznikiem izolacyjnym oraz ładowarka akumulatorów.
18. Zbiornik paliwa o pojemności minimum 90 l.

19. Zbiornik paliwa wyposażony w zawór trójdrożny.
20. Prądnica bezszczotkowa, samowzbudna, napięcie 400 V.
21. Moc dla PRP: minimum 55 kVA przy temperaturze otoczenia 40°C.
22. Moc dla ESP: minimum 60 kVA przy temperaturze otoczenia 27°C.
23. Stopień ochrony IP23.
24. Klasa izolacji H, impregnacja ciśnieniowa VPI.
25. Materiał uzwojeń: 100% miedź.
26. Poskok uzwojenia 2/3; liczba wyprowadzeń: 12.
27. Elektroniczny regulator napięcia AVR, dokładność regulacji ±1%.
28. Podtrzymanie prądu zwarciowego 300% In przez 10 s.
29. Zawartość harmonicznych THC < 3%.
30. Reaktancja Xd'' nie większa niż 12%.
31. Sprawność przy 100% obciążenia: minimum 89%.
32. Sterownik mikroprocesorowy z graficznym wyświetlaczem LCD.
33. Menu co najmniej w języku polskim i angielskim; programowanie z poziomu klawiatury sterownika.
34. Stopień ochrony panelu od frontu IP65.
35. Napięcie zasilania sterownika 8-32 V DC.
36. Pomiar napięć i prądów w trzech fazach oraz mocy czynnej, biernej i pozornej agregatu.
37. Pełne zabezpieczenie silnika i prądnicy; pomiar ciśnienia oleju, temperatury silnika i poziomu paliwa.
38. Sygnalizacja stanów alarmowych, historia zdarzeń oraz licznik godzin pracy.
39. Automatyczny start przez kontrolę napięcia (AMF) oraz możliwość startu przez zdalny styk.
40. Współpraca z układem SZR; trzy tryby pracy: OFF, MAN i AUT.
41. Kontrola czasu przeglądów.
42. Wbudowany port RS485, obsługa protokołu Modbus oraz możliwość programowania ze smartfona przez Wi-Fi.
43. Wyposażenie elektryczne agregatu:
    a. Metalowa szafka sterownicza z zamykanymi drzwiami.
    b. Wyłącznik główny 4-biegunowy z zabezpieczeniem różnicowoprądowym 30 mA.
    c. Przycisk zatrzymania awaryjnego.
    d. Ochronny punkt uziemiający.
    e. Czujnik ciśnienia oleju (analogowo-cyfrowy), czujnik temperatury silnika (analogowo-cyfrowy) oraz analogowy czujnik poziomu paliwa.
    f. Gniazda odbioru mocy.
    g. Przystosowanie do współpracy z układem SZR zgodnie z danymi przyłączeniowymi producenta.
44. Zużycie paliwa przy 50% / 75% / 100% obciążeniu: odpowiednio maksymalnie 5,4 / 8,1 / 11,2 l/h.
45. Czas pracy przy 50% / 75% / 100% obciążeniu: odpowiednio minimum 16,7 / 11,1 / 8 h.
46. Przyczepa fabrycznie nowa.
47. Jednoosiowa przyczepa do transportu agregatu prądotwórczego.
48. DMC minimum 1300 kg.
49. Platforma ładunkowa minimum 2400 x 1200 mm.
50. Rama ze stali ocynkowanej ogniowo.
51. Homologacja WE dla przyczepy specjalnej - agregat prądotwórczy.
52. Jedna oś hamowana o nośności minimum 1300 kg.
53. Dyszel prosty o stałej wysokości sprzęgu.

54. Zaczep kulowy.
55. Koło manewrowe.
56. Podłoga z antypoślizgowej, wodoodpornej sklejki.
57. Koła na zewnątrz platformy.
58. Cztery stabilizujące podpory rurowe.
59. Instalacja oświetleniowa.
60. Elementy do bezpiecznego mocowania agregatu.
61. Zakres dostawy
    a. Dostawa kompletnego agregatu prądotwórczego wraz z przyczepą.
    b. Pierwsze uruchomienie.
    c. Sprawdzenie działania agregatu i współpracy podstawowych układów zabezpieczeń.
    d. Szkolenie obsługi.
    e. Dokumentacja w języku polskim.
    f. Gwarancja minimum 24 miesiące.

6. Wdrożenie, konfiguracja i hardening rozwiązań OT

Przedmiotem zamówienia jest wykonanie kompletnej usługi instalacji, konfiguracji, uruchomienia, zabezpieczenia i przekazania do eksploatacji:

1. Systemu IDS dla sieci OT;
2. Sprzętowej sondy OT;
3. Integracji systemu IDS OT z pozostałymi rozwiązaniami bezpieczeństwa Zamawiającego.
4. Usługa musi doprowadzić do uruchomienia produkcyjnego systemu umożliwiającego:
    a. pasywne monitorowanie ruchu OT;
    b. wykrywanie aktywów;
    c. rozpoznawanie protokołów przemysłowych;
    d. wykrywanie zagrożeń i anomalii;
    e. identyfikowanie podatności;
    f. generowanie alarmów;
    g. raportowanie;
    h. przekazywanie zdarzeń do systemu SIEM.
5. Wdrożenie musi zostać przeprowadzone w sposób niezakłócający ciągłości działania procesów technologicznych.
6. Przed rozpoczęciem instalacji Wykonawca przeprowadzi techniczną analizę przedwdrożeniową.
7. Analiza musi obejmować co najmniej:
    a. ustalenie lokalizacji systemu centralnego i sondy;
    b. identyfikację monitorowanego segmentu OT;
    c. wskazanie przełącznika i portu źródłowego dla SPAN;
    d. identyfikację istniejących sieci VLAN;
    e. identyfikację połączeń pomiędzy IT, OT i Internetem;
    f. rozpoznanie głównych urządzeń OT;
    g. rozpoznanie wykorzystywanych protokołów przemysłowych;
    h. oszacowanie przepustowości ruchu przekazywanego do sondy;
    i. ustalenie wymaganej adresacji zarządzającej;
    j. ustalenie zasad synchronizacji czasu;
    k. ustalenie zasad retencji danych;
    l. określenie wymaganych integracji.
8. Wykonawca zainstaluje centralny komponent systemu IDS OT jako maszynę wirtualną albo w innej

architekturze wynikającej z dostarczonego produktu.

9. Wersja systemu musi być zgodna z wersją oprogramowania dostarczonej sondy.
10. Instalacja nie może wymagać obowiązkowego przesyłania danych OT do chmury producenta.
11. Wykonawca zamontuje sondę w uzgodnionej lokalizacji. Zakres obejmuje:
    a. fizyczny montaż;
    b. podłączenie zasilania;
    c. podłączenie do UPS, jeżeli jest dostępny;
    d. podłączenie interfejsu zarządzającego;
    e. podłączenie interfejsów monitorujących;
    f. oznaczenie przewodów i portów;
    g. nadanie adresu zarządzającego;
    h. zmianę wszystkich haseł domyślnych;
    i. aktualizację firmware do wersji zatwierdzonej przez producenta;
    j. podłączenie sondy do centralnego systemu.
12. Interfejs monitorujący musi pracować pasywnie.
13. Odłączenie lub awaria sondy nie może przerywać komunikacji urządzeń produkcyjnych.
14. Po podłączeniu sondy Wykonawca musi zweryfikować:
    a. odbieranie ruchu przez sondę;
    b. brak nadmiernego odrzucania pakietów;
    c. widoczność wymaganych sieci VLAN;
    d. widoczność ruchu dwukierunkowego;
    e. brak wpływu na komunikację produkcyjną.
15. Wykonawca skonfiguruje pasywne wykrywanie aktywów OT.
16. Wykonawca przygotuje początkowy eksport rejestru aktywów.
17. Rejestr musi zostać przekazany w formacie edytowalnym.
18. Wykonawca aktywuje parsery protokołów występujących w środowisku Zamawiającego.
19. Nie należy uruchamiać wszystkich dostępnych parserów bez sprawdzenia ich przydatności.
20. System musi prawidłowo rozpoznawać co najmniej jeden protokół rzeczywiście występujący w monitorowanej sieci.
21. Wykonawca uruchomi proces budowania bazowego profilu normalnej komunikacji.
22. Okres uczenia powinien wynosić minimum 14 dni, chyba że charakter środowiska wymaga innego okresu.
23. Profil musi uwzględniać:
    a. cykliczną komunikację urządzeń;
    b. komunikację okresową;
    c. połączenia realizowane tylko w określonych godzinach;
    d. czynności serwisowe;
    e. procesy wykonywane wyłącznie w określone dni.
24. W okresie uczenia alarmy behawioralne mogą pracować w trybie obserwacji.
25. Po zakończeniu okresu uczenia Wykonawca:
    a. przeanalizuje wykryte odchylenia;
    b. usunie oczywiste fałszywe alarmy;
    c. zatwierdzi prawidłową komunikację;
    d. aktywuje docelowe mechanizmy alarmowania.
26. Wykonawca skonfiguruje poziomy ważności alarmów:
    a. krytyczny;
    b. wysoki;
    c. średni;
    d. niski;
    e. informacyjny.
27. Należy aktywować alarmy co najmniej dla:

a. nowego nieznanego urządzenia;
b. nowego połączenia IT–OT;
c. połączenia z adresem publicznym;
d. użycia nietypowego protokołu;
e. skanowania sieci;
f. wykrycia znanej próby ataku;
g. nietypowej komendy zapisu;
h. zmiany normalnego wzorca komunikacji;
i. utraty kontaktu z krytycznym urządzeniem;
j. utraty komunikacji z sondą;
k. błędu aktualizacji systemu;
l. zbliżającego się wyczerpania przestrzeni dyskowej.

28. Dla każdego alarmu wysokiego i krytycznego należy wskazać zalecany sposób reakcji.
29. Wykonawca skonfiguruje mechanizm przypisywania znanych podatności do wykrytych aktywów.
30. Wdrożenie nie obejmuje automatycznego instalowania poprawek na urządzeniach OT.
31. Wykonawca skonfiguruje przesyłanie zdarzeń do systemu SIEM.
32. Automatyczne działania SOAR wpływające na OT muszą wymagać zatwierdzenia człowieka.
33. Niedopuszczalne jest automatyczne blokowanie portu, urządzenia albo adresu w sieci OT wyłącznie na podstawie pojedynczego alarmu IDS.
34. Hardening systemu IDS i sondy. Wykonawca musi wykonać co najmniej:
    a. zmianę wszystkich domyślnych haseł;
    b. utworzenie imiennych kont administratorów;
    c. utworzenie roli tylko do odczytu;
    d. usunięcie lub zablokowanie zbędnych kont;
    e. wdrożenie zasady minimalnych uprawnień;
    f. uruchomienie MFA, jeżeli rozwiązanie je obsługuje;
    g. ograniczenie dostępu do konsoli do sieci zarządzającej;
    h. ograniczenie dostępu zdalnego;
    i. wyłączenie HTTP, Telnet i innych niezabezpieczonych usług;
    j. wymuszenie HTTPS i SSH;
    k. instalację certyfikatu TLS;
    l. skonfigurowanie bezpiecznych ustawień TLS;
    m. skonfigurowanie synchronizacji czasu;
    n. skonfigurowanie rejestrowania działań administratorów;
    o. przekazywanie logów administracyjnych do SIEM;
    p. wyłączenie nieużywanych interfejsów i usług;
    q. skonfigurowanie automatycznego zakończenia nieaktywnej sesji;
    r. zabezpieczenie kopii konfiguracji;
    s. ograniczenie dostępu do mechanizmów aktualizacji;
    t. sprawdzenie aktualności oprogramowania.
35. Hardening nie obejmuje samodzielnej zmiany konfiguracji urządzeń PLC, RTU, HMI, SCADA ani pozostałych urządzeń technologicznych, chyba że Zamawiający odrębnie zatwierdzi konkretną zmianę.
36. Wykonawca skonfiguruje wykonywanie kopii:
    a. konfiguracji systemu;
    b. konfiguracji sondy;
    c. bazy danych;
    d. własnych reguł;
    e. ustawień integracji;
    f. certyfikatów i kluczy niezbędnych do odtworzenia.
37. Kopie zostaną objęte systemem backupowym dostarczanym w ramach zamówienia.
38. Dane tajne w kopiach muszą być zaszyfrowane.

39. Wykonawca przekaże procedurę odtworzenia.
40. Wykonawca przeprowadzi szkolenie dla minimum dwóch administratorów.
41. Szkolenie musi trwać minimum 8 godzin.
42. Zakres szkolenia musi obejmować:
    a. architekturę systemu;
    b. obsługę konsoli;
    c. przegląd aktywów;
    d. analizę topologii;
    e. analizę alarmów;
    f. analizę protokołów OT;
    g. analizę podatności;
    h. tworzenie reguł;
    i. wyszukiwanie zdarzeń;
    j. eksport PCAP;
    k. generowanie raportów;
    l. obsługę integracji z SIEM;
    m. wykonywanie kopii konfiguracji;
    n. bezpieczną aktualizację systemu;
    o. postępowanie w przypadku awarii sondy.
43. Szkolenie musi zostać przeprowadzone w języku polskim.
44. Zamawiający otrzyma materiały szkoleniowe w formie elektronicznej.
45. Wykonawca przekaże dokumentację obejmującą co najmniej:
    a. opis architektury;
    b. schemat logiczny i fizyczny;
    c. lokalizację sondy;
    d. wykaz portów SPAN/TAP;
    e. adresację;
    f. wykaz aktywów;
    g. wykaz monitorowanych sieci i VLAN;
    h. listę rozpoznanych protokołów;
    i. listę aktywnych reguł;
    j. opis wykonanych ustawień hardeningu;
    k. procedurę backupu i odtwarzania;
    l. procedurę postępowania po utracie komunikacji z sondą;
46. Dokumentacja musi zostać przekazana w formacie PDF oraz edytowalnym w terminie do 14 dni kalendarzowych od zakończenia prac technicznych.
47. Wykonawca musi zapewnić osobę posiadającą doświadczenie w:
    a. sieciach OT/ICS;
    b. pasywnym monitorowaniu ruchu;
    c. protokołach przemysłowych;
    d. systemach IDS lub NDR;
    e. bezpiecznym prowadzeniu zmian w środowiskach produkcyjnych.
48. Wykonawca odpowiada za współpracę specjalistów sieciowych, systemowych i OT.
49. Podstawą odbioru będzie:
    a. zakończenie instalacji;
    b. pozytywne wykonanie testów;
    c. przekazanie dokumentacji;
    d. przeprowadzenie szkolenia;
    e. przekazanie Zamawiającemu danych administracyjnych;
    f. usunięcie błędów krytycznych i wysokich.
50. Błędy krytyczne i wysokie muszą zostać usunięte przed odbiorem.

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego **Cyberbezpieczne Wodociągi ,** Inwestycja C3.1.1. Cyberbezpieczeństwo - Cyber PL , infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo - Krajowy Plan Odbudowy i Zwiększania Odporności