Zamawiający:

Zakład Wodociągów, Kanalizacji i Oczyszczalnia Ścieków „WOD-KAN" Spółka z ograniczoną odpowiedzialnością
06-500 Mława, ul. Płocka 106, NIP: 569 000 32 88, REGON: 130020022, KRS 0000106569, +48 23 654 60 70, sekretariat@wod-kan-mlawa.com.pl

Załącznik nr 1
do Specyfikacji Warunków Zamówienia

OPIS PRZEDMIOTU ZAMÓWIENIA

dla zamówienia o wartości nieprzekraczającej 432 000 euro pod nazwą:

„Wzmocnienie cyberodporności IT i OT oraz ciągłości działania poprzez wdrożenie kluczowych środków technicznych oraz rozwój kompetencji"

Zamówienie realizowane jest w ramach projektu grantowego pod nazwą „Cyberbezpieczne Wodociągi" – Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności, Inwestycja C3.1.1. Cyberbezpieczńsowto – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi.

Numer sprawy: **KT-421**

Zatwierdził: Marek Dusiński - Prezes Zarządu

wod kan MŁAWA
Elektronicznie podpisany przez Marek Dusiński
Data: 2026.04.22 13:26:41 +02'00'

.....

Zamawiający określa, że przedmiotem niniejszego postępowania o udzielenie zamówienia jest realizacja usług oraz dostawa sprzętów oraz oprogramowania. Zamówienie realizowane jest zgodnie założeniami projektu grantowego pod nazwą „Cyberbezpieczne Wodociągi" – Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności, Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi.

Szczegółowy zakres niniejszego postępowania obejmuje:

- **dla części 1:**
  - usługa przeprowadzenia audytu początkowego Systemu Zarządzania Bezpieczeństwa Informacji oraz Systemu Zarządzania Ciągłością Działania wraz z oceną stopnia zgodności z wymaganiami cyberbezpieczeństwa (KRI oraz uoKSC);
  - usługa przeprowadzenia audytu początkowego Systemu Zarządzania Bezpieczeństwa Informacji oraz Systemu Zarządzania Ciągłością Działania wraz z oceną stopnia zgodności z wymaganiami cyberbezpieczeństwa (KRI oraz uoKSC);
  - usługa opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz Systemu Zarządzania Ciągłością Działania
  - usługa przeprowadzenia szkolenia dla kadry kierowniczej z zakresu cyberbezpieczeństwa, w tym Systemu Zarządzania Bezpieczeństwem Informacji oraz Systemu Zarządzania Ciągłością Działania
- **dla części 2:**
  - usługa przeprowadzenia szkolenia dla pracowników z zakresu cyberbezpieczeństwa budującego świadomość cyberzagrożeń i sposobów ochrony (2 szt.)
- **dla części 3:**
  - dostawa fizycznego serwera dla obszaru IT wraz z oprogramowaniem do wirtualizacji;
  - dostawa oprogramowania typu XDR dla obszaru IT oraz OT
  - dostawa urządzeń NGFW wraz z oprogramowaniem dla obszaru IT;
  - dostawa urządzeń UTM wraz z oprogramowaniem dla obszaru OT;
  - dostawa oprogramowania do monitorowania infrastruktury informatycznej dla obszaru IT oraz OT;
  - dostawa oprogramowania SIEM dla obszaru IT oraz OT;
  - dostawa oprogramowania SOAR dla obszaru IT oraz OT;
  - dostawa serwera fizycznego do wykonywania kopii zapasowych dla obszaru IT oraz OT;

- dostawa oprogramowania do wykonywania kopii zapasowych dla obszaru IT oraz OT;
- dostawa oprogramowania NAC dla obszaru IT oraz OT;
- dostawa szafy rack;
- dostawa macierzy dyskowej wraz z dyskami twardymi dla obszaru IT;
- dostawa oprogramowania IDS dedykowanego sieciom OT;
- dostawa sprzętowych sond do monitorowania sieci OT;
- dostawa serwera fizycznego dla obszaru OT;
- dostawa zarządzalnych urządzeń sieciowych;
- dostawa urządzeń access point;
- usługa wdrożenia i konfiguracji urządzeń, oprogramowania i rozwiązań z zakresu bezpieczeństwa

- dla części 4:

  - dostawa agregatu prądotwórczego.

CZĘŚĆ 1 Usługi audytorskie

1. usługa przeprowadzenia audytu początkowego Systemu Zarządzania Bezpieczeństwa Informacji oraz Systemu Zarządzania Ciągłością Działania wraz z oceną stopnia zgodności z wymaganiami cyberbezpieczeństwa (KRI oraz uoKSC)

Przedmiotem zamówienia jest wykonanie kompleksowej usługi audytorskiej obejmującej:

1. audyt Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
2. audyt Systemu Zarządzania Ciągłością Działania (SZCD),
3. ocenę zgodności organizacyjnej, technicznej, proceduralnej i formalnoprawnej Zamawiającego z wymaganiami dotyczącymi bezpieczeństwa informacji, cyberbezpieczeństwa oraz odporności operacyjnej.

Audyty mają charakter **audytu początkowego** realizowanego w ramach projektu grantowego „Cyberbezpieczne Wodociągi" i mają służyć ustaleniu stanu wyjściowego bezpieczeństwa organizacji, identyfikacji luk, podatności, braków organizacyjnych i proceduralnych, a także określeniu rekomendowanych działań naprawczych, doskonalących i wdrożeniowych, które powinny zostać zrealizowane w toku projektu.

Zakres audytu musi uwzględniać specyfikę działalności przedsiębiorstwa wodociągowo-kanalizacyjnego, w tym środowisk IT i OT, systemów sterowania, automatyki przemysłowej, systemów telemetrycznych, systemów SCADA, systemów zdalnego monitoringu i infrastruktury krytycznej lub mającej istotne znaczenie dla ciągłości świadczenia usług zbiorowego zaopatrzenia w wodę i odprowadzania ścieków.

Audyty mają zostać przeprowadzone w oparciu o aktualnie obowiązujące oraz mające zastosowanie przepisy prawa, normy, wytyczne i dobre praktyki, w szczególności:

- rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI), Dz.U. 2024 poz. 773;
- ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tekst jednolity Dz.U. 2026 poz. 20, z uwzględnieniem zmian wprowadzonych ustawą z dnia 23 stycznia 2026 r., Dz.U. 2026 poz. 252;
- dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2), jako punkt odniesienia dla oceny dojrzałości organizacyjnej i technicznej w zakresie zarządzania ryzykiem cyberbezpieczeństwa, obsługi incydentów, ciągłości działania, bezpieczeństwa łańcucha dostaw, polityk, procedur, testowania i nadzoru;
- PN-EN ISO/IEC 27001 – wymagania dla systemu zarządzania bezpieczeństwem informacji;
- PN-EN ISO/IEC 27002 – wytyczne dotyczące stosowania zabezpieczeń bezpieczeństwa informacji;
- PN-EN ISO/IEC 27005 – wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji;
- PN-EN ISO 22301 – wymagania dla systemu zarządzania ciągłością działania;
- PN-EN ISO 22313 – wytyczne do wdrażania i utrzymania systemu ciągłości działania;
- aktualne wytyczne i dobre praktyki ENISA dotyczące środków zarządzania ryzykiem cyberbezpieczeństwa, wdrażania wymagań NIS2 oraz bezpieczeństwa łańcucha dostaw.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie co najmniej do:

1. przeprowadzenia analizy dokumentacji Zamawiającego, w szczególności polityk, procedur, instrukcji, rejestrów, planów, analiz ryzyka, planów ciągłości działania, planów odtworzeniowych, dokumentacji technicznej, dokumentacji systemów teleinformatycznych oraz dokumentacji dotyczącej środowisk OT/ICS/SCADA;
2. przeprowadzenia wywiadów i warsztatów z przedstawicielami Zamawiającego, w tym z kierownictwem, personelem odpowiedzialnym za IT, OT, cyberbezpieczeństwo, utrzymanie ruchu, automatykę, eksploatację sieci, ochronę danych, zarządzanie kryzysowe i ciągłość działania;
3. przeprowadzenia oceny dojrzałości SZBI oraz SZCD, obejmującej co najmniej:

   - ład organizacyjny i odpowiedzialności,
   - polityki i procedury,
   - zarządzanie ryzykiem,
   - zarządzanie incydentami,
   - zarządzanie podatnościami,
   - bezpieczeństwo zasobów informacyjnych,
   - bezpieczeństwo infrastruktury IT i OT,
   - bezpieczeństwo sieci i segmentację,
   - kontrolę dostępu,
   - zarządzanie kopiami zapasowymi i odtwarzaniem,
   - rejestrowanie i monitorowanie zdarzeń,
   - bezpieczeństwo dostawców i łańcucha dostaw,
   - zarządzanie zmianą,
   - odporność operacyjną,
   - plany ciągłości działania i odtwarzania po awarii,
   - testowanie rozwiązań awaryjnych i planów ciągłości działania,
   - świadomość i kompetencje personelu;

4. przeprowadzenia oceny zgodności z wymaganiami KRI, w szczególności w zakresie organizacji bezpieczeństwa informacji, zarządzania ryzykiem, środków technicznych i organizacyjnych, monitorowania, rozliczalności, kopii zapasowych, ciągłości działania i nadzoru nad systemami teleinformatycznymi;
5. przeprowadzenia oceny zgodności z wymaganiami wynikającymi z ustawy o krajowym systemie cyberbezpieczeństwa, w tym w zakresie organizacji systemu bezpieczeństwa, zarządzania incydentami, środków bezpieczeństwa, nadzoru, dokumentowania działań oraz gotowości do spełniania obowiązków podmiotów objętych regulacją;
6. przeprowadzenia oceny zgodności i dojrzałości względem wymagań NIS2, w szczególności w obszarze:

   - polityk analizy ryzyka i bezpieczeństwa systemów informacyjnych,
   - obsługi incydentów,
   - ciągłości działania, backupu i disaster recovery,
   - bezpieczeństwa łańcucha dostaw,
   - bezpieczeństwa nabywania, rozwoju i utrzymania systemów,
   - oceny skuteczności środków zarządzania ryzykiem,
   - cyberhigieny i szkoleń,
   - kryptografii i, tam gdzie zasadne, szyfrowania,
   - bezpieczeństwa zasobów ludzkich i kontroli dostępu,
   - stosowania uwierzytelniania wieloskładnikowego oraz bezpiecznej komunikacji;

7. przeprowadzenia oceny obszarów branżowych specyficznych dla przedsiębiorstwa wodociągowo-kanalizacyjnego, w szczególności:

   - bezpieczeństwa systemów sterowania przemysłowego i automatyki,
   - rozdzielenia i zabezpieczenia stref IT/OT,
   - połączeń zdalnych do infrastruktury technologicznej,
   - bezpieczeństwa telemetryki, przepompowni, stacji uzdatniania wody, oczyszczalni ścieków, przepływomierzy, czujników i urządzeń terenowych,
   - odporności na zakłócenia procesów technologicznych,
   - bezpieczeństwa dostępu serwisowego producentów i integratorów,
   - bezpieczeństwa aktualizacji, zmian konfiguracyjnych i prac serwisowych w środowiskach OT;

8. identyfikacji niezgodności, luk, ryzyk, podatności organizacyjnych i technicznych oraz obszarów wymagających pilnej interwencji;
9. opracowania raportu końcowego z audytu początkowego.

Minimalne wymagania dotyczące raportu z audytu początkowego

Raport z audytu musi zawierać co najmniej:

1. opis celu, zakresu i metodyki audytu;
2. opis stanu istniejącego;
3. ocenę zgodności z wymaganiami KRI, uoKSC, NIS2 oraz wskazanymi normami;
4. ocenę dojrzałości SZBI i SZCD;
5. identyfikację luk, niezgodności, słabości i ryzyk;
6. ocenę wpływu stwierdzonych słabości na bezpieczeństwo świadczenia usług wodociągowo-kanalizacyjnych;
7. rekomendacje działań naprawczych, usprawniających i rozwojowych;
8. propozycję priorytetyzacji działań według istotności, pilności i wpływu na ciągłość działania;
9. wskazanie rekomendowanych działań krótko-, średnio- i długoterminowych;
10. macierz zgodności lub tabelę odniesień do wymagań prawnych, normatywnych i branżowych;
11. podsumowanie dla kierownictwa w formie syntetycznej, umożliwiające podjęcie decyzji zarządczych.

Raport powinien być sporządzony w sposób praktyczny i wdrożeniowy, tak aby mógł stanowić podstawę do realizacji projektu poprawy cyberbezpieczeństwa, wdrożenia lub aktualizacji dokumentacji systemowej, planowania inwestycji technicznych oraz przygotowania organizacji do spełniania wymagań wynikających z przepisów krajowych i unijnych.

Zamawiający wymaga ponadto, aby w ramach audytu końcowego zostały przeprowadzone testy penetracyjne. Zamawiający określa, że minimalny zakres testów penetracyjnych (przy czym przez testy penetracyjne należy rozumieć przeprowadzenie testów mających na celu wykrycie nieznanych podatności - skanowanie pod kątem znanych podatności narzędziami typu Nessus, OpenVAS (Greenbone), BurpSuite, Acunetix i inne tożsame i podobne, nie spełnia wymagania testów penetracyjnych) wykonanych przez certyfikowanego pentestera musi obejmować przynajmniej:

- zewnętrzne testy penetracyjne infrastruktury informatycznej:

- analiza topologii brzegu sieci - ocena struktury i zabezpieczeń brzegów sieci oddzielających wewnętrzne zasoby od Internetu;
- weryfikacja mechanizmów ochronnych - przegląd i testowanie zabezpieczeń zastosowanych na granicy sieci, w tym firewalli, systemów wykrywania i zapobiegania intruzom (IDS/IPS) oraz innych mechanizmów ochronnych;
- wykrywanie usług sieciowych udostępnianych do Internetu - skanowanie portów i usług dostępnych publicznie w celu identyfikacji potencjalnych wejść dla atakujących;
- detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet - identyfikacja wersji oprogramowania serwerowego dostępnego publicznie, co może pomóc w wykryciu znanych podatności.
- exploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet - próby eksploatacji zidentyfikowanych podatności w celu oceny ryzyka;
- przedstawienie rozwiązań zwiększających bezpieczeństwo styku sieci lokalnej z siecią Internet - rekomendacje dotyczące wzmocnienia zabezpieczeń brzegu sieci.

- wewnętrzne testy penetracyjne infrastruktury informatycznej:
  - analiza topologii sieci LAN - ocena struktury i zabezpieczeń wewnętrznej sieci LAN;
  - weryfikacja mechanizmów ochronnych w sieci - analiza i testowanie wewnętrznych zabezpieczeń sieciowych, w tym segregacji sieci i izolacji urządzeń;
  - analiza komunikacji sieciowej - monitoring i analiza ruchu sieciowego w poszukiwaniu nietypowych wzorców mogących wskazywać na naruszenia bezpieczeństwa;
  - skanowanie portów TCP/UDP i wykrywanie usług sieciowych - identyfikacja usług i aplikacji działających w sieci wewnętrznej;
  - skanowanie hostów aktywnych w sieci - lokalizacja i analiza aktywnych urządzeń w sieci wewnętrznej;
  - exploitacja dostępnych urządzeń oraz usług w sieci LAN - próby eksploatacji znalezionych podatności w celu oceny wewnętrznych ryzyk bezpieczeństwa;
  - proces tworzenia i odtwarzania kopii zapasowych - ocena procedur backupu i możliwości odzyskania danych;
  - monitorowanie ruchu sieciowego - sprawdzenie systemów monitorowania w celu wykrywania podejrzanych aktywności i naruszeń bezpieczeństwa;
  - przedstawienie rozwiązań zwiększających bezpieczeństwo sieci LAN - rekomendacje dotyczące poprawy zabezpieczeń wewnętrznej sieci LAN;

- audyt serwisów WWW obejmujący swoim zakresem:
  - wersje serwera HTTP i systemu CMS - sprawdzenie aktualności i bezpieczeństwa zainstalowanych wersji, z naciskiem na znane podatności;
  - bezpieczeństwo komunikacji - ocena aktualności certyfikatów X.509, wersji protokołu TLS i stosowanych algorytmów kryptograficznych, zapewniająca poufność i integralność przesyłanych danych.

- audyt serwisów pocztowych obejmujący:
  - mechanizmy SPF, DKIM i DMARC - analiza poprawności wdrożenia tych mechanizmów w celu zapobiegania fałszowaniu adresów e-mail i zwiększenia wiarygodności wysyłanych wiadomości.

- bezpieczeństwo mechanizmów TLS - ocena poprawności i bezpieczeństwa wdrożenia mechanizmów szyfrowania TLS w komunikacji pocztowej.

Wymagania wobec sposobu realizacji usługi

Wykonawca zobowiązany jest przeprowadzić audyt z należytą starannością, w sposób niezależny, obiektywny i zapewniający poufność informacji pozyskanych w toku realizacji zamówienia.

Zamawiający wymaga, aby wnioski z audytu uwzględniały zarówno ogólne wymagania systemowe, jak i specyfikę branży wodociągowo-kanalizacyjnej, w tym konieczność zapewnienia ciągłości świadczenia usług publicznych, bezpieczeństwa procesów technologicznych, niezawodności infrastruktury oraz ochrony danych i systemów wykorzystywanych w eksploatacji sieci wodociągowej i kanalizacyjnej.

Zamawiający wymaga, aby audyt przeprowadzony był w formie stacjonarnej, w oparciu o przeprowadzoną wizję lokalną. Jedynie w przypadku konieczności uzupełnień, dopuszczalna jest forma zdalna

Wymaga się, aby z przeprowadzonego audytu Wykonawca opracował i przedłożył Zamawiającemu raport w wersji papierowej i elektronicznej. Raport z audytu powinien być podpisany przez audytora opracowującego audyt. Zamawiający zastrzega prawo do wniesienia uwag do przedłożonej dokumentacji, a Wykonawca zobowiązuje się do jej skorygowania i uwzględnienia wniesionych uwag.

2. usługa przeprowadzenia audytu końcowego Systemu Zarządzania Bezpieczeństwa Informacji oraz Systemu Zarządzania Ciągłością Działania wraz z oceną stopnia zgodności z wymaganiami cyberbezpieczeństwa (KRI oraz uoKSC)

Przedmiotem zamówienia jest wykonanie kompleksowej usługi audytorskiej obejmującej:

1. audyt Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
2. audyt Systemu Zarządzania Ciągłością Działania (SZCD),
3. ocenę zgodności organizacyjnej, technicznej, proceduralnej i formalnoprawnej Zamawiającego z wymaganiami dotyczącymi bezpieczeństwa informacji, cyberbezpieczeństwa oraz odporności operacyjnej.

Audyty mają charakter audytu końcowego realizowanego w ramach projektu grantowego „Cyberbezpieczne Wodociągi” i mają służyć ocenie stanu docelowego bezpieczeństwa organizacji po realizacji działań przewidzianych w projekcie, weryfikacji stopnia wdrożenia zaleceń wynikających z audytu początkowego, ocenie skuteczności zastosowanych środków organizacyjnych i technicznych oraz potwierdzeniu poziomu zgodności Zamawiającego z wymaganiami dotyczącymi bezpieczeństwa informacji, cyberbezpieczeństwa i ciągłości działania.

Zakres audytu musi uwzględniać specyfikę działalności przedsiębiorstwa wodociągowo-kanalizacyjnego, w tym środowisk IT i OT, systemów sterowania, automatyki przemysłowej, systemów telemetrycznych, systemów SCADA, systemów zdalnego monitoringu i

infrastruktury krytycznej lub mającej istotne znaczenie dla ciągłości świadczenia usług zbiorowego zaopatrzenia w wodę i odprowadzania ścieków.

Audyty mają zostać przeprowadzone w oparciu o aktualnie obowiązujące oraz mające zastosowanie przepisy prawa, normy, wytyczne i dobre praktyki, w szczególności:

- rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI), Dz.U. 2024 poz. 773;
- ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tekst jednolity Dz.U. 2026 poz. 20, z uwzględnieniem zmian wprowadzonych ustawą z dnia 23 stycznia 2026 r., Dz.U. 2026 poz. 252;
- dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2), jako punkt odniesienia dla oceny dojrzałości organizacyjnej i technicznej w zakresie zarządzania ryzykiem cyberbezpieczeństwa, obsługi incydentów, ciągłości działania, bezpieczeństwa łańcucha dostaw, polityk, procedur, testowania i nadzoru;
- PN-EN ISO/IEC 27001 – wymagania dla systemu zarządzania bezpieczeństwem informacji;
- PN-EN ISO/IEC 27002 – wytyczne dotyczące stosowania zabezpieczeń bezpieczeństwa informacji;
- PN-EN ISO/IEC 27005 – wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji;
- PN-EN ISO 22301 – wymagania dla systemu zarządzania ciągłością działania;
- PN-EN ISO 22313 – wytyczne do wdrażania i utrzymania systemu ciągłości działania;
- aktualne wytyczne i dobre praktyki ENISA dotyczące środków zarządzania ryzykiem cyberbezpieczeństwa, wdrażania wymagań NIS2 oraz bezpieczeństwa łańcucha dostaw.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie co najmniej do:

1. przeprowadzenia analizy dokumentacji Zamawiającego, w tym dokumentacji opracowanej, wdrożonej lub zaktualizowanej w toku realizacji projektu, w szczególności polityk, procedur, instrukcji, rejestrów, planów, analiz ryzyka, planów ciągłości działania, planów odtworzeniowych, dokumentacji technicznej, dokumentacji systemów teleinformatycznych oraz dokumentacji dotyczącej środowisk OT/ICS/SCADA;
2. przeprowadzenia wywiadów i warsztatów z przedstawicielami Zamawiającego, w tym z kierownictwem, personelem odpowiedzialnym za IT, OT, cyberbezpieczeństwo, utrzymanie ruchu, automatykę, eksploatację sieci, ochronę danych, zarządzanie kryzysowe i ciągłość działania;
3. przeprowadzenia oceny dojrzałości SZBI oraz SZCD, obejmującej co najmniej:

    - ład organizacyjny i odpowiedzialności,
    - polityki i procedury,
    - zarządzanie ryzykiem,
    - zarządzanie incydentami,
    - zarządzanie podatnościami,
    - bezpieczeństwo zasobów informacyjnych,
    - bezpieczeństwo infrastruktury IT i OT,
    - bezpieczeństwo sieci i segmentację,
    - kontrolę dostępu,
    - zarządzanie kopiami zapasowymi i odtwarzaniem,
    - rejestrowanie i monitorowanie zdarzeń,
    - bezpieczeństwo dostawców i łańcucha dostaw,
    - zarządzanie zmianą,

- odporność operacyjną,
- plany ciągłości działania i odtwarzania po awarii,
- testowanie rozwiązań awaryjnych i planów ciągłości działania,
- świadomość i kompetencje personelu;

4. przeprowadzenia oceny zgodności z wymaganiami KRI, w szczególności w zakresie organizacji bezpieczeństwa informacji, zarządzania ryzykiem, środków technicznych i organizacyjnych, monitorowania, rozliczalności, kopii zapasowych, ciągłości działania i nadzoru nad systemami teleinformatycznymi;
5. przeprowadzenia oceny zgodności z wymaganiami wynikającymi z ustawy o krajowym systemie cyberbezpieczeństwa, w tym w zakresie organizacji systemu bezpieczeństwa, zarządzania incydentami, środków bezpieczeństwa, nadzoru, dokumentowania działań oraz gotowości do spełniania obowiązków podmiotów objętych regulacją;
6. przeprowadzenia oceny zgodności i dojrzałości względem wymagań NIS2, w szczególności w obszarze:

   - polityk analizy ryzyka i bezpieczeństwa systemów informacyjnych,
   - obsługi incydentów,
   - ciągłości działania, backupu i disaster recovery,
   - bezpieczeństwa łańcucha dostaw,
   - bezpieczeństwa nabywania, rozwoju i utrzymania systemów,
   - oceny skuteczności środków zarządzania ryzykiem,
   - cyberhigieny i szkoleń,
   - kryptografii i, tam gdzie zasadne, szyfrowania,
   - bezpieczeństwa zasobów ludzkich i kontroli dostępu,
   - stosowania uwierzytelniania wieloskładnikowego oraz bezpiecznej komunikacji;

7. przeprowadzenia oceny obszarów branżowych specyficznych dla przedsiębiorstwa wodociągowo-kanalizacyjnego, w szczególności:

   - bezpieczeństwa systemów sterowania przemysłowego i automatyki,
   - rozdzielenia i zabezpieczenia stref IT/OT,
   - połączeń zdalnych do infrastruktury technologicznej,
   - bezpieczeństwa telemetryki, przepompowni, stacji uzdatniania wody, oczyszczalni ścieków, przepływomierzy, czujników i urządzeń terenowych,
   - odporności na zakłócenia procesów technologicznych,
   - bezpieczeństwa dostępu serwisowego producentów i integratorów,
   - bezpieczeństwa aktualizacji, zmian konfiguracyjnych i prac serwisowych w środowiskach OT;

8. weryfikacji stopnia realizacji zaleceń wynikających z audytu początkowego oraz oceny skuteczności wdrożonych działań naprawczych, organizacyjnych i technicznych;
9. oceny, czy wdrożone rozwiązania przyczyniły się do podniesienia poziomu bezpieczeństwa, odporności operacyjnej i ciągłości działania Zamawiającego;
10. identyfikacji niezgodności, luk, ryzyk resztkowych, podatności organizacyjnych i technicznych oraz obszarów wymagających dalszych działań doskonalących;
11. opracowania raportu końcowego z audytu końcowego.

Minimalne wymagania dotyczące raportu końcowego z audytu końcowego

Raport końcowy z audytu musi zawierać co najmniej:

1. opis celu, zakresu i metodyki audytu;

2. opis stanu istniejącego na dzień zakończenia realizacji audytu;
3. ocenę zgodności z wymaganiami KRI, uoKSC, NIS2 oraz wskazanymi normami;
4. ocenę dojrzałości SZBI i SZCD;
5. ocenę stopnia wdrożenia zaleceń wynikających z audytu początkowego;
6. identyfikację pozostających luk, niezgodności, słabości i ryzyk;
7. ocenę wpływu wdrożonych rozwiązań na bezpieczeństwo świadczenia usług wodociągowo-kanalizacyjnych;
8. ocenę skuteczności wdrożonych działań naprawczych, usprawniających i rozwojowych;
9. wskazanie ryzyk resztkowych oraz obszarów wymagających dalszego doskonalenia;
10. macierz zgodności lub tabelę odniesień do wymagań prawnych, normatywnych i branżowych;
11. podsumowanie dla kierownictwa w formie syntetycznej, umożliwiające ocenę osiągniętego poziomu zgodności i podjęcie dalszych decyzji zarządczych.

Raport powinien być sporządzony w sposób praktyczny i wdrożeniowy, tak aby stanowił potwierdzenie osiągniętych efektów projektu, podstawę do odbioru rezultatów działań zrealizowanych w ramach projektu poprawy cyberbezpieczeństwa oraz materiał służący do dalszego utrzymania, monitorowania i doskonalenia systemów bezpieczeństwa informacji i ciągłości działania.

Zamawiający wymaga ponadto, aby w ramach audytu końcowego zostały przeprowadzone testy penetracyjne. Zamawiający określa, że minimalny zakres testów penetracyjnych (przy czym przez testy penetracyjne należy rozumieć przeprowadzenie testów mających na celu wykrycie nieznanych podatności - skanowanie pod kątem znanych podatności narzędziami typu Nessus, OpenVAS (Greenbone), BurpSuite, Acunetix i inne tożsame i podobne, nie spełnia wymagania testów penetracyjnych) wykonanych przez certyfikowanego pentestera musi obejmować przynajmniej:

- zewnętrzne testy penetracyjne infrastruktury informatycznej:
  - analiza topologii brzegu sieci - ocena struktury i zabezpieczeń brzegów sieci oddzielających wewnętrzne zasoby od Internetu;
  - weryfikacja mechanizmów ochronnych - przegląd i testowanie zabezpieczeń zastosowanych na granicy sieci, w tym firewalli, systemów wykrywania i zapobiegania intruzom (IDS/IPS) oraz innych mechanizmów ochronnych;
  - wykrywanie usług sieciowych udostępnianych do Internetu - skanowanie portów i usług dostępnych publicznie w celu identyfikacji potencjalnych wejść dla atakujących;
  - detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet - identyfikacja wersji oprogramowania serwerowego dostępnego publicznie, co może pomóc w wykryciu znanych podatności.
  - exploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet - próby eksploatacji zidentyfikowanych podatności w celu oceny ryzyka;
  - przedstawienie rozwiązań zwiększających bezpieczeństwo styku sieci lokalnej z siecią Internet - rekomendacje dotyczące wzmocnienia zabezpieczeń brzegu sieci.

- wewnętrzne testy penetracyjne infrastruktury informatycznej:
  - analiza topologii sieci LAN - ocena struktury i zabezpieczeń wewnętrznej sieci LAN;

- weryfikacja mechanizmów ochronnych w sieci - analiza i testowanie wewnętrznych zabezpieczeń sieciowych, w tym segregacji sieci i izolacji urządzeń;
- analiza komunikacji sieciowej - monitoring i analiza ruchu sieciowego w poszukiwaniu nietypowych wzorców mogących wskazywać na naruszenia bezpieczeństwa;
- skanowanie portów TCP/UDP i wykrywanie usług sieciowych - identyfikacja usług i aplikacji działających w sieci wewnętrznej;
- skanowanie hostów aktywnych w sieci - lokalizacja i analiza aktywnych urządzeń w sieci wewnętrznej;
- exploitacja dostępnych urządzeń oraz usług w sieci LAN - próby eksploatacji znalezionych podatności w celu oceny wewnętrznych ryzyk bezpieczeństwa;
- proces tworzenia i odtwarzania kopii zapasowych - ocena procedur backupu i możliwości odzyskania danych;
- monitorowanie ruchu sieciowego - sprawdzenie systemów monitorowania w celu wykrywania podejrzanych aktywności i naruszeń bezpieczeństwa;
- przedstawienie rozwiązań zwiększających bezpieczeństwo sieci LAN - rekomendacje dotyczące poprawy zabezpieczeń wewnętrznej sieci LAN;

- audyt serwisów WWW obejmujący swoim zakresem:
  - wersje serwera HTTP i systemu CMS - sprawdzenie aktualności i bezpieczeństwa zainstalowanych wersji, z naciskiem na znane podatności;
  - bezpieczeństwo komunikacji - ocena aktualności certyfikatów X.509, wersji protokołu TLS i stosowanych algorytmów kryptograficznych, zapewniająca poufność i integralność przesyłanych danych.

- audyt serwisów pocztowych obejmujący:
  - mechanizmy SPF, DKIM i DMARC - analiza poprawności wdrożenia tych mechanizmów w celu zapobiegania fałszowaniu adresów e-mail i zwiększenia wiarygodności wysyłanych wiadomości.
  - bezpieczeństwo mechanizmów TLS - ocena poprawności i bezpieczeństwa wdrożenia mechanizmów szyfrowania TLS w komunikacji pocztowej.

Wymagania wobec sposobu realizacji usługi

Wykonawca zobowiązany jest przeprowadzić audyt z należytą starannością, w sposób niezależny, obiektywny i zapewniający poufność informacji pozyskanych w toku realizacji zamówienia. Wykonawca powinien dysponować personelem posiadającym doświadczenie w audytach bezpieczeństwa informacji, cyberbezpieczeństwa, ciągłości działania oraz – co najmniej w zakresie zespołu realizującego – doświadczenie w audytach środowisk przemysłowych lub infrastruktury krytycznej, usług kluczowych albo sektorów komunalnych.

Zamawiający wymaga, aby wnioski z audytu uwzględniały zarówno ogólne wymagania systemowe, jak i specyfikę branży wodociągowo-kanalizacyjnej, w tym konieczność zapewnienia ciągłości świadczenia usług publicznych, bezpieczeństwa procesów technologicznych, niezawodności infrastruktury oraz ochrony danych i systemów wykorzystywanych w eksploatacji sieci wodociągowej i kanalizacyjnej.

Zamawiający wymaga przeprowadzenia audytu w formie stacjonarnej. Jedynie w przypadku konieczności uzupełnień, dopuszczalna jest forma zdalna

Zamawiający wymaga, aby Wykonawca opracował i przedłożył raport w wersji papierowej i elektronicznej. Raport z audytu powinien być podpisany przez audytora opracowującego audyt. Zamawiający zastrzega prawo do wniesienia uwag do przedłożonej dokumentacji, a Wykonawca zobowiązuje się do jej skorygowania i uwzględnienia wniesionych uwag.

3. usługa opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz Systemu Zarządzania Ciągłością Działania

Przedmiotem zamówienia jest realizacja usługi polegającej na opracowaniu, dostosowaniu oraz przygotowaniu do wdrożenia kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej „SZBI", oraz Systemu Zarządzania Ciągłością Działania w obszarze systemów teleinformatycznych, zwanego dalej „SZCD", na podstawie wyników przeprowadzonego audytu początkowego, z uwzględnieniem stanu organizacyjnego, technicznego i formalnoprawnego Zamawiającego.

Celem usługi jest opracowanie spójnej, kompletnej i praktycznej dokumentacji systemowej, dostosowanej do specyfiki przedsiębiorstwa wodociągowo-kanalizacyjnego, jego struktury organizacyjnej, realizowanych procesów, wykorzystywanej infrastruktury, posiadanych zasobów informacyjnych, środowisk IT i OT, systemów automatyki przemysłowej, telemetryki, systemów SCADA, zdalnego monitoringu oraz wymagań związanych z zapewnieniem ciągłości świadczenia usług zbiorowego zaopatrzenia w wodę i odprowadzania ścieków.
Dokumentacja musi zostać opracowana w sposób umożliwiający jej faktyczne wdrożenie i stosowanie przez Zamawiającego, a nie wyłącznie w charakterze formalnym. Wymaga się, aby dokumentacja była wzajemnie spójna, jednolita terminologicznie, zgodna z zakresem działalności Zamawiającego oraz możliwa do wykorzystania jako podstawa organizacji bezpieczeństwa informacji, cyberbezpieczeństwa, ochrony danych, ciągłości działania i odporności operacyjnej.
Dokumentacja powinna zostać opracowana w oparciu o aktualnie obowiązujące przepisy prawa, normy, wytyczne i dobre praktyki, w szczególności:

- rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. 2024 poz. 773;
- ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tekst jednolity Dz.U. 2026 poz. 20, z uwzględnieniem zmian wprowadzonych ustawą z dnia 23 stycznia 2026 r., Dz.U. 2026 poz. 252;
- dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2), jako punkt odniesienia dla wymagań dotyczących zarządzania ryzykiem cyberbezpieczeństwa, ciągłości działania, obsługi incydentów, bezpieczeństwa łańcucha dostaw, zarządzania podatnościami, cyberhigieny i nadzoru;
- PN-EN ISO/IEC 27001 – wymagania dla systemu zarządzania bezpieczeństwem informacji;
- PN-EN ISO/IEC 27002 – wytyczne dotyczące stosowania zabezpieczeń bezpieczeństwa informacji;
- PN-EN ISO/IEC 27005 – wytyczne dotyczące zarządzania ryzykiem w bezpieczeństwie informacji;
- PN-EN ISO 22301 – wymagania dla systemu zarządzania ciągłością działania;
- PN-EN ISO 22313 – wytyczne do wdrażania i utrzymania systemu ciągłości działania;
- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) oraz ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych;

- aktualne wytyczne i dobre praktyki ENISA dotyczące środków zarządzania ryzykiem cyberbezpieczeństwa oraz odporności sektorów krytycznych.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do opracowania dokumentacji w taki sposób, aby obejmowała co najmniej:

1. zasady organizacji bezpieczeństwa informacji i cyberbezpieczeństwa u Zamawiającego;
2. zasady zarządzania ryzykiem w obszarze informacji, systemów teleinformatycznych, cyberbezpieczeństwa i ciągłości działania;
3. zasady klasyfikacji informacji, ochrony zasobów informacyjnych i odpowiedzialności za zasoby;
4. zasady ochrony systemów teleinformatycznych, infrastruktury sieciowej, stanowisk roboczych, serwerów, urządzeń mobilnych oraz środowisk IT i OT;
5. zasady ochrony systemów automatyki przemysłowej, telemetryki, zdalnych połączeń technicznych oraz środowisk SCADA, w zakresie adekwatnym do działalności Zamawiającego;
6. zasady zarządzania incydentami bezpieczeństwa informacji, incydentami cyberbezpieczeństwa i naruszeniami ochrony danych osobowych;
7. zasady zapewnienia ciągłości działania w obszarze systemów teleinformatycznych i procesów krytycznych dla świadczenia usług wodociągowo-kanalizacyjnych;
8. zasady tworzenia, testowania, przechowywania i odtwarzania kopii zapasowych;
9. zasady nadzoru nad dostawcami, usługami zewnętrznymi oraz bezpieczeństwem łańcucha dostaw;
10. zasady monitorowania, przeglądów, testów, audytów, działań korygujących i ciągłego doskonalenia;
11. zasady zgodności z wymaganiami KRI, uKSC, RODO, NIS2 oraz wymaganiami normatywnymi wskazanymi przez Zamawiającego.

Opracowana dokumentacja musi:

- być dostosowana do rzeczywistych warunków organizacyjnych i technicznych Zamawiającego;
- uwzględniać specyfikę przedsiębiorstwa wodociągowo-kanalizacyjnego, w tym procesów technologicznych i eksploatacyjnych;
- być oparta na wynikach audytu początkowego oraz zidentyfikowanych ryzykach, lukach i potrzebach organizacji;
- zawierać wzory rejestrów, formularzy, upoważnień, ewidencji, kart, raportów, planów i oświadczeń, tam, gdzie jest to niezbędne do praktycznego stosowania dokumentacji;
- być opracowana w sposób umożliwiający przyjęcie dokumentów do stosowania w drodze właściwych aktów wewnętrznych Zamawiającego;
- zachowywać spójność pomiędzy dokumentami głównymi, procedurami i załącznikami;
- zawierać logiczne powiązanie pomiędzy SZBI, SZCD, ochroną danych osobowych, zarządzaniem incydentami oraz zarządzaniem ryzykiem;
- uwzględniać podział odpowiedzialności pomiędzy kierownictwo, administratorów, użytkowników, osoby odpowiedzialne za infrastrukturę technologiczną, osoby odpowiedzialne za cyberbezpieczeństwo oraz inne role występujące u Zamawiającego.

Dokumentacja systemowa musi obejmować co najmniej następujące dokumenty główne oraz dokumenty pomocnicze.

1. Polityka Bezpieczeństwa Informacji, w tym w szczególności:

- cele bezpieczeństwa informacji i zasady ich monitorowania;

- opis kontekstu organizacji, interesariuszy oraz czynników wewnętrznych i zewnętrznych;
- zakres SZBI;
- zasady zarządzania dokumentacją systemową;
- role, odpowiedzialności i uprawnienia w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa;
- zasady nadzoru kierownictwa, przeglądów zarządzania i ciągłego doskonalenia;
- zasady klasyfikacji informacji i postępowania z informacjami;
- zasady czystego biurka i czystego ekranu;
- zasady bezpieczeństwa zasobów ludzkich;
- zasady dopuszczania użytkowników do pracy z informacją i systemami;
- zasady zgłaszania oraz obsługi incydentów bezpieczeństwa informacji i cyberbezpieczeństwa;
- zasady monitorowania zgodności z wymaganiami prawnymi, normatywnymi i wewnętrznymi.

2. Polityka Bezpieczeństwa Teleinformatycznego, w tym w szczególności:

- procedura zarządzania dostępem i uprawnieniami;
- procedura uwierzytelniania, stosowania haseł oraz – tam gdzie zasadne – uwierzytelniania wieloskładnikowego;
- procedura bezpieczeństwa sieci teleinformatycznych;
- procedura segmentacji i separacji środowisk IT oraz OT, jeżeli występują;
- procedura użytkowania poczty elektronicznej i korzystania z Internetu;
- procedura bezpiecznej pracy zdalnej;
- procedura korzystania z urządzeń mobilnych i nośników przenośnych;
- procedura szyfrowania danych oraz zasad stosowania kryptografii;
- procedura wykonywania, przechowywania, testowania i odtwarzania kopii zapasowych;
- procedura monitorowania, rejestrowania zdarzeń oraz przeglądu logów;
- procedura zarządzania podatnościami, aktualizacjami i poprawkami bezpieczeństwa;
- procedura zarządzania zmianą w systemach teleinformatycznych;
- procedura przeglądów i konserwacji systemów teleinformatycznych;
- procedura ponownego wykorzystania, przekazania i bezpiecznej utylizacji nośników danych;
- ewidencja sprzętu, oprogramowania, zasobów teleinformatycznych i kont uprzywilejowanych;
- wzory raportów administratora lub osoby odpowiedzialnej za utrzymanie systemów;
- rejestr użytkowników połączeń zdalnych, w tym VPN, jeżeli jest stosowany.

3. Polityka Bezpieczeństwa Fizycznego i Środowiskowego, w tym w szczególności:

- zasady ochrony fizycznej budynków, pomieszczeń i stref;
- procedura zarządzania kluczami, kartami dostępu, kodami i innymi środkami wejścia;
- wykaz pomieszczeń lub części pomieszczeń stanowiących obszar przetwarzania informacji;
- zasady dostępu do serwerowni, punktów dystrybucyjnych, sterowni, pomieszczeń technicznych i innych obszarów wrażliwych;
- ewidencja osób upoważnionych do przebywania w zabezpieczonych obszarach;
- zasady ochrony urządzeń, infrastruktury krytycznej i zasobów technicznych przed uszkodzeniem, utratą, sabotażem lub nieuprawnionym dostępem;
- procedura postępowania w zabezpieczonych obszarach;
- zasady nadzoru nad gośćmi, serwisantami i podmiotami zewnętrznymi;

- zasady reagowania na zdarzenia fizyczne wpływające na bezpieczeństwo informacji i ciągłość działania.

4. Polityka Ochrony Danych Osobowych, w tym w szczególności:

- zasady przetwarzania danych osobowych zgodnie z RODO i ustawą o ochronie danych osobowych;
- zasady realizacji obowiązków administratora;
- zasady nadawania, zmiany i cofania upoważnień do przetwarzania danych osobowych;
- ewidencja osób upoważnionych do przetwarzania danych osobowych;
- oświadczenia o zachowaniu poufności;
- wzory rejestrów udostępnień danych osobowych, jeżeli są stosowane;
- wzory umów powierzenia przetwarzania danych osobowych i wykaz tych umów;
- wzory dokumentów związanych z realizacją praw osób, których dane dotyczą;
- rejestr realizacji żądań osób, których dane dotyczą;
- wzór rejestru czynności przetwarzania oraz – jeżeli zasadne – rejestru kategorii czynności przetwarzania;
- metodologia szacowania ryzyka dla ochrony danych osobowych, zintegrowana z ryzykiem bezpieczeństwa informacji i cyberbezpieczeństwa;
- procedura postępowania w przypadku naruszenia ochrony danych osobowych;
- wzory dokumentów pomocniczych dotyczących analizy naruszeń, zgłoszeń i oceny ryzyka;
- wzór raportu z audytu zgodności z RODO, jeżeli Zamawiający wymaga takiego dokumentu w ramach dokumentacji systemowej.

5. Dokumentacja zarządzania ryzykiem, w tym w szczególności:

- metodyka szacowania ryzyka dla bezpieczeństwa informacji, cyberbezpieczeństwa, ciągłości działania oraz – jeśli Zamawiający tego wymaga – ochrony danych osobowych;
- kryteria oceny prawdopodobieństwa, skutku, poziomu ryzyka i akceptacji ryzyka;
- zasady postępowania z ryzykiem;
- wzory kart ryzyka, rejestru ryzyk, planów postępowania z ryzykiem i przeglądów ryzyka;
- powiązanie wyników analizy ryzyka z doborem zabezpieczeń i dokumentacją SZBI/SZCD.

6. Dokumentacja SZCD dla STI, w tym w szczególności:

- polityka ciągłości działania w obszarze systemów teleinformatycznych;
- zakres SZCD;
- zasady identyfikacji procesów krytycznych oraz zasobów wspierających;
- zasady przeprowadzania analizy wpływu na działalność (BIA) dla obszaru teleinformatycznego;
- zasady analizy zagrożeń i scenariuszy zakłócających;
- plany ciągłości działania i procedury awaryjne dla systemów, usług i zasobów krytycznych;
- procedury odtworzeniowe i przywracania funkcjonowania po incydencie lub awarii;
- zasady określania parametrów odtworzeniowych, w tym RTO i RPO, tam gdzie jest to zasadne;
- zasady organizacji pracy awaryjnej, komunikacji kryzysowej i eskalacji;
- zasady testowania planów ciągłości działania i dokumentowania wyników testów;
- zasady przeglądu i aktualizacji SZCD.

7. Dokumentacja branżowa dla środowisk IT/OT/SCADA

Dokumentacja powinna obejmować także odpowiednie procedury lub zasady dotyczące co najmniej:

- zarządzania dostępem do systemów OT/SCADA;
- rozdziału stref i połączeń pomiędzy IT i OT;
- bezpiecznego dostępu serwisowego dostawców i integratorów;
- bezpieczeństwa aktualizacji, modyfikacji konfiguracji i prac utrzymaniowych w środowisku technologicznym;
- zasad postępowania w przypadku awarii lub incydentu dotyczącego infrastruktury technologicznej;
- zasad dokumentowania zmian w środowisku OT;
- zasad ograniczania ryzyka dla procesów technologicznych istotnych dla dostaw wody i odbioru ścieków.

Wymagania dotyczące rezultatów usługi:

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przekazania Zamawiającemu co najmniej:

1. kompletnej dokumentacji SZBI;
2. kompletnej dokumentacji SZCD w obszarze STI;
3. kompletu wymaganych załączników, rejestrów, wzorów, formularzy i ewidencji;
4. mapy lub wykazu dokumentów wraz z określeniem ich wzajemnych powiązań;
5. wykazu wymagań prawnych, normatywnych i organizacyjnych, do których odnosi się dokumentacja;
6. zestawienia dokumentów opracowanych, zaktualizowanych lub rekomendowanych do wdrożenia;
7. wersji edytowalnej dokumentacji umożliwiającej dalszą aktualizację przez Zamawiającego.

Wymagania wobec sposobu realizacji usługi:

Wykonawca zobowiązany jest do realizacji usługi z należytą starannością, w sposób uwzględniający wyniki audytu początkowego, rzeczywiste potrzeby Zamawiającego oraz specyfikę działalności Zamawiającego.
Wykonawca zobowiązany jest do:

- analizy dokumentacji wejściowej Zamawiającego;
- uwzględnienia istniejących rozwiązań organizacyjnych i technicznych;
- dostosowania dokumentacji do struktury organizacyjnej Zamawiającego;
- uwzględnienia obowiązków wynikających z KRI, uKSC, RODO oraz wymagań wynikających z NIS2 jako punktu odniesienia dojrzałościowego i organizacyjnego;
- zapewnienia spójności pomiędzy dokumentacją SZBI, SZCD, ochroną danych osobowych, zarządzaniem incydentami i analizą ryzyka;
- przekazania dokumentów w formie umożliwiającej ich zatwierdzenie i wdrożenie przez Zamawiającego.

Zamawiający wymaga, aby dokumentacja uwzględniała zarówno wymagania systemowe, jak i specyfikę branży wodociągowo-kanalizacyjnej, w tym potrzebę zapewnienia ciągłości świadczenia usług publicznych, ochrony infrastruktury technicznej, bezpieczeństwa procesów technologicznych, bezpieczeństwa dostępu zdalnego, bezpieczeństwa dostawców oraz odporności na zakłócenia i incydenty mogące wpływać na funkcjonowanie przedsiębiorstwa. Sektor krytyczny i branżowy kontekst takiego podejścia są szeroko akcentowane w materiałach ENISA dotyczących cyberbezpieczeństwa sektorów krytycznych

Zamawiający dopuszcza możliwość realizacji usługi w formie zdalnej.

4. usługa przeprowadzenia szkolenia dla kadry kierowniczej z zakresu cyberbezpieczeństwa, w tym Systemu Zarządzania Bezpieczeństwem Informacji oraz Systemu Zarządzania Ciągłością Działania

Przedmiotem zamówienia jest realizacja szkolenia z zakresu cyberbezpieczeństwa przeznaczonego dla kadry zarządzającej, osób odpowiedzialnych za bezpieczeństwo informacji, cyberbezpieczeństwo, ciągłość działania, IT, OT/ICS oraz osób pełniących funkcje decyzyjne i nadzorcze u Zamawiającego.

Celem szkolenia jest zapewnienie właściwego zrozumienia, wdrożenia oraz nadzoru nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz Systemu Zarządzania Ciągłością Działania (SZCD), a także budowanie kompetencji w zakresie zarządzania bezpieczeństwem informacji i cyberbezpieczeństwem w kontekście działalności przedsiębiorstwa wodociągowo-kanalizacyjnego.

Szkolenie powinno uwzględniać specyfikę organizacji, w tym środowisk IT, OT/ICS/SCADA oraz znaczenie ciągłości działania procesów technologicznych.

Minimalny zakres szkolenia powinien obejmować co najmniej:

1. Wprowadzenie do SZBI i SZCD - omówienie roli systemów zarządzania bezpieczeństwem informacji i ciągłością działania w organizacji oraz ich znaczenia dla funkcjonowania przedsiębiorstwa wodociągowo-kanalizacyjnego.
2. Podstawy prawne i normatywne - przegląd wymagań wynikających z KRI, ustawy o krajowym systemie cyberbezpieczeństwa, RODO oraz odniesienie do wymagań NIS2 i norm ISO (27001, 27002, 27005, 22301).
3. Polityka bezpieczeństwa informacji i struktura dokumentacji SZBI - omówienie kluczowych dokumentów systemowych (PBI, PBT, PBF, procedury), ich roli, zakresu oraz zasad stosowania w organizacji.
4. System zarządzania ciągłością działania (SZCD) - zasady identyfikacji procesów krytycznych, planów ciągłości działania, procedur awaryjnych oraz roli kadry w zapewnieniu ciągłości funkcjonowania organizacji.
5. Zarządzanie ryzykiem - zasady identyfikacji, analizy i oceny ryzyka w obszarze bezpieczeństwa informacji, cyberbezpieczeństwa oraz ciągłości działania, w tym rola kierownictwa w procesie akceptacji ryzyka.
6. Role i odpowiedzialności w SZBI i SZCD - obowiązki kierownictwa, administratorów, użytkowników oraz osób odpowiedzialnych za IT, OT i bezpieczeństwo informacji.
7. Zarządzanie incydentami i naruszeniami - zasady zgłaszania, obsługi i nadzoru nad incydentami bezpieczeństwa informacji, cyberbezpieczeństwa oraz naruszeniami ochrony danych osobowych.
8. Bezpieczeństwo środowisk IT/OT/ICS w ujęciu zarządczym - kluczowe ryzyka dla infrastruktury technicznej, znaczenie separacji IT/OT, nadzoru nad dostępem oraz bezpieczeństwa usług zewnętrznych.
9. Nadzór nad dokumentacją i zgodnością - zasady przeglądów, audytów, monitorowania zgodności oraz ciągłego doskonalenia SZBI i SZCD.
10. Budowanie świadomości i kultury bezpieczeństwa - znaczenie szkoleń, komunikacji wewnętrznej oraz zaangażowania kadry zarządzającej w utrzymanie skutecznego systemu bezpieczeństwa.

Wymagania dotyczące realizacji szkolenia

Zamawiający wymaga, aby szkolenie:

- było bezpośrednio powiązane z opracowaną dokumentacją SZBI i SZCD u Zamawiającego;
- miało charakter praktyczny i odnosiło się do rzeczywistych procesów i ryzyk występujących w organizacji;
- uwzględniało przykłady sytuacji decyzyjnych, incydentów oraz odpowiedzialności kadry zarządzającej;
- wspierało wdrożenie i stosowanie dokumentacji systemowej w praktyce;
- zostało przeprowadzone w sposób umożliwiający aktywny udział uczestników (np. dyskusja, omówienie przypadków).

Szkolenie powinno stanowić integralny element wdrożenia SZBI i SZCD oraz wspierać Zamawiającego w osiągnięciu zgodności z wymaganiami KRI, uKSC oraz dobrymi praktykami wynikającymi z norm ISO i dyrektywy NIS2.

Zamawiający wymaga przeprowadzenia szkolenia w wymiarze nie krótszym niż **2 godziny zegarowe** dla jednej grupy uczestników (łączna ilość osób: minimum 10) .

Zamawiający wymaga, aby szkolenie zostało zrealizowane w formie stacjonarnej, zaś po ukończeniu szkolenia przez uczestników wymagane jest wydanie stosownych certyfikatów potwierdzających udział w szkoleniu.

CZĘŚĆ 2 Usługi szkoleniowe z zakresu cyberbezpieczeństwa

1. usługa przeprowadzenia szkolenia dla pracowników z zakresu cyberbezpieczeństwa budującego świadomość cyberzagrożeń i sposobów ochrony (2 szt.)

Zamawiający wymaga przeprowadzenia dwóch odrębnych szkoleń z zakresu cyberbezpieczeństwa, dostosowanych do specyfiki działalności przedsiębiorstwa wodociągowo-kanalizacyjnego, z uwzględnieniem środowisk IT, OT oraz ICS/SCADA**.**

Celem szkoleń jest podniesienie świadomości pracowników w zakresie cyberzagrożeń, sposobów ich rozpoznawania, zapobiegania incydentom oraz właściwego reagowania w przypadku wystąpienia zdarzeń mogących wpływać na bezpieczeństwo informacji, systemów teleinformatycznych oraz ciągłość świadczenia usług wodociągowo-kanalizacyjnych.

Szkolenie nr 1 – zakres dla pracowników IT

Zamawiający wymaga, aby podczas szkolenia poruszone zostały kluczowe aspekty cyberbezpieczeństwa w środowisku IT, w tym m.in.:

1. Wprowadzenie do cyberbezpieczeństwa – znaczenie cyberbezpieczeństwa w działalności przedsiębiorstwa wodociągowo-kanalizacyjnego oraz rola pracowników IT w utrzymaniu bezpieczeństwa informacji i systemów.
2. Podstawowe zasady cyberbezpieczeństwa – omówienie podstawowych reguł ochrony danych, systemów, kont użytkowników i zasobów informatycznych.
3. Phishing i inne ataki socjotechniczne – rozpoznawanie i ochrona przed próbami wyłudzenia informacji, fałszywymi wiadomościami, spoofingiem oraz oszustwami telefonicznymi.
4. Zagrożenia związane z ransomware i malware – identyfikacja zagrożeń, podstawowe mechanizmy działania oraz sposoby zapobiegania i reagowania.
5. Bezpieczna obsługa poczty elektronicznej – zasady korzystania z e-maila, rozpoznawanie podejrzanych wiadomości, załączników i linków.
6. Zarządzanie hasłami i autoryzacja – tworzenie silnych haseł, zasady bezpiecznego uwierzytelniania oraz znaczenie MFA.
7. Zarządzanie dostępem do systemów i informacji – nadawanie uprawnień, kontrola dostępu i ograniczanie nadmiernych uprawnień.
8. Kopie zapasowe i odtwarzanie danych – znaczenie backupu oraz podstawowe zasady ochrony danych przed utratą.
9. Zarządzanie podatnościami i aktualizacjami – znaczenie aktualizacji, poprawek bezpieczeństwa i ograniczania podatności systemów.
10. Reagowanie na incydenty bezpieczeństwa – procedury postępowania w przypadku incydentu, zgłaszanie zdarzeń oraz ograniczanie skutków incydentów.

Szkolenie nr 2 – zakres dla pracowników OT/ICS/SCADA

Zamawiający wymaga, aby podczas szkolenia poruszone zostały kluczowe aspekty cyberbezpieczeństwa w środowisku OT/ICS/SCADA, w tym m.in.:

1. Wprowadzenie do cyberbezpieczeństwa środowisk OT/ICS – znaczenie cyberbezpieczeństwa dla systemów sterowania, automatyki, telemetryki i ciągłości działania zakładu wod-kan.
2. Podstawowe zasady bezpieczeństwa w środowisku OT – omówienie reguł bezpiecznej pracy z systemami sterowania, urządzeniami terenowymi i infrastrukturą technologiczną.

3. Zagrożenia dla środowisk OT/ICS/SCADA – identyfikacja typowych zagrożeń, w tym nieautoryzowanego dostępu, błędów konfiguracji, infekcji oraz niekontrolowanych połączeń zdalnych.
4. Bezpieczny dostęp do systemów i urządzeń – zasady nadawania uprawnień, kontroli dostępu oraz ograniczania dostępu serwisowego.
5. Segmentacja środowisk IT i OT – znaczenie separacji sieci i ograniczania ryzyka przenikania zagrożeń pomiędzy środowiskami.
6. Bezpieczeństwo pracy serwisowej i utrzymaniowej – zasady bezpiecznego prowadzenia prac technicznych, zmian konfiguracyjnych i dostępu podmiotów zewnętrznych.
7. Bezpieczeństwo stacji operatorskich, systemów telemetrycznych i urządzeń terenowych – podstawowe zasady ochrony urządzeń i systemów przed nieuprawnionym dostępem i zakłóceniem pracy.
8. Kopie zapasowe i gotowość awaryjna – znaczenie kopii konfiguracji, odtwarzania systemów i przygotowania do pracy w warunkach zakłócenia.
9. Reagowanie na incydenty w środowisku OT – rozpoznawanie nieprawidłowości, zasady zgłaszania i współpracy z personelem IT oraz kierownictwem.
10. Znaczenie ciągłości działania – wpływ incydentów cyberbezpieczeństwa na ciągłość świadczenia usług wodociągowo-kanalizacyjnych i bezpieczeństwo procesów technologicznych.

Zamawiający wymaga, aby szkolenia zostały zaprojektowane w taki sposób, aby nie tylko podnosiły świadomość w zakresie cyberbezpieczeństwa, ale także rozwijały praktyczne umiejętności uczestników w rozpoznawaniu zagrożeń, ograniczaniu ryzyka oraz właściwym reagowaniu na incydenty. Zakres tematyczny szkoleń powinien być zgodny z wymogami projektu i stanowić integralną część działań służących podnoszeniu poziomu bezpieczeństwa informacji, cyberbezpieczeństwa oraz ciągłości działania u Zamawiającego.
Zamawiający informuje, że szkolenia powinny zostać przeprowadzone dla łącznej liczby uczestników wskazanej przez Zamawiającego wynoszącej ….. osób, z podziałem na dwie grupy szkoleniowe, po minimum 2 godziny zegarowe dla każdej z grup. Zamawiający wymaga, aby szkolenia zostały zorganizowane w formie stacjonarnej, zaś po ukończeniu szkolenia przez uczestników wymagane jest wydanie stosownych certyfikatów potwierdzających udział w szkoleniu.

CZĘŚĆ 3 Dostawa sprzętu IT

1. dostawa fizycznego serwera dla obszaru IT wraz z oprogramowaniem do wirtualizacji

Zamawiający wymaga dostawy serwera fizycznego do zainstalowania rozwiązań z zakresu bezpieczeństwa wraz z oprogramowaniem do wirtualizacji, spełniającego wszystkie poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Rack o wysokości max 1U • Min. 8 slotów na dyski 2.5” • Możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. • Obsługa procesorów 144 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 4TB pamięci RAM.
Procesor	• Zainstalowany jeden procesor min. 16-rdzeniowe, min. 2.3GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 199 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej.
Pamięć RAM	• 64 GB DDR5 RDIMM 6400MT/s
Kontroler RAID	• Sprzętowy kontroler dyskowy • Możliwość konfiguracji poziomów RAID: 0, 1, 10 (oraz tryb Non-RAID). • Wsparcie dla dysków samoszyfrujących • Obsługa dysków 12Gbps SAS3, 6Gbps SATA3/SAS2 oraz NVMe (Gen3 i Gen4)
Pamięć masowa	• Możliwość instalacji dysków SATA/SAS. • Zainstalowane 4 dyski SAS o pojemności min. 2.4 TB, 12Gbps, 2,5“ Hot-Plug.

Parametr	Charakterystyka (wymagania minimalne)
Gniazda rozszerzeń	• Minimum 2x slot PCIe x16 generacji 5. Dodatkowo min. 1 sloty w standardzie OCP 3.0 (x16) przeznaczone dla kart sieciowych.
Interfejsy sieciowe/FC/SAS	• 4 interfejsy sieciowe 10/25 GbE SFP28 (porty nie mogą być osiągnięte poprzez zainstalowanie karty w wymaganych slotach PCIe). • 1 przewód typu DAC , SFP+ to SFP+, 10GbE 3 m

Wbudowane porty	• 4 porty USB w tym min:
	  ○ 1 port USB 2.0 Type-C dostępne z przodu obudowy
	  ○ 2 porty USB 3.1 typ A dostępne z tyłu obudowy
	  ○ 1 port USB 3.0 dostępne wewnątrz obudowy
	• Port VGA z tyłu obudowy
	Nie dopuszcza się stosowania kart PCIe.

Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
Zasilanie	• Redundantne, Hot-Plug min. 800W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją

Parametr	Charakterystyka (wymagania minimalne)
	złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

Diagnostyka	• System powiadomień LED o funkcjonalności:
	  ○ Informacji o statusie zasilania serwera
	  ○ Pomocy w zlokalizowaniu serwera
	  ○ Informacji o błędach, powiązanej z logami systemowymi.

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez sześciu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych

Parametr	Charakterystyka (wymagania minimalne)
	• Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. • Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe Możliwość rozszerzenia funkcjonalności o: • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej • Automatyczne odświeżanie certyfikatów SSL • monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: Zainstalowane oprogramowanie producenta do zarządzania, spełniające poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji

Parametr	Charakterystyka (wymagania minimalne)
	• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera.

Parametr	Charakterystyka (wymagania minimalne)
	• Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczone jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego

Parametr	Charakterystyka (wymagania minimalne)
	▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania

Parametr	Charakterystyka (wymagania minimalne)
	○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki

Parametr	Charakterystyka (wymagania minimalne)

	sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)
	• Wirtualny asystent
	  ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;
	• Możliwość rozszerzenia funkcjonalności
	  ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
	• Inne
	Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android

System operacyjny/dodatkowe oprogramowanie	• Dostarczony system operacyjny przez wzgląd na kompatybilność z obecnie posiadaną infrastrukturą. • Licencja na Windows Server 2025 Standard, licencja pokrywająca wszystkie fizyczne rdzenie w serwerze, pozwalająca na uruchomienie oprogramowania na minimum 2 maszynach wirtualnych. Nośnik CD/DVD umożliwiający downgrade do wersji Windows Server 2022 Stadnard.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku.

Parametr	Charakterystyka (wymagania minimalne)
	• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
Dokumentacja	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie

Parametr	Charakterystyka (wymagania minimalne)
	konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

2. dostawa oprogramowania typu XDR dla obszaru IT oraz OT

Zamawiający wymaga dostawy oprogramowania typu XDR dla ochrony obszaru IT (ilość stacji roboczych: 20) oraz obszaru OT (ilość stacji roboczych: 5) spełniającego wszystkie poniższe wymagania. Wymaga się dostawy dla łącznej ilości 25 użytkowników na okres 12 miesięcy.

Centralne zarządzanie:

1. Rozwiązanie musi udostępniać konsolę centralnego zarządzania w wersji lokalnej (on-prem) oraz w wersji chmurowej, hostowanej bezpośrednio przez producenta rozwiązania. (SaaS).
2. Rozwiązanie musi udostępniać konsolę centralnego zarządzania przynajmniej w języku polskim i angielskim.
3. Rozwiązanie musi udostępniać możliwość zmiany języka bez przeinstalowania ani ponownego uruchamiania usług centralnego zarządzania.
4. Rozwiązanie musi udostępniać konsolę centralnego zarządzania zabezpieczoną za pośrednictwem protokołu szyfrowanego SSL/TLS.
5. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft ENTRA ID.

6. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft Active Directory.
7. Rozwiązanie musi udostępniać mechanizm wykrywający sklonowane maszyny na podstawie unikalnego identyfikatora sprzętowego stacji.
8. Rozwiązanie musi udostępniać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiająca co najmniej:
   - pośredniczenie w komunikacji pomiędzy zarządzanym urządzeniem, a serwerem centralnego zarządzania.
   - pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacji producenta.
   - buforowanie ruchu HTTPS.
9. Rozwiązanie musi udostępniać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
10. Rozwiązanie musi udostępniać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli centralnego zarządzania.
11. Rozwiązanie musi udostępniać uwierzytelnianie dwuskładnikowe co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
    - Google Authenticator;
    - Microsoft Authenticator;
    - Authy;
    - Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
12. Rozwiązanie musi udostępniać minimum 80 szablonów raportów, przygotowanych przez producenta, które mogą być dowolnie modyfikowane przez administratora.
13. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
14. 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 oraz ochrony;
    - wersja systemu operacyjnego;
    - podzespoły komputera.
15. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
    - wyrażenie CRON;
    - codziennie;
    - cotygodniowo;
    - co miesiąc;
    - co rok;
    - po wystąpieniu nowego zdarzenia;

- po automatycznym umieszczeniu hosta w grupie dynamicznej.

16. Rozwiązanie musi udostępniać możliwość tagowania obiektów.
17. Rozwiązanie musi udostępniać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.
18. Rozwiązanie musi udostępniać eksport danych w co najmniej następujących formatach:
    - JSON;
    - LEEF;
    - CEF.

Ochrona stacji roboczych – Windows:

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi udostępniać możliwość instalacji co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu:
    - Wirus.
    - Trojan.
    - Robak.
    - Adware.
    - Spyware.
    - Dialer.
    - Phishing.
    - Backdoor.
4. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi udostępniać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
    - technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych;
    - technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service);
    - technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
8. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi udostępniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:

- całego dysku;
- wybranych katalogów;
- pojedynczych plików;
- plików spakowanych oraz skompresowanych;
- dysków sieciowych;
- dysków przenośnych.

11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    - wybranych plików;
    - wybranych procesów;
    - wybranych lokalizacji;
    - wybranych rozszerzeń;
    - nazwy wykrycia;
    - sumy kontrolnej (SHA1).
12. Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology.
13. Rozwiązanie musi udostępniać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    - sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego;
    - konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników;
    - konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
14. Rozwiązanie musi udostępniać 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).
15. Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. Rozwiązanie musi udostępniać 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
17. Rozwiązanie musi udostępniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

    A. Typ urządzenia:
    - pamięci masowe;
    - optyczne pamięci masowe;
    - pamięci masowe Firewire;
    - urządzenia do tworzenia obrazów;

- drukarki USB;
- urządzenia Bluetooth;
- czytniki kart inteligentnych;
- modemy;
- porty LPT/COM;
- Uuządzenia przenośne.

B. Parametry urządzenia:

- numer seryjny.
- producent;
- model.

C. Typ dostępu:

- brak możliwości zapisu;
- pełen dostęp;
- ostrzeżenie użytkownika;
- brak dostępu.

18. Rozwiązanie musi udostępniać moduł HIPS, który musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - 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,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

    A. 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.

    B. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

    C. Raport musi posiadać co najmniej:

    - listę zainstalowanych aplikacji;
    - listę usług systemowych;

- informacje o systemie operacyjnym i sprzęcie;
- listę aktywnych procesów i połączeń sieciowych;
- harmonogram systemu operacyjnego;
- szczegóły pliku hosts;
- informacje o sterownikach.

20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:
    - antywirus;
    - zapora osobista;
    - sandbox;
    - antyspyware;
    - metody heurystyczne.
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.

A. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
B. Ochrona musi być realizowana w oparciu o co najmniej:
    - globalna czarna lista RBL,
    - czarna lista użytkownika,
    - biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.

23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
    A. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
        - Skanowanie portów TCP oraz UDP,
        - Wykrywanie duplikacji adresu IP,
        - Atak zatruwania ARP,
        - Nieprawidłowa długość pakietu TCP oraz UDP.

    B. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
        - RDP,
        - SMB,
        - My SQL,
        - MS SQL.

    C. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.

A. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.

B. Zapora osobista musi posiadać co najmniej cztery tryby pracy:

- tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
- tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
- tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.
    - Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
    - Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
    - W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.

26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.

A. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.

B. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:

- Treść komunikatu.
- Obraz.

Ochrona stacji roboczych – MacOS:

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
    - Wirus.
    - Trojan.
    - Robak.
    - Adware.
    - Spyware.

- Dialer.
- Phishing.
- Backdoor.

4. 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.
5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi chronić pliki co najmniej za pomocą:
   - sygnatur wirusów;
   - reputacji chmurowej.
7. Rozwiązanie musi umożliwiać 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).
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   - sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu;
   - konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników;
   - konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   - całego dysku;
   - wybranych katalogów;
   - pojedynczych plików;
   - plików spakowanych oraz skompresowanych;
   - dysków sieciowych;
   - dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    - wybranych plików,
    - wybranych procesów,
    - wybranych lokalizacji,
    - wybranych rozszerzeń,
    - nazwy wykrycia,
    - sumy kontrolnej (SHA1).

11. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.

A. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.

B. Zapora osobista musi posiadać co najmniej dwa tryby pracy:

- tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
- tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

Ochrona stacji roboczych - Linux

1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:
   - Ubuntu Desktop,
   - Red Hat Enterprise Linux,
   - Linux Mint.
2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:
   - Cinnamon.
   - GNOME.
   - KDE.
   - MATE.
   - XFCE.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   - Wirus.
   - Trojan.
   - Robak.
   - Adware.
   - Spyware.
   - Dialer.
   - Phishing.
   - Backdoor.
4. 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.
5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   - konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników;

- konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   - całego dysku;
   - wybranych katalogów;
   - pojedynczych plików;
   - plików spakowanych oraz skompresowanych;
   - dysków sieciowych;
   - dysków przenośnych.
8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   - wybranych plików;
   - wybranych procesów;
   - wybranych lokalizacji;
   - wybranych rozszerzeń.
9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

   A. Typ urządzenia:
   - pamięci masowe,
   - optyczne pamięci masowe,

   B. Parametry urządzenia:
   - numer seryjny,
   - producent,
   - model.

   C. Typ dostępu:
   - brak możliwości zapisu,
   - pełen dostęp,
   - brak dostępu.

Ochrona serwera - Windows Server

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze.
9. Rozwiązanie musi zapewniać skanowanie na żądanie.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania.
11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów w usłudze OneDrive.
12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów.
13. Rozwiązanie musi być wyposażone we wbudowaną funkcję generowania raportu.
14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej.
15. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w Hyper-V.
16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników.
18. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze.
19. Rozwiązanie musi posiadać wbudowany system IDS.
20. Rozwiązanie musi posiadać moduł zapory osobistej.
21. Zapora osobista musi działać w oparciu o reguły i posiadać co najmniej 60 wbudowanych reguł.

Ochrona serwera - Linux

1. Rozwiązanie musi wspierać systemy w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux.
2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń: Wirus, Trojan, Robak, Adware, Spyware, Dialer, Phishing, Backdoor.
3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne.
5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze.
8. Rozwiązanie musi zapewniać skanowanie na żądanie.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania.
10. Rozwiązanie musi pozwalać na uruchomienie lokalnej konsoli administracyjnej z poziomu przeglądarki.
11. Rozwiązanie musi w pełni wspierać rozwiązanie Dell EMC Isilon.
12. Rozwiązanie musi działać w architekturze mikro-serwisów.
13. Rozwiązanie musi wykrywać podejrzane działania w kontenerach i blokować je.

Mobile Device Management

1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
3. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli: usunięcie zawartości, przywrócenie do ustawień fabrycznych, zablokowanie, sygnał dźwiękowy, lokalizację GPS, resetowanie hasła.
4. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
5. MDM musi umożliwiać konfigurację dla iOS/iPadOS (e-mail, VPN, Wi-Fi, certyfikaty, tryb jednej aplikacji) oraz dla Android (blokady połączeń, Wi-Fi, VPN, aktualizacje, tapeta).

Mobile Threat Defense (MTD) dla systemu Android

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: Inteligentne i Dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania w trybie bezczynności.
4. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia (złożoność kodu blokady, przywrócenie do ustawień fabrycznych, czas ważności kodu).
5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę, pakiet, kategorię, uprawnienia, pochodzenie.
6. Rozwiązanie musi posiadać ochronę przed zagrożeniami typu phishing.

Sandbox w chmurze

1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego.
2. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi wspierać systemy: Windows 10/11, Windows Server, macOS 11+, RHEL, Rocky Linux, Ubuntu, Debian, SLES, Oracle Linux, Amazon Linux.
4. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
5. Rozwiązanie musi wykorzystywać chmurę producenta.
6. Rozwiązanie musi posiadać możliwość określenia plików do przesłania automatycznie.
7. Administrator musi mieć możliwość zdefiniowania czasu usunięcia przesłanych plików.
8. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru próbek.
9. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń.
10. Administrator musi mieć możliwość podejrzenia listy plików przesłanych do analizy.
11. Rozwiązanie musi pozwalać na analizowanie plików bez względu na lokalizację.
12. Rozwiązanie pozwala na wysłanie próbki do analizy przez użytkownika.

13. Przeanalizowane pliki muszą zostać oznaczone: czysty, podejrzany, bardzo podejrzany, szkodliwy.
14. Rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików.
15. Wykryte zagrożenia muszą być przeniesione do kwarantanny.

Szyfrowanie

1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.
3. Rozwiązanie musi wspierać systemy Windows 10/Windows 11.
4. Rozwiązanie musi umożliwiać zarządzanie szyfrowaniem FileVault w macOS.
5. Rozwiązanie musi posiadać autentykację typu pre-boot.
6. Administrator musi mieć możliwość wygenerowania hasła odzyskiwania.
7. Rozwiązanie musi umożliwiać szyfrowanie tylko na komputerach z UEFI.
8. Rozwiązanie musi umożliwiać logowanie SSO z Active Directory.
9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM 2.0.
10. Rozwiązanie musi wspierać dyski z funkcją OPAL 2.0.
11. Administrator musi mieć możliwość wygenerowania pliku odzyskiwania.
12. Rozwiązanie musi umożliwiać automatyczne wstrzymanie uwierzytelnienia przy aktualizacji systemu.

Endpoint Detection and Response / eXtended Detection and Response

1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Ochrona EDR / XDR musi być realizowana przy pomocy dedykowanego konektora.
3. Rozwiązanie musi zbierać informacje z systemu: tworzenie procesów, usługi, harmonogram, pliki, rejestr, biblioteki DLL, logowania, elementy sieciowe.
4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł alarmowych.
5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń.
6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.
7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych z podglądem szczegółów.
8. Rozwiązanie musi dawać możliwość wykonywania czynności dla plików wykonywalnych i DLL.
9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów.
10. Rozwiązanie musi umożliwiać sesję terminalową PowerShell.
11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji do tworzenia wykluczeń.
12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami (VirusTotal).
13. Rozwiązanie musi umożliwiać zaawansowane wyszukiwanie w XDR.

Wsparcie techniczne

1. Rozwiązanie musi udostępniać wsparcie techniczne w języku polskim przez cały okres trwania licencji.

Okres licencji

1. Zamawiający wymaga dostawy licencji na okres 12 miesięcy.

Szkolenie

Zamawiający wymaga jednocześnie, aby jeden z administratorów IT Zamawiającego został przeszkolony z zakresu obsługi oferowanego rozwiązania. Zamawiający dopuszcza szkolenie w formule online, jednak wymaga się, aby trwało ono nie mniej niż 10 h (rozdzielone na dwa dni szkoleniowe) i aby swoim zakresem obejmowało przynajmniej:

1. Konsola centralnego zarządzania
2. Ochrona stacji roboczych
3. Grupy statyczne i dynamiczne
4. Zadania klienta i serwera
5. Wdrażanie agentów
6. Zadania systemu operacyjnego
7. Polityki
8. Zestawy uprawnień
9. Zagrożenia i wykrywanie
10. Raportowanie

A ponadto w odniesieniu bezpośrednio do obszaru XDR:

1. Tworzenie i modyfikacja reguł
2. Tworzenie zaawansowanych wykluczeni
3. Analiza powłamaniowa.

3. Dostawa urządzeń NGFW wraz z oprogramowaniem dla obszaru IT

Zamawiający wymaga dostawy dwóch jednakowych urządzeń NGFW wraz z oprogramowaniem, spełniających wszystkie poniższe wymagania.

Dostarczane urządzenia muszą być fabrycznie nowe, wolne od wad fizycznych i prawnych systemu bezpieczeństwa sieciowego klasy NGFW (Next-Generation Firewall) / UTM (Unified Threat Management). Urządzenia mają zapewniać wysoki poziomu bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego, kompleksowej ochrony przed złośliwym oprogramowaniem i atakami sieciowymi, a także umożliwienie bezpiecznego dostępu zdalnego oraz efektywnego zarządzania ruchem sieciowym.

Wszystkie zaoferowane urządzenia, komponenty sprzętowe, oprogramowanie oraz subskrypcje/licencje muszą być fabrycznie nowe (nieużywane, nieregenerowane, nienaprawiane), pochodzić z oficjalnego i autoryzowanego kanału sprzedaży producenta oraz posiadać pełne wsparcie techniczne producenta świadczone na terytorium Rzeczypospolitej

Polskiej. Wykonawca jest zobowiązany do dostarczenia rozwiązania spełniającego wszystkie wymagania opisane w niniejszym dokumencie, przy czym przedstawione w poniższych sekcjach parametry techniczne, funkcjonalne i sprzętowe stanowią wymagania minimalne (obligatoryjne) Zamawiającego.

Opis wymagań dla pojedynczego urządzenia:

Obsługa sieci

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.

Zapora korporacyjna (firewall)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. 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.
5. 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.
6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

Intrusion prevention system (IPS)

1. 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.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. 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.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
7. 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.
8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
9. 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).
10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

Kształtowanie pasma (Traffic Shapping)

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

Ochrona antywirusowa

1. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub

wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.

2. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).
3. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź, gdy analiza skanerem antywirusowym została zakończona błędem.
4. Skaner antywirusowy ma pochodzić od europejskiego producenta.
5. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
6. 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.

Ochrona antyspam

1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyspam ma działać w oparciu o:

   a. białe/czarne listy,

   b. DNS RBL,

   c. Skaner heurystyczny.
3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

Wirtualne sieci prywatne (VPN)

1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:

   a. PPTP VPN,

   b. IPSec VPN,

   c. SSL VPN.
3. SSL VPN ma działać w trybie tunelu.
4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.

5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal).
6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

Filtr dostępu do stron WWW

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.
3. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.
4. Administrator ma mieć możliwość dodawania własnych kategorii URL.
5. 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.
6. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
7. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
8. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
9. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
10. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
11. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

Uwierzytelnianie

1. 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.

2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
3. 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.

4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
7. 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).
8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
9. 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.
10. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

Administracja łączami do Internetu (ISP)

1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

   a. równoważenie względem adresu źródłowego,

   b. równoważenie względem połączenia.

3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).

5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

Routing (trasowanie)

1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
5. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

Administracja urządzeniem

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. 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.
6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH).
7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.

10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
17. 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.
18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

Raportowanie

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.

7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

Pozostałe usługi i funkcje

1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
3. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
5. 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).
6. Urządzenie ma posiadać usługę DNS Proxy.
7. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
9. Urządzenie musi mieć zaimplementowane Open API.
10. 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.

Gwarancja i serwis

1. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

Parametry sprzętowe

1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.

3. Liczba portów Ethernet 2,5Gbps – min. 8.
4. Liczba portów światłowodowych 1Gbps – min. 1.
5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
6. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps.
7. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps.
8. Przepustowość filtrowania Antywirusowego – minimum 1Gbps.
9. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps.
10. Liczba tuneli VPN IPSec – minimum 100.
11. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100.
12. Obsługa interfejsów 802.11q (VLAN) – minimum 128.
13. Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę.
14. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
15. Urządzenie nie ma limitu na liczbę użytkowników.
16. Liczba reguł filtrowania – minimum 8 192.
17. Liczba tras statycznego routingu – minimum 512.
18. Liczba tras dynamicznego routingu – minimum 10 000.
19. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
20. Urządzenie musi być wyposażone w moduł TPM.

Szkolenie:

Zamawiający wymaga jednocześnie, aby jeden z administratorów IT Zamawiającego został przeszkolony z zakresu obsługi oferowanego rozwiązania. Zamawiający dopuszcza szkolenie w formule online, jednak wymaga się, aby trwało ono nie mniej niż 15 h (rozdzielone na trzy dni) i aby swoim zakresem obejmowało przynajmniej:

1. Podstawowe informacje o urządzeniach
2. Zbieranie logów i monitorowanie
3. Obiekty, typy i ich wykorzystanie
4. Konfiguracja sieci
5. Translacja adresów sieciowych
6. Translacja połączeń wychodzących i przychodzących
7. Translacja dwukierunkowa
8. Filtrowanie ruchu sieciowego
9. Ochrona aplikacji

10. Użytkownicy i uwierzytelnianie
11. Konfiguracja usługi katalogowej
12. VPN jako wirtualne sieci prywatne
13. SSL VPN

4. Dostawa urządzeń UTM wraz z oprogramowaniem dla obszaru OT

Zamawiający wymaga dostawy urządzenia klasy minimum UTM wraz z oprogramowaniem, spełniających wszystkie poniższe wymagania.

Dostarczane urządzenie muszą być fabrycznie nowe, wolne od wad fizycznych i prawnych systemu bezpieczeństwa sieciowego klasy minimum UTM (Unified Threat Management). Urządzenie ma zapewniać wysoki poziomu bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego, kompleksową ochronę przed złośliwym oprogramowaniem i atakami sieciowymi, a także umożliwiać bezpieczny dostęp zdalny oraz efektywne zarządzanie ruchem sieciowym.

Obsługa sieci

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.

Zapora korporacyjna (firewall)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. 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.
5. 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.
6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

Intrusion prevention system (ips)

1. 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.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. 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.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
7. 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.
8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
9. 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).
10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

Kształtowanie pasma (Traffic Shapping)

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

Wirtualne sieci prywatne (VPN)

1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:

   a. IPSec VPN,

   b. SSL VPN.

3. SSL VPN ma działać w trybie tunelu.
4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.

5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
7. W ramach licencji dostępny jest klient SSLVPN pod systemy: Windows, Linux, macOS objęty gwarancją i wsparciem równolegle ze wsparciem dla rozwiązania UTM.
8. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
9. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
10. Rozwiązanie ma umożliwiać wykorzystanie algorytmów post-kwantowej kryptografii w szyfrowaniu IPSec w standardzie ML-KEM.

Uwierzytelnianie

1. 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.

   d. Microsoft Entra ID, opartej na protokole OpenID Connect.

2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
3. 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.

4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
7. 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).
8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
9. 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.
10. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

Administracja łączami do internetu (ISP)

1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

   a. równoważenie względem adresu źródłowego,

   b. równoważenie względem połączenia.

3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
5. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

Administracja urządzeniem

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. 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.
6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH).
7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.

10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
17. 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

18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

Raportowanie

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
4. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
5. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
6. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
7. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 2 i 3.
8. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

Pozostałe usługi i funkcje

1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.

2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
3. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
5. 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).
6. Urządzenie ma posiadać usługę DNS Proxy.
7. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
9. Urządzenie musi mieć możliwość wykorzystania REST API.
10. 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.

Gwarancja i serwis

1. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

Parametry sprzętowe

1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
2. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
3. Liczba portów Ethernet 10/100/1000Mbps – min. 2, z możliwością rozszerzenia do 4.
4. Urządzenie ma pozwalać na dodanie min. 2 portów światłowodowych 1Gbps.
5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
6. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
7. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2.6Gbps.
8. Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 0,8 Gbps.
9. Liczba tuneli VPN IPSec – minimum 200.
10. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
11. Obsługa interfejsów 802.11q (VLAN) – minimum 393.
12. Liczba równoczesnych sesji – minimum 500 000 i nie mniej niż 20 000 nowych sesji/sekundę.
13. Liczba reguł filtrowania – minimum 8 192.
14. Liczba tras statycznego routingu – minimum 2 048.
15. Liczba tras dynamicznego routingu – minimum 10 000.
16. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
17. Urządzenie musi być wyposażone w moduł TPM.
18. Urządzenie ma posiadać pasywny system chłodzenia.
19. Urządzenie ma posiadać redundantne zasilanie DC, 2x12-48VDC.
20. Urządzenie ma być przystosowane do pracy w temperaturach od -40oC do +70oC przy wilgotności od 0% do 95% (bez kondensacji).
21. Obudowa urządzenia ma zapewniać ochronę wg. kodów IP – IP30.

22. Urządzenie ma pozwalać na aktywowanie funkcjonalności tzw. hardware bypass, tj. zapewnienie ciągłości transmisji pomiędzy dwoma dedykowanymi interfejsami Ethernet pomimo awarii sprzętowej lub programowej urządzenia.
23. Średni czas bezawaryjnej pracy (MTBF) w temperaturze 25 °C ma być nie mniejszy niż 35 lat.
24. Urządzenie nie ma limitu na liczbę użytkowników.
25. Urządzenie ma umożliwiać bezpośredni montaż na szynie typu DIN (35mm).

5. dostawa oprogramowania do monitorowania infrastruktury informatycznej dla obszaru IT oraz OT

Zamawiający wymaga dostawy centralnego systemu zarządzania spełniającego wszystkie poniższe wymagania ogólne.

Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.
Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.
Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
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.
Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.
Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
Oprogramowanie musi współpracować z serwerem MSSQL Server od wersji 2017
Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych.
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.
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).
Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
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).
Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).
Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
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.
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.
Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
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).
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.
Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.
Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

Wymagania w zakresie inwentaryzacji komputerów

Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.

Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
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
Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.
Oprogramowanie musi umożliwiać analizę sprzętową: - płyty głównej w zakresie model, producent, nr. seryjny, - CPU w zakresie nazwy, modelu, producenta, częstotliwości, - HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci, - RAM w zakresie wielkości pamięci, - karty sieciowej w zakresie model, adres IP, adres MAC, - karty graficznej w zakresie model.
Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.
Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
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)
Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB
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)
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).

Wymagania w zakresie inwentaryzacji oprogramowania

Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.

Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.

Zdalny pulpit, zdalne zarządzanie komputerem

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).
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.
Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
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).
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.
Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.

Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Monitoring komputerów

Oprogramowanie umożliwia zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
Oprogramowanie umożliwia analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
Oprogramowanie umożliwia analizę efektywności pracy użytkowników na poszczególnych aplikacjach
Oprogramowanie umożliwia 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).
Oprogramowanie umożliwia tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
Oprogramowanie umożliwia podział stron na dozwolone i zabronione.
Oprogramowanie umożliwia wydruki tabelaryczne oraz graficzne (wykresy aktywności).
Oprogramowanie umożliwia okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
Oprogramowanie umożliwia rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
Oprogramowanie umożliwia odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.
Oprogramowanie umożliwia analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).
Oprogramowanie umożliwia monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
Oprogramowanie umożliwia monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków odbywa się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.
Oprogramowanie po zainstalowaniu przesyła 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.

Backup danych użytkownika

Oprogramowanie umożliwia tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
Oprogramowanie umożliwia globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
Oprogramowanie umożliwia definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.
Oprogramowanie Agenta umożliwia kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
Mechanizm archiwizacji danych realizowany jest przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)

Oprogramowanie umożliwia definiowanie cyklu archiwizacji.
Oprogramowanie umożliwia automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.

Automatyzacja

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.
Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
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.
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.
Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).
Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
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.
Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.
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.
Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.
Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis: 1. 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) 2. 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)

3. 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 4. 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. 5. Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego. W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.
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.)
Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji
Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika
Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)
Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)
Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)
Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)
Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.

System wewnętrznego komunikatora dla użytkowników

Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.
Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej.
Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami
Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania.
Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia.
Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora).
Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej.

Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej).
Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami.
Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych.
Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video).
Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami
Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych.

Zamawiający określa również wymagania dla oprogramowania w zakresie zarządzania procesami i usługami.

ServiceDesk – Zarządzanie zgłoszeniami

Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności: • Zarządzanie problemem • Zarządzanie incydentem • Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy) • Zarządzanie umowami serwisowymi • Definicje poziomów SLA (reakcja, naprawa)
Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.
Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW
Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).
Obsługa listy zgłoszeń serwisowych musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.
Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.
Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.
Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmu SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.
Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.
Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.
Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.
Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.

Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.
Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.
Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.
Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.
Oprogramowanie musi umożliwiać tworzenie szablonów zadań.
Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.
Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.
Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.
Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.
Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.
Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.
Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.
Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.
Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu (wraz z grafiką) oraz wstawiania załączników.
Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja o awarii komputera).
Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).
Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.
Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.
Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.
Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.
Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia (w komentarzach) korespondencji

mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.
Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń)
Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).
Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.
Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)
Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia: • Zmiana statusu po przejęciu zgłoszenia przez opiekuna. • Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna. • Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia. • Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika. • Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika. • Zamykanie zgłoszenia po upływie czasu reklamacji. • Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów. • Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza. • Walidacja zamkniętych zadań w zamykanym zgłoszeniu. • Systemowe potwierdzanie realizacji zgłoszenia. • Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.
Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.
Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.
Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.
Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).
Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika
Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia
Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń)
Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji (dymku) podczas pracy z systemem
Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB
Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku)
Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia

Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia
Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja)
Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu
Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą
Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności
Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu
Oprogramowanie musi umożliwiać definiowanie reguł biznesowych za pomocą graficznego/blokowego kreatora.
Oprogramowanie musi umożliwiać definiowanie obiegów za pomocą graficznego/blokowego kreatora.
Oprogramowanie musi umożliwiać tworzenie niestandardowych raportów za pomocą kreatora.
Oprogramowanie musi umożliwiać definiowanie poziomu dostępu do zgłoszeń dla dynamicznych grup użytkowników.
Oprogramowanie musi umożliwiać definiowanie formularzy dla zgłoszeń w danej kategorii za pomocą kreatora Drag&Drop z możliwością określenia układu kolumn.
Oprogramowanie musi umożliwiać tworzenie dowolnej liczby Dashboard-ów dla użytkownika za pomocą kreatora Drag&Drop.
Oprogramowanie musi umożliwiać zmianę układu szczegółów zgłoszenia za pomocą kreatora Drag&Drop.
Oprogramowanie musi umożliwiać udostępniania ogłoszeń w formie Widget-u oraz okienka modalnego z wymaganym potwierdzeniem dla użytkownika.
Oprogramowanie musi umożliwiać zaprojektowanie dowolnego szablonu protokołu zgłoszenia.
Oprogramowanie musi udostępniać matrycę(wpływ/pilność) dla obliczania priorytetu zgłoszeń.
Oprogramowanie musi umożliwiać zmianę koloru dla statusu/priorytetu/wpływu/pilności zgłoszenia prezentowanego na liście zgłoszeń.
Oprogramowanie musi umożliwiać definiowanie dowolnych kolejek zgłoszeń.
Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa.
Oprogramowanie musi umożliwiać wybór trybu ciemnego(nocnego)
Oprogramowanie musi umożliwiać obsługę zgłoszeń w widoku Kanban z możliwością jego konfiguracji w zakresie grupowania, sortowania oraz nakładania filtrów w logice AND/OR

ServiceDesk – Zarządzanie wnioskami

Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych).
Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika.
Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu.

ServiceDesk – Zarządzanie uprawnieniami

Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych
Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych
Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych)
Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych
Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek
Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych
Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu)
Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku
Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika)
Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób
Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych
Oprogramowanie w zakresie modułu ServicDesk musi umożliwiać integracje z systemami trzecimi poprzez REST API
Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika

ServiceDesk – zarządzanie rezerwacjami

Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie.
Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji.
Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika.
Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem.
Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza.
Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników.

ServiceDesk – automatyzacja operacji za pomocą sztucznej inteligencji

Oprogramowanie dla realizacji wymagań związanych z automatyzacją z wykorzystaniem sztucznej inteligencji musi umożliwiać integrację z usługą OpenAI (ChatGPT) za pomocą indywidualnego klucza API
Oprogramowanie musi umożliwiać automatyczne sugerowanie rozwiązań użytkownikom na etapie rejestracji nowego zgłoszenia. Potencjalna odpowiedź sztucznej inteligencji musi bazować na analizie treści zgłoszenia, kategorii oraz historii wszystkich wewnętrznych rozwiązanych zgłoszeń.

Oprogramowanie musi umożliwiać wzbogacanie odpowiedzi inżynierów o sugerowane rozwiązania sztucznej inteligencji oparte na opisie zgłoszenia.
Oprogramowanie musi umożliwiać automatyczne tworzenie artykułów w bazie wiedzy przez generator treści AI na podstawie historii rozwiązanych zgłoszeń.
Oprogramowanie musi umożliwiać tworzenie automatycznych podsumowań tematyki wybranego zgłoszenia bazując na analizie historii komentarzy oraz przedstawiać najbardziej prawdopodobne rozwiązanie problemu.
Oprogramowanie musi umożliwiać automatyczne tworzenie okresowych podsumowań opisujących aktualny stan techniczny i kondycję krytycznych elementów zarządzanej infrastruktury IT.
Oprogramowanie musi umożliwiać automatyczne generowanie sugestii dotyczących zalecanych działań mogących korzystnie wpłynąć na stabilność i bezpieczeństwo infrastruktury IT.

CMDB

Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI)
Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe
Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI
Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny
Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI
Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji
Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej (grid z możliwością jego modyfikacji w zakresie widoczności kolumn, ich szerokości oraz kolejności) oraz graficznej (wizualizacja sieci połączeń między elementami CI, z możliwością rozwijania widoku o dalsze poziomy relacji poszczególnych obiektów. Manualnie stworzony widok musi umożliwiać zapamiętanie pozycji elementów oraz widoczności poszczególnych jego elementów)
Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji
Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy elementami bazy CMDB w tym m.in. usługami, sprzętem, organizacją oraz pracownikami
Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji
Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV)
Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji
Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji wg posiadanych atrybutów
Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowe i odwrotnej
Oprogramowanie w zakresie modułu CMDB musi umożliwiać integracje z systemami trzecimi poprzez REST API
Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji

Zarządzanie zasobami oraz użytkownikami

Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.
Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.
Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania komputera z pracownikiem, licencją, dowolnym innym zasobem) wraz z zapisem historii relacji zasobów.
Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.
Oprogramowanie musi umożliwiać zdefiniowanie dowolnego typu zasobu inwentaryzacyjnego (np. telefon, drukarka, komputer) w strukturze drzewiastej wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów oraz bieżący podgląd atrybutów poszczególnego zasobu po jego zeskanowaniu
Oprogramowanie musi umożliwiać import danych z pliku CSV zawierającego dowolne informacje inwentaryzacyjne z wprowadzanych do systemu urządzeń w zakresie m.in.: numer faktury, numer seryjny, model, nazwa, data zakupu.
Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.
Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu
Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF
Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków
Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji
Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu
Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu
Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu
Oprogramowanie musi umożliwiać pogląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu
Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego
Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu
Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami
Oprogramowanie musi umożliwiać seryjne dodawanie zasobów
Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów
Oprogramowanie musi udostępniać kreator raportów dla zasobów
Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów) zasobu z innego typ zasobu

Oprogramowanie musi udostępniać możliwość kopiowania formularz dla określonego typu(ów) zasobu z innego typ zasobu
Oprogramowanie musi umożliwiać ewidencję magazynów
Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych
Oprogramowanie musi umożliwiać ewidencję produktów magazynowych
Oprogramowanie musi udostępniać informację o stanie magazynowym(ilościowo)
Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM
Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn
Oprogramowanie musi umożliwiać wydawanie zasobów ewidencjonowanych i eksploatacyjnych z magazynu
Oprogramowanie musi umożliwiać zwrot zasobów na magazyn
Oprogramowanie musi umożliwiać zmianę szablonów dokumentów PZ/PW/RW/MM
Oprogramowanie musi umożliwiać wyszukiwanie dokumentów po dowolnym atrybucie
Oprogramowanie musi umożliwiać zarządzanie organizacjami/typami organizacji (np. klient, podwykonawca)
Oprogramowanie musi umożliwiać dowolne przypisanie osoby do organizacji
Oprogramowanie musi umożliwiać tworzenia dynamicznych grup użytkowników
Oprogramowanie musi umożliwiać zarządzanie kontaktami osób/organizacji
Oprogramowanie musi umożliwiać zarządzanie nieobecnościami użytkowników
Oprogramowanie musi umożliwiać zarzadzanie uprawnieniami i poziomami dostępu do danych w zakresie zarządzania zasobami
Oprogramowanie w zakresie modułu Zasobów musi umożliwiać integracje z systemami trzecimi poprzez REST API
Oprogramowanie musi umożliwiać automatyczne pobieranie danych rejestrowych kontrahentów z bazy GUS

Zarządzanie dokumentami

Oprogramowanie musi umożliwiać centralną ewidencję dokumentów
Oprogramowanie musi umożliwiać zawierać dedykowany formularz dodawania nowego dokumentu z możliwością edycji widocznych oraz wymaganych atrybutów dokumentu
Oprogramowanie musi umożliwiać dołączenie skanu dokumentu (m.in.: skany faktur, umów)
Oprogramowanie musi umożliwiać stworzenie dedykowanego zbioru ról i uprawnień w zakresie obsługi rejestru dokumentów
Oprogramowanie musi umożliwiać utworzenie pomocniczych rejestrów oraz słowników
Oprogramowanie musi umożliwiać przeszukiwanie bazy dokumentów oraz kontrahentów po dowolnie wskazanym atrybucie opisującym
Oprogramowanie musi umożliwiać utworzenie rejestru osób reprezentujących
Oprogramowanie musi umożliwiać analizę zmian wartości dowolnych atrybutów opisujących dokument w zakresie daty zmiany, aktualnej/poprzedniej wartości oraz osoby dokonującej zmiany

Wymagania formalne wraz z usługą szkolenia

W okresie 12 miesięcy od wdrożenia wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.
Obsługa serwisowa musi być realizowana przez Producenta oprogramowania, w dni robocze w godzinach 8-16 w języku polskim, zgodnie z poniższymi parametrami:

Typ zgłoszenia	Opis	Czas Reakcji (godziny robocze)	Czas Realizacji (godziny robocze)
Błąd Krytyczny	Nieprawidłowości, która uniemożliwia dalsze korzystanie z Systemu - awaria	2h	8h
Usterka Ważna	Nieprawidłowości utrudniającej korzystanie z Systemu, ale w stopniu umożliwiającym dalsze korzystanie	8h	40h
Usterka	Nieprawidłowości utrudniająca korzystanie z Systemu, ale w stopniu umożliwiającym i nieutrudniającym w sposób znaczny dalsze korzystanie	24h	144h

Dostarczone licencje na oprogramowanie muszą objąć co najmniej 25 stanowisk komputerowych z systemem klasy Microsoft Windows oraz 10 urządzeń mobilnych z system Android. Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 2 licencje dostępowych do konsoli zarządzającej.

Zamawiający wymaga od wykonawcy, aby w terminie 5 dni od zakończenia prac wdrożeniowych przeprowadził szkolenie administracyjne z obsługi systemu (wymagane co najmniej 2 sesje szkoleniowe po 4 godziny każda)

Zamawiający wymaga, aby producent oferowanego oprogramowania przedstawił ważny certyfikat potwierdzający, że proces wytwarzania oprogramowania odbywa się zgodnie z międzynarodową normą ISO/IEC 27001. W celu potwierdzenia zgodności, do oferty należy dołączyć kopię certyfikatu ISO/IEC 27001.

Zamawiający wymaga, aby oferowane oprogramowanie w zakresie:

- Zarządzanie incydentami (Incident Management),
- Zarządzanie problemami (Problem Management),
- Zarządzanie bazą wiedzy (Knowledge Management),
- Zarządzanie zasobami (Asset Management).

posiadało aktualny certyfikat zgodności z najlepszymi praktykami IT Service Management, wydany przez niezależną organizację certyfikującą (np. Pink Elephant). Do oferty należy dołączyć kopię stosownego certyfikatu oraz wskazać link do strony internetowej organizacji certyfikującej, na której potwierdzona jest zgodność oferowanego rozwiązania z ww. procesami ITSM.

Ponadto, Zamawiający informuje, że w przypadku wątpliwości, co do zgodności zaoferowanego rozwiązania z wymogami, 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.

6. dostawa oprogramowania SIEM dla obszaru IT oraz OT

Zamawiający wymaga dostawy centralnego systemu zbierania logów, analizy zdarzeń bezpieczeństwa spełniającego poniższe wymagania.

Wymagania dla funkcjonalności SIEM:

System musi zapewniać funkcjonalność co najmniej w zakresie:

1. Centralne gromadzenie, analizę i korelację logów z różnych źródeł, umożliwiając monitorowanie zdarzeń bezpieczeństwa całej infrastruktury informatycznej.
2. Wykrywanie zagrożeń i incydentów bezpieczeństwa (np. ataków, prób nieautoryzowanego dostępu, podatności w używanych bibliotekach etc)
3. Monitorowanie integralności plików i konfiguracji (w tym wybranych wpisów rejestru na systemach windowsowych)
4. Pracę agentową i bezagentową (np zbieranie przez syslog dla urządzeń sieciowych i innych systemów bez możliwości instalacji agenta).
5. Generowanie powiadomień email, komunikatory, webhook.
6. Brak ograniczeń licencyjnych per wolumen logów.
7. Logowanie przez AD/LDAP/SAML/Kerberos.

Wymagania w zakresie monitorowania:

System musi umożliwiać ciągłe monitorowania zasobów informatycznych, w tym serwerów, stacji roboczych, urządzeń sieciowych, aplikacji, a także środowisk wirtualnych.
System musi zapewniać funkcjonalność co najmniej w zakresie:

1. Monitoring agentowy i bezagentowy (SNMP / IPMI).
2. Monitorowanie wydajności i dostępności zasobów. Elastyczny mechanizm definiowania parametrów monitorowanych oraz sposobu powiadamiania administratorów o wykrytych nieprawidłowościach, takich jak przekroczenie progów wydajnościowych, awarie usług czy niedostępność komponentów.
3. Tworzenie dashboardów i raportów. Tworzenie zaawansowanych pulpitów użytkownika i automatyczne eskalacje zgłoszeń.
4. Integracja z innymi narzędziami, np. do zarządzania zdarzeniami lub automatyzacji procesów utrzymania infrastruktury IT.
5. Logowanie za pomocą AD/LDAP/SAML/Kerberos.

Wymagania w zakresie platformy logów:

Platforma ma zapewnić centralne zbieranie logów z różnych źródeł (serwery, urządzenia sieciowe, aplikacje), oferując mechanizmy indeksowania, wyszukiwania oraz korelacji danych zdarzeniowych.
System musi zapewniać funkcjonalność co najmniej w zakresie:

1. Centralny odbiór logów (agent / syslog / Beats).
2. Indeksowanie i zaawansowane wyszukiwanie.
3. Tworzenie dashboardów i raportów.
4. Korelacje i wykrywanie anomalii.
5. Skalowalność klastra.
6. Retencja logów. Konfiguracja musi zagwarantować przechowywanie logów minimum 12 miesięcy. Po tym okresie automatyczne archiwizowanie i szyfrowanie.
7. Integracje i dostęp
    - Dostęp przez Service Accounts i SSO (AD/LDAP/SAML/Kerberos).
    - Integracje: AD, EDR
    - Powiadomienia: email, Teams / Slack / Telegram przez webhook.

Zamawiający wymaga, aby system i jego wszystkie składowe uruchomiony był w środowisku wirtualnym Zamawiającego.

Zamawiający preferuje rozwiązania open-source, bez ograniczeń licencyjnych dotyczących liczby źródeł logów, agentów oraz monitorowanych hostów, zaś w przypadku zastosowania rozwiązań komercyjnych – ilość stacji roboczych objętych systemem wynosi 25 - ilość serwerów objętych systemem wynosi 4.

7. dostawa oprogramowania SOAR dla obszaru IT oraz OT

Zamawiający wymaga dostawy rozwiązania typu SOAR dla obszaru IT oraz OT, które stanowić ma system logowania i raportowania dla dostarczanych w ramach niniejszego postępowania rozwiązań NGFW i UTM. Łączna ilość urządzeń – 3 szt. Wymaga się, aby rozwiązanie SOAR spełniało wszystkie poniższe wymagania.

Wymagania ogólne:

1. W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
2. Rozwiązanie musi zostać dostarczone w postaci maszyny wirtualnej instalowanej w środowisku Vmware lub Windows Hyper-V.
3. Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
4. Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.
5. Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.
6. Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.
7. Rozwiązanie musi posiadać predefiniowane panele dla informacji z urządzeń pracujących w sieci OT.

Zarządzanie Logami:

1. Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.
2. Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.
3. Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).
4. Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.

Rodzaje wyszukiwania

1. Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.
2. Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).
3. Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.
4. Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).

5. Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów).
6. Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.

Raportowanie

1. Rozwiązanie musi umożliwiać tworzenie statycznych raportów.
2. Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.
3. Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.
4. Rozwiązanie musi umożliwiać tworzenie własnych raportów.
5. Rozwiązanie musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) z funkcjonalnością „drill-down”.

Zarządzanie incydentami

1. Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.
2. Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.

Wymagania systemowe

1. Liczba zdarzeń na sekundę (EPS): min. 10 000
2. Zarządzanie logami: min 1 rok
3. Liczba obsługiwanych urządzeń min. 500
4. Liczba zapisu zdarzeń na dobę: min 13000 MB
5. System logów musi wspierać hiperwizory: Vmware ESXi oraz Microsoft HyperV

5. dostawa serwera fizycznego do wykonywania kopii zapasowych dla obszaru IT oraz OT

Zamawiający wymaga dostawy serwera fizycznego do wykonywania kopii zapasowych, spełniającego wszystkie poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Rack o wysokości max 1U • Min. 8 slotów na dyski 2.5” • Możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora.

Parametr	Charakterystyka (wymagania minimalne)
	• Obsługa procesorów 144 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 4TB pamięci RAM.
Procesor	• Zainstalowany jeden procesor min. 12-rdzeniowe, min. 2.2GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 145 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej.
Pamięć RAM	• 64 GB DDR5 RDIMM 6400MT/s
Kontroler RAID	• Sprzętowy kontroler dyskowy • Możliwość konfiguracji poziomów RAID: 0, 1, 10 (oraz tryb Non-RAID). • Wsparcie dla dysków samoszyfrujących • Obsługa dysków 12Gbps SAS3, 6Gbps SATA3/SAS2 oraz NVMe (Gen3 i Gen4)
Pamięć masowa	• Możliwość instalacji dysków SATA/SAS. • Zainstalowane 4 dyski SAS o pojemności min. 2.4 TB, 12Gbps, 2,5“ Hot-Plug.
Gniazda rozszerzeń	• Minimum 2x slot PCIe x16 generacji 5. Dodatkowo min. 1 sloty w standardzie OCP 3.0 (x16) przeznaczone dla kart sieciowych.
Interfejsy sieciowe/FC/SAS	• 4 interfejsy sieciowe 10/25 GbE SFP28 (porty nie mogą być osiągnięte poprzez zainstalowanie karty w wymaganych slotach PCIe). • 1 przewód typu DAC , SFP+ to SFP+, 10GbE 3 m

Wbudowane porty	• 4 porty USB w tym min:
	  ○ 1 port USB 2.0 Type-C dostępne z przodu obudowy
	  ○ 2 porty USB 3.1 typ A dostępne z tyłu obudowy
	  ○ 1 port USB 3.0 dostępne wewnątrz obudowy
	• Port VGA z tyłu obudowy
	Nie dopuszcza się stosowania kart PCIe.

Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
Zasilanie	• Redundantne, Hot-Plug min. 800W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych

Parametr	Charakterystyka (wymagania minimalne)
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

Diagnostyka	• System powiadomień LED o funkcjonalności:
	  ○ Informacji o statusie zasilania serwera
	  ○ Pomocy w zlokalizowaniu serwera
	  ○ Informacji o błędach, powiązanej z logami systemowymi.

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH

Parametr	Charakterystyka (wymagania minimalne)
	• możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez sześciu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. • Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe Możliwość rozszerzenia funkcjonalności o: • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej • Automatyczne odświeżanie certyfikatów SSL

Parametr	Charakterystyka (wymagania minimalne)
	• monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: Zainstalowane oprogramowanie producenta do zarządzania, spełniające poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)

Parametr	Charakterystyka (wymagania minimalne)
	• Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczone jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:
	• Monitoring:
	  ○ ilość podłączonych oraz rozłączonych systemów
	  ○ stan podłączonych urządzeń
	  ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów
	  ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
	  ○ informacje o statusie gwarancji dla poszczególnych urządzeń
	  ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń

Parametr	Charakterystyka (wymagania minimalne)
	○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.

Parametr	Charakterystyka (wymagania minimalne)
	▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO,

Parametr	Charakterystyka (wymagania minimalne)
	○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android

Parametr	Charakterystyka (wymagania minimalne)
System operacyjny/dodatkowe oprogramowanie	• Dostarczony system operacyjny przez wzgląd na kompatybilność z obecnie posiadaną infrastrukturą. • Licencja na Windows Server 2025 Standard, licencja pokrywająca wszystkie fizyczne rdzenie w serwerze, pozwalająca na uruchomienie oprogramowania na minimum 2 maszynach wirtualnych. • Nośnik CD/DVD umożliwiający downgrade do wersji Windows Server 2022 Stadnard. • 25x Windows Server 2025/2022 User CALs
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
Dokumentacja	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.

Parametr	Charakterystyka (wymagania minimalne)

	• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
	• Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.
	• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
	• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
	• Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
	  ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
	  ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
	  ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
	  ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
	  ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część,

Parametr	Charakterystyka (wymagania minimalne)
	znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

6. dostawa oprogramowania do wykonywania kopii zapasowych dla obszaru IT oraz OT

Zamawiający wymaga dostarczenia licencji na oprogramowanie do tworzenia kopii zapasowych w modelu wieczystym (perpetual) Wymaga się ponadto świadczenia usługi wsparcia technicznego producenta na okres 12 miesięcy.

Zamawiający wymaga, aby oprogramowanie obejmowało rozmiar środowiska podlegającego ochronie - obecne środowisko informatyczne, składające się z następujących elementów:

- 7 maszyn wirtualnych uruchomionych na platformie [np. VMware vSphere / Microsoft Hyper-V / Nutanix AHV / Proxmox];
- 7 serwerów fizycznych;
- 25 stacji roboczych (PC/laptopy).

Aplikacje biznesowe i zasoby plikowe Zaoferowane oprogramowanie musi zapewnić ochronę dla specyficznych aplikacji i baz danych działających w powyższym środowisku.

Ponadto system musi realizować kopie zapasowe udziałów plikowych znajdujących się na urządzeniach NAS (obsługa protokołów SMB/NFS) o łącznej pojemności do 5 TB.

Wymagania ogólne dla oprogramowania:

Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner Peer Insights: i spełniać minimalne wymaganie : - minimalna liczba referencji 500, - minimalna ocena z referencji 4,6.

Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x, 8.x i 9.0 oraz Microsoft Hyper-V 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą

być dostępne dla powyższych platform wirtualizacyjnych, chyba, że wyszczególniono inaczej

Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.8.x - 7.3, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.5 lub nowszy, Proxmox VE 8.2, 8.3, 8.4 lub 9.0 oraz Scale Computing HyperCore 9.4.32.218226 – 9.5.x.

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

System backupowy musi mieć możliwość wdrożenia wszystkich komponentów (np. serwer backupowy, serwer pośredniczący, repozytorium) na platformach Windows oraz Linux

System backupowy musi mieć mieć możliwość wdrożenia w oparciu o tzw. appliance zgodny z wytycznymi bezpieczeństwa DISA (Defense Information Systems Agency)

Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej

Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków

Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.

Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć wiele wirtualnych puli pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej 20 pamięci masowych w pojedyńczej puli.

Oprogramowanie musi pozwalać na przechowywanie kopii bezpieczeństwa w chmurze producenta.

Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage, IBM Cloud Storage, 11:11 Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.

Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania do backupu oraz odtwarzania obrazu maszyny wirtualnej

Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)

Oprogramowanie musi umożliwiać tworzenie logicznie odseparowanych środowisk dla różnych organizacji/działów. Dodatkowo system musi wspierać kontrolę dostępu w oparciu o role (RBAC) - predefiniowane lub własne

Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API

Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji

Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji

Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania

Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej

Oprogramowanie musi umożliwiać integracje z różnymi dostarczycielami tożsamości (IdP - Identity Providers) z wykorzystaniem protokołu SAML (np. Entra ID, Okta)

Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora, reset zablokowanego konta)

Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS)

Oprogramowanie musi posiadać integracje z systemami typu SIEM

Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej oraz analizy istniejącej instalacji systemu backupowego. Powinna istnieć możliwość wyłączenia tej opcji.

Oprogramowanie musi pozwalać na wydawanie komend głosowych asystentowi AI.

Wymagania RPO

Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna conajmniej dla platformy VMware i Hyper-V

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.

Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.

Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).

Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)

Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.

Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 - 2025 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere lub dowolnego systemu operacyjnego Windows Server 2016-2025 (z innych platfrom - fizycznych, wirtualnych, chmurowych). Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.

Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik

Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)

Wymagania RTO:

Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.

Dodatkowo dla środowiska vSphere, Hyper-V, Nutanix AHV i MS Azure powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)

Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w platformę. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami

Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny, zarówno fizycznej jak i wirtualnej

Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików

Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell

Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM

Oprogramowanie musi wspierać bezagentowy backup, spójny aplikacyjnie (tzw. Application Consistent) dla maszyn wirtualnych z platfrom vSphere, Hyper-V, Nutanix AHV, Proxmox.

Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej (Minimum dla Active Directory, MS Exchange, MS SQL, MS Sharepoint, Oracle i PostgreSQL).

Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects oraz pozwalać na odtworzenie haseł.

Oprogramowanie musi pozwalać na backup i odtwarzanie usługi Entra ID. W szczególności użytkowników, grupy, role, jednostki administracyjne, entrprise applications, Conditional Access Policies, Intune Policies oraz logi audytowe i sign-in.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2

Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)

Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych

Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem

Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

Oprogramowanie musi posiadać swój wbudowany program antywirusowy zoptymalizowany do przeszukiwania kopii backpowych

Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware

Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania

Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków

Oprogramowanie musi posiadać mechanizm wykrywania oznak ataku hakerskiego tzw Indicators of Compromise

Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR/XSIAM, CrowdStrike Falcon LogScale, Microsoft Sentinel.

Środowisko fizyczne

Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego

Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych

Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Rocky Linux, AlmaLinux

Rozwiązanie musi wspierać system operacyjny macOS

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix

Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)

Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster

Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów

Rozwiązanie musi wspierać backup podłączonych dysków USB

Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym

Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)

Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone

Rozwiązanie musi wspierać kontrolę pasma sieciowego

Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych

Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN

Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft

Rozwiązanie musi wspierać technologię BitLocker

Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania

Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange, Microsoft Active Directory, Microsoft Sharepoint, Microsoft SQL, Oracle, PostgreSQL oraz MongoDB

Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych

Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle i PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.

Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform

Rozwiązanie musi wspierać szyfrowanie

Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne

Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego

Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej

Rozwiązanie musi wspierać tworzenie wielu zadań backupowych

Monitoring

System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich

System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 7.x – 9.0 zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie

System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2016 – 2025 oraz Azure Stack HCI zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter

System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn

System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel

System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk

System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora

System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów

System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)

System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna

System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego

System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta

System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.

System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware

Raportowanie

System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 7.x – 9.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie

System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2016 – 2025 oraz Azure Stack HCI zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.

System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V

System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Adobe PDF

System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc

System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach

System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów

System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych

System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych

System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury

System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta

System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.

System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.

System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware

System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)

System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

System musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej oraz analizy istniejącej instalacji systemu backupowego. Powinna istnieć możliwość wyłączenia tej opcji.

7. dostawa oprogramowania NAC dla obszaru IT oraz OT

Zamawiający wymaga dostarczenia rozwiązania typu NAC (Network Access Control), służącego do monitorowania sieci lokalnych w celu uwidocznienia pracujących w nich urządzeń oraz wykrywania nowych urządzeń pojawiających się w sieci, w czasie rzeczywistym. Rozwiązanie musi raportować aktualny stan każdego urządzenia, z uwzględnieniem takich atrybutów, jak adres MAC, adres IP, nazwa hosta, system operacyjny,

itp., pozyskując te informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.).

Rozwiązanie ma za zadanie zapewnić, aby tylko urządzenia, których aktualny stan spełnia zdefiniowaną przez administratora politykę bezpieczeństwa, mogły bez ograniczeń ze strony NAC pracować w sieci lokalnej. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenia, których aktualny stan nie spełnia danych warunków polityki bezpieczeństwa (np. nowe, po raz pierwszy pojawiające się urządzenie lub stacja robocza z wyłączonym oprogramowaniem antywirusowym). Mechanizm kwarantanny powinien umożliwiać całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, jak również blokowanie częściowe, w zakresie definiowanym przez administratora (przez wskazanie adresów IP, z którymi urządzenie może się komunikować). Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej.

Rozwiązanie musi posiadać funkcjonalność typu Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów.

Wymagania ogólne rozwiązania NAC

1. Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci.
2. Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezaufanym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci.
3. Musi umożliwiać sprawdzanie statusu aktualizacji oprogramowania antywirusowego i poprawek systemowych na zarządzanych stacjach roboczych Windows i w przypadku niespełniania określonych wymagań, automatycznie ograniczać tym stacjom roboczym możliwość pracy w sieci.
4. Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci.
5. Musi mieć funkcję wykrywania faktu skanowania urządzeń i portów wykonywanego przez urządzenie w sieci lokalnej i automatycznie blokować takie urządzenie, aby zapobiegać potencjalnemu szerzeniu się malware.
6. Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej.
7. Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej.
8. Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS
9. Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową
10. Wymaga się, aby rozwiązanie było dostarczone w postaci maszyny wirtualnej na platformę VMware oraz Hyper-V. System musi pozwalać na monitorowanie łącznie co najmniej 200 urządzeń

11. Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej i dostarczone z licencją pozwalającą na monitorowanie 50 urządzeń wraz ze wsparciem technicznym na okres 1 roku.
12. Wsparcie techniczne musi obejmować dostarczanie aktualizacji oprogramowania/firmware oraz pomoc techniczną producenta w dni robocze w godzinach pracy.

Wymagania szczegółowe – monitorowanie podsieci

1. Rozwiązanie musi w czasie rzeczywistym raportować widoczność wszystkich urządzeń pracujących w monitorowanych podsieciach.
2. Rozwiązanie musi wykrywać nowe nieznane urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysyłać powiadomienie mailowe do administratora
3. Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie
4. Rozwiązanie musi posiadać funkcję pułapki sieciowej (honeypot), symulującą w każdej monitorowanej podsieci standardowe usługi sieciowe, co najmniej: ssh, telnet, ftp i smb. Rozwiązanie musi rejestrować każdą próbę zalogowania się do takiej symulowanej usługi, zapisując użytą nazwę użytkownika, hasło użytkownika i źródłowy MAC/IP.
5. Rozwiązanie musi określać aktualny stan każdego urządzenia, pozyskując informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.) oraz odświeżać te informacje cyklicznie. Musi być możliwość wykorzystania pozyskanych informacji do definiowania polityk bezpieczeństwa.
6. Rozwiązanie musi chronić przed podszywaniem się pod adres MAC (MAC spoofing), umożliwiając zdefiniowanie „odcisku palca” (fingerprint) dla każdego zaufanego urządzenia. Odcisk palca musi być kombinacją co najmniej: adresu MAC, adresu IP, nazwy hosta, nazwy systemu operacyjnego, otwartych portów TCP. Jeśli przeprowadzana cyklicznie weryfikacja odcisku palca wykaże jego zmianę, urządzenie powinno zostać zablokowane.
7. Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy

Wymagania szczegółowe – polityka bezpieczeństwa

1. Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci.
2. W definiowaniu polityki bezpieczeństwa musi być możliwość wykorzystania informacji o aktualnym stanie urządzenia, pozyskanych bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.), poprzez integrację z tymi systemami.
3. Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci:

a. pełny dostęp
b. blokowanie (całkowity brak dostępu)
c. ograniczony dostęp

4. Zakres ograniczonego dostępu powinien być definiowany przez administratora, np. w postaci list ACL, określających, do których adresów IP i portów urządzenie ma dostęp. Musi być możliwość zdefiniowania wielu różnych zakresów ograniczonego dostępu.
5. Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu.
6. Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny.
7. Musi być możliwość łatwego, manualnego tworzenie białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci.

Wymagania szczegółowe – mechanizm kwarantanny

1. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa.
2. Mechanizm kwarantanny powinien umożliwiać:

a. całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym,
b. częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować.

3. Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny.
4. Dla urządzeń zaufanych, czyli w polityce bezpieczeństwa spełniających kryteria pełnego dostępu do sieci, rozwiązanie nie powinno w żaden sposób przekierowywać ani blokować komunikacji wychodzącej z tych urządzeń.
5. Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp.
6. Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej, musi być niezależny od stosowanych w sieci przełączników, zarządzalnych bądź niezarządzalnych.
7. Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj. w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci
8. Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno.

Wymagania szczegółowe – integracja z systemami zewnętrznymi

1. Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD.
2. Rozwiązanie powinno umożliwiać sprawdzanie statusu oprogramowania antywirusowego, poprawek systemowych i firewalla bezpośrednio na zarządzanych stacjach roboczych Windows w domenie AD, w sposób bezagentowy, przy użyciu WMI.
3. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym poprawkami Windows i sprawdzanie statusu zainstalowanych poprawek na zarządzanych urządzeniach z systemem Windows. Wymagana jest możliwość integracji co najmniej z systemami: Microsoft WSUS.

4. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym agentami antywirusowymi i sprawdzanie statusu agentów AV zainstalowanych na zarządzanych urządzeniach (co najmniej, czy agent jest zainstalowany, aktywny i ma aktualne sygnatury wirusów). Wymagana jest możliwość integracji co najmniej z systemami: Bitdefender, Carbon Black, CrowdStrike, Cybereason, Eset, FireEye, Microsoft Defender, SentinelOne, Sophos, Symantec, Trellix, TrendMicro, Webroot.
5. Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-4, do definiowania polityki bezpieczeństwa.
6. Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalla) i na podstawie zawartych w nich informacji blokować wskazane podejrzane urządzenie.

Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal)

1. Rozwiązanie musi posiadać wbudowaną funkcję Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. NAC musi przekierowywać ruch HTTP/S od nieznanych urządzeń do tego portalu.
2. Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora.
3. Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory
4. Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń.
5. Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych.
6. Captive Portal musi umożliwiać osobom nie będącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci.
7. W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy.
8. Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu.
9. Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa.
10. Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci.
11. Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do internetu.
12. Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych.
13. Rozwiązanie musi umożliwiać zatwierdzenie dostępu dla zarejestrowanego urządzenia gościa i konsultanta drogą mailową. Osoba zatwierdzająca powinna otrzymać z systemu e-mail z wnioskiem o dostęp i udzielić go, odpowiadając na maila lub klikając przygotowany link w treści maila.
14. Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant.

15. Wygląd Captive Portal musi być edytowalny w zakresie co najmniej zmiany firmowego logo i kolorów oraz informacji, jakie we wniosku rejestracyjnym musi podać gość lub konsultant.

Pozostałe wymagania

1. Rozwiązanie powinno oferować uwierzytelnianie administratora za pomocą dodatkowego faktora, oprócz hasła (2FA).
2. Rozwiązanie powinno oferować możliwość zainstalowania opcjonalnego agenta na zarządzanych stacjach roboczych (wymagane wsparcie dla Windows, Linux i MacOS), który przesyła do serwera zarządzającego NAC szczegółowe informacje na temat stacji roboczej, umożliwiając definiowanie na bazie tych informacji precyzyjnych polityk bezpieczeństwa.
3. Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning.
4. Rozwiązanie nie powinno pogarszać wydajność łącz WAN.
5. Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci.

8. dostawa szafy rack

Zamawiający wymaga dostawy 1 szt. wolnostojącej szafy rack o wysokości roboczej wynoszącej 32U. Wymagana szerokość montażowa wynosząca 19”. Oferowana szafa powinna pozwalać na obciążenie maksymalne wynoszące nie mniej niż 800 kg. Wymagany ponadto minimum jeden zamek drzwi przednich, oraz minimum 1 zamek drzwi tylnych/bocznych.

9. dostawa macierzy dyskowej wraz z dyskami twardymi dla obszaru IT

Zamawiający wymaga dostawy macierzy dyskowej wraz z dyskami twardymi, spełniających wszystkie poniższe wymagania.

Element konfiguracji/ cecha/ funkcjonalność	Wymagania minimalne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 12 dysków 3.5”
Przestrzeń dyskowa	Zainstalowane: 5 x dysk SAS o pojemności min. 8 TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).

	Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów 25Gb iSCSI (4 porty na kontroler)
Kable/wkładki	4x przewód DAC 10GbE SFP+/SFP+ min. 3m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.

	Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.

	Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające spełnienie powyższych zaleceń.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Oferowany model macierzy w momencie składania oferty nie może mieć ogłoszonej daty końca sprzedaży. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające brak ogłoszenia takiej daty. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Warunki gwarancji	Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:

	• Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. • Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. • Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. • Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. • Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

10. dostawa urządzeń UPS do zabezpieczenia serwerów (3 szt.)

Zamawiający wymaga dostawy identycznych, fabrycznie nowych zasilaczy awaryjnych UPS w ilości 3 szt., przeznaczonych do zabezpieczenia i podtrzymania zasilania serwerów Zamawiającego. Wszystkie zaoferowane urządzenia, komponenty sprzętowe (w tym akumulatory) oraz oprogramowanie muszą być fabrycznie nowe (nieużywane, nieregenerowane, nienaprawiane), pochodzić z oficjalnego kanału sprzedaży producenta oraz posiadać pełne wsparcie techniczne i gwarancyjne świadczone na terytorium Rzeczypospolitej Polskiej. Wykonawca jest zobowiązany do dostarczenia sprzętu spełniającego wszystkie wymagania opisane w niniejszym dokumencie, przy czym przedstawione w poniższej tabeli parametry techniczne i funkcjonalne stanowią wymagania minimalne Zamawiającego.

Nazwa komponentu	Wymagane parametry techniczne
Technologia	online, VFI-SS-111,
Moc wyjściowa	2kVA/2kW; PF=1
Obudowa	Rack/Tower
Napięcie wejściowe	110 ÷ 300 V AC ± 2 %
Napięcie znamionowe (wartość skuteczna)	230V AC
Prąd znamionowy (wejście)	10,7A
Częstotliwość napięcia wejściowego (zakres oraz tolerancja)	45 ÷ 55 / 55 ÷ 65 Hz ± 1 Hz

Częstotliwość znamionowa napięcia wejściowego	50Hz / 60Hz
Zniekształcenia prądu wejściowego THDi	< 5%
Zakres napięcia wyjściowego	200/208/220/230/240V AC konfigurowalne z poziomu oprogramowania oraz z menu zasilacza na wyświetlaczu LCD (domyślnie 230V AC
Zniekształcenia napięcia wyjściowego THDu	< 1% dla Pmax (liniowe) < 5% (nieliniowe wg PN EN 62040-3)
Gniazda wyjściowe	4x IEC320 C13 (10A) sterowalne + 4x IEC320 C13 (10A)
Akumulatory wewnętrzne UPS	Minimum 6 szt. akumulatorów 12V9Ah
Moduły bateryjne	Opcja – możliwość podpięcia do 4szt modułów (każdy z minimum 12szt akumulatorów 12V9Ah)
Czas podtrzymania UPS dla obciążenia 2kW/1,6kW/1kW	6 / 8,5 / 16 min
Czas podtrzymania UPS + MODUŁ dla obciążenia 2kW/1,6kW/1kW	27 / 37 / 62 min
Przeciążalność	105-125% - 5min / 125-150% - 30s / >150% - 500ms
EPO	Wymagane – standard NC
Sygnalizacja	akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę bateryjną, pracę w trybie online, obejście bypass
Język oprogramowania	polski i angielski do wyboru z poziomu interfejsu użytkownika
Konfiguracja minimalnego poziomu naładowania baterii po powrocie zasilania sieciowego (po rozładowaniu baterii przed ponownym samoczynnym załączeniem zasilania na wyjściu)	Wymagane, konfigurowalne z poziomu oprogramowania (przez USB)
Wymagane certyfikaty	CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument)
Komunikacja z urządzeniem	RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; SNMP - dopuszczalna jako opcjonalna karta
Wymiary UPS (rack) (wys x szer x gł)	Nie więcej niż 86 x 439 x 600 mm

Oprogramowanie do monitorowania pracy zasilacza UPS	Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności; możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania); oświadczenie producenta o posiadaniu pełnych praw oraz licencji do oprogramowania
Serwis producenta	wymagany, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty
Gwarancja	Minimum 24 miesiące elektronika, 24 miesiące akumulatory, serwis door to door, czas naprawy 5 dni roboczych
Dokumentacja	Instrukcja w języku polskim

11. dostawa oprogramowania IDS dedykowanego sieciom OT wraz ze sprzętowymi sondami do monitorowania sieci OT oraz usługą szkoleniową

Zamawiający informuje, że przedmiotem zamówienia jest:

1. dostawa systemu monitorowania sieci przemysłowej służącego do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS),
2. dostawa licencji oraz sond sprzętowych,
3. udzielenie wsparcia dla administratorów Zamawiającego,
4. organizacja i realizacja szkoleń dla dwóch administratorów Zamawiającego.

Funkcjonalność i specyfikacja.

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:
   a. pasywne monitorowanie sieci przemysłowej Zamawiającego,

b. automatyczne tworzenie graficznej mapy rządzeń min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach.
c. szczegółową inwentaryzację urządzeń,
d. automatyczne odzwierciedlenie połączeń komunikacyjnych,
e. informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji,
f. wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST,
g. budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji,
h. 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.:
a. malware/"zero-day",
b. atak DOS/DDOS,
c. atak typu ATP,

d. spyware, skanowanie sieci,
e. zagrożenia Man-in-the-Middle,
f. anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność, komend, skanowanie PLC, skanowanie urządzeń sterujących,
g. wykrywanie połączeń do innej sieci LAN/internet,
h. 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. Sondy sprzętowe muszą posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej min. AES128.
41. Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.
42. Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem bateryjnym do 30 minut przy zaniku zasilania z sieci.
43. Sonda sprzętowa musi wspierać: DHCP, stały adres IP.
44. Sonda sprzętowa musi być zabezpieczona przed ingerencją tzn.: dane muszą zostać skasowane przy próbie odczytu pamięci FLASH.
45. Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.
46. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.
47. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.
48. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.
49. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.
50. 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.
51. Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazaną część ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.
52. Sonda sprzętowa musi umożliwiać przekazywać do systemu IDS strumień sieciowy w formacie IPFIX.

Dostawa:

1. Zamawiający wymaga, aby Wykonawca dostarczył:
   a. sondy sprzętowe w liczbie 3 szt. do monitorowania sieci przemysłowej,
   b. licencję wieczystą na system IDS dla nielimitowanej liczby monitorowanych urządzeń,
   c. usługi wsparcia serwisowego producenta systemu IDS na okres 12 miesięcy.

Zamawiający wymaga, aby serwis producenta systemu IDS obejmował

- dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim;
- dostęp do nowych wersji systemu IDS;
- dostęp do aktualizacji i poprawek systemu IDS.
- dostęp do aktualizacji oprogramowania sond sprzętowych;
- wymianę uszkodzonych sond sprzętowych w razie awarii;
- przekazanie danych kontaktowych do działu technicznego producenta systemu IDS;
- wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas;

wdrożenia i późniejszej eksploatacji.

- wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.

2. Wykonawca zainstaluje i zalicencjonuje oraz skonfiguruje system IDS w środowisku serwerowym wskazanym przez Zamawiającego.
3. Licencje systemowe oraz sprzęt serwerowy zapewni Zamawiający.
4. 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.
5. Wykonawca przeprowadzi pełną konfigurację i wdrożenia systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.
6. Wykonawca przekaże Zamawiającemu wszelkie hasła, użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.
7. Dla całego powyższego zakresu dot. instalacji, konfiguracji i parametryzacji Wykonawca przeprowadzi testy sprawdzające prawidłowość jego wykonania i działania.
8. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.
9. Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego z konfiguracji i administracji systemem IDS. Zamawiający dopuszcza realizację szkolenia zdalnie w minimum 6 h bloku czasowym.

12. dostawa serwera fizycznego dla obszaru OT

Zamawiający wymaga dostawy serwera fizycznego dla obszaru IT, stanowiącego bazę dla rozwiązań bezpieczeństwa (w tym IDS i XDR), spełniającego wszystkie poniższe wymagania.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Rack o wysokości max 1U • Min. 8 slotów na dyski 2.5” • Możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. • Obsługa procesorów 144 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 4TB pamięci RAM.
Procesor	• Zainstalowany jeden procesor min. 16-rdzeniowe, min. 2.3GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 199 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej.
Pamięć RAM	• 64 GB DDR5 RDIMM 6400MT/s
Kontroler RAID	• Sprzętowy kontroler dyskowy • Możliwość konfiguracji poziomów RAID: 0, 1, 10 (oraz tryb Non-RAID). • Wsparcie dla dysków samoszyfrujących • Obsługa dysków 12Gbps SAS3, 6Gbps SATA3/SAS2 oraz NVMe (Gen3 i Gen4)
Pamięć masowa	• Możliwość instalacji dysków SATA/SAS. • Zainstalowane 4 dyski SAS o pojemności min. 2.4 TB, 12Gbps, 2,5“ Hot-Plug.
Gniazda rozszerzeń	• Minimum 2x slot PCIe x16 generacji 5. Dodatkowo min. 1 sloty w standardzie OCP 3.0 (x16) przeznaczone dla kart sieciowych.

Parametr	Charakterystyka (wymagania minimalne)
Interfejsy sieciowe/FC/SAS	• 4 interfejsy sieciowe 10/25 GbE SFP28 (porty nie mogą być osiągnięte poprzez zainstalowanie karty w wymaganych slotach PCIe). • 1 przewód typu DAC , SFP+ to SFP+, 10GbE 3 m

Wbudowane porty	• 4 porty USB w tym min:
	  ○ 1 port USB 2.0 Type-C dostępne z przodu obudowy
	  ○ 2 porty USB 3.1 typ A dostępne z tyłu obudowy
	  ○ 1 port USB 3.0 dostępne wewnątrz obudowy
	• Port VGA z tyłu obudowy
	Nie dopuszcza się stosowania kart PCIe.

Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
Zasilanie	• Redundantne, Hot-Plug min. 800W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera

Parametr	Charakterystyka (wymagania minimalne)
	• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Diagnostyka	• System powiadomień LED o funkcjonalności: o Informacji o statusie zasilania serwera o Pomocy w zlokalizowaniu serwera o Informacji o błędach, powiązanej z logami systemowymi.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez sześciu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.

Parametr	Charakterystyka (wymagania minimalne)
	• Monitorowanie zużycia dysków SSD • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. • Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera • kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania • możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień • możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera • możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer • możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe Możliwość rozszerzenia funkcjonalności o: • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch • możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej • Automatyczne odświeżanie certyfikatów SSL • monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

Parametr	Charakterystyka (wymagania minimalne)
	Zainstalowane oprogramowanie producenta do zarządzania, spełniające poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich

Parametr	Charakterystyka (wymagania minimalne)
	• Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. Oprogramowanie dostarczone jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring:

Parametr	Charakterystyka (wymagania minimalne)
	○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu

Parametr	Charakterystyka (wymagania minimalne)
	▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. o Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów o Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware

Parametr	Charakterystyka (wymagania minimalne)
	○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń

Parametr	Charakterystyka (wymagania minimalne)
	w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. o Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. o Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. o Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia o Urządzenie Producenta dostarczane w ramach postępowania o Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent o Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności o Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
System operacyjny/dodatkowe oprogramowanie	• Dostarczony system operacyjny przez wzgląd na kompatybilność z obecnie posiadaną infrastrukturą. • Licencja na Windows Server 2025 Standard, licencja pokrywająca wszystkie fizyczne rdzenie w serwerze, pozwalająca na uruchomienie oprogramowania na minimum 2 maszynach wirtualnych.

Parametr	Charakterystyka (wymagania minimalne)
	• Nośnik CD/DVD umożliwiający downgrade do wersji Windows Server 2022 Stadnard.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
Dokumentacja	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.

Parametr	Charakterystyka (wymagania minimalne)

	• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
	• Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.
	• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
	• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
	• Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
	  ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
	  ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
	  ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.

Parametr	Charakterystyka (wymagania minimalne)
	○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

13. dostawa zarządzalnych urządzeń sieciowych

Zamawiający wymaga dostawy zarządzalnych urządzeń sieciowych (przełączników sieciowych):

- 24 portowe – 3 sztuki;
- 24 portowe z obsługą POE– 1 sztuka.

A) Zamawiający wymaga, aby przełączniki 24portowe spełniały wszystkie poniższe wymagania:

Liczba urządzeń: 3 sztuki

Przedmiotem zamówienia jest dostawa 3 sztuk fabrycznie nowych, nieużywanych przełączników sieciowych warstwy 3 (L3), dedykowanych do pracy w warstwie dostępu lub agregacji. Urządzenia muszą być w pełni kompatybilne z nowoczesnymi standardami sieciowymi, zapewniać wysoką dostępność dzięki redundantnemu zasilaniu oraz obsługiwać zaawansowane protokoły routingu.

Szczegółowe wymagania techniczne

Lp.	Nazwa parametru	Wymagane parametry
1	Obudowa	Obudowa urządzenia musi być przystosowana do montażu w standardowej szafie 19” Maksymalne wymiary: Szerokość – 44,5 cm Głębokość – 27,5 cm Wysokość – 4,5 cm. Waga do 4 kg
2	Interfejsy	Minimum 24 gigabitowe interfejsy RJ-45 100/1000 Mbps, 2 interfejsy 100M/1G/2.5G/5G/10G Ethernet (RJ-45) 4 interfejsy 1G SFP/10G SFP+ Port konsoli USB-C
3	Wydajność	• Potencjał przełączania nie mniejszy niż 168 Gbps • Prędkość przełączania nie mniejsza niż 125 Mbps • Bufor pakietu nie mniejszy niż 2 Mbyte • Tabela adresów MAC nie mniejsza niż 32K • Jumbo frame (byte) – 9K • Flash nie mniej 64 MB • RAM nie mniej niż 1GB • L3 forwarding table - Max. 1 K IPv4 entries; Max. 512 IPv6 entries • Routing table - 64
4	Tryby pracy	• Urządzenie musi umożliwiać zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmury, dostarczony bezpłatnie przez producenta urządzenia
5	Zgodność ze standardami	• IEEE 802.3z 1000BASE-X • IEEE 802.3ab 1000BASE-T Ethernet • IEEE 802.3an 10G BASE-T Ethernet • IEEE 802.3ae 10 Gbit/s Ethernet over fiber • IEEE 802.3az EEE • IEEE 802.3x flow control • IEEE 802.1AB LLDP/LLDP-MED • IEEE 802.1Q VLAN tagging • IEEE 802.1p Class of Service (CoS) prioritization • IEEE 802.1X port authentication
6	Odporność i dostępność	• IEEE 802.1D Spanning Tree Protocol (STP) • IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) • IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) • Static port trunking • IEEE 802.3ad LACP • Loop guard (with broadcast packet detection mechanism) • Root guard • BPDU guard • ErrDisable recovery • Dual configuration files • Dual images • ZULD • Flex link • Physical stacking • Flexible stacking

7	Kontrola ruchu	• 802.1Q static VLANs/dynamic VLANs: 4 K/4 K • Port-based VLAN • VLAN isolation • Vendor ID based VLAN • Protocol-based VLAN • IP subnet-based VLAN • MAC-based VLAN • Private VLAN • Voice VLAN • Independent VLAN Learning (IVL) • VLAN Translation • VLAN trunking • VLAN mapping • VLAN routing • IEEE 802.1AD VLAN stacking (QinQ) • VLAN ingress filtering • LACP algorithm of source/ destination IP or MAC • GVRP • L2PT
8	Bezpieczeństwo	• Port security • Layer 2 MAC filtering • Layer 3 IP filtering • Layer 4 TCP/UDP socket filtering • Static MAC forwarding • Multiple RADIUS servers • Multiple TACACS+ servers • 802.1x VLAN and 802.1p assignment by RADIUS • Login authentication by RADIUS • Login authentication by TACACS+ • TACACS+ accounting • RADIUS accounting • Authorization on RADIUS • Compound authentication • Authorization on TACACS+ • SSH v2 • SSL • MAC freeze • IP source guard (IPv4/IPv6) • DHCP snooping • DHCP Server Guard • ARP inspection • ARP freeze • Anti-ARP scan • Static IP-MAC-Port binding • Policy-based security filtering • Port isolation • MAC search • Guest VLAN • ACL packet filtering (IPv4/IPv6) • CPU protection • Interface related trap enable/disable (by port) • MAC-based authentication per VLAN • BPDU transparency • WoL/WoL Relay • Password encryption

		• Password complexity • Brute-force attack protection • SSH public key authentication
9	QoS	• No. of hardware queues per port (Standalone/stacking): 8/6 • Storm control and event log: Broadcast, multicast, unknown unicast (DLF) • Port-based rate limiting (ingress/ egress) • Rate limiting per IP/TCP/UDP per port • Policy-based rate limiting • 802.3x flow control • 802.1p Class of Service (SPQ, WFQ, WRR, hybrid-SPQ combination capable) • DiffServ (DSCP) • Storm Control: Broadcast/Unknown Multicast/Unknown Unicast (DLF)
10	Layer 2 Multicast	• L2 multicast • IGMP snooping (v1, v2, v3) • IGMP snooping fast leave • IGMP snooping immediate leave • Configurable IGMP snooping timer and priority • IGMP snooping statistics • IGMP throttling • IGMP filtering • IGMP proxy mode & snooping mode selection • Multicast load balance over trunking port • Static mulitcast • MVR support • MLD snooping (MLD v1/v2)
11	Routing	• Static route • IP port moving • Policy-based route
12	Zarządzanie	• SNMP v1, v2c, v3 • SNMP trap group • RMON (1, 2, 3, 9) • ICMP echo/echo reply • Syslog • IEEE 802.1AB LLDP/LLDP-MED • Custom default • Syslog (IPv4/IPv6) • Display port utilization • DHCP relay per VLAN • DHCP smart relay • DHCP relay option 82 • SSH Remote Command Execution
13	Zarządzanie IPv6	• IPv6 over Ethernet (RFC 2464) • IPv6 addressing architecture (RFC 4291) • Dual stack (RFC 4213) • ICMPv6 (RFC 4443) • Path MTU (RFC 1981) • Minimum path MTU size of 1280 (RFC 5095) • Encapsulation for maximum PMTU of 1500 • Neighbor discovery (RFC 4861) • DHCPv6 snooping • IPv6 binding- static/dynamic • Extend Radius server

		• DHCPv6 relay • Default DHCP client mode
14	Zarządzanie urządzeniem	• Standalone management by Web interface • Cloud management • Networked AV mode by Web Interface • Optimized Dante and AES67 in Networked AV mode • Intuitive Cloud connection status • Management through Console, Telnet, SNMP • Remote firmware upgrade by FTP/ Web/TFTP • Configuration saving and retrieving • Multiple logins supported • Configure clone • Custom default Configuration • Multilevel CLI • CLI (Cisco-like) • DHCP server • DHCP relay per VLAN • DHCP client IPv4/IPv6 • DHCP client option 60 • DHCP option 82 • Daylight saving • DHCP relay MAC proxy • Auto PD Recovery • NTP supports IPv4/IPv6 • Port mirroring • Policy-based mirroring • Mirror CPU • VLAN-based mirroring • USB-C out-of-band console port • Auto PD Recovery • LLDP power via MDI • sFlow • Fiber Module Rescue • SSH Remote Command Execution
15	MIB	• RFC 1066 TCP/IP-based MIB • RFC 1213, 1157 SNMPv2c/v3 MIB • RFC 1493, 4188 bridge MIB • RFC 1643 Ethernet MIB • RFC 1757 RMON group 1, 2, 3, 9 • RFC 2011, 2012, 2013 SNMPv2 MIB • RFC 2233 SMIv2 MIB • RFC 2358 Ethernet-like MIB • RFC 2674 bridge MIB extension • RFC 2819, 2925 remote management MIB • RFC 3621 power Ethernet MIB • RFC 4022 management information base for transmission control protocol • RFC 4113 management information base for user datagram protocol • RFC 4292 IP forwarding table MIB • RFC 4293 Management Information Base (MIB) for IP • Cable diagnostic MIB
16	Zakres temperaturowy pracy	-20°C do 50°C
17	Zasilanie	Maksymalna moc pobierana przez urządzenie nie może przekraczać 38W.

18	Ochrona przed wyładowaniami elektrostatycznymi/ przepięciami	Zabezpieczenie przeciwprzepięciowe portu Ethernet – 2KV Ochrona zasilacza Linia-GND – 2KV Ochrona zasilacza Linia-Linia – 1KV Ochrona ESD portu Ethernet (powietrze/kontakt) - 8 KV/6 KV
19	Rozpraszanie ciepła (BTU/godz.)	128.28
20	Hałas akustyczny przy 25°C (min./maks., dBA)	27.19/47.88
21	MTBF (hr)	Parametr te nie powinien być niższy niż 520,185
22	Gwarancja	Urządzenie powinno posiadać ograniczoną dożywotnią gwarancję producenta
23	Serwis	W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje w następnym dniu roboczym, po którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat.
24	Wymagane Certyfikaty	Bezpieczeństwo • LVD • BSMI EMC • FCC Part 15 (Class A) • CE EMC (Class A) • BSMI EMC RoHS • Level A
25	Pozostałe	Sprzęt musi być fabrycznie nowy i pochodzić z polskiego kanału dystrybucji

B) Zamawiający wymaga, aby przełączniki 24portowe z obsługą POE spełniały wszystkie poniższe wymagania:

Liczba urządzeń: 1 sztuka

Przedmiotem zamówienia jest dostawa 1 sztuki fabrycznie nowego, nieużywanych przełącznika sieciowego warstwy 3 (L3) wyposażonego w 24 porty Gigabit Ethernet z obsługą PoE+ oraz 6 dedykowanych portów uplink 10G SFP+. Urządzenie musi zapewniać pełną wydajność przekazywania pakietów (wire-speed) oraz wspierać zaawansowane mechanizmy wirtualizacji i wysokiej dostępności.

Szczegółowe wymagania techniczne

Interfejsy fizyczne i zasilanie PoE

- Porty dostępowe: 24 porty 10/100/1000Base-T (RJ45) z obsługą PoE+.

- Obsługa standardów PoE: Pełna zgodność z IEEE 802.3af (PoE) oraz IEEE 802.3at (PoE+).
- Budżet mocy PoE: Całkowity budżet mocy dostępnej dla urządzeń końcowych musi wynosić minimum 370W.
- Porty uplink: 6 portów 10GbE SFP+ (obsługujących wkładki 1G SFP oraz 10G SFP+).
- Porty dodatkowe: * 1 port konsolowy (RJ45).
    - 1 port zarządzający 10/100/1000Base-T (Out-of-band management).
    - 1 port USB 2.0 do archiwizacji konfiguracji i aktualizacji oprogramowania.

Wydajność i parametry systemowe (zgodnie z architekturą urządzenia)

- Wydajność przełączania (Switching Capacity): Minimum 168 Gbps.
- Szybkość przesyłania pakietów (Forwarding Rate): Minimum 125 Mpps.
- Tablica adresów MAC: Minimum 32 000 wpisów.
- Tablica routingu IPv4 (L3): Minimum 12 000 wpisów.
- Tablica routingu IPv6 (L3): Minimum 6 000 wpisów.
- Tablica sąsiedztwa (Adjacency table): Minimum 8 000 wpisów.
- Pamięć operacyjna: Minimum 1 GB RAM.
- Pamięć Flash: Minimum 512 MB.
- Ramki Jumbo: Obsługa do 10 240 Bajtów.

Funkcjonalność Warstwy 2 (L2)

- VLAN: Obsługa 4096 identyfikatorów VLAN (IEEE 802.1Q), GVRP, QinQ (Basic, Selective), Voice VLAN, MAC-based VLAN.
- Spanning **Tree:** IEEE 802.1D (STP), 802.1w (RSTP), 802.1s (MSTP), Root Guard, BPDU Guard.
- **Agregacja portów:** IEEE 802.3ad (LACP) – do 128 grup agregacji.
- **Inne:** Loopback Detection, Flow Control (802.3x), Port Mirroring (Many-to-One, RSPAN, ERSPAN).

Funkcjonalność Warstwy 3 (L3)

- Routing Statyczny: IPv4, IPv6.
- Routing Dynamiczny IPv4: RIP v1/v2, OSPF v2, BGP4.
- Routing Dynamiczny IPv6: OSPFv3, BGP4+.
- Multicast: IGMP Snooping (v1/v2/v3), MLD Snooping (v1/v2), PIM-SM, PIM-DM, PIM-SSM, MSDP.

- Redundancja: VRRP oraz VRRPv3.
- Mechanizmy dodatkowe: Policy Based Routing (PBR) dla IPv4 i IPv6, uRPF, BFD.

Wirtualizacja i Wysoka Dostępność

- VSF (Virtual Switch Framework): Obsługa wirtualizacji stosu umożliwiająca połączenie wielu fizycznych jednostek w jeden logiczny system zarządzany przez jeden adres IP.
- Stacking: Możliwość łączenia w stos przy wykorzystaniu standardowych portów 10G SFP+.
- MRPP (Multi-layer Ring Protection Protocol): Wsparcie dla szybkich protokołów pierścieniowych (czas rekonfiguracji poniżej 50ms).

Bezpieczeństwo i Jakość Usług (QoS)

- Listy kontroli dostępu (ACL): Standardowe i rozszerzone (L2/L3/L4), IPv6 ACL, Time-based ACL.
- Bezpieczeństwo portów: IEEE 802.1X (Port-based, MAC-based), RADIUS/TACACS+, Guest VLAN.
- Ochrona sieci: DHCP Snooping, Dynamic ARP Inspection (DAI), IP Source Guard, Port Security.
- QoS: 8 kolejek sprzętowych na port, priorytetyzacja SP, WRR, SWRR, WDRR, klasyfikacja ruchu oparta na 802.1p, DSCP, IP Precedence.

Zarządzanie i Administracja

- Zarządzanie przez CLI (Telnet, SSH v1/v2), interfejs Web (HTTP/HTTPS), SNMP v1/v2c/v3.
- Obsługa RMON (grupy 1, 2, 3, 9).
- Monitoring: sFlow, LLDP / LLDP-MED, NTP.
- Zarządzanie PoE: Harmonogramy pracy portów (PoE schedule), ustalanie priorytetów zasilania, monitoring mocy.

Warunki fizyczne i zasilanie

- Redundancja zasilania: Urządzenie musi posiadać dwa sloty na moduły zasilania AC z obsługą wymiany podczas pracy (Hot-Swap).
- Zasilacze w zestawie: Urządzenie musi zostać dostarczone z kompletem dwóch zasilaczy AC zapewniających pełną redundancję 1+1.
- Obudowa: Wysokość 1U, przystosowana do montażu w szafie rack 19" (uchwyty w zestawie).
- Chłodzenie: Aktywne, wentylatory z automatyczną regulacją obrotów.
- Temperatura pracy: 0°C do 50°C.

Gwarancja i wymagania dodatkowe

- Gwarancja: Minimum 24 miesiące gwarancji producenta.
- Aktualizacje: Darmowy dostęp do nowych wersji oprogramowania systemowego w okresie trwania gwarancji.
- Certyfikaty: CE, RoHS.

14. dostawa urządzeń access point

Zamawiający wymaga dostawy dwóch jednakowych urządzeń access point z spełniających wymagania techniczne dla każdej ze sztuk:

Lp.	Nazwa parametru	Wymagane parametry
1	Obudowa	Obudowa urządzenia musi być przystosowana do montażu do sufitowego
2	Ilość portów	Urządzenie w standardzie musi posiadać 2 porty 1/2.5 Gbps LAN
3	Tryb pracy	Urządzenie musi umożliwiać pracę w jednym z poniższych trybów: • samodzielny (standalone) • zdalną konfigurację i monitorowanie poprzez panel sterowania dostępny w technologii chmury, dostarczony bezpłatnie przez producenta urządzenia
4	Funkcje WLAN	Urządzenie musi: • posiadać co najmniej dwa radia • obsługiwać MU-MIMO • minimalny zysk anteny 1.49 dBi dla pasma 2,4Ghz (2x2: 2SS) • minimalny zysk anteny 2.78 dBi dla pasma 5Ghz (4x4: 4SS) • minimalny zysk anteny 3.17 dBi dla pasma 6Ghz (4x4: 4SS) • minimalna prędkość przesyłu danych: 688 Mbps dla pasma 2,4Ghz • minimalna prędkość przesyłu danych: 8646 Mbps dla pasma 5Ghz • minimalna prędkość przesyłu danych: 11530 Mbps dla pasma 6Ghz • obsługiwać Band Steering • obsługiwać WDS/Mesh • obsługiwać DCS i Load Ballancing • obsługiwać Fast Roaming (Pre-authentication, PMK caching and 802.11 r/k/v) • obsługiwać technologię advanced cellular coexistence
5	Bezpieczeństwo	Urządzenie musi: wspierać: • WEP • WPA • WPA2 • WPA3 • IEEE 802.1X • MAC filtering • L2 isolation • RADIUS authentication • Rogue AP detection
6	Funkcje sieci	Urządzenie musi: wspierać: • IPv6 • VLANs

		• WMM • U-APSD
7	Zarządzanie	Urządzenie musi: wspierać zarzadzanie poprzez: • Web UI • CLI • SNMP • Cloud
8	Zasilanie	Punkt dostępowy musi umożliwiać jego zasilanie z PoE, Maksymalny pobór mocy nie może być większy niż 22 W
9	MTBF (hr)	Parametr te nie powinien być niższy niż 691,722
10	Gwarancja	Urządzenie powinno być objęte ograniczoną dożywotnią gwarancją producenta
11	Serwis	W przypadku awarii urządzenia, wysyłka zastępczego produktu następuje następnego dnia roboczego po tym, w którym zgłoszona zostanie awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat.
12	Wymagane Certyfikaty	Radio: FCC Part 15C, FCC Part 15E, FCC Part 2.1091, ETSI EN 300 328, EN 301 893, Draft EN 303 687, EN 50385, EN 50665, EN IEC 62311, LP0002 EMC: FCC Part 15B, EN 301 489-1, EN 301 489-17, EN55032, EN55035, EN61000-3-2/-3, EN60601-1-2, BSMI CNS15936 Bezpieczeństwo: EN 62368-1, IEC 62368-1, BSMI CNS15598-1
13	Pozostałe	Sprzęt musi być nowy i pochodzić z polskiego kanału dystrybucji

15. usługa wdrożenia i konfiguracji urządzeń, oprogramowania i rozwiązań z zakresu bezpieczeństwa

Zamawiający wymaga kompleksowej usługi wdrożeniowej, obejmującej następujące etapy:

Montaż i instalacja fizyczna:

- Instalacja wszystkich urządzeń w szafach teleinformatycznych Zamawiającego.
- Połączenie dostarczonych urządzeń wyłącznie w obrębie szaf teleinformatycznych za pomocą dedykowanych przewodów miedzianych i światłowodowych (patchcordów).
- Montaż punktów dostępowych w wyznaczonych punktach obiektu, przy założeniu, że niezbędne okablowanie sieciowe oraz punkty logiczne są już doprowadzone do miejsc montażu (zakres prac nie obejmuje układania tras kablowych poza szafami).
- Instalacja systemów operacyjnych serwerowych oraz oprogramowania do zarządzania wirtualizacją na dostarczonych serwerach.
    - Konfiguracji nowych serwerów i oprogramowania w obu serwerowniach Zamawiającego (dwie lokalizacje).

Konfiguracja tożsamości i usług katalogowych:

1. Utworzenie nowej struktury usługi katalogowej:

2. Konfiguracja serwerów odpowiedzialnych za autoryzację i uwierzytelnianie w serwerowni Zamawiającego pod adresem ul. Płocka 106, 06 – 500 Mława.
3. Przygotowanie struktury organizacyjnej i polityk bezpieczeństwa (hasła, dostęp do zasobów, aktualizacje).
4. Instalacji systemu operacyjnego oraz systemów virtualych Hyper-V lub równoważnych na nowych serwerach.
5. Instalacji na serwerze wirtualnych systemów operacyjnych:
   - pierwszy Windows Serwer 2025 lub równoważny wraz z konfiguracją primary domain
   - drugi wirtualny system operacyjny Windows Serwer 2025 lub równoważny z konfiguracją secondary domain, uruchomieniu usług automatycznego nadawania adresów (DHCP) oraz rozwiązywania nazw (DNS).
   - Instalacji CALI, konfiguracji podstawowych polityk domeny.
   - Wdrożenie do nowej domeny 25 funkcjonujących u Zamawiającego komputerów.
6. Jedno miesięcznej dedykowanej opieki powdrożeniowej realizowanej zdalnie – wymagane jest, aby do opieki wyznaczony był dedykowany inżynier dostarczonego sprzętu i oprogramowania. Wsparcie powdrożeniowe musi być świadczone w dni robocze w godzinach 7:00 – 15:00.

Konfiguracja systemów bezpieczeństwa i zarządzania:

1. **Systemy sieciowe:**
   1) Uruchomienie reguł filtrowania ruchu, konfiguracja bezpiecznych połączeń między oddziałami, aktywacja systemów ochrony przed atakami.
   2) Dostawę oraz konfigurację nowych urządzeń sieciowych UTM w serwerowniach (dwie);
   3) Zamawiający wymaga, aby Wykonawca w ramach dostawy zagwarantował Zamawiającemu:
      - analizę aktualnej struktury sieci lokalnej oraz obecnie funkcjonujących u Zamawiającego starych dostępów do internetu.
      - instalacja/konfiguracja zaoferowanego rozwiązania w infrastrukturze sieciowej Zamawiającego musi być wykonana zgodnie z wymaganiami Zamawiającego (dotyczy polityk bezpieczeństwa, dostępów zdalnych, integracji z domeną lokalną.
      - Zamawiający wymaga konfiguracji połączeń VPN typu remote access (client-to-site) umożliwiających bezpieczny dostęp użytkowników zdalnych do zasobów sieci lokalnej. Zamawiający wymaga zestawienia szyfrowanych połączeń typu site-to-site VPN (IPsec) pomiędzy 3 nowymi urządzeniami UTM w celu połączenia sieci lokalnych.
      - po zakończeniu instalacji – instruktarz z wykonanej konfiguracji na zainstalowanym środowisku UTM,
2. **System ochrony końcówek:**
   1) Instalacja systemu XDR administracyjnego z panelem sterowania agentami, przygotowanie polityk ochrony i wdrożenie oprogramowania na stacjach roboczych i serwerach.

3. **Archiwizacja:**

1) Konfiguracja przestrzeni dyskowej, przygotowanie planów i harmonogramów kopii zapasowych dla systemów wirtualnych i baz danych.
2) Wdrożenie musi obejmować instalację na serwerze Zamawiającego, konfigurację scenariuszy co najmniej 2 serwerów wirtualnych lub standardowych.
3) Podłączenie do macierzy nowych serwerów oraz obecnie funkcjonujących u Zamawiającego Dell R320; Dell R330.

4. **Kontrola dostępu:**

1) Uruchomienie mechanizmów wykrywania urządzeń, portalu dla gości oraz automatycznego izolowania zainfekowanych hostów w systemie NAC.
2) Wdrożenie i harmonogram ramowy dla systemu NAC:

- Wdrożenia oraz konfiguracja nowego systemu NAC muszą odbyć się w dwóch lokalizacjach Zamawiającego (dwie serwerownie):

- Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
- Podstawowa konfiguracja Systemu NAC **(integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA**).
- Konfiguracja posiadanego urządzenia firewall (pod kątem separacji sieci na vlan'y, obejmującego modyfikacje routing'u, interfejsów, reguł firewall i innych elementów konfiguracji wymaganych w procesie separacji sieci na vlan'y, etc.).
- Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
- Integracja posiadanych przez Zamawiającego urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
- Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.
- Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.

Licencja wsparcia technicznego producenta oprogramowania:

- Wykonawca dostarczy systemy NAC wraz z dożywotnią licencją oraz licencją serwisową od producenta oprogramowania na wsparcie do terminu wymaganego w OPZ.
- Licencja wsparcia technicznego producenta oprogramowania powinna obejmować minimalnie wymagania:
  - Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC
  - Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
  - Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.

- Dostęp do dokumentacji i instrukcji na stronie internetowej.
- Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

Zamawiający wymaga, aby w ramach dostawy Wykonawca zagwarantował dodatkowo:

- Ze względu na zakup w tym postępowaniu nowego urządzenia klasy firewall Wykonawca skonfiguruje je również pod kątem separacji sieci na vlan'y (wymagane przes system NAC), obejmującego modyfikacje routing'u, reguł firewall i innych elementów konfiguracji wymaganych w procesie separacji sieci na vlan'y.

5. **Monitoring:** Instalacja systemów na nowych serwerach i skonfigurowanie zbierania informacji o zdarzeniach z urządzeń sieciowych i serwerów oraz monitoringu ich dostępności.

6. **Zarządzanie IT:**

- Wdrożenie musi obejmować instalację i konfigurację na serwerze Zamawiającego.
- Uruchomienie bazy zasobów oraz portalu do obsługi zgłoszeń użytkowników.
- Konfigurację obsługi poniższych scenariuszy:
    1) Zarządzanie incydentami (Incident Management),
    2) Zarządzanie problemami (Problem Management),
    3) Zarządzanie bazą wiedzy (Knowledge Management),
    4) Zarządzanie zasobami (Asset Management).

CZĘŚĆ 4 Dostawa agregatu prądotwórczego

1. Dostawa agregatu prądotwórczego

Zamawiający wymaga, aby oferowany agregat prądotwórczy wykonany był z obowiązującymi normami i standardami:

Dyrektywy Unii Europejskiej:

Oznaczenie	Tytuł
2006/42/WE	Dyrektywa Maszynowa
2014/30/UE	Dyrektywa w sprawie kompatybilności elektromagnetycznej (EMC)
2014/35/UE	Dyrektywa w sprawie sprzętu elektrycznego przewidzianego do stosowania w określonych granicach napięcia (LVD)
2000/14/WE ze zm. 2005/88/WE	Dyrektywa w sprawie emisji hałasu do środowiska przez urządzenia używane na zewnątrz pomieszczeń

Normy techniczne:

Oznaczenie	Zakres
ISO 8528-1:2005	Agregaty prądotwórcze prądu przemiennego — klasyfikacja, parametry znamionowe i charakterystyki pracy
PN-EN ISO 8528-13:2016-07	Agregaty prądotwórcze prądu przemiennego — wymagania bezpieczeństwa
PN-EN ISO 3744:2011	Akustyka — wyznaczanie poziomów mocy akustycznej źródeł hałasu (metodologia pomiarów)

Zamawiający wymaga, aby oferowany agregat był w wersji obudowanej, z obudową dźwiękochłonną, wyciszoną specjalną, niepalną pianką wygłuszającą, z niezbędnymi drzwiami dostępowymi i serwisowymi.

Wymagana moc znamionowa agregatu – 40 kVA (32 kW).
Wymagana moc awaryjna agregatu nie mniej niż – 44 kVA (35 kW).
Napięcie – 400/230 V.
Częstotliwość – 50Hz.

Zamawiający wymaga, aby agregat pochodził z seryjnej i bieżącej produkcji, był wyprodukowany w Polsce i posiadał oznaczenie CE. Oferowane urządzenie powinno być w całości spreparowane przez jednego producenta, który powinien posiadać wdrożone systemy ISO9001:2015 oraz AQAP 2110:2016. Ponadto wymaga się, aby producent urządzenia posiadał certyfikat wdrożenia i stosowania systemów zgodnie z wymaganiami norm PN-EN ISO 14001:2015, PN-EN ISO 45001:2024 oraz PN-EN ISO/IEC 27001:2023.

Zamawiający zastrzega, że jakiekolwiek modyfikacje urządzenia ingerujące w jego konstrukcję nie są dopuszczane.

Wymagana bardzo mocna konstrukcja z możliwością transportu wózkiem widłowym, dźwigiem, HDS – na pasach, widłach lub łańcuchach. Klasa wykonania minimum G3.

Rama dodatkowo izolowana od podłoża za pomocą stóp (stożków) gumowych przykręcanych do ramy, z możliwością regulacji wysokości (poziomowania).

Wymagany zewnętrzny przycisk zatrzymania awaryjnego, a także gniazdo potrzeb własnych agregatu.

Zaciski na listwie sterowniczej:
- NC do podłączenia zewnętrznego stopu pożarowego;
- dla kabla potrzeb własnych agregatu;
- dla kabla sterowniczego, sterowania układem SZR.

Wymagane wysokowydajne amortyzatory drgań silnika i prądnicy.

Wymiary nie przekraczające (dł. x szer. x wys.) – 2300 x 1000 x 1545 [mm].

Wymagany zbiornik paliwa co najmniej 100 litrów w ramie agregatu, pozwalający na ciągłą pracę agregatu:
- przy 75% obciążeniu co najmniej 11,6h;
- przy 100% obciążeniu co najmniej 9,7h.

Wymagany pojemnościowy czujnik poziomu paliwa z procentowym wskazaniem na sterowniku, a także wbudowany alarm poziomu paliwa poniżej 15 procent (rezerwa).

Wymagane także wyłączenie agregatu przy 5 procentach poziomu paliwa (zabezpieczenie przed zapowietrzeniem). Wymagany również korek spustowy zbiornika oraz co najmniej jeden niezależny otwór w zbiorniku zaślepiony deklem na śrubach, umożliwiający montaż i podłączenie dodatkowej instalacji paliwowej, lub przeniesienie wlewu paliwa na drugą stronę zbiornika.

Stalowy tłumik dźwięków minimum -35db(A) – wymaga się, aby zabudowany był wewnątrz agregatu.

Wymagania odnośnie do silnika:
- silnik turbodiesel (np. Y4105D lub inny równoważny spełniający wymagania);
- silnik diesla o mocy znamionowej PRP nie mniejszej niż – 38kW;
- liczba i układ cylindrów – 4 L;
- wymagany typ wtrysku – bezpośredni;
- elektroniczna regulacja obrotów;
- podgrzewanie bloku – grzałka silnika kontrolowana przez sterownik agregatu;
- spalanie przy 75% obciążenia nie więcej niż – 8,7 l/h;
- spalanie przy 100% obciążenia nie więcej niż – 10,4 l/h;
- wlew paliwa - korek zamykany kluczykiem, wewnątrz obudowy;

- filtr powietrza suchy;
- silnik chłodzony glikolem;
- prędkość obrotowa – 1500 r.p.m.;
- układ elektryczny 12V;
- akumulator 12V;
- automatyczna ładowarka buforowa akumulatora/ów w czasie czuwania;
- osłona elementów gorących oraz ruchomych.

Wymagania odnośnie do prądnicy:

- wyposażona w automatyczną regulację napięcia;
- obudowa (wg IEC-34-5) - IP23;
- złącze – elastyczny dysk;
- klasa izolacji – H;
- wymagane wykonanie, gdzie stojan prądnicy jest nawinięty z poskokiem 2/3, ponieważ zapewnia to eliminację krotności trzeciej harmonicznej (3, 9, 15, itd.) napięcia wyjściowego. Poskok 2/3 minimalizuje indukowanie się nadmiernych prądów w obwodzie neutralnym;
- wytrzymałość zwarciowa prądnicy >300% obciążenia znamionowego.

Wymagania odnośnie do sterownika:

SMART 500 MKII lub inny równoważny spełniający wszystkie opisane wymagania, z pełną obsługą rozwiązań producenta, z komunikatami w języku polskim, pozwalający na kontrolę parametrów sieci i agregatu (napięć , prądów, mocy, częstotliwości, cosϕ, napięcia ładowania akumulatora, ilość paliwa w zbiorniku, czasu pracy agregatu, parametrów silnika).

Panel sterownika wyposażony w tabliczkę z diodami sygnalizacyjnymi dla łatwej obsługi i szybkiej identyfikacji stanów pracy urządzenia. Wymagana jest identyfikacja alarmów dotyczących działania baterii, pracy alternatora, poziomu paliwa, ciśnienia oleju oraz dwa dodatkowe do zdefiniowania. Sterownik musi posiadać w tylnej ścianie wolne sloty do podłączenia dodatkowych modułów sygnalizacyjnych np. GSM, ETHERNET, styków/wyjść przekaźnikowych dla sygnałów bezpotencjałowych (do zdefiniowania przez użytkownika)

Szafa elektryczna/automatyki agregatu zbudowana na podzespołach renomowanych producentów elektryki i elektroniki, według norm i standardów.

Sterownik musi posiadać - Datakom SMART 500-MK2 - ekonomiczny kontroler agregatu gotowy do integracji BMS i monitorowania poprzez Internet.

Cechy:

- obsługa agregatów na olej napędowy i gaz;
- obsługa 400 Hz;
- dziennik – minimum 400 zdarzeń;
- możliwość edycji wszystkich parametrów na panelu przednim;
- 3-poziomowe hasło konfiguracyjne;
- graficzny wyświetlacz LCD minimum 128x64;

- języki do pobrania (domyślnie – polski);
- wyświetlanie przebiegów napięcia i prądów;
- analiza harmonicznych;
- wyjścia 16 A MCB i GCB;
- 8 konfigurowalnych wejść cyfrowych;
- wejścia rozszerzalne do 40;
- 6 konfigurowalnych wyjść cyfrowych;
- wyjścia z możliwością rozszerzenia do 38;
- 3 konfigurowalne wejścia analogowe;
- zarówno CANBUS-J1939, jak i MPU;
- 3 konfigurowalne alarmy serwisowe;
- tygodniowy harmonogram pracy;
- ręczna „precyzyjna regulacja prędkości” w wybranych ECU;
- automatyczne sterowanie pompą paliwa;
- ochrona przed nadmierną mocą;
- odwrotna ochrona zasilania;
- zabezpieczenie przed przeciążeniem IDMT;
- zrzut obciążenia, obciążenie zastępcze;
- zarządzanie wieloma obciążeniami;
- zabezpieczenie od asymetrii prądu;
- ochrona przed asymetrią napięcia;
- zegar czasu rzeczywistego z podtrzymaniem bateryjnym;
- kontrola prędkości biegu jałowego;
- ładowanie akumulatora włączone;
- wiele parametrów nominalnych;
- napęd Tactor i MCB;
- 4 kwadrantowe liczniki mocy agregatu;
- liczniki zasilania sieciowego;
- wskazania poziomu paliwa;
- wyświetlacz diagnostyczny modemu;
- konfigurowalny przez USB, RS-485 i GPRS;
- darmowy program konfiguracyjny;
- gotowy do centralnego monitorowania;
- obsługa mobilnych agregatów prądotwórczych;
- łatwa aktualizacja oprogramowania sprzętowego USB;
- stopień ochrony IP65 ze standardową uszczelką.

Wymagane pomiary:

- napięcia sieci i agregatu PN / PP;
- częstotliwość sieci i agregatu;
- prądy fazowe sieci i agregatu;
- prądy neutralne sieci i agregatu;
- sieć i agregat, faza i suma, kW, kVA, kVAr, pf;
- prędkość silnika;
- napięcie baterii;
- temperatura silnika;
- ciśnienie oleju;
- zużycie paliwa (dla silników wyposażonych w ECU);

Wymagana komunikacja:

- 4-pasmowy modem GPRS;
- Port USB;
- RS-485 (2400-115200) – opcjonalnie;
- RS-232 (2400-115200);
- J1939-CANBUS;
- centralny monitoring internetowy
- wysyłanie wiadomości SMS;
- wysyłanie e-mail - opcjonalnie
- darmowe oprogramowanie na PC;
- Modbus RTU.

Agregat powinien zapewnić wysyłanie sygnałów alarmowych z wykorzystaniem sieci GSM na trzy podane telefony komórkowe. Wymagane są co najmniej 4 sygnały alarmowe: start agregatu (po zaniku sieci), niski poziom paliwa (rezerwa), stop agregatu (po powrocie sieci), awaria agregatu (alarm globalny).

Zamawiający wymaga także wyposażenia w układ SZR typu RTSE na przełączniku z napędem silnikowym, np. Socomec ATyS d M 63 A lub innym równoważnym spełniającym wymagania.

Wymagany układ SZR zbudowany jest na bazie przełącznika źródła zasilania z napędem silnikowym (1-0-2), składającego się z dwóch niezależnych rozłączników izolacyjnych ze wspólnym napędem silnikowym, z możliwością przełączania elektrycznego w trybie automatycznym oraz ręcznego przy pomocy dołączonej rączki.

Układ SZR musi być zbudowane w oparciu o przełączniki z napędem silnikowym o pozycjach łączeniowych I-0-II. Każdy z przełączników musi składać się z dwóch niezależnych rozłączników wraz z blokadą mechaniczną i elektryczną. Obwody elektryczne obu rozłączników muszą posiadać blokadę elektryczną uniemożliwiającą podanie napięcia na oba rozłączniki jednocześnie.

1. Blokada elektryczna - odpowiednie połączenie modułu sterowania uniemożliwiające równoczesne wysterowanie tych samych pozycji.
2. Blokada mechaniczna – przełącznik źródła zasilana z napędem silnikowym składający się z dwóch niezależnych rozłączników. Zamienne załączenie rozłączników odbywa się z przerwą czasową i przez pozycję 0.
3. Blokada programowa – blokada ta uniemożliwia jednoczesne wysterowanie dwóch przekaźników zabudowanych wewnątrz układu SZR.

Zamienne załączanie rozłączników musi odbywać się z przerwą czasową i zawsze przez pozycję „0”. Dzięki temu nie będzie istniała możliwości (nawet przy uszkodzeniu układu sterowania) jednoczesnego załączenia obu łączników czyli spotkania się napięcia sieci i generatora.

Wymagane tryby sterowania:

1. Sterowanie automatyczne- momencie zaniku napięcia sieci sterownik agregatu musi rozpoczyna odliczanie zaprogramowanej zwłoki czasowej. Po upłynięciu nastawionego czasu i utrzymującego się braku napięcia sieci sterownik musi przełączać się w pozycję „0" i wystawiać sygnał START agregat, który rozpocząć ma procedurę startu silnika napędzającego generator według zaprogramowanych w sterowniku agregatu parametrów (czas startowania i przerwa, ilość możliwych prób startowania itp.). Po pojawieniu się napięcia generatora, sterownik agregatu musi sprawdzać jego parametry (wartość, częstotliwość) i gdy mieszczą się w dopuszczalnych granicach - przełączać układ w pozycję „II" przechodząc przez pozycję „0" i załączać kierunek zasilania z generatora. Tym samym napięcie generatora podawane ma być na odbiory.
2. Powrót napięcia - w momencie ponownego pojawienia się napięcia sieci i jego utrzymywania się przez odpowiedni czas, sterownik agregatu musi przełączać układ w pozycję „I" przechodząc przez pozycję „0" i załączać kierunek zasilania z sieci. Następnie wymagane jest utrzymywanie jeszcze pracę silnika przez określony czas ok. 2 min, w celu umożliwienia wychłodzenia silnika bez obciążenia. Po upłynięciu tego czasu, sterownik agregatu musi samoczynnie wyłączać silnik napędzający generator i wracać do stanu wyjściowego tzn. do czuwania i monitorowania sieci.
3. Sterowanie ręczne mechaniczne- wymagane, aby przełącznik SZR można przestawiać przy pomocy dołączonej rączki. Tryb ma służyć wyłącznie na poczet sytuacji awaryjnych.

Wymagane także zabezpieczenie przed przedostaniem się napięcia generatora na sieć energetyczną. W przypadku wyłączenia energii przez Zakład Energetyczny musi istnieć pewność, że napięcie z agregatu nie przedostanie się do sieci zasilającej. Podobnie rzecz ma się w drugim kierunku -napięcie z sieci nie może zostać podane na agregat. Powyższe należy zapewnić poprzez:

1. Budowa mechaniczna przełącznika – przełącznik źródła zasilania z napędem silnikowym o trzech stabilnych pozycjach 1-0-2, musi składać się z dwóch niezależnych rozłączników 4-polowych izolacyjnych (tory główne) połączonych mechanicznie w sposób uniemożliwiający ich jednoczesne załączenie. Przełączenie źródeł musi odbywać się z przejściem przez pozycję 0.
2. Blokada elektryczna sterowania przełącznika – przełącznik musi posiadać wewnętrzną blokadę uniemożliwiającą równoczesne wysterowanie dwóch pozycji przełącznika. Blokadę elektryczną zapewniać ma także układ mini SZR-a na zasilaniu i sterowaniu przełącznika zbudowany na ministycznikach z własną blokadą mechaniczną i elektryczną.
3. Blokada programowa – blokada ta musi uniemożliwia jednoczesne wysterowanie dwóch przekaźników zabudowanych wewnątrz sterownika agregatu podających sygnały do przełączania SZR-a.

Zamawiający wymaga również, aby przed dostarczeniem agregatu na obiekt możliwe było przeprowadzenie próby FAT urządzenia u producenta, w obecności komisji zamawiającego. Wymaga się dołączenia protokołu z próby FAT do dokumentacji powykonawczej.

Podsumowanie dokumentu:

Wszystkie urządzenia i sprzęty oferowane przez Wykonawcę muszą być fabrycznie nowe i dostarczane z oficjalnych kanałów dystrybucyjnych dostępnych w Polsce. Oprogramowanie oferowane przez Wykonawcę również musi pochodzić z oficjalnych źródeł dystrybucyjnych w Polsce.

W ramach realizacji umowy, Wykonawca jest zobowiązany do zapewnienia usługi transportu, co jest uwzględnione w jego ofercie cenowej. Zamawiający nie wymaga usługi montażu czy konfiguracji, o ile nie zostało to wprost określone przy szczegółowym opisie konkretnego produktu. Zamawiający samodzielnie zajmie się usunięciem zbiorczych elementów opakowania, takich jak kartony, papier czy folia.

Zamawiający dopuszcza możliwość zastosowania rozwiązań równoważnych. W przypadku pojawienia się w specyfikacji odniesień do nazw własnych, znaków towarowych, modeli, czy określonych producentów, należy je rozumieć jako wskazania oczekiwanej jakości oraz efektu końcowego. Przyjęte parametry stanowią standard, do którego Wykonawca musi się odnosić.

Wykonawca ma prawo zaproponować rozwiązania równoważne, pod warunkiem, że spełniają one wymogi jakościowe i funkcjonalne określone w postępowaniu.

Zamawiający nie wymaga korzystania z produktów, materiałów czy urządzeń konkretnego producenta. Wszelkie propozycje rozwiązań równoważnych muszą jednak spełniać minimalne wymagania określone w specyfikacji oraz zapewniać prawidłowe działanie przedmiotu zamówienia. Rozwiązania równoważne muszą odpowiadać przyjętym standardom technicznym i jakościowym.

Przez rozwiązania równoważne rozumie się takie, które gwarantują parametry techniczne, jakościowe i użytkowe nie gorsze od tych wskazanych w opisie przedmiotu zamówienia. Wykonawca, powołując się na rozwiązania równoważne, zobowiązany jest wykazać, że jego oferta spełnia wymagania określone przez Zamawiającego.

Jeśli w opisie przedmiotu zamówienia zostały wskazane konkretne typy, znaki towarowe, marki, producenci, dostawcy, patenty, źródła czy szczególne procesy, które charakteryzują produkty lub usługi, Zamawiający dopuszcza zaproponowanie rozwiązań równoważnych, pod warunkiem, że zapewnią one parametry techniczne nie gorsze od tych określonych oraz będą zgodne z funkcjonalnością użytkową (tożsamość funkcji), parametrami technicznymi (wytrzymałość, trwałość, dane techniczne), bezpieczeństwem użytkowania itd.