Załącznik nr 6 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

INFORMACJE OGÓLNE:

1. Przedmiotem zamówienia jest Dostawa sprzętu komputerowego, oprogramowania wraz z usługą wdrożenia oraz wykonanie audytu, przygotowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), przeprowadzenie szkoleń, usługa SOC w ramach projektu „Podniesienie poziomu cyberbezpieczeństwa w Głubczyckich Wodociągach i Kanalizacji Sp. z o.o." w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo - CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności.

2. Celem zamówienia jest zapewnienie bezpieczeństwa informacji i ciągłości działania systemów IT/OT wykorzystywanych w zarządzaniu infrastrukturą wodociągową, zgodnie z wymogami Krajowego Planu Odbudowy i Zwiększania Odporności.

ZAKRES PRZEDMIOTOWY ZAMÓWIENIA:

Przedmiot zamówienia obejmuje:

1. Zakup sprzętu komputerowego wraz z profesjonalną usługą wdrożenia

2.Zakup oprogramowania wraz z profesjonalną usługą wdrożenia

3.Zakup zintegrowanego systemu bezpieczeństwa wraz z wdrożeniem i usługa SOC

4.Wykonanie audytu bezpieczeństwa IT i OT

5.Przygotowanie dokumentacji SZBI, planów ciągłości działania wraz z audytem SZBI/KRI i szkoleniem

6.Szkolenia dla pracowników, kadry zarządzającej oraz szkolenie powiązane z testami socjotechnicznymi

WYMAGANIA TECHNICZNE I FUNKCJONALNE:

1. Wszystkie dostarczane rozwiązania muszą być fabrycznie nowe, wolne od wad fizycznych i prawnych.

2. Dostarczane oprogramowanie musi być licencjonowane na Zamawiającego, z prawem do użytkowania bezterminowo lub przez okres wskazany w ofercie (min. 36 miesięcy).

3. Wykonawca zapewni kompatybilność wszystkich systemów i możliwość ich integracji.

4. Rozwiązania muszą być zgodne z obowiązującymi normami i standardami (w szczególności: ISO 27001, NIST Cybersecurity Framework, dyrektywa NIS2).

HARMONOGRAM REALIZACJI ZAMÓWIENI:

Szczegółowy harmonogram realizacji zamówienia Wykonawca przekaże w ciągu 10 dni od dnia podpisania umowy.

GWARANCJA I WSPARCIE TECHNICZNE:

1. Wykonawca udzieli gwarancji na dostarczone rozwiązania na okres minimum 36 miesięcy od daty odbioru końcowego.

2. W okresie gwarancji Wykonawca zapewni:

usuwanie wad i usterek w terminie do 2 dni roboczych od zgłoszenia,

helpdesk techniczny (e-mail, telefon) w godzinach 8:00-16:00 dni robocze,

zdalny dostęp do systemów w celu diagnostyki i naprawy (za zgodą Zamawiającego),

aktualizacje oprogramowania i łaty bezpieczeństwa.

WYMAGANIA DODATKOWE:

1. Wykonawca zapewni bezpieczeństwo danych osobowych i poufność informacji podczas realizacji zamówienia (zgodnie z RODO).

2. Wykonawca zobowiązany jest do zachowania poufności informacji uzyskanych w trakcie realizacji zamówienia.

3. Wszelkie prace instalacyjne i konfiguracyjne będą przeprowadzane w uzgodnieniu z Zamawiającym, w sposób minimalizujący zakłócenia w funkcjonowaniu infrastruktury.

4. Wykonawca ponosi odpowiedzialność za szkody powstałe w trakcie realizacji zamówienia.

UWAGA: Opis przedmiotu zamówienia stanowi minimalne wymagania Zamawiającego. Wykonawca może zaoferować rozwiązania o parametrach równoważnych lub lepszych, pod warunkiem spełnienia wszystkich wymagań funkcjonalnych określonych w niniejszym opisie.

WYMAGANIA DOTYCZĄCE KOSZTÓW UTRZYMANIA INFRASTRUKTURY:

Zamawiający dąży do uzyskania rozwiązania charakteryzującego się optymalnym stosunkiem ceny zakupu do kosztów eksploatacyjnych. W interesie Zamawiającego leży wybór systemu bezpieczeństwa, którego długoterminowe utrzymanie nie będzie generować nadmiernych obciążeń finansowych.

W związku z powyższym Zamawiający premiuje systemy tanie w utrzymaniu. Przyjmuje się, że łączny koszt utrzymania infrastruktury przez okres 36 miesięcy (obejmujący licencje, wsparcie techniczne, aktualizacje, usługi SOC oraz inne bieżące koszty eksploatacyjne) **nie może przekroczyć 20% łącznej ceny realizacji zamówienia (cena kwalifikowana, o której mowa w § 4 ust. 2 pkt a) wzoru umowy).**

WAŻNE: Oferty, w których łączny koszt utrzymania infrastruktury przez 36 miesięcy przekroczy 20% ceny realizacji zamówienia, zostaną odrzucone jako niezgodne z wymaganiami określonymi w Specyfikacji Warunków Zamówienia, na podstawie art. 226 ust. 1 pkt 5 ustawy Prawo zamówień publicznych.

Wykonawca zobowiązany jest przedstawić w ofercie szczegółowy harmonogram kosztów utrzymania w rozbiciu miesięcznym (zgodnie z Załącznikiem nr 3 do SWZ), obejmujący wszystkie przewidywane wydatki związane z eksploatacją dostarczonego rozwiązania przez okres 36 miesięcy od dnia odbioru.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA:

I. Przygotowanie dokumentacji SZBI wraz z opracowaniem planów ciągłości działania i odtwarzania po awarii, Audyt Systemu Zarządzania Bezpieczeństwem Informacji, Audyt zgodności KRI/uoKSC przez wykwalifikowanych audytorów. Szkolenia z zakresu cyberbezpieczeństwa – szkolenia dla kadry, istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarzadzania bezpieczeństwem informacji IT/OT/ICS

1. Opracowanie, wdrożenie, przegląd, aktualizację dokumentację wraz z przekazaniem praw autorskich udokumentowanego Systemu Zarządzania Bezpieczeństwem Informacji, Audyt Systemu Zarządzania Bezpieczeństwem Informacji, Audyt zgodności KRI/uoKSC przez wykwalifikowanych audytorów, zgodnie z wymaganiami:
    1) PN-EN ISO/IEC 27001:2023, PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005, PN-EN ISO/IEC 22301 zwanych dalej ISO
    2) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2025 poz. 1703 tj. lub nowsza),
    3) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz. U. z 2026 r. poz. 20 oraz poz. 252) zwanej dalej KSC
    4) 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) zwanej dalej KRI
    5) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) zwanej dalej RODO

2. Szkolenia z zakresu cyberbezpieczeństwa – szkolenia dla kadry, istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarzadzania bezpieczeństwem informacji
3. Zakres przedmiotu zamówienia:

1) Przygotowanie do 10 dni roboczych od dnia podpisania umowy harmonogramu realizacji zamówienia oraz propozycję wstępnie planowanych terminów spotkań przedstawicieli Zamawiającego i Wykonawca z podziałem na poszczególne etapy:
   a. ETAP I wykonanie analizy stanu obecnego,
   b. ETAP II opracowanie wymaganej dokumentacji,
   c. ETAP II wdrożenie przygotowanej dokumentacji
   d. ETAP IV Szkolenia z zakresu cyberbezpieczeństwa – szkolenia dla kadry, istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarzadzania bezpieczeństwem informacji
   e. Etap V Audyt SZBI oraz audyt zgodności wdrożonej dokumentacji z KRI/uoKSC przez niezależnego, wykwalifikowanego audytora
2) W ramach etapu pierwszego Wykonawca przeprowadzi analizę stanu obecnego w zakresie bezpieczeństwa informacji raz ciągłości działania u Zamawiającego.Na podstawie wyników analizy Wykonawca przygotuje raport zawierający: opis stanu obecnego, identyfikację luk i obszarów wymagających poprawy, propozycję koncepcji wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji. Raport zostanie przekazany Zamawiającemu do akceptacji Kryteria odbioru: Raport zaakceptowany przez Zamawiającego.
3) W ramach etapu drugiego Wykonawca opracuje kompletną dokumentację SZBI, Planów Zarządzania Ciągłością Działania (BCB) i Planów Odtwarzania po Awarii (DRP), zgodną z ISO, ustawami o KSC, KRI oraz RODO (w tym przepisami wykonawczymi). Dokumentacja uwzględni wyniki Etapu 1 oraz wymagania wymienionych ustaw i norm.
   Kryteria odbioru: Kompletna dokumentacja przekazana w formie edytowalnej (Word/Excel) i zaakceptowana przez Zamawiającego. Wykonawca uwzględni rekomendacje organizacyjno-techniczne z ww. norm i przepisów, w tym rejestry ryzyka oraz analizę ryzyka.
4) W ramach etapu trzeciego Wykonawca przeprowadzi wdrożenie przygotowanej dokumentacji, uwzględniając wymagania i specyfikę Zamawiającego, poprzez:
   a. Opracowanie i uzgodnienie planu wdrożenia (z harmonogramem i przypisanymi rolami).
   b. Wsparcie w wprowadzeniu procedur do praktyki organizacyjnej
   c. Przekazanie raportu z wdrożenia z listą wdrożonych elementów i rekomendacjami.

   Kryteria odbioru: Raport z wdrożenia zaakceptowany przez Zamawiającego.

5) W ramach etapu czwartego Wykonawca przeprowadzi szkolenie z zakresu wdrażanego SZBI i PBI odpowiednio do zdefiniowanych ról oraz stanowisk pracy. Szkolenia muszą być sprofilowane i dostosowane do ról pełnionych w organizacji (np. Zarząd, administracja, pracownicy techniczni IT/OT). Wykonawca przedstawi Zamawiającemu do akceptacji szczegółowy program szkolenia dla poszczególnych ról wraz z harmonogramem planu szkoleń na min. 14 dni przed planowanym rozpoczęciem szkoleń. Program szkoleń musi obejmować ogólny zakres zagadnień min.:
   a. Struktura i cele Systemu Zarządzania Bezpieczeństwem Informacji,
   b. Aspekt praktyczny wdrożenia SZBI, rola i odpowiedzialność kierownictwa oraz pracowników w jego funkcjonowaniu,
   c. Polityki i procedury związane z bezpieczeństwem informacji,
   d. Rodzaje i rozpoznawanie zagrożeń oraz ich wpływ na działalność organizacji,
   e. Konsekwencje zagrożeń związanych z ryzykiem utraty danych, naruszeniem bezpieczeństwa informacji,
   f. Ochrona danych i informacji, w tym podstawowe zasady ochrony danych osobowych i informacji wrażliwych, zgodnie z obowiązującymi przepisami (np. RODO) oraz metody i zastosowane techniki zabezpieczeń,
   g. Zasady bezpiecznego korzystania z infrastruktury IT oraz z systemów informatycznych,
   h. Reagowanie na incydenty bezpieczeństwa, w tym procedury zgłaszania incydentów bezpieczeństwa oraz sposoby ich dokumentowania,
   i. Metody ciągłego doskonalenia SZBI - audyty oraz działania korygujące
   j. Podnoszenie świadomości oraz kompetencji z zakresu bezpieczeństwa informacji jako proces przy pełnym udziale kierownictwa oraz pracowników w organizacji,

   Kryteria odbioru: Potwierdzenia udziału (program szkoleń, listy obecności, testy wiedzy).

6) W ramach etapu V Wykonawca zapewni przeprowadzenia audytu SZBI oraz audyt zgodności z KRI, KSC przez niezależnego, wykwalifikowanego audytora, który dokona oceny funkcjonowania SZBI i przestawi jego wyniki w formie raportu z audytu.
   Kryteria odbioru: Raport z audytu przekazany i zaakceptowany przez Zamawiającego.
7) Wykonawca w dokumentacji uwzględni rekomendacji organizacyjno-technicznych ń norm PN-EN ISO/IEC 27001:2023, PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005 oraz PN-EN ISO/IEC 22301, ustawy KSC, KRI, RODO

8) Wykonawca uwzględnienie w dokumentacji wymagań wynikających z ww. ustaw oraz powiązanych przepisów wykonawczych.
9) Opracowanie polityk, procedur, instrukcji, rejestrów, wzorów dokumentów i pozostałych elementów wymaganych przez normy i przepisy prawa.
10) Przygotowanie rejestrów ryzyka oraz analizy ryzyka.

4. Dokumentacja powstała w wyniku realizacji zamówienia musi:
   1) Być spójna, aktualna, logicznie uporządkowana oraz przygotowana w sposób umożliwiający wdrożenie i utrzymanie SZBI, BCP, DRP przez Wykonawcę u Zamawiającego.
   2) Sporządzona w formie pisemnej w języku polskim i zostać przekazana w wersji edytowalnej oraz w wersji nieedytowalnej (PDF).
   3) Obejmować pełny zakres wymagany do zgodności z PN-EN ISO/IEC 27001:2023, PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005 i PN-EN ISO/IEC 22301, ustawy KSC, KRI, RODO w tym wszystkie dokumenty obligatoryjne oraz dodatkowe dokumenty niezbędne dla spełnienia wymagań prawnych i organizacyjnych Zamawiającego.
5. Wymagania ogólne:
   1) Wykonawca zapewni i przygotuje rozwiązanie do komunikacji zdalnej oraz prowadzenia repozytorium dokumentacji zawierającą wszystkie uzgodnienia, notatki, raporty powiązane z realizacją zamówienia oraz dokumentację opracowaną w ramach realizacji umowy.
   2) Zamawiający dopuszcza możliwość prowadzenia spotkań, wywiadów drogą zdalną (z wykorzystaniem dostarczonego przez Wykonawcę systemu do komunikacji zdalnej), w sytuacji, w której w trakcie tych spotkań nie ma potrzeby bezpośredniego dostępu do zasobów/aktywów na miejscu w siedzibie Zamawiającego
   3) Zamawiający zastrzega sobie prawo do wnoszenia uzasadnionych uwag do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany do uwzględnienia w dokumentach uwag wniesionych przez Zamawiającego o ile proponowane zmiany nie mają wpływu na prawidłową realizację umowy przez Wykonawcę o czym Wykonawca poinformuje Zamawiającego.
   4) Każdy etap prac uznaje się za zakończony po przyjęciu przez obie strony raportu z zakończenia prac danego etapu.
   5) Informacje, które będą przekazywane w celu realizacji niniejszego projektu, stanowią informacje chronione, w związku z tym realizacja projektu będzie wymagała akceptacji zapisów o zachowaniu poufności i zapewnieniu stosownej ochrony, w tym również dla danych osobowych
   6) Zamawiający wymaga przeniesienia na Zamawiającego przez Wykonawcę autorskich praw majątkowych do wszystkich dokumentów przekazanych jako produkty zamówienia.
   7) Po zakończeniu szkoleń Wykonawca przeprowadzi test sprawdzający wiedze uczestników szkolenia oraz przekaże Zamawiającemu kompletną dokumentację potwierdzającą ich przeprowadzenie (programy, listy obecności, wyniki testów)
   8) W przypadku, gdy audyty wykonane w etapie V wykażą braki lub niezgodności Wykonawca dokona poprawek do przygotowanej dokumentacji w ramach umowy.

II. Szkolenia z zakresu cyberbezpieczeństwa - podstawowe szkolenia budujące świadomość cyber zagrożeń i sposobów ochrony dla pracowników IT/OT/ICS

1. Przedmiot zamówienia

Przedmiotem zamówienia jest zaprojektowanie, przygotowanie oraz przeprowadzenie kompleksowych szkoleń e-learningowych z zakresu cyberbezpieczeństwa, z uwzględnieniem aktualnych zagrożeń, wymagań organizacyjnych oraz obowiązujących regulacji, w szczególności dyrektywy NIS2 oraz najlepszych praktyk bezpieczeństwa informacji.

Szkolenia są przeznaczone dla wszystkich pracowników Zamawiającego, w tym w szczególności dla:

- kadry zarządzającej,
- pracowników administracyjno-biurowych,
- personelu technicznego i IT,

Celem zamówienia jest:

- podniesienie poziomu świadomości cyberzagrożeń,

- ograniczenie ryzyka incydentów powodowanych przez czynnik ludzki,
- zwiększenie zgodności organizacji z wymaganiami NIS2, RODO oraz norm ISO,
- wzmocnienie kultury bezpieczeństwa informacji w organizacji.

2. Zakres merytoryczny szkoleń

Zakres szkolenia obejmuje kompleksowy program edukacyjny, podzielony na niezależne, logiczne moduły tematyczne. Każdy moduł zakończony jest pytaniami sprawdzającymi wiedzę uczestnika, a całość szkolenia – egzaminem końcowym.

Zamawiający dopuszcza elastyczny podział tematów, o ile wszystkie poniższe obszary zostaną w pełni omówione.

Struktura i zakres merytoryczny:

A. Wprowadzenie do cyberbezpieczeństwa i dyrektywy NIS2

- Cyberbezpieczeństwo – podstawowe pojęcia, role i znaczenie
- NIS2 w pigułce – zakres stosowania, podmioty objęte, kluczowe obowiązki
- Obowiązki raportowania incydentów (24h / 72h / 30 dni)
- Kultura bezpieczeństwa – rola każdego pracownika

B. Podstawy cyberbezpieczeństwa

- Triada CIA, różnice IT / OT / IoT / ICS
- Typowe wektory ataków
- Model Cyber Kill Chain oraz MITRE ATT&CK – wersja dla nie techników
- Ryzyko: zagrożenia, podatności, skutki i mechanizmy kontroli
- Aktualne trendy zagrożeń (deepfake, QRishing, MFA fatigue)
- Dobre praktyki użytkownika (zasada najmniejszych uprawnień, aktualizacje, backupy)

C. Socjotechnika i phishing

- Rodzaje ataków: phishing, spear-phishing, whaling, smishing, vishing, search engine phishing
- Anatomia fałszywej wiadomości (nagłówki, linki, domeny, DKIM/SPF/DMARC)
- Złośliwe oprogramowanie dystrybuowane poprzez phishing
- QRishing i ataki w przestrzeni fizycznej
- Symulator phishingowy – 10 wiadomości + ocena ryzyka
- Weryfikacja wiarygodności stron i formularzy
- Procedura postępowania po kliknięciu / utracie poświadczeń

D. Hasła, MFA i nowoczesne uwierzytelnianie

- Dlaczego hasła zawodzą (reuse, wycieki, brute-force, credential stuffing)
- Silne frazy hasłowe, menedżer haseł – najlepsze praktyki
- MFA / 2FA w praktyce: TOTP, FIDO2 / Passkeys, push notifications
- Ryzyka związane z MFA (MFA fatigue, SIM-swapping)

E. Poczta elektroniczna, social media, komunikatory i urządzenia mobilne

- Bezpieczna poczta: załączniki, makra, linki, spoofing, DLP
- Media społecznościowe: OSINT, oversharing, impersonacja, deepfake
- Komunikatory i VoIP – phishing przez chat, podsłuch, prywatność
- Urządzenia mobilne: zagrożenia, MDM, złośliwe aplikacje

F. Incydenty i studia przypadków (ze szczególnym uwzględnieniem OT/ICS)

- Stuxnet, Industroyer 2, ataki na wodociągi i uzdatnianie wody
- Norsk Hydro – lekcje z ransomware
- Incydenty sektorowe (energia, transport, zdrowie, administracja)

- Analiza przyczyn rzeczywistych wycieków danych

G. Kradzież tożsamości i ochrona danych osobowych

- Metody pozyskiwania danych (phishing, OSINT, infostealer, wycieki)
- Objawy przejęcia tożsamości i natychmiastowe działania
- Ochrona danych w praktyce (MFA, monitoring, alerty)

H. Malware, ransomware oraz zagrożenia sprzętowe

- Rodzaje malware (ransomware, trojany, keyloggery, botnety)
- Ataki MITM i podsłuch w sieciach Wi-Fi
- Urządzenia typu Flipper Zero, USB Rubber Ducky – realne ryzyko vs mity
- Strategia backupów 3-2-1 + testy odtwarzania

I. Bezpieczeństwo aplikacji i zarządzanie podatnościami

- Jak powstają podatności (błędy programistyczne, konfiguracja, EOL)
- OWASP Top 10 – wersja zrozumiała dla nie techników
- Shadow IT i nieautoryzowane narzędzia

J. Bezpieczeństwo OT/ICS – podstawy dla wszystkich pracowników

- Różnice IT vs OT, model Purdue
- Dlaczego systemy OT są szczególnie narażone
- Typowe scenariusze ataków na sektor energetyczny, wodny, transport i ochronę zdrowia
- Podstawowe dobre praktyki operacyjne w OT

K. Reagowanie na incydenty i raportowanie (NIS2)

- Cykl życia incydentu
- Wymagania raportowe NIS2 (progi istotności, terminy)
- Praktyczne playbooki: phishing, ransomware, utrata urządzenia, wyciek danych

3. Forma realizacji szkoleń

Szkolenia zostaną:

- zrealizowane w formule e-learningowej,
- udostępnione na platformie szkoleniowej Wykonawcy do 31.12.2026,
- zakończone testami cząstkowymi oraz egzaminem końcowym.

Po pozytywnym zaliczeniu egzaminu uczestnik otrzyma imienny certyfikat ukończenia szkolenia.

4. Wymagania techniczne.

- System musi być dostępny poprzez przeglądarkę internetową bez konieczności instalacji dodatkowego oprogramowania po stronie użytkownika.
- Interfejs użytkownika musi być dostępny w języku polskim

4.1 System musi mieć możliwość zarządzania użytkownikami

4.2 System musi mieć możliwość zarządzanie kursami

4.3 System musi posiadać funkcję oceniania i raportowania

- dziennik ocen,
- raporty postępów,

- eksport danych.

5.1 Bezpieczeństwo

- System musi zapewniać:
    - szyfrowanie transmisji (HTTPS),
    - kontrolę dostępu,
    - rejestrowanie zdarzeń.
- System musi być zgodny z przepisami:
    - RODO (GDPR),
    - krajowymi regulacjami dotyczącymi ochrony danych.
- Kopie zapasowe muszą być przechowywane wyłącznie w centrach danych na terenie Polski.

5.3 Niezawodność i dostępność

- SLA min. 99,5%,
- backup i disaster recovery realizowane w obrębie Polski,
- monitoring systemu.

5.5 Interfejs użytkownika

- responsywność (RWD),
- obsługa urządzeń mobilnych,
- możliwość personalizacji.

7. Wymagania organizacyjne

- Platforma szkoleniowa musi być dostępna do 31.12.2026:
    - utrzymywana w bezpiecznym centrum danych na terenie Polski,
    - zgodna z normami ISO/IEC 27001, 27017, 27018 lub równoważnymi.
- Materiały szkoleniowe:
    - przygotowane w języku polskim,
    - aktualne względem stanu wiedzy i regulacji,
- Każdy moduł zawiera:
    - treść edukacyjną,
    - pytania sprawdzające,
    - egzamin końcowy obejmujący cały zakres szkolenia.
- Certyfikat ukończenia szkolenia zawiera:
    - imię i nazwisko uczestnika,

- nazwę szkolenia,
- datę ukończenia,

8. Wymagania wobec Wykonawcy

Wykonawca:

- zapewni realizację szkolenia przez osoby z doświadczeniem w obszarze cyberbezpieczeństwa,
- dostarczy autorskie, rzetelne materiały szkoleniowe,
- zapewni aktualność szkoleń w trakcie realizacji zamówienia.
- Zapewni dostęp do konsultantów w wymiarze do 4 h dla kadry zarządzającej po zakończonym procesie szkoleniowym (zdany egzamin)
- Wykonawca musi jednoznacznie wskazać:
  - lokalizację centrum danych (adres lub operator),
  - model hostingu (dedykowany / chmura prywatna / kolokacja).
- Wykonawca musi zapewnić:
  - wsparcie techniczne.

9. Odbiór i rozliczenie

Za należyte wykonanie zamówienia uznaje się:

- uruchomienie szkoleń,
- przeprowadzenie egzaminów,
- wydanie certyfikatów

III. Szkolenie z zakresu cyberbezpieczeństwa. Szkolenie specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu grantowego IT/OT/ICS

Zakres szkolenia:

Szkolenie specjalistyczne dedykowane dla dwóch grup:

- **Kadry zarządzającej** (dyrekcja, kierownictwo)
- **Specjalistów IT/OT/ICS** (administratorzy, osoby techniczne)

Główny cel szkolenia: Przedstawienie i omówienie wdrożonych oraz planowanych rozwiązań bezpieczeństwa w ramach realizowanego projektu grantowego, ich celu, zasad działania oraz roli w podniesieniu poziomu bezpieczeństwa organizacji.

Zakres merytoryczny (ogólny):

1. **Kontekst projektu grantowego** Cele cyberbezpieczeństwa projektu, przyjęta architektura bezpieczeństwa IT/OT oraz powiązanie z wymaganiami regulacyjnymi (m.in. NIS2).
2. **Zastosowane i planowane środki ochrony** Omówienie kluczowych mechanizmów bezpieczeństwa wdrożonych w projekcie (m.in. segmentacja sieci, kontrola dostępu, monitoring, ochrona przed ransomware, zdalny dostęp, ochrona systemów OT/ICS).
3. **Rola i odpowiedzialność kadry zarządzającej** Cyberbezpieczeństwo z perspektywy biznesowej, zarządzanie ryzykiem, raportowanie incydentów, BCP/DR oraz ocena efektywności inwestycji.
4. **Aspekty techniczne dla specjalistów IT/OT** Zasady działania wdrożonych rozwiązań, ich konfiguracja, integracja oraz najlepsze praktyki eksploatacji w środowisku IT/OT/ICS.

5. **Warsztaty i ćwiczenia praktyczne** Analiza rzeczywistych rozwiązań z projektu, omówienie scenariuszy incydentów oraz procedur reagowania.
6. **Podsumowanie i rekomendacje** Ocena bieżącego stanu bezpieczeństwa oraz wskazanie kierunków dalszego rozwoju.

Forma realizacji:

- Szkolenie stacjonarne / hybrydowe
- Podział na sesje dla zarządu i dla zespołu technicznego (lub wspólne)

IV. Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami

W pierwszej kolejności należy przeprowadzić kontrolowaną kampanię phishingowa, po której odbędzie się szkolenie wykorzystujące rzeczywiste wyniki symulacji jako główny przykład praktyczny. Po kampanii należy dokonać szczegółowej analizy reakcji pracowników (ze szczególnym uwzględnieniem osób odpowiedzialnych w ramach SZBI) oraz wskazanie konkretnych obszarów wymagających poprawy.

Zakres realizacji:

A. Szkolenie i kampania (testy socjotechniczne)

1. Kampania phishingowa (testy socjotechniczne)

Przeprowadzenie realistycznej, kontrolowanej kampanii phishingowej mającej na celu symulację rzeczywistych ataków socjotechnicznych. Kampania będzie obejmować m.in. próby:

- wyłudzenia danych dostępowych do systemów wewnętrznych,
- wyłudzenia informacji finansowych,
- przejęcia kont firmowych,
- wprowadzenia złośliwego oprogramowania.

Celem kampanii jest identyfikacja słabych punktów w organizacji oraz podniesienie świadomości personelu poprzez pokazanie rzeczywistych mechanizmów ataków.

2. Szkolenie

Forma: zdalna lub stacjonarna **Maksymalna liczebność grupy:** 30 osób **Czas trwania:** do 6 godzin (1 dzień)

Zakres merytoryczny szkolenia:

I. Zagrożenia w cyberprzestrzeni

- Phishing (w tym: phishing, spear phishing, whaling, smishing, vishing, phishing wyszukiwarkowy)
- Ransomware
- Wycieki danych
- Ataki na urządzenia IoT
- Omówienie rzeczywistych, aktualnych incydentów bezpieczeństwa

II. Zasady cyberhigieny i bezpieczeństwa

- Bezpieczeństwo haseł i autoryzacji
- Bezpieczna praca z pocztą elektroniczną
- Bezpieczeństwo urządzeń mobilnych
- Bezpieczne korzystanie z urządzeń drukujących i nośników USB
- Bezpieczne korzystanie z Internetu i mediów społecznościowych

III. Warsztaty praktyczne

- Bezpieczne przekazywanie wrażliwych danych
- Bezpieczna praca w Internecie

- Praktyczne korzystanie z menedżera haseł
- Podstawy OSINT (biały wywiad) – jak chronić organizację przed pozyskiwaniem informacji o sobie

V. Klaster dwóch serwerów pod rozwiązania bezpieczeństwa posiadający rozwiązania: system typu SAN, RAID,, serwer do systemu wirtualizacji, Serwer w HA, Usługi konfiguracji i hardeningu systemów/urządzeń.

Komponent	Parametr/warunek
Serwer	Serwer fabrycznie nowy, nie powystawowy, nierekondycjonowany, nie poleasingowy, nie będący przedmiotem prezentacji - rok produkcji nie starszy niż: 2026. Obsługujący system typu SAN, RAID, spięty w klaster HA, wraz z usługą konfiguracji i harderingu. Z usługi konfiguracji i harderingu należy przygotować raport zawierający zakres wykonanych czynności konfiguracyjno/zabezpieczających. Dostarczony sprzęt musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski.
Przeznaczenie	Serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA dla OT i IT
Ilość	2 szt.
Obudowa	Do instalacji w szafie Rack 19”, wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych oraz ramieniem do mocowania kabli. Wszystkie wyspecyfikowanie elementy serwera muszą być w niej zamontowane
Procesor	Zainstalowany jeden procesory minimum 16 rdzeniowy min. 3.2 GHz Wynik wydajności procesora nie powinien być niższy niż 380 punkty base w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org), dla serwera oferowanego producenta.
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania min. dwóch procesorów
Pamięć operacyjna	Zainstalowane minimum 256 GB pamięci RAM działających z maksymalną prędkością przewidzianą przez producenta procesora. Minimum 32 sloty na pamięć. Możliwość rozbudowy do min. 8TB RAM.
Zabezpieczenie pamięci	Min. Memory mirroring, ECC,
Procesor Graficzny	Zintegrowana karta graficzna osiągająca rozdzielczość min. 1920x1200
Dyski	W chwili dostawy serwer musi posiadać zainstalowane 2 sztuki dysków SSD o pojemności min. 480GB każdy połączonych w raid 1.
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 1000W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Interfejsy sieciowe	- Zainstalowana jedna min. 2 portowa karta 10Gb - Zainstalowana jedna dwu portowa karta/ lub dwie karty jednoportowe SAN FC/ISCSI kompatybilna z dostarczaną macierzą Jeden port RJ-45 o przepustowości min. 1GbE dedykowany dla karty zarządzającej. - Wykonawca musi dostarczy niezbędne okablowanie, wkładki potrzebne do podłączenia serwera z macierzą oraz switchem warstwy Core . Wszystkie dostarczone elementy muszą być kompatybilne z oferowanym sprzętem
Sloty I/O	Serwer w momencie dostawy powinien posiadać wolne min. 2 sloty PCIe x16

Dodatkowe porty	• z przodu obudowy: min. 1x USB, zewnętrzny dedykowany port diagnostyczny, możliwość instalacji portu video cyfrowego lub analogowego, • z tyłu obudowy: min. 2x USB ,1x VGA, 1x RJ-45 do zarządzania serwerem. • wewnątrz obudowy: min. 1x USB
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, Minimalne wymagania: • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty, zasilacze, wentylatory • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. • Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Zdalne włączanie/wyłączanie/restart • Pod montowanie lokalnych mediów • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • SSH • Możliwość mapowania obrazów ISO
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
Systemy operacyjne	Wspierane systemy min. Microsoft Windows Server 2022, 2025; Red Hat Enterprise Linux, SUSE Linux Enterprise Server 15 SP5, VMware vSphere (ESXi).
Gwarancja	Min. 36 miesięcy gwarancji producenta z reakcją NBD w trybie 24/7. Zamawiający wymaga, aby Serwis gwarancyjny świadczony był wyłącznie przez producenta oferowanego sprzętu lub przez jego autoryzowany serwis, w tym celu Wykonawca wykupi/zapewni pełne wsparcie producenta dla Zamawiającego przez okres obowiązywania Gwarancji.

VI. Profesjonalna usługa wdrożenia dla klastra dwóch serwerów

W ramach profesjonalnej usługi wdrożenia należy wykonać:

1. Przygotowanie i dostawa

- Dostarczenie serwerów zgodnego ze specyfikacją techniczną z OPZ
- Dostarczenie wszystkich niezbędnych akcesoriów, kabli, szyn montażowych (rail kit)
- Zapewnienie wymaganych licencji

2. Montaż i instalacja fizyczna / logiczna

- Transport i wniesienie sprzętu do serwerowni Zamawiającego na pierwszym pietrze bez Windy.
- Montaż w szafie rack (w tym okablowanie zasilające i sieciowe).
- Instalacja systemu hypervisora wirtualizacyjnego
- Konfiguracja poziomu sprzętowego (RAID, BIOS/UEFI, ustawienia karty do zarządzania, aktualizacja firmware'u).

3. Konfiguracja podstawowa i zaawansowana

- Konfiguracja sieci (adresy IP, VLAN-y, bonding/teaming, firewall).
- Konfiguracja pamięci masowej (RAID levels, partycjonowanie, integracja z dostarczaną macierzą SAN).
- Ustawienie wysokiej dostępności HA.
- Konfiguracja backupu i snapshotów
- Wdrożenie zasad bezpieczeństwa (hardening serwera zgodnie z dobrymi praktykami, np. CIS Benchmarks, KRI).
- Integracja z istniejącą infrastrukturą Zamawiającego

4. Testy i odbiory

- Przeprowadzenie testów funkcjonalnych, obciążeniowych, wydajnościowych i sprawdzenie poprawności działania HA.
- Sporządzenie protokołów testów i usunięcie ewentualnych usterek.
- Ostateczny odbiór techniczny przez Zamawiającego.

5. Dokumentacja

- Przygotowanie pełnej dokumentacji powdrożeniowej, w tym:
  - Dokumentacja techniczna konfiguracji serwera
  - Instrukcje administracyjne
  - Schematy połączeń
  - Spis haseł i certyfikatów (w bezpiecznej formie)
  - Opis wykonanych prac

VII. Macierz dyskowa posiadająca rozwiązania: macierz dyskowa, RAID, SAN

Komponent	Parametr/warunek
Macierz dyskowa	Macierz fabrycznie nowa, nie powystawowa, nierekondycjonowana, nie poleasingowa, nie będąca przedmiotem prezentacji - rok produkcji nie starszy niż: 2026.
Przeznaczenie	Macierz dyskowa niezbędna do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa w tym usług HA dla OT i IT
Obudowa	Macierz musi mieć możliwość zainstalowania w standardowej szafie rack 19". Rozmiar jednostki sterującej macierzą nie może przekraczać 2U. Możliwość montażu min. 24 dysków Możliwość rozbudowy o dodatkowe półki
Kontrolery	Wymagane dwa moduły sterujące macierzą pracujące w trybie active-active. W przypadku wystąpienia awarii sprawny moduł musi automatycznie przejąć obsługę wszystkich zasobów prezentowanych przez macierz. Kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC i LAN.
Dostępne porty	Oferowana macierz musi posiadać w chwili dostawy minimum po 4 porty SAN FC/ISCSI na kontroler (w sumie 8 portów na macierz), które mają możliwość pracy z prędkością min. 10 Gb. Do każdego z kontrolerów musi być dostarczone po 2 wkładki min. 10Gb wraz z kablami światłowodowymi o długości min. 5m lub kable DAC 10Gb o długości min. 5 m.

	Wykonawca musi dostarczy niezbędne okablowanie, wkładki potrzebne do podłączenia macierzy z serwerami oraz switchami warstwy Core. Wszystkie dostarczone elementy muszą być kompatybilne z oferowanym sprzętem
Cache	Każdy z modułów sterujących (kontroler) musi być wyposażony w min 24GB pamięci cache zabezpieczonej mechanizmem mirroringu. Pamięć podręczna musi być zabezpieczona przed utratą danych w przypadku zaniku zasilania. Ponadto macierz musi umożliwiać utworzenie dedykowanej przestrzeni SSD stanowiącej pamięć cache pośredniczącą w operacjach odczytów danych z macierzy.
Dyski	Macierz musi obsługiwać dyski min. SSD, SAS, NL-SAS. Macierz w momencie dostarczenia musi być wyposażona w minimum 4 dyski 2,5" SAS SSD o pojemności minimum 1.94 TB każdy oraz 12 dysków 2.5 cala HDD SAS 10 K min. 2.4 TB każdy
Funkcjonalność	-Macierz musi obsługiwać typy protekcji RAID min. 1,5,6,10 -Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie dynamicznego alokowania przestrzeni dyskowej (tzw. *„thin provisioning"*). -Macierz musi posiadać automatyczny monitoring z możliwością informowania o awariach poprzez protokół smtp oraz snmp oraz możliwość wysyłania powiadomień awarii do wskazanych odbiorców. -Macierz musi mieć możliwość wykonywania minimum 512 kopii migawkowych -Macierz musi umożliwiać asynchroniczną replikację danych -Możliwość tworzenia logicznych odseparowanych volumenów(LUN). -Macierz musi posiadać funkcjonalność klonowania danych. -Macierz musi umożliwiać konfigurację spare -Wymagane wielopoziomowe zarządzanie dostępami do macierzy z podziałem na możliwość modyfikacji konfiguracji oraz możliwość tylko odczytu. -Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwiema ścieżkami).
Licencje	Dostarczona macierz musi posiadać wszystkie dostępne w niej funkcjonalności. Jeśli wymagane są do tego celu licencje, to należy je dostarczyć.
Zarzadzanie macierzą	Dostępne dwa porty 1Gbe Base-T Zarządzanie macierzą powinno być możliwe za pomocą graficznego interfejsu użytkownika dostępnego poprzez protokół https, oraz za pomocą linii komend cli osiągalnej poprzez protokół ssh. Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control.
Inne	-Wymagana jest bezprzerwowa wymiana następujących elementów macierzy: kontrolery, moduły I/O, dyski, zasilacze oraz moduły SFP+. -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. -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. Obsługa systemów operacyjnych hosta: Microsoft Windows Server; Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise Server (SLES); VMware vSphere
Gwarancja	36 miesięcy gwarancji producenta on-site z czasem reakcji NBD. Serwis świadczony przez producenta macierzy lub przez autoryzowanego partnera serwisowego. Dyski w razie awarii pozostają własnością zamawiającego. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.

VIII. Profesjonalna usługa wdrożenia dla macierzy dyskowej

W ramach profesjonalnej usługi wdrożenia należy wykonać:

1. Przygotowanie i dostawa

- Dostarczenie fabrycznie nowej macierzy dyskowej zgodnej ze szczegółową specyfikacją techniczną z OPZ
- Dostarczenie wszystkich niezbędnych komponentów: dyski, wkładki SFP/QSFP, licencje
- Zapewnienie licencji na wymaganą pojemność użytkową i funkcjonalności

2. Montaż i instalacja fizyczna

- Transport i wniesienie sprzętu do serwerowni Zamawiającego na pierwszym piętrze bez windy.
- Montaż macierzy i ewentualnych półek dyskowych w szafie rack 19" (w tym okablowanie zasilające redundantne).
- Utylizacja opakowań na koszt Wykonawcy.
- Podłączenie zasilania, sieci SAN, LAN – dostarczenie i instalacja wszystkich kabli

3. Konfiguracja podstawowa i zaawansowana

- Aktualizacja firmware'u kontrolerów, dysków i wszystkich komponentów do najnowszej wersji zalecanej przez producenta.
- Konfiguracja kontrolerów w trybie active-active
- Stworzenie puli dyskowej / RAID
- Konfiguracja LUN-ów / wolumenów / share'ów plikowych zgodnie z wymaganiami Zamawiającego.
- Konfiguracja ścieżek multipathing (minimum 2 niezależne ścieżki do każdego hosta).
- Integracja z istniejącą infrastrukturą:
    - Serwerami fizycznymi i wirtualnymi dostarczanymi w ramach Zamówienia
    - Przełącznikami
    - Systemem backupu
    - Monitoringiem (SNMP, email)
- Hardening macierzy (zabezpieczenie dostępu: HTTPS, SSH, wyłączenie niepotrzebnych protokołów, silne hasła, ewentualnie integracja z AD/LDAP).

5. Testy i odbiory

- Przeprowadzenie testów wydajnościowych (IOPS, throughput) –
- Testy funkcjonalne: snapshoty, odtwarzanie, failover, thin provisioning,
- Testy wysokiej dostępności i odporności na awarię kontrolera/dysku/ścieżki.
- Sporządzenie protokołów testowych i usunięcie usterek.
- Ostateczny odbiór techniczny przez Zamawiającego.

6. Dokumentacja

- Pełna dokumentacja powdrożeniowa w języku polskim, zawierająca:
    - Schemat architektury i połączeń
    - Konfigurację macierzy (pool'e, LUN-y, polityki, snapshoty)
    - Opis ustawień bezpieczeństwa
    - Instrukcje administracyjne
    - Spis licencji i haseł (w bezpiecznej formie)
    - Rozwiązywania problemów

IX. Oprogramowanie do wirtualizacji, usługi konfiguracji i hardeningu systemów/urządzeń.

Przedmiotem dostawy jest system wirtualizacyjny, na którym zostaną zainstalowane produkty z zakresu cyberbezpieczeństwa wraz z usługą harderingu systemu o parametrach:

1. Wymagania ogólne i Architektura

- **Typ rozwiązania:** Oprogramowanie typu Hypervisor natywny (Type 1 / Bare-Metal), instalowane bezpośrednio na zasobach sprzętowych serwera.
- **Generacja maszyn VM:** Pełna obsługa maszyn wirtualnych I generacji (Generation 1 w trybie legacy) i II generacji (Generation 2), wspierających UEFI, Secure Boot oraz architekturę 64-bitową bez emulacji urządzeń typu Legacy.

- **Skalowalność pojedynczej VM:** Możliwość przydzielenia do jednej maszyny wirtualnej minimum **32 procesorów wirtualnych (vCPU)** oraz min. **1 TB pamięci RAM**.
- **Format dysków:** Obsługa standardu **VHDX** pozwalającego na tworzenie wolumenów o rozmiarze min. **64 TB** z wbudowaną ochroną metadanych przed skutkami nagłej utraty zasilania.

2. Integracja z Macierzą Dyskową poprzez SAN

- **Obsługa protokołu sieci SAN FC/ISCSI:** Natywne wsparcie dla komunikacji z macierzą poprzez interfejs FC/ISCSI w topologii z przełącznikami (Fabric) oraz w połączeniu bezpośrednim (**Direct Attach / Point-to-Point**).
- **Wirtualny Fibre Channel (vFC):** Możliwość mapowania fizycznych portów HBA hosta bezpośrednio do maszyn wirtualnych (z wykorzystaniem NPIV), umożliwiając maszynom VM bezpośredni dostęp do LUN-ów macierzy.
- **Mechanizm MPIO:** Pełna obsługa wielościeżkowości (Multi-Path I/O) z wykorzystaniem modułów **DSM (Device Specific Module)** dostarczanych przez producenta macierzy, w celu zapewnienia redundancji i równoważenia obciążeń.
- **Optymalizacja Storage:** Wsparcie dla technologii **ODX (Offloaded Data Transfer)** – system musi oddelegować operacje kopiowania danych bezpośrednio na kontrolery macierzy, oraz technologii **UNMAP (SCSI)** w celu automatycznego odzyskiwania wolnego miejsca na macierzy.

3. Wysoka Dostępność i Mobilność (Klastrowanie)

- **Live Migration:** Możliwość przenoszenia działających maszyn wirtualnych między węzłami klastra bez przerywania dostępności usług, z wykorzystaniem akceleracji sprzętowej (RDMA) lub kompresji.
- **Storage Migration:** Funkcja przenoszenia plików dysków maszyn VM pomiędzy różnymi zasobami pamięci masowej w trybie online (bez wyłączania VM).
- **Cluster Shared Volumes (CSV):** Wsparcie dla współdzielonego systemu plików pozwalającego wielu hostom na jednoczesny dostęp do tych samych wolumenów macierzy FC.
- **Dynamic Memory:** System musi dynamicznie zarządzać pamięcią RAM maszyn wirtualnych, oddając nieużywane zasoby do puli hosta (Memory Ballooning).

4. Bezpieczeństwo

- **Virtual TPM (vTPM):** Możliwość przypisania wirtualnego modułu TPM 2.0 do każdej maszyny VM w celu obsługi szyfrowania BitLocker oraz wymogów nowoczesnych systemów operacyjnych.
- **Shielded VMs:** Obsługa izolowanych maszyn wirtualnych chroniących dane przed nieautoryzowanym dostępem na poziomie administratora hosta.
- **Discrete Device Assignment (DDA):** Możliwość bezpośredniego przypisania fizycznego urządzenia PCIe (np. karty GPU lub NVMe) do konkretnej maszyny wirtualnej.

5. Kompatybilność z Systemem Backup i Infrastrukturą

- **Veeam Integration:** Pełna, natywna kompatybilność z posiadanym systemem **Veeam Backup & Replication** (wersja 12 lub nowsza). System musi wspierać backup bez agentowy.
- **Resilient Change Tracking (RCT):** Wsparcie dla natywnego mechanizmu śledzenia zmienionych bloków (RCT) w celu realizacji szybkich przyrostowych kopii zapasowych.
- **VSS Hardware Provider:** System musi umożliwiać integrację z dostarczoną macierzą poprzez sterowniki Hardware VSS Provider, w celu oddelegowania tworzenia migawek (snapshots) na poziom sprzętowy macierzy.
- **Certyfikacja:** Oferowany system musi znajdować się na liście kompatybilność producenta serwerów i macierzy oraz posiadać status rozwiązania wspieranego i certyfikowanego przez producenta sprzętu. Ta informacja musi znaleźć się na stronie producenta sprzętu.

6. Wsparcie producenta oraz licencjonowanie

Dostarczane oprogramowanie musi posiadać możliwość instalacji bezpłatnych poprawek bezpieczeństwa co najmniej do 2034 r. Dostarczane licencje muszą być zgodne dla dostarczanego sprzętu oraz muszą być za licencjonowane wszystkie fizyczne core serwerów. Dostarczona licencja musi być wieczysta.

X. Profesjonalna usługa wdrożenia dla systemu do wirtualizacji

W ramach profesjonalnej usługi wdrożenia należy wykonać:

1. Dostawa i licencje

- Dostarczenie licencji systemu wirtualizacyjnego
- Dostarczenie innych niezbędnych licencji.

2. Instalacja i konfiguracja podstawowa

- Instalacja oprogramowania na wszystkich serwerach fizycznych przeznaczonych do roli hostów wirtualizacji.
- Konfiguracja hiperwizora w trybie **Type-1** (bare-metal).
- Tworzenie i konfiguracja wirtualnych przełączników sieciowych (External, Internal, Private) z obsługą VLAN, trunking oraz Jumbo Frames.
- Konfiguracja pamięci Dynamic Memory oraz innych mechanizmów optymalizacji zasobów.
- Aktualizacja wszystkich komponentów oraz firmware serwerów do najnowszych wersji zalecanych przez producenta.

3. Konfiguracja wysokiej dostępności

- Zbudowanie klastra **Failover Cluster** z możliwością późniejszej rozbudowy.
- Konfiguracja **Live Migration** oraz **Shared Nothing Live Migration**.
- Konfiguracja **Storage Live Migration**.
- Włączenie i konfiguracja mechanizmu **Replica** do celów Disaster Recovery.
- Konfiguracja **Cluster-Aware Updating (CAU)**.

4. Zaawansowane funkcje bezpieczeństwa i optymalizacji

- Konfiguracja wsparcia dla **Shielded Virtual Machines** (ochronione maszyny wirtualne) wraz z vTPM i Host Guardian Service
- Włączenie mechanizmów **SR-IOV** oraz **VMQ** na kartach sieciowych.
- Konfiguracja **Nested Virtualization**.
- Hardening środowiska zgodnie z najlepszymi praktykami bezpieczeństwa producenta.

5. Integracja z infrastrukturą Zamawiającego

- Integracja z dostarczaną macierzą dyskową (w tym obsługa multipathing, ODX – Offloaded Data Transfer, thin provisioning).
- Integracja z Active Directory Domain Services.
- Integracja z systemem backupu Zamawiającego (Veeam).
- Konfiguracja odpowiednich polityk i uprawnień dostępu do środowiska wirtualizacji.

6. Migracja maszyn wirtualnych (jeśli dotyczy)

- Opracowanie i wykonanie planu migracji istniejących maszyn wirtualnych systemów bezpieczeństwa ze starego środowiska na nowe (vmware).
- Przeprowadzenie migracji w sposób możliwie bezprzerwowy (z minimalnym czasem przestoju).
- Testy poprawności działania zmigrowanych maszyn wirtualnych.

7. Testy i odbiór

- Przeprowadzenie testów funkcjonalnych, wydajnościowych oraz testów wysokiej dostępności (m.in. Live Migration, failover węzła klastra, Replica).
- Sporządzenie szczegółowych protokołów testowych.
- Usunięcie wszystkich usterek wykrytych podczas testów.
- Ostateczny odbiór techniczny środowiska wirtualizacji przez Zamawiającego.

8. Dokumentacja

- Przygotowanie kompletnej dokumentacji powdrożeniowej zawierającej:
  - Schemat architektury środowiska wirtualizacyjnego
  - Konfigurację klastra, sieci wirtualnych i maszyn wirtualnych

- Opis ustawień bezpieczeństwa i hardeningu
- Instrukcje administracyjne
- Spis licencji

XI. System operacyjny

Przedmiotem zamówienia jest dostawa licencji Microsoft Windows Server 2025 Standard (lub równoważnego) na potrzeby infrastruktury IT Zamawiającego dostarczanej w ramach Zamówienia. Licencji wieczysta, nowa, nigdy nie aktywowana. Licencje muszą pochodzić z oficjalnego kanału dystrybucyjnego producenta lub jej autoryzowanego partnera. Licencje będą użytkowane na dostarczanym klastrze serwerów oraz serwerze do backupu. Wykonawca dostarczy 5 licencji systemu operacyjnego.

Wymagania równoważne:

Opis wymagania
System operacyjny przeznaczony do serwerów
Licencja typu **wieczysta**,
Licencje muszą pochodzić z oficjalnego kanału dystrybucyjnego producenta lub jej autoryzowanego partnera.
Tworzenie i zarządzanie kontrolerami domeny (Active Directory Domain Services),
Obsługę usług DNS, DHCP, File Services i Hyper-V,
Zarządzanie uprawnieniami i użytkownikami,
Możliwość instalacji w środowisku fizycznym lub wirtualnym (VMware/Hyper-V),
Zarządzanie zdalne (Windows Admin Center, PowerShell).
Wersja 64-bitowa
Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne aktualizacji do co najmniej 2029 roku
Graficzny Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polski i angielski
Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego
Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,

XII. Profesjonalna usługa wdrożenia dla systemu operacyjnego

1. Instalacja systemu operacyjnego

- Czysta instalacja (clean install) systemu
- Aktualizacja systemu do najnowszej wersji kumulacyjnej oraz wszystkich sterowników sprzętowych (w tym sterowników serwera od producenta sprzętu).
- Konfiguracja podstawowych ustawień systemu: nazwa komputera, adresy IP, DNS, timezone, aktualizacje automatyczne zgodnie z polityką bezpieczeństwa Zamawiającego.

2. Migracja Active Directory Domain Services (AD DS)

Wykonawca zobowiązany jest przeprowadzić migrację środowiska Active Directory w sposób **bezprzerwowy** (zero-downtime lub z minimalnym planowanym przestojem) przy użyciu metody **side-by-side migration** (dodanie nowych kontrolerów domeny przed wycofaniem starych).

Zakres migracji AD obejmuje co najmniej:

- Przygotowanie środowiska (sprawdzenie zdrowia AD, replikacji, DCDiag, Repadmin, backup System State).
- Dołączenie nowych serwerów do istniejącej domeny.
- Instalacja roli **Active Directory Domain Services** oraz **DNS Server** na nowych serwerach.
- Promocja nowych serwerów do roli **Domain Controller** (w tym Global Catalog).
- Weryfikacja replikacji AD, synchronizacji czasu oraz poprawności działania usług katalogowych.
- Przeniesienie wszystkich ról **FSMO** (Schema Master, Domain Naming Master, PDC Emulator, RID Master, Infrastructure Master) na nowe kontrolery domeny.
- Podniesienie poziomu funkcjonalnego domeny (**Domain Functional Level**) oraz lasu (**Forest Functional Level**) do poziomu zainstalowanego systemu
- Wycofanie (demotion) starych kontrolerów domeny z poprzednich wersji systemu Windows Server.
- Czyszczenie metadanych starych kontrolerów domeny (metadata cleanup).
- Konfiguracja i optymalizacja **Active Directory** pod kątem bezpieczeństwa (hardening)

3. Dodatkowa konfiguracja

- Konfiguracja **Group Policy** – przeniesienie starych
- Integracja z dostarczonym środowiskiem wirtualizacyjnym
- Konfiguracja monitoringu zdarzeń AD
- Zmiana nazwy domeny

4. Testy i odbiór

- Przeprowadzenie kompleksowych testów środowiska Active Directory (replilkacja, logowanie użytkowników, dostęp do zasobów, Group Policy, aplikacje zależne od AD).
- Testy wydajnościowe i obciążeniowe kontrolerów domeny.
- Sporządzenie szczegółowych protokołów testowych wraz z wynikami narzędzi diagnostycznych (DCDiag, Repadmin, NLTest itp.).
- Usunięcie wszystkich usterek wykrytych w trakcie testów.
- Ostateczny odbiór techniczny migracji AD przez Zamawiającego.

5. Dokumentacja

- Przygotowanie kompletnej dokumentacji powdrożeniowej zawierającej:
    - Schemat topologii Active Directory (przed i po migracji)
    - Rozmieszczenie ról FSMO
    - Poziomy funkcjonalne domeny i lasu
    - Konfigurację GPO
    - Opis wykonanych kroków migracji
    - Instrukcje administracyjne i procedury awaryjne

XIII. Serwer kopi zapasowej posiadający rozwiązania: Macierz dyskowa, RAID.

Komponent	Parametr/warunek
Serwer	Serwer fabrycznie nowy, nie powystawowy, nierekondycjonowany, nie poleasingowy, nie będący przedmiotem prezentacji - rok produkcji nie starszy niż: 2026. Posiadający macierz dyskową i obsługujący RAID. Dostarczony sprzęt musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski.
Przeznaczenie	Serwer do wykonywania kopii zapasowych
Ilość	1 szt.
Obudowa	Do instalacji w szafie Rack 19”, wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych wraz z ramieniem do zarządzania kablami. Wszystkie wyspecyfikowanie elementy serwera muszą być w niej zamontowane.
Procesor	Zainstalowany 1 procesor min, 16 rdzeniowy. Wynik wydajności procesora dla proponowanego serwera nie powinien być niższy niż 185 punkty base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org).
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania min. 1 procesor
Pamięć operacyjna	Zainstalowane minimum 32GB pamięci RAM działających z maksymalną prędkością przewidzianą przez producenta procesora. Minimum 16 sloty na pamięć. Możliwość rozbudowy do min. 4TB RAM.
Zabezpieczenie pamięci	Min. Memory mirroring, ECC
Procesor Graficzny	Zintegrowana karta graficzna osiągająca rozdzielczość min. 1920x1200
Dyski	W chwili dostawy serwer musi posiadać zainstalowane minimum: • 2 sztuki dysków SSD o pojemności min. 480GB każdy. • 4 sztuki dysków SATA o pojemności min. 16 TB każdy. Możliwość instalacji min. 12 dysków 3,5” Wymagana możliwość instalacji dwóch dysków SSD / NVMe M.2 zabezpieczonych sprzętowym RAID. Dyski muszą mieć możliwość wymiany na gorąco.
Kontroler dyskowy	Zainstalowany sprzętowy kontroler obsługujący min. SATA 6 Gb, SAS 12Gb obsługujący min. 16 dysków. Kontroler musi posiadać min. 8GB pamięci Flash. Kontroler musi obsługiwać poziomy RAID –min. 0, 1, 10, 5, 50. Zainstalowana jedna min. dwu portowa karta obsługująca SAS 12Gb ze złączami SFF-8644 do podłączenia biblioteki taśmowej.
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 1000W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Interfejsy sieciowe	Zainstalowana czteroportowa karta 10GB SFP. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
Sloty I/O	Serwer w momencie dostawy powinien posiadać 2 sloty PCIe Gen5 z czego 1 slot x16, 1 slot OCP Gen5

Dodatkowe porty	• z przodu obudowy: min. 1x USB, zewnętrzny dedykowany port diagnostyczny • z tyłu obudowy: min. 2x USB, 1x VGA, 1x RJ-45 do zarządzania serwerem. • wewnątrz obudowy: min. 1x USB
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1.
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, Minimalne wymagania: • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty , zasilacze, wentylatory • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. • Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Zdalne włączanie/wyłączanie/restart • Pod montowanie lokalnych mediów • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • SSH • Możliwość mapowania obrazów ISO
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
Systemy operacyjne	Wspierane systemy min. Microsoft Windows Server 2022, 2025; Red Hat Enterprise Linux, SUSE Linux Enterprise Server 15 SP5, VMware vSphere (ESXi).
Gwarancja	36 miesięcy gwarancji producenta z oknem serwisowym 24x7, z reakcją NBD. Uszkodzone nośniki danych pozostają własnością zamawiającego. Zamawiający wymaga, aby Serwis gwarancyjny świadczony był wyłącznie przez producenta oferowanego sprzętu lub przez jego autoryzowany serwis, w tym celu Wykonawca wykupi/zapewni pełne wsparcie producenta dla Zamawiającego przez okres obowiązywania Gwarancji.

XIV. Profesjonalna usługa wdrożenia dla serwera kopii zapasowej

W ramach profesjonalnej usługi wdrożenia należy wykonać:

1. Instalacja i konfiguracja podstawowa

- Instalacja systemu Operacyjnego
- instalacji oprogramowania do backupu Veeam
- Konfiguracja repozytorium backupu na macierzy dyskowej serwera
- Konfiguracja biblioteki taśmowej
- Konfiguracja/migracja harmonogramu wykonywania kopii zapasowych (codzienne/incremental + pełne okresowe).

2. Zakres ochrony backupu

System kopii zapasowych musi zapewniać co najmniej backup i możliwość odtworzenia:

- Pełnego serwera (Bare Metal Recovery – BMR)
- System State oraz Active Directory (w tym autoritative restore)
- Maszyn wirtualnych (w tym Cluster Shared Volumes, checkpointów)
- Wolumenów danych, folderów i pojedynczych plików
- Aplikacji bazodanowych SQL Server

- Całego środowiska wirtualizacji

3. Integracja z infrastrukturą Zamawiającego

- Integracja z dostarczaną macierzą dyskową oraz serwerami
- Integracja z środowiskiem wirtualizacyjnym i Active Directory.
- Konfiguracja polityk retencji backupów zgodnie z wymaganiami Zamawiającego (np. 7 dni dziennych, 4 tygodnie tygodniowych, 12 miesięcy miesięcznych).

4. Testy odtwarzania (Restore Test)

- Przeprowadzenie testów odtwarzania (Restore Test) dla co najmniej:
  - Pojedynczego pliku/folderu
  - Całej maszyny wirtualnej
  - Bare Metal Recovery serwera fizycznego
  - Active Directory (non-authoritative i authoritative restore)
- Sporządzenie protokołu z wynikami testów odtwarzania.

5. Testy i odbiór

- Przeprowadzenie testów funkcjonalnych, wydajnościowych oraz testów RPO/RTO.
- Usunięcie wszystkich usterek wykrytych podczas testów.
- Ostateczny odbiór techniczny systemu backupu przez Zamawiającego.

6. Dokumentacja

- Przygotowanie kompletnej dokumentacji powdrożeniowej zawierającej:
  - Schemat architektury systemu backupu
  - Konfigurację harmonogramów i polityk retencji
  - Procedury odtwarzania (step-by-step)
  - Opis ustawień bezpieczeństwa i szyfrowania
  - Instrukcje administracyjne

Wykonawca zobowiązany jest wykonać wszystkie prace zgodnie z najlepszymi praktykami producenta wybranego rozwiązania backupowego oraz zaleceniami producenta oprogramowania do wirtualizacji, tak aby system kopii zapasowych był w pełni funkcjonalny, bezpieczny i zapewniał wymagany poziom RPO oraz RTO.

XV. Biblioteka taśmowa do streamer'a, napęd streamer i kasety do streamer'a

Komponent	Parametr/warunek
Biblioteka taśmowa	Biblioteka taśmowa fabrycznie nowa, nie powystawowa, nierekondycjonowana, nie poleasingowa, nie będący przedmiotem prezentacji - rok produkcji nie starszy niż: 2026.
Obudowa	Do zamontowania w szafie rack, maksymalnie 1U. Wbudowany czytnik kodów kreskowych. Dostarczony odpowiedni zestaw umożliwiający instalacje urządzenia w szafie rack.
Napęd LTO	W chwili dostawy w bibliotece powinien być zainstalowany napęd LTO8 SAS.
Okablowanie	Wraz z urządzeniem powinno być dostarczone odpowiednie okablowanie umożliwiające podłączenie napędu LTO8 SAS do serwera rack wyposażonego w porty SAS SFF-8644.
Liczba slotów LTO	Minimum 8, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów W komplecie jedna taśma czyszcząca oraz 10 taśm LTO8 wraz z kodami kreskowymi
Zasilanie	Zainstalowany minimum jeden zasilacz wystarczający do obsługi dostarczonej konfiguracji biblioteki w raz z kablem odpowiednim do podłączenia z PDU z wyjściem C13.
Dodatkowe	Interfejs do zarządzania poprzez przeglądarkę WWW oraz panel operatorski z wyświetlaczem LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie urządzenia. Wsparcie dla aplikacji Veeam Biblioteka taśmowa kompatybilna z dostarczanym serwerem do backupu
Gwarancja	36 miesięcy gwarancji producenta w trybie on-site NBD.

XVI. Profesjonalna usługa wdrożenia dla Biblioteka taśmowa do streamer'a, napęd streamer i kasety do streamer'a

Wykonawca jest zobowiązany do dostarczenia, instalacji, konfiguracji oraz wdrożenia do produkcji **biblioteki taśmowej** (tape library) jako elementu długoterminowego archiwum i off-line backupu w środowisku Zamawiającego.

1. Dostawa i komponenty

- Dostarczenie fabrycznie nowej biblioteki taśmowej zgodnej ze specyfikacją techniczną zawartą w OPZ
- Dostarczenie napędów taśmowych, nośników taśmowych (w tym czyszczące), oraz wszystkich akcesoriów montażowych.
- Zapewnienie niezbędnych licencji dla biblioteki
- Dostarczenie początkowej puli nośników taśmowych określonych w OPZ.

2. Montaż i instalacja fizyczna

- Transport, wniesienie i montaż biblioteki taśmowej w szafie rack 19" w serwerowni Zamawiającego.
- Podłączenie zasilania oraz okablowanie SAS do serwerów backupu
- Instalacja i konfiguracja karty HBA w serwerze backupowym.
- Aktualizacja firmware'u biblioteki, wszystkich napędów taśmowych oraz komponentów do najnowszych wersji zalecanych przez producenta.

3. Konfiguracja podstawowa i zaawansowana

- Konfiguracja biblioteki.
- Integracja biblioteki z systemem/ serwerem kopii zapasowych – konfiguracja jako urządzenie docelowe dla backupów długoterminowych.
- Ustawienie polityk czyszczenia napędów, inwentaryzacji nośników oraz alertów (SNMP, e-mail).
- Hardening urządzenia

4. Testy i weryfikacja

- Przeprowadzenie testów funkcjonalnych: zapis/odczyt danych, inwentaryzacja biblioteki, zmiana nośników,
- Testy wydajnościowe (szybkość zapisu/odczytu dla LTO).
- Testy odtwarzania danych z taśmy (restore test) – co najmniej pojedynczego pliku, maszyny wirtualnej i/lub Bare Metal Recovery.
- Sporządzenie protokołów testowych z wynikami.
- Usunięcie wszystkich usterek wykrytych podczas testów.

5. Dokumentacja

- Przygotowanie kompletnej dokumentacji powdrożeniowej zawierającej:
  - Schemat podłączenia biblioteki (fizyczny i logiczny)
  - Konfigurację partycji, napędów i polityk
  - Procedury obsługi codziennej (ładowanie nośników, czyszczenie)
  - Procedury odtwarzania danych z taśmy
  - Opis ustawień bezpieczeństwa
  - Spis nośników i licencji

Wykonawca zobowiązany jest wykonać wszystkie prace zgodnie z najlepszymi praktykami producenta biblioteki taśmowej oraz zaleceniami producenta systemu do wirtualizacji i systemem kopii zapasowych, tak aby biblioteka stanowiła niezawodne, długoterminowe rozwiązanie archiwizacji danych.

XVII. UTM wraz licencjami, posiadający rozwiązania: Firewall, NGFW, UTM, Oprogramowania antywir., IPS/IDS, VPN, proxy serwer, system typu sandbox, system typu WAF, System typu Web Secure Gateway, usługi konfiguracji i hardeningu systemów/urządzeń

Urządzenie służące do zabezpieczenia internetowego minimalne wymagania:
Wymaganie ogólne
Urządzenie musi być fabrycznie nowe, nie powystawowe, nierekondycjonowane, nie poleasingowe, nie będąca przedmiotem prezentacji - rok produkcji nie starszy niż: 2026.
Zakresem dostawy objęte jest urządzenie klasy UTM spełniające funkcję NGFW,

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.
System musi wspierać IPv4 oraz IPv6 w zakresie: • firewall, • ochrony w warstwie aplikacji, • protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii
W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
Monitoring stanu realizowanych połączeń VPN.
Interfejsy, Dysk, Zasilanie
System realizujący funkcję Firewall musi dysponować minimum 8 portami Gigabit Ethernet RJ-45 oraz 2 portami SFP Gigabit Ethernet.
System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe
W zakresie Firewall'a obsługa nie mniej niż 1,5mln jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.
Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps.
Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps.
Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 715 Mbps.
Funkcje Systemu Bezpieczeństwa
W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
Kontrola Aplikacji.
Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
Ochrona przed atakami - Intrusion Prevention System.
System Web Secure Gateway oraz proxy serwer pozwalający na kontrole stron WWW.
Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
Zarządzanie pasmem (QoS, Traffic shaping).
Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
Analiza ruchu szyfrowanego protokołem SSL.
Polityki, Firewall
Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: Translację jeden do jeden oraz jeden do wielu.
Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa min. DMZ, LAN, WAN.
Połączenia VPN
System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site.
System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o min. HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
Routing i obsługa łączy WAN
W zakresie routingu rozwiązanie powinno zapewniać obsługę min.: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły min.: RIPv2, OSPF, BGP oraz PIM.
Zarządzanie pasmem
System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL
Ochrona przed malware
Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
Ochrona przed atakami
Ochrona IPS/IDS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
Mechanizmy ochrony dla aplikacji Web’owych(WAF) na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji
Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji
System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Zarządzanie
Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach min. 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie
Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
Musi istnieć możliwość logowania do serwera SYSLOG.
Licencje
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: • Kontrola Aplikacji, IPS/IDS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen
Gwarancja
System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania, funkcji ochrony.
Dostarczane rozwiązania muszą posiadać licencję bezterminową z wyłączeniem aktualizacji baz funkcji ochronnych systemu
Dostarczany sprzęt musi być kompatybilny z UTM Fortigate 80F w zakresie HA

XVIII. Wdrożenie UTM z licencjami

Wykonawca jest zobowiązany do dostarczenia, instalacji, konfiguracji wraz z profesjonalną usługą wdrożenia **UTM (Unified Threat Management)** jako centralnego elementu ochrony sieci i bezpieczeństwa środowiska Zamawiającego.

1. Dostawa i licencje

- Dostarczenie fabrycznie nowego urządzenia UTM zgodnego ze specyfikacją techniczną zawartą w OPZ
- Zapewnienie wszystkich wymaganych licencji
- Dostarczenie wszystkich akcesoriów montażowych, kabli oraz zasilaczy

2. Montaż i instalacja fizyczna

- Transport, wniesienie i montaż urządzenia UTM w szafie rack 19” w serwerowni Zamawiającego.
- Podłączenie zasilania oraz wszystkich interfejsów sieciowych (LAN, WAN, DMZ, porty HA).
- Aktualizacja firmware’u urządzenia UTM oraz wszystkich modułów bezpieczeństwa do najnowszej stabilnej wersji zalecanej przez producenta.

3. Konfiguracja podstawowa i zaawansowana

- Konfiguracja wysokiej dostępności (High Availability) w trybie Active-Passive
- Konfiguracja stref bezpieczeństwa (Security Zones): LAN, WAN, DMZ, Wi-Fi, Guest Network itp.
- Tworzenie i wdrożenie polityk bezpieczeństwa (Security Policies):
    - Firewall
    - Intrusion Prevention System (IPS)
    - Antywirus i Anti-Malware (w tym skanowanie ruchu HTTP/HTTPS)
    - Web & URL Filtering
    - Anti-Spam i Anti-Phishing
    - Kontrola aplikacji
    - SSL/TLS Inspection
- Konfiguracja tuneli VPN (IPsec Site-to-Site oraz SSL VPN / Remote Access VPN) dla użytkowników zdalnych i oddziałów.
- Konfiguracja mechanizmów uwierzytelniania (Active Directory integration, RADIUS, MFA).
- Włączenie i konfiguracja logowania oraz raportowania zdarzeń bezpieczeństwa.
- Konfiguracja alertów i powiadomień (e-mail, SNMP).
- Przeprowadzenie harderingu urządzenia

4. Integracja z infrastrukturą Zamawiającego

- Integracja z dostarczaną i obecną infrastrukturą sieciową (przełączniki, routery, serwery).
- Integracja z Active Directory Domain Services (uwierzytelnianie użytkowników).

5. Migracja i przejście na produkcję

- Testowe uruchomienie nowego UTM
- Przełączenie ruchu produkcyjnego na nowe urządzenie UTM.
- Optymalizacja reguł i polityk bezpieczeństwa po migracji.

6. Testy i odbiór

- Testy scenariuszy awaryjnych (failover HA, restart urządzenia).
- Weryfikacja skonfigurowanych zabezpieczeń.
- Usunięcie wszystkich usterek wykrytych podczas testów.
- Ostateczny odbiór techniczny systemu UTM przez Zamawiającego.

7. Dokumentacja

- Przygotowanie kompletnej dokumentacji powdrożeniowej zawierającej:
    - Schemat architektury bezpieczeństwa
    - Konfigurację polityk bezpieczeństwa i stref
    - Opis reguł firewall i VPN
    - Procedury administracyjne i awaryjne
    - Instrukcje zarządzania i raportowania

Wykonawca zobowiązany jest wykonać wszystkie prace zgodnie z najlepszymi praktykami bezpieczeństwa (w tym zaleceniami producenta UTM oraz wytycznymi KR, KSCI i RODO), tak aby system UTM zapewnił wysoki poziom ochrony, wykrywania zagrożeń oraz kontroli ruchu sieciowego w środowisku Zamawiającego.

XIX. Rozbudowa oprogramowania antywir. o moduły: oprogramowania do badania podatności, zarządz. podatnościami, oprogram. antywir., oprogram. Antyspamowe ochronę przed ransomware, EDR, XDR, zarządzanie urządzeniami mobilnymi (MDM), sandbox, MFA, system typu RADIUS, konfiguracja i hardening systemów/urządzeń.

Aktualizacja licencji oprogramowania antywirusowego ESET PROTECT Entry ON-PREM (nr licencji 33D-8JM-5XB) dla 50 stanowisk posiadanej przez zamawiającego do ESET PROTECT Elite dla 60 stanowisk na okres 36 miesięcy
Zamawiający dopuszcza rozwiązanie równoważne które będzie dostarczone na min. 60 stanowisk, wraz z wdrożeniem, konfiguracją i szkoleniem dla administrator oraz spełni następujące funkcjonalności:
Konsola administracyjna
Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
Ochrona stacji roboczych
Rozwiązanie musi wspierać systemy operacyjne min. Windows 10/Windows 11.
Rozwiązanie musi wspierać architekturę ARM64.
Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji min. adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
Rozwiązanie musi integrować się z Intel Threat Detection Technology.
Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM, urządzeń przenośnych.
Rozwiązanie musi posiadać moduł HIPS który może pracować 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.
Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego min. Microsoft Outlook.
Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
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.
Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o wbudowane kategorie i podkategorii.
Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
Rozwiązanie musi posiadać funkcjonalność ochrony przed ransomware w postaci 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.
Ochrona serwera
Rozwiązanie musi wspierać systemy min. Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: Ubuntu Server 18.04 LTS i nowsze, Debian 10 i nowsze, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8
Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
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 posiadać możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przez uruchomieniem systemu operacyjnego.

Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
Rozwiązanie musi posiadać wbudowany system IPS/IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IPS/IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
Szyfrowanie
System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows min. 10, 11 w wersji 32-bit i 64-bit.
System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
Ochrona urządzeń mobilnych opartych o system Android
Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi min.: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia, d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS.
Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o min.: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła.
Sandbox w chmurze
Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
Rozwiązanie musi wykorzystywać do działania chmurę producenta.
Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym min. archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu min. .jar, .reg, .msi.
Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
Przeanalizowane pliki muszą zostać odpowiednio oznaczone
W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.
Moduł EDR/XDR
Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: min. nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
Serwer musi posiadać min. 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
Konsola administracyjna musi mieć możliwość tagowania obiektów.
Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
Moduł zarządzania podatnościami i aktualizacjami
Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11), aplikacjach zainstalowanych na zarządzanych stacjach oraz zarządzania podatnościami.
Baza wykrywanych podatności musi zawierać minimum 35000 CVE.
Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.
Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum: - nazwę aplikacji lub systemu operacyjnego - punktacje CVSS - opis wykrytej podatności - wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta
Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach
Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.

Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.
Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.
Ochrona poprzez dwuskładnikowe uwierzytelnianie typu
Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: min. 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
Rozwiązanie musi wspierać system operacyjne min. Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11.
Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego
Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.
Mobile Device Management
Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania
MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami: Android, iOS, iPadOS
MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: – usunięcie zawartości urządzenia, – przywrócenie urządzenia do ustawień fabrycznych, – zablokowanie urządzenia, – uruchomienie sygnału dźwiękowego, – lokalizację GPS, – Resetowanie hasła blokady ekranu.
MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
MDM musi umożliwiać dla iOs i iPadOS co najmniej: – konfigurację kont e-mail, – konfigurację połączeń VPN, – Konfigurację połączeń Wi-Fi, – Konfigurację listy certyfikatów, – możliwość uruchomienia trybu jednej aplikacji.
MDM musi umożliwiać dla Android co najmniej: – blokadę wykonywania połączeń, – blokadę konfiguracji sieci Wi-Fi, – blokadę konfiguracji tuneli VPN, – zarządzenie aktualizacjami sytemu operacyjnego, – blokadę zmiany tapety urządzenia.

XX. Usługa wdrożenia dla rozbudowy oprogramowania antywirusowego o nowe moduły

Wykonawca jest zobowiązany do zakupu, dostarczenia licencji, instalacji, konfiguracji, migracji oraz wdrożenia do produkcji systemu oprogramowania antywirusowego wraz z wdrożeniem wieloskładnikowego uwierzytelniania (MFA) z wykorzystaniem kluczy sprzętowych, modułu EDR/XDR, zarządzania podatnościami oraz MDM.

1. Dostawa licencji

- Dostarczenie ważnych licencji na wymaganą liczbę endpointów (serwery fizyczne, maszyny wirtualne, stacje robocze, urządzenia mobilne) zgodnie ze specyfikacją Zamawiającego.

2. Instalacja i konfiguracja nowej konsoli

- Instalacja nowej instancji lub migracja konsoli On-Premises
- Aktualizacja konsoli do najnowszej wersji dostępnej zalecanej przez producenta
- Konfiguracja roli serwera, bazy danych oraz wszystkich komponentów (Apache, ERA, etc.).
- Hardening konsoli zgodnie z najlepszymi praktykami bezpieczeństwa i polityką Zamawiającego.

3. Migracja i aktualizacja obecnej konsoli

- Opracowanie i wykonanie planu migracji z istniejącej konsoli na nową (jeśli będzie taka potrzeba)
- Eksport i import certyfikatów CA, polityk oraz konfiguracji.
- Migracja wszystkich zarządzanych urządzeń (agentów) bez utraty historii i polityk.
- Aktualizacja agentów na wszystkich endpointach do najnowszej wersji kompatybilnej
- Weryfikacja poprawności migracji (replikacja polityk, widoczność urządzeń, raporty).
- Minimalizacja przestoju środowiska podczas migracji.

4. Konfiguracja wymaganych modułów

- **Multi-Factor Authentication (MFA)**: Wdrożenie modułu z obowiązkowym wsparciem kluczy sprzętowych (FIDO2 hardware keys). Konfiguracja MFA dla logowania do konsoli, VPN, RDP, Outlook, komputera oraz innych usług zintegrowanych z Active Directory.
- **EDR / XDR**: Włączenie i konfiguracja modułu – pełna widoczność, threat hunting, analiza zdarzeń, korelacja alertów oraz automatyczna odpowiedź na incydenty.
- **Zarządzanie podatnościami (Vulnerability & Patch Management)**: Włączenie ciągłego skanowania podatności, priorytetyzacji ryzyka oraz automatycznego/manualnego łatania aplikacji trzecich.
- **Mobile Device Management (MDM)**: Konfiguracja zarządzania urządzeniami mobilnymi (Android, iOS) – polityki bezpieczeństwa, zdalne blokowanie, wymazywanie danych, zarządzanie aplikacjami.
- Konfiguracja polityk ochrony
- Integracja z Active Directory,

5. Testy i weryfikacja

- Przeprowadzenie testów działania wszystkich wdrożonych modułów
- Testy migracji (poprawność przeniesienia agentów i polityk).
- Sporządzenie protokołów testowych z wynikami.
- Usunięcie wszystkich usterek wykrytych podczas testów.
- Ostateczny odbiór techniczny systemu przez Zamawiającego.

6. Dokumentacja

- Przygotowanie kompletnej dokumentacji powdrożeniowej zawierającej:
    - Schemat architektury
    - Konfigurację polityk bezpieczeństwa, MFA, XDR, Vulnerability Management i MDM
    - Procedury migracji i aktualizacji agentów
    - Instrukcje zarządzania konsolą oraz reagowania na incydenty
    - Opis ustawień bezpieczeństwa i hardeningu

Wykonawca zobowiązany jest wykonać wszystkie prace zgodnie z oficjalną dokumentacją producenta, najlepszymi praktykami bezpieczeństwa oraz wymaganiami KRI, KSC i RODO, tak aby system zapewnił kompleksową ochronę endpointów, wykrywanie zaawansowanych zagrożeń oraz efektywne zarządzanie bezpieczeństwem w całym środowisku Zamawiającego.

XXI. Zakup switch warstwy core spięte w klaster HA posiadający rozwiązania: Zarządzalnego switch z obsługą VLAN, MACsec, standard 802.1X, Usługa segmentacji sieci, zarządzalne urządzenie siecowe HA, usługi konfiguracji i hardeningu systemów/urządzeń.

Komponent	Parametr/warunek
Switch	Switch fabrycznie nowy, nie powystawowy, nierekondycjonowany, nie poleasingowy, nie będący przedmiotem prezentacji - rok produkcji nie starszy niż: 2026
Ilość sztuk	2 szt.
Obudowa	Obudowa o maksymalnej wysokości 1 U umożliwiająca montaż w szafie rack 19” wraz z wszystkimi niezbędnymi elementami do jej zamontowania
Porty	– Min. 16 portów 1 Gigabit – Min. 8 portów 10G – Min. 4 porty SFP+ 10 Gigabit
Wydajność	– Zdolność przełączania: min. 272 Gbs oaz min. 352 Gb/s (z podłączeniem do stosu) – Przekazywanie (pakiet 64-bajtowy): min. 214 mpps – Zdolność buforowania pakietów (MB): min. 12 – Reguły ACL: min. 1000 – Obsługa aktywnych sieci VLANs: min. 500 – Wielkość tablicy adresów MAC min. 16K wpisów – Pamięć RAM min. 2 GB – Pamięć Flash min. 4 GB – Obsługiwane ramki Jumbo do 9KB – Przepustowość w ramach stosu –min. 80Gb/s
Funkcjonalność	– Możliwość tworzenia połączeń agregowanych – Możliwość łączenia minimum 8 przełączników w stos z możliwością zarządzania cały stosem pod jednym adresem IP – Możliwość łączenia przełączników w stos w topologii pierścienia. – Tryb HA dla urządzeń pracujących w stosie – Należy dostarczyć wszystkie niezbędne elementy do połączenia w stos/stack – Redundantne wentylatory – Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap)
Obsługa protokołów, zgodność z normami i funkcje	NTP, IGMPv1/2/3 i MLDv1/2 Snooping, LLDP, LLDP-MED, 802.1Q, Layer 2 traceroute, serwer DHCP, IEEE 802.1X, Guest VLAN, uwiezytelnianie w oparciu o adres MAC, uwierzytelnianie w oparciu o portal www dla klientów bez suplikanta 802.1X, CoA, Port Security, DHCP Snooping, Dynamic ARP Inspection , IP Source Guard, TACACS+, RADIUS, obsługa ACL, IEEE 802.1ae (MACSec switch-switch) dla wszystkich portów gcm –aes-128 z MKA, CoPP, Private Vlan, RADSEC, sprawdzanie autentyczności oprogramowania, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzeni, Kontrola sztormów dla ruchu broadcast/multicast/unicast,, Routing statyczny dla IPv4 i IPv6, Routing dynamiczny – RIP, OSPF do 1000 tras, PIM Stub do 1000 tras, PBR, VRRP, GRE, SPAN, RSPAN, przechwytywanie ruchu z określonego portu fizycznego, Funkcjonalność sondy IP SLA Responder, port konsoli, Dedykowany port Ethernet do zarządzania out-of-band,, SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,, RESTCONF, gNMI , REP, STP, przełącznik L2/L3, QOS, ping, traceroute, IEEE 802.3ad,
Gwarancja	Gwarancja czasu życia (Limited Lifetime warranty) obejmująca: - przełącznik - dostęp do nowych wersji oprogramowania w okresie gwarancji Min. 36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 8x5

Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Inne	Musi zostać dostarczone kompletne rozwiązanie wraz ze wszystkimi niezbędnymi podzespołami, kablami zasilającymi, elementami do montażu w szafie, oprogramowaniem oraz dokumentacją. Wszystkie wymienione w tabeli parametry i funkcjonalności muszą być dostępne w dostarczonym rozwiązaniu wraz z niezbędnymi licencjami.

XXII. Profesjonalna usługa wdrożenia dla zakup switch warstwy core spięte w klaster HA

Wykonawca jest zobowiązany do dostarczenia, instalacji, konfiguracji oraz wdrożenia do produkcji **klastra wysokiej dostępności przełączników rdzeniowych (Core Switch HA Cluster)** jako centralnego elementu szkieletu sieciowego Zamawiającego, zapewniającego redundancję, wysoką przepustowość i brak pojedynczego punktu awarii.

1. Dostawa sprzętu i licencji

- Dostarczenie fabrycznie nowych przełączników rdzeniowych (minimum 2 sztuki) zgodnych ze specyfikacją techniczną zawartą w OPZ
- Zapewnienie wszystkich wymaganych licencji na funkcje wysokiej dostępności (HA), stacking/virtual chassis, routing Layer 3, zaawansowane funkcje bezpieczeństwa oraz zarządzanie.
- Dostarczenie wszystkich akcesoriów

2. Montaż i instalacja fizyczna

- Transport, wniesienie i montaż przełączników w szafie rack 19” w serwerowni Zamawiającego
- Podłączenie zasilania, wszystkich urządzeń oraz kabli dla stack.
- Aktualizacja firmware’u wszystkich przełączników do najnowszej stabilnej wersji zalecanej przez producenta.

3. Konfiguracja wysokiej dostępności

- Zbudowanie klastra HA w technologii producenta działającego w trybie **Active-Active** lub **Active-Passive** z automatycznym failoverem.
- Konfiguracja mechanizmów redundancji:
- Podział ruchu i load-balancing pomiędzy węzłami klastra.
- Hardening urządzeń

4. Integracja z infrastrukturą Zamawiającego

- Integracja z istniejącymi przełącznikami dystrybucyjnymi / dostępowymi
- Integracja z systemem UTM oraz serwerami
- Konfiguracja VLAN-ów zgodnie z polityką Zamawiającego.
- Integracja z systemem monitoringu (SNMPv3, syslog, NetFlow/sFlow) i alertowania.
- Konfiguracja backupu konfiguracji przełączników.

5. Migracja i przejście na produkcję

- Opracowanie i wykonanie planu migracji z istniejących przełączników rdzeniowych na nowy klaster HA (z minimalnym lub zerowym przestojem).
- Testowe uruchomienie nowego klastra równolegle
- Przełączenie ruchu produkcyjnego na nowy klaster HA.
- Optymalizacja konfiguracji po migracji.

6. Testy i odbiór

- Przeprowadzenie testów wysokiej dostępności (awaria jednego przełącznika, awaria linku, failover, recovery).
- Testy scenariuszy awaryjnych oraz obciążeniowych.
- Sporządzenie szczegółowych protokołów testowych.
- Usunięcie wszystkich usterek wykrytych podczas testów.
- Ostateczny odbiór techniczny klastra HA przez Zamawiającego.

7. Dokumentacja

- Przygotowanie kompletnej dokumentacji powdrożeniowej zawierającej:
    - Schemat fizyczny i logiczny klastra Core HA
    - Konfigurację stacking
    - Procedury failover i recovery
    - Instrukcje administracyjne i zarządzanie
    - Spis licencji i numerów seryjnych

Wykonawca zobowiązany jest wykonać wszystkie prace zgodnie z najlepszymi praktykami producenta przełączników oraz ogólnymi standardami projektowania sieci wysokiej dostępności, tak aby klaster Core HA zapewniał ciągłość działania sieci szkieletowej bez pojedynczego punktu awarii.

XXIII. Zakup switch dostępowych posiadający rozwiązania: Zarządzalnego switch z obsługą VLAN, MACsec, standard 802.1X, Usługa segmentacji sieci,, usługi konfiguracji i hardeningu systemów/urządzeń.

Switch dostępowy	
Komponent	**Parametr/warunek**
Switch	Switch fabrycznie nowy, nie powystawowy, nierekondycjonowany, nie poleasingowy, nie będący przedmiotem prezentacji - rok produkcji nie starszy niż: 2026
Ilość sztuk	4 szt.
Obudowa	Obudowa o maksymalnej wysokości 1 U umożliwiająca montaż w szafie rack 19” wraz z wszystkimi niezbędnymi elementami do jej zamontowania
Porty	– Min. 24 portów 1000 Base-T – Min. 4 SFP+ 10 Gigabit
Wydajność	– Zdolność przełączania: min. 128 Gbs – Przekazywanie: min. 95 mpps – Zdolność buforowania (MB): min. 6 – Reguły ACL: min. 1000 – Obsługa aktywnych sieci VLANs: min. 500 – Wielkość tablicy adresów MAC min. 16k wpisów – Pamięć RAM min. 2 GB – Pamięć Flash min. 4 GB – Obsługiwane ramki Jumbo do 9KB
Obsługa protokołów, zgodność z normami i funkcje	NTP, IGMPv1/2/3 i MLDv1/2 Snooping, LLDP, LLDP-MED, 802.1Q, Layer 2 traceroute, serwer DHCP, IEEE 802.1X, Guest VLAN, uwiezytelnianie w oparciu o adres MAC, uwierzytelnianie w oparciu o portal www dla klientów bez suplikanta 802.1X, CoA, Port Security, DHCP Snooping, Dynamic ARP Inspection , IP Source Guard, TACACS+, RADIUS, obsługa ACL, IEEE 802.1ae (MACSec switch-switch) dla wszystkich portów gcm – aes-128 z MKA, CoPP, Private Vlan, RADSEC, sprawdzanie autentyczności oprogramowania, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzeni, Kontrola sztormów dla ruchu broadcast/multicast/unicast,, Routing statyczny dla IPv4 i IPv6, Routing dynamiczny – RIP, OSPF do 1000 tras, PIM Stub do 1000 tras, PBR, VRRP, GRE, SPAN, RSPAN, przechwytywanie ruchu z określonego portu fizycznego, Funkcjonalność sondy IP SLA Responder, port konsoli, Dedykowany port Ethernet do zarządzania out-of-band,, SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,, RESTCONF, gNMI , REP, STP, przełącznik L2/L3, QOS, ping, traceroute, IEEE 802.3ad,
Gwarancja	Gwarancja czasu życia (Limited Lifetime warranty) obejmująca: - przełącznik - dostęp do nowych wersji oprogramowania w okresie gwarancji Min. 36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 8x5
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Inne	Musi zostać dostarczone kompletne rozwiązanie wraz ze wszystkimi niezbędnymi podzespołami, kablami zasilającymi, elementami do montażu w szafie, oprogramowaniem oraz dokumentacją. Wszystkie wymienione w tabeli parametry i funkcjonalności muszą być dostępne w dostarczonym rozwiązaniu wraz z niezbędnymi licencjami.
Dodatkowe okablowanie	– 4 wkładki SFP+ 10 GB kompatybilne ze switchami core – 4 kable DAC SFP+ do podłączenia ze switchami core

XXIV. Profesjonalna usługa wdrożenia dla zakup switch dostępowych

1. Dostawa sprzętu i licencji

- Dostarczenie fabrycznie nowych przełączników dostępowych zgodnych ze specyfikacją techniczną zawartą w OPZ
- Zapewnienie wszystkich wymaganych licencji na funkcje
- Dostarczenie niezbędnych akcesoriów

2. Montaż i instalacja fizyczna

- Transport, wniesienie i montaż przełączników dostępowych w szafach rack 19" w wybranych lokalizacjach Zamawiającego
- Podłączenie zasilania
- Okablowanie uplinków do przełączników rdzeniowych
- Aktualizacja firmware'u / systemu operacyjnego wszystkich przełączników dostępowych do najnowszej stabilnej wersji zalecanej przez producenta.

3. Konfiguracja podstawowa i zaawansowana

- Konfiguracja przełączników w trybie **Layer 2**
- Tworzenie i konfiguracja VLAN-ów zgodnie z polityką segmentacji sieci Zamawiającego.
- Konfiguracja mechanizmów wysokiej dostępności łączy
- Hardening urządzeń (zmiana haseł domyślnych, wyłączenie niepotrzebnych usług, SSHv2, ograniczenie dostępu zarządzania).

4. Integracja z infrastrukturą Zamawiającego

- Integracja z klastrem przełączników rdzeniowych
- Integracja z systemem monitoringu Zamawiającego (SNMPv3, syslog, NetFlow/sFlow).

5. Testy i odbiór

- Przeprowadzenie testów funkcjonalnych
- Testy wydajnościowe i obciążeniowe.
- Testy scenariuszy awaryjnych
- Sporządzenie szczegółowych protokołów testowych.
- Usunięcie wszystkich usterek wykrytych podczas testów.
- Ostateczny odbiór techniczny przełączników dostępowych przez Zamawiającego.

6. Dokumentacja

- Przygotowanie kompletnej dokumentacji powdrożeniowej zawierającej:
  - Schemat fizyczny i logiczny rozmieszczenia przełączników dostępowych
  - Konfigurację VLAN-ów, polityk bezpieczeństwa
  - Schematy okablowania uplinków
  - Procedury administracyjne i awaryjne
  - Spis numerów seryjnych, licencji oraz konfiguracji backupowych

Wykonawca zobowiązany jest wykonać wszystkie prace zgodnie z najlepszymi praktykami producenta przełączników oraz ogólnymi standardami projektowania sieci dostępowej, tak aby przełączniki access zapewniały niezawodne, bezpieczne i łatwe w zarządzaniu podłączenie wszystkich urządzeń końcowych w środowisku Zamawiającego.

XXV. Dostawa systemów bezpieczeństwa wraz z usługą SOC: Oprogramowanie do badania podatności, zarządzania podatnościami, system typu SIEM, SOAR, usługa reagowania na incydenty w środowisku IT/OT, konfiguracja i hardening systemów/urządzeń, System typu Menadżer logów, system typu DLP. Usługa wdrożenia systemów bezpieczeństwa wraz z usługa SOC.

1. Przedmiot zamówienia

Przedmiotem zamówienia jest zakup, dostarczenie, wdrożenie oraz uruchomienie zintegrowanego systemu przeciwdziałania cyberzagrożeniom, umożliwiającego ich wykrywanie, analizę i obsługę przy wykorzystaniu mechanizmów uczenia maszynowego (Machine Learning) oraz zapewniającego automatyzację i orkiestrację reakcji na incydenty bezpieczeństwa (SOAR), wraz ze świadczeniem usługi Security Operations Center (SOC). Usługa SOC musi być świadczona całodobowo

(24/7/365) w oparciu o system bezpieczeństwa SIEM/SOAR, który powinien znajdować się na dedykowanym środowisku wysokiej dostępności HA w profesjonalnym Data Center spełniający minimum wymogi TIER III i znajdujący się na terenie Unii Europejskiej.

2. Cel zamówienia

Celem zamówienia jest zwiększenie poziomu bezpieczeństwa teleinformatycznego Zamawiającego poprzez:

- zapewnienie ciągłego monitorowania zdarzeń bezpieczeństwa,
- szybkie wykrywanie, klasyfikowanie i reagowanie na cyberzagrożenia,
- ograniczenie skutków incydentów bezpieczeństwa,
- spełnienie wymagań wynikających z obowiązujących przepisów prawa oraz dobrych praktyk w zakresie cyberbezpieczeństwa.

3. Zakres zamówienia

W ramach zakresu zamówienia Wykonawca dostarczy zintegrowany system bezpieczeństwa wraz z usługami:

- Oprogramowanie do badania podatności,
- Oprogramowanie do zarządzania podatnościami,
- System typu SIEM
- System typu SOAR,
- Usługa reagowania na incydenty w środowisku IT/OT,
- Usługi konfiguracji i hardeningu systemów/urządzeń,
- System typu Menadżer logów,
- Oprogramowanie przeciwdziałającemu wyciekowi danych DLP,
- System typu Skaner podatności. ,
- Usługa SOC (Security Operation Center) ,
- Usługi reagowania na incydenty w środowisku IT/OT/ICS,
- Oprogramowanie typu Menadżer logów,
- Oprogramowanie do badania podatności systemów informatycznych,
- Oprogramowanie do badania podatności serwisów WWW,
- Oprogramowanie typu sandbox do badania bezpieczeństwa aplikacji oraz plików

Powyższe systemy bezpieczeństwa i usługi muszą być wdrożone w min. następujących obszarach bezpieczeństwa:

- Bezpieczeństwo systemów informatycznych,
- Bezpieczeństwo serwisów www,
- Bezpieczeństwa sieci,
- Monitorowanie bezpieczeństwa,
- Reagowanie w zakresie bezpieczeństwa,
- Bezpieczeństwo systemów sterowania przemysłowego,
- Bezpieczeństwo sieci OT,
- Monitorowanie bezpieczeństwa OT,
- Reagowanie w zakresie bezpieczeństwa OT,
- Zabezpieczenie systemów bezpieczeństwa wizyjnego, fizycznego i technicznego SUW (Stacji Uzdatniania Wody), punktów ujęć wody, przepompowni i oczyszczalni ścieków działających w sieci

Zakres zamówienia obejmuje:

- dostarczenie licencji/systemu informatycznego spełniającego wymagania Zamawiającego,
- profesjonalna usługa wdrożenia systemu w środowisku Zamawiającego,
- integrację systemu z istniejącymi rozwiązaniami bezpieczeństwa i systemami IT/OT Zamawiającego,
- Wdrożenie mechanizmów uczenia maszynowego wspierających wykrywanie anomalii i zagrożeń,
- Uruchomienie funkcjonalności automatyzacji i orkiestracji reakcji na incydenty (SOAR),
- przeprowadzenie testów poprawności działania systemu,
- Konfiguracja i hardering systemu

- Świadczenie usługi Security Operations Center (SOC)
- przeszkolenie administratorów i użytkowników wskazanych przez Zamawiającego,
- świadczenie wsparcia technicznego i utrzymanie.

4. Wymagania funkcjonalne systemu

System musi umożliwiać co najmniej:

- monitorowanie zdarzeń bezpieczeństwa w czasie rzeczywistym,
- korelację zdarzeń z wielu źródeł danych (np. systemy sieciowe, serwery, stacje robocze, aplikacje),
- wykrywanie zagrożeń z wykorzystaniem algorytmów uczenia maszynowego oraz analizy behawioralnej,
- klasyfikację i priorytetyzację incydentów bezpieczeństwa,
- automatyczne podejmowanie zdefiniowanych akcji reakcyjnych (np. blokada, izolacja, powiadomienia),
- orkiestrację procesów obsługi incydentów zgodnie z przygotowanymi scenariuszami (playbookami),
- raportowanie i wizualizację danych dotyczących stanu bezpieczeństwa.

5. Wymagania techniczne i bezpieczeństwa

System powinien:

- być zgodny z obowiązującymi standardami bezpieczeństwa (ISO/IEC 27001 lub równoważnymi),
- zapewniać mechanizmy kontroli dostępu i rejestrowania działań użytkowników,
- umożliwiać skalowanie wraz z rozwojem infrastruktury Zamawiającego,
- nie powodować degradacji wydajności środowiska IT Zamawiającego,
- usługa SOC musi być świadczona przez personel posiadający odpowiednie kwalifikacje i doświadczenie.

6. Wdrożenie i szkolenia

Wykonawca zobowiązany jest do:

- opracowania harmonogramu wdrożenia uzgodnionego z Zamawiającym,
- przeprowadzenia wdrożenia produkcyjnego systemu,
- przeszkolenia administratorów w zakresie konfiguracji, obsługi i utrzymania systemu,
- przekazania dokumentacji technicznej i użytkowej w języku polskim.

7. Wsparcie i serwis

W ramach zamówienia Wykonawca zapewni:

- wsparcie techniczne w okresie gwarancji – system musi być objęty minimum 36-miesięcznym wsparciem producenta,
- aktualizacje systemu i sygnatur zagrożeń,
- usuwanie zgłoszonych awarii i nieprawidłowości w określonym czasie reakcji.

8. Usługa Security Operations Center (SOC)

Usługa SOC obejmuje:

- Monitoring bezpieczeństwa IT:
  - całodobowy (24/7/365) monitoring zdarzeń bezpieczeństwa w systemach IT;
  - zbieranie, korelację i analizę logów z:
    - systemów operacyjnych,
    - urządzeń sieciowych,
    - systemów bezpieczeństwa (min. firewall/UTM, IDS/IPS, WAF, EDR/XDR),
    - aplikacji i baz danych;
  - wykrywanie anomalii, prób naruszenia bezpieczeństwa oraz incydentów;
  - analizę zdarzeń przy użyciu narzędzi klasy SIEM oraz SOAR.
- Monitoring bezpieczeństwa OT:

- systemów SCADA, DCS, PLC, HMI;
- sieci przemysłowych i protokołów OT (m.in. Modbus, Profinet, OPC, EtherNet/IP);
- urządzeń automatyki i infrastruktury produkcyjnej.

Monitoring OT musi być realizowany w sposób pasywny, niezakłócający pracy procesów technologicznych i spełniający wymagania bezpieczeństwa operacyjnego.
Zakres obejmuje:

- identyfikację i inwentaryzację zasobów OT;
- wykrywanie nieautoryzowanych zmian konfiguracji i komunikacji;
- detekcję anomalii oraz zagrożeń specyficznych dla środowisk OT;
- korelację zdarzeń OT z incydentami w środowisku IT.

9. Obsługa incydentów bezpieczeństwa

– SOC zapewnia pełny cykl obsługi incydentu, obejmujący:
  - identyfikację incydentu,
  - klasyfikację incydentu (np. niekrytyczny/krytyczny),
  - ocenę wpływu incydentu na działalność Zamawiającego,
  - podjęcie działań reagujących (automatycznych lub manualnych),
  - dokumentowanie przebiegu incydentu.
– W ramach reagowania SOC realizuje m.in.:
  - blokowanie podejrzanych adresów IP lub domen,
  - izolację zainfekowanych stacji roboczych lub serwerów,
  - blokowanie lub resetowanie kont użytkowników,
  - rekomendowanie działań naprawczych i zapobiegawczych.

10. Eskalacja i komunikacja

– Wykonawca zapewni wielopoziomowy model eskalacji, obejmujący co najmniej:
  - analityków I linii SOC,
  - analityków II/III linii SOC,
  - kontakt z wyznaczonymi osobami po stronie Zamawiającego.
– O wykryciu incydentów o wysokim i krytycznym poziomie istotności Zamawiający musi być informowany niezwłocznie, zgodnie z ustalonym SLA, co najmniej:
  - drogą telefoniczną,
  - oraz drogą elektroniczną (e-mail / system zgłoszeń).

11. Poziomy SLA

Wykonawca zapewni czasy reakcji SOC:

- 2h na podjęcie incydentu
- N – niekrytyczny - 48h na rozwiązanie incydentu
- K – krytyczny - 4h na rozwiązanie incydentu

11. Zakres obowiązków dla poszczególnych Linii wsparcia SOC:

Wykonawca w ramach realizowanej usługi musi zapewnić 3 linie wsparcia:

– Wymagania dla Linii I SOC
  - tryb 24/7/365,
  - ciągła weryfikacja zdarzeń przesyłanych ze źródeł do systemu SIEM,
  - analiza zdarzeń zgodnie z ustalonymi z Zamawiającym procedurami i scenariuszami, w tym ustalenie typu i poziomu incydentu oraz eliminacja tzw. false-positive,
  - wystawienie zgłoszenia w systemie obsługi Incydentów bezpieczeństwa, w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa oraz udokumentowanie w nim wszystkich zebranych informacji na temat danego incydentu,
  - obsługa incydentów w zakresie opracowanych wspólnie z Zamawiającym scenariuszy reakcji dla I linii,
  - w przypadku Incydentów, dla których nie zostały opracowane scenariusze reakcji, nastąpi przekazanie obsługi Incydentu do II linii SOC,

- raportowanie - realizacja okresowych raportów podsumowujących ilość incydentów i czasy obsługi,
- czas zamknięcia lub przekazania zgłoszenia (do II linii SOC lub Zamawiającego – zgodnie z procedurą) od momentu reakcji nie może być dłuższy niż 60 minut.
- identyfikacja i weryfikacja alarmów na bazie zaimplementowanych reguł korelacyjnych w SIEM,
- potwierdzenie wystąpienia incydentu,
- triage – ocena stopnia niebezpieczeństwa związanego z potwierdzonym incydentem.

– Wymagania dla Linii II SOC
  - tryb 8/5, w razie incydentów krytycznych, Zamawiający wymaga, aby Wykonawca pracował w dyżurach 24/7,
  - zdalna analiza otrzymanego zgłoszenia, zebranie wszystkich niezbędnych informacji do poprawnego obsłużenia incydentu, weryfikacja poprawności i kompletności dostarczonych danych źródłowych,
  - opracowanie scenariusza mitygacji zagrożenia wynikającego z incydentu oraz wsparcie pracowników Zamawiającego przy realizacji przygotowanego scenariusza,
  - przygotowanie scenariusza działań mitygacyjnych mających na celu usunięcie skutków incydentu,
  - szczegółowa analiza incydentu wraz z rekomendacjami, powinna być zakończona raportem, w zależności od dostępności danych, zawiera takie informacje jak:
    a. Data i godzina wykrycia incydentu.
    b. Unikalny identyfikator zdarzenia.
    c. Kiedy incydent wystąpił?
    d. Kto lub jaki proces był sprawcą incydentu?
    e. Co się wydarzyło?
    f. Gdzie wydarzenie miało miejsce?
    g. Dlaczego zdarzenie mogło wystąpić?
    h. Jakie czynności zostały przeprowadzone w celu powstrzymania incydentu?
  - opracowanie wniosków z incydentu, mających na celu ograniczenie możliwości powtórzenia się danego typu incydentu w przyszłości,
  - analiza, w ramach której wykonywane będą: analiza logów pod kątem zabezpieczenia Zamawiającego przed pojawiającymi się nowymi zagrożeniami, nie objętych dotychczasowymi regułami zaimplementowanymi w systemie SIEM, jak i procedurami reakcji dla I linii SOC,
  - analiza logów pod kątem optymalizacji informacji o zagrożeniach w SIEM,
  - proponowanie nowych scenariuszy bezpieczeństwa lub przygotowywanie ich na zlecenie Zamawiającego do wdrożenia w systemie SIEM,
  - proponowanie optymalizacji (tuning) aktualnie działających scenariuszy bezpieczeństwa,
  - proponowanie rozszerzenia zakresu monitorowania o kolejne systemy teleinformatyczne Zamawiającego,
  - Utrzymanie systemu SIEM: aktualizacje i patche Systemu, zmiany konfiguracji, wsparcie serwisowe, obsługa awarii, przegląd i strojenie Systemu,
  - analiza przesłanych próbek Malware,

12. Raportowanie

Usługa SOC musi obejmować:

- bieżący dostęp Zamawiającego do informacji o incydentach,
- raporty okresowe (np. miesięczne), zawierające co najmniej:
  - liczbę i rodzaj wykrytych incydentów,
  - czas reakcji i obsługi incydentów,
  - trendy i rekomendacje dotyczące poprawy bezpieczeństwa,
- raporty ad-hoc w przypadku incydentów krytycznych.

13. Infrastruktura Zamawiającego

– Zamawiający wskazuje jako źródła dla logów następujące systemy:
- Komputery z systemem Windows
- Urządzenia sieciowe
- Serwery, Macierze, Serwery plików

- VM z Windows Server
- VM z Linux
- Bazy Danych
- Aplikacje dziedzinowe
- System SCADA
- Oprogramowanie antywirusowe
- Inne systemy i urządzenia przesyłające logi zgodne określonym standardem w Załączniku nr 1

– Logi zebrane ze wskazanych przez Zamawiającego źródeł będą składowane przez Wykonawcę za okres pierwszych 12 miesięcy na kolektorze logów umiejscowionym w infrastrukturze Zamawiającego oraz za okres od 12 do 24 miesięcy w formie zarchiwizowanej na wskazanym zasobie dyskowym.

14. Termin wykonania przedmiotu zamówienia

– Wykonawca zobowiązany jest do realizacji przedmiotu zamówienia w dwóch etapach:
  - **ETAP I** – dostarczenie, wdrożenie i uruchomienie usługi
    ETAP I obejmuje dostarczenie wszystkich elementów niezbędnych do realizacji usługi, ich wdrożenie oraz uruchomienie usługi i zostanie zrealizowany w terminie do 60 dni roboczych od dnia zawarcia umowy.
  - **ETAP II** – świadczenie usługi Security Operations Center (SOC)
    ETAP II obejmuje świadczenie usługi będącej przedmiotem zamówienia przez okres **36 miesięcy**, liczony od dnia podpisania protokołu odbioru potwierdzającego prawidłowe wdrożenie i uruchomienie usługi, o którym mowa w ETAPIE I.
– Odbiór prac w ramach ETAPU I zostanie dokonany na podstawie protokołu odbioru podpisanego przez obie strony, w terminie do 7 dni kalendarzowych od dnia zgłoszenia przez Wykonawcę gotowości instalacji do odbioru albo – w przypadku stwierdzenia usterek w trakcie odbioru – od dnia potwierdzenia przez Zamawiającego usunięcia przez Wykonawcę zgłoszonych usterek.
– Za dzień rozpoczęcia świadczenia usługi, uznaje się dzień następujący po dniu podpisania protokołu odbioru
– Całkowity termin realizacji przedmiotu zamówienia obejmuje okres realizacji ETAPU I oraz okres świadczenia usługi w ramach ETAPU II.

Szczegółowy opis funkcjonalny zintegrowanego systemu bezpieczeństwa

1. Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi. oraz przeprowadzenie szkoleń z obsługi oraz administrowania wdrożonego systemu SIEM/SOAR dla administratorów systemów IT u Zamawiającego.

2. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.

3. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach.

4. System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI;

5. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.

6. System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.

7. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.

8. Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.

9. Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.

10. Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.

11. System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku, gdy będzie to konieczne przywrócić jedną z poprzednich wersji.

12. System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg" znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.

13. Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni, w której te logi są przesyłane. Przykładowo, jeżeli logi są przesyłane w standardzie CEF system dobierze odpowiedni parser, w przypadku, gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora.

14. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.

15. System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo, jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku, gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.

16. Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.

17. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów.

18. Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe.

19. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.

20. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.

21. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.

22. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.

23. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.

24. Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie" na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów.

25. System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.

26. System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług.

27. System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.

28. System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.

29. Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje:

a. nowe zasoby wykryte w sieci,

b. typy wykrytych zasobów (np.: serwer lub stacja robocza),

c. zastosowane na nich zabezpieczenia,

d. usługi, z którymi się komunikują,

e. nowe usługi wykryte na zasobie

f. komunikację do usług wykrytych na zasobie.

30. System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.

31. System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.

32. Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi, której ta komunikacja dotyczy.

33. System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników:

a. fqdn,

b. e-mail,

c. nazwa pliku,

d. ścieżka do pliku,

e. hash,

f. adres IP,

g. klucz rejestru,

h. cmd.

34. System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest, aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (https://www.misp-project.org/).

35. System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu).

36. Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).

37. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie. Minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.

38. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.

39. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności (np.: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).

40. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.

41. System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.

42. Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration), umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.

43. System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności:

a. id techniki,

b. taktykę,

c. platformy których dotyczy,

d. potencjalne źródła,

e. opis zagrożenia,

f. mityzację,

g. sposób detekcji,

h. referencje.

44. System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.

45. Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).

46. System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum:

a. rozdzielenie procesu nauczania zachowania użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych,

b. rozdzielenie procesu nauczania zachowania stacji roboczych od serwerów,

c. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji,

d. rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.

47. System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).

48. Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji.

49. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).

50. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.

51. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.

52. System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać:

a. sparsowane pola oraz ich wartości,
b. listy referencyjne,
c. atrybuty użytkowników z Active Directory,
d. atrybuty komputerów z Active Directory,
e. bazę wskaźników kompromitacji (IOC),
f. informacje z elektronicznej dokumentacji,
g. anomalie w zachowaniu użytkowników (UBA),
h. anomalie w zachowaniu zasobów (EBA),
i. podatności na zasobach,
j. wyniki analizy konfiguracji,
k. techniki MITRE ATT&CK®,

53. Reguły korelacyjne bazujące na sparsowanych polach i ich wartościach muszą umożliwić:

a. wykrycie dowolnej treści w logach,
b. wykrycie zmiany jednego z kilku pól,
c. wykrycie zaniku wiadomości,
d. wykrycie nowej wartości pola w zadanym okresie czasu,
e. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności,
f. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu,
g. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu,
h. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa,
i. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu,
j. wykrycie chwilowego wzrostu (tzw. peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu,
k. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa,
l. wykrycie ilości uruchomionych procesów w zadanym okresie czasu,
m. wykrycie skanowania portów.

54. Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić:

a. wykrycie wystąpienia wartości pola na wybranej liście,
b. wykrycie niewystępowania wartości pola na wybranej liście,
c. wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku, z którego został uruchomiony),
d. wykrycie niewystąpienia pary wartości na wybranej liście
e. (np.: nazwa użytkownika wraz aplikacją, z którą się wcześniej nie łączył).

55. Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić:

a. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory,
b. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory,

c. wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta).

d. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins),

e. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.

56. Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić:

a. wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory,

b. wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory,

c. wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.

57. Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić:

a. wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji;

b. wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji;

c. wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji;

58. Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić:

a. wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu,

b. wykrycie połączenia do usługi przez nieautoryzowanego użytkownika,

c. wykrycie nieautoryzowanej usługi na serwerze,

d. wykrycie nieautoryzowanego połączenia do usługi na serwerze,

e. wykrycie nieautoryzowanego połączenia z serwera usług,

f. wykrycie nieautoryzowanego połączenia do sieci Internet.

59. Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić:

a. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,

b. wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware,

c. wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie,

d. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.

60. Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić:

a. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania,

b. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware,

c. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie,

d. wykrycie anomalii związanych z procesami uruchamianymi na serwerach.

61. Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić:

a. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności,

b. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności,

c. wykrycie zdarzeń o wysokim „severity” na zasobach posiadającego krytyczne podatności,

d. wykrycie zdarzeń o wysokim „severity” do zasobów posiadających krytyczne podatności.

62. Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą pozwalać na:

a. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków,

b. wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł niespełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

63. Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić:

a. wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,

b. wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP,

c. wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.

64. Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.:

a. wykrycie anomalii na koncie uprzywilejowanym użytkownika,

b. wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej,

c. wykrycie wielu typów anomalii na komputerze z krytyczną podatnością,

d. wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi,

e. wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.

65. System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać:

a. sparsowane pola oraz ich wartości,

b. atrybuty użytkowników z Active Directory,

c. atrybuty komputerów z Active Directory,

d. informacje z elektronicznej dokumentacji.

66. Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, iż każde kolejne zdarzenie wynikające z reguł korelacyjnych, spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po:

a. adresie IP,

b. koncie domenowym użytkownika,

c. strefie bezpieczeństwa,

d. zakresie adresów IP.

67. Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop" umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.

68. System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.

69. Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in.

a. wszystkie skorelowane zdarzenia,

b. korespondencja pocztowa,

c. załączniki z próbkami lub dowodami,

d. wskaźniki kompromitacji (IoC),

e. informacje pozyskane z innych systemów.

70. System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.

71. Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.: na podstawie pozyskanego wskaźnika kompromitacji (IoC) zmienić status zdarzenia na incydent bezpieczeństwa.

72. Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji, system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane:

a. identyfikację celu i źródła zagrożenia,

b. nazwę oraz adres IP źródła zagrożenia,

c. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza,

d. lokalizację z które pochodzi zagrożenie np.: Internet,

e. strefę bezpieczeństwa z której pochodzi zagrożenie,

f. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło,

g. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification),

h. nazwę oraz adres IP celu zagrożenia,

i. zabezpieczenia lokalne chroniące cel zagrożenia,

j. strefę bezpieczeństwa w której znajduje się cel zagrożenia.

73. Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Na przykład: dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku, gdy jest on zabezpieczony przez rozwiązanie klasy WAF (Web Application Firewall).

74. Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami. Przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem.

75. Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła jak i celu zagrożenia w następującym zakresie:

a. nazwy zasobu,

b. rodzaju zasobu,

c. ważności zasobu dla organizacji,

d. rodzaj przetwarzanych informacji,

e. usług, które ten zasób świadczy,

f. lokalizację użytkowników, którzy z niego korzystają,

g. usługi, z których zasób korzysta.

76. System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu, którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do

krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych.

77. Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to:

a. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie,

b. segregacja – segregacja i kwalifikacja zdarzeń,

c. incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa,

d. fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm,

e. zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie.

System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo: umożliwiać przejście ze statusu „incydent bezpieczeństwa" do statusu „zdarzenie zamknięte", ale zablokować zmianę ze statusu „incydent bezpieczeństwa" na status „fałszywy alarm".

78. System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.

79. System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia, z którym są grupowane oraz synchronizować z nim statusy. Dla zdarzeń przetwarzanych przez operatora, zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych. Na przykład: zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach z nim powiązanych.

80. Obsługiwane zdarzenia muszą zapewniać historyczność, obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowane w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi). Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów.

81. Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.

82. W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Na przykład: jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie porównać je ze wszystkimi wskaźnikami typu FQDN oraz HASH, zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.

83. System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.

84. W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny pozwalający mu na:

a. podgląd aktywności zagrożonego zasobu na linii czasu,

b. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku,

c. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu,

d. podgląd reguły korelacyjnej, która wygenerowała zdarzenie,

e. w przypadku wykrytej techniki MITRE ATT&CK® jej szczegółowy opis,

f. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich,

g. gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o:

- listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po,
- listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym,

h. gotowe i proste w użyciu filtry rozszerzajcie analizę logów o:

- listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym,
- listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.

85. Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

a. warunki powiadomień,
   - zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
   - zdarzeń o przekroczonych czasach SLA o definiowalny okres,
   - zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
   - zdarzeń, których priorytet osiągnął określoną wartość,
   - zdarzeń zakwalifikowanych jako incydent bezpieczeństwa,
   - zdarzeń, na których doszło do naruszenia bezpieczeństwa,
   - zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną,
   - zdarzeń realizujących zdefiniowaną usługę,
   - zdarzeń przetwarzających sklasyfikowane informację,
   - zdarzeń przetwarzanych na krytycznych zasobach,

b. odbiorców powiadomień, w tym:
   - operatora, któremu zostało przydzielone zdarzenie,
   - właściciela zasobu, na którym wystąpiło zdarzenie,
   - zespół obsługi, który odpowiada za obsługę zdarzeń,
   - właściciela usługi, która jest realizowana na zasobie, na którym wystąpiło zdarzenie,
   - podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną.

c. kanały powiadomień, m.in. e-mail, sms, komunikator,

d. zastosowanie mechanizmów grupowania:
   - grupowanie wielu powiadomień w jednej wiadomości,
   - ograniczenie liczby wierszy powiadomienia do określonej wartości.

86. System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku, gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

a. utworzenia nowego zdarzenia z określonym priorytetem,
b. utworzenia nowego zdarzenia na zasobie krytycznym,
c. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę,
d. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe,
e. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej,
f. modyfikacji przydzielonego operatorowi zdarzania przez innego operatora,
g. zamknięcia przydzielonego operatorowi zdarzania przez innego operatora,
h. przejęcia przydzielonego operatorowi zdarzania przez innego operatora.

87. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego:

a. wybór raportu, który ma zostać wysłany,
b. zdefiniowanie jego tytułu,

c. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,

d. możliwość ograniczenia cyklu do dni powszednich,

e. określenie daty przesłania pierwszego raportu,

f. możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do:

- zdefiniowanej daty końcowej,

- określnej liczby raportów,

g. określenie odbiorców raportu.

88. System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (Playbook).

89. Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry:

a. strefę bezpieczeństwa w której została wykryta podatność,

b. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie,

c. rodzaj zasobu, którego dotyczy ta podatność,

d. ważność tego zasobu dla organizacji,

e. przetwarzane na tym zasobie informacje, np.: dane osobowe,

f. usługi realizowane przez ten zasób, np.: DNS,

g. wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact” = High,

h. poprawność konfiguracji zasobu, na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł,

i. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet.

90. W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.

91. Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:

a. wyliczonym priorytecie podatności,

b. aktualnym statusie obsługi,

c. ważności zasobu, na którym została wykryta,

d. adresie IP tego systemu,

e. parametrów SLA związanych z tym statusem,

f. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,

g. parametrach CVSS, np.: lista podatności których „Access Complexity (AC)” = „low” oraz „Access Vector (AV) = „Network”.

92. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień dla kadry zarządzającej, obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienia kierowników jednostek organizacyjnych w następujących sytuacjach:

a. przekroczenia czasu reakcji o określony czas np.: o godzinę,

b. możliwości przekroczenia czasu reakcji, np.: została godzina, aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji,

c. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe,

d. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym,

e. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę,

f. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe,

g. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych,

h. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę,

i. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe,

j. przekroczenia czasu reakcji dla podatności na zasobie krytycznym,

k. przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,

93. Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących:

a. warunki powiadomień,

- podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi,
- podatności o przekroczonych czasach SLA o definiowalny okres,
- podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA,
- podatności, których priorytet osiągnął określoną wartość,
- zdarzeń realizujących zdefiniowaną usługę,
- zdarzeń przetwarzających sklasyfikowane informację,
- zdarzeń przetwarzanych na krytycznych zasobach,

b. odbiorców powiadomień, w tym:

- operatora, któremu została przydzielona podatność,
- właściciela zasobu, na którym wystąpiła podatność,
- zespół obsługi, który odpowiada za obsługę podatności,
- właściciela usługi, na która jest realizowana na zasobie, na którym wystąpiła podatność,
- podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną.

c. kanały powiadomień, m.in. e-mail, sms, komunikator,

d. zastosowanie mechanizmów grupowania:

- grupowanie wielu powiadomień w jednej wiadomości,
- ograniczenie liczby wierszy powiadomienia do określonej wartości.

94. System powinien posiadać gotowe szablony powiadomień, pozwalające na wysyłanie powiadomień jego operatorom w przypadku, gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach:

a. przydzielenia nowej podatności do obsługi z określonym priorytetem,

b. przydzielenia nowej podatności do obsługi na zasobie krytycznym,

c. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę,

d. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe,

e. modyfikacji przydzielonej operatorowi podatności przez innego operatora,

f. zamknięcia przydzielonej operatorowi podatności przez innego operatora,

g. przejęcia przydzielonej operatorowi podatności przez innego operatora.

95. Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora pozwalającego na:

a. wybór raportu, który ma zostać wysłany,

b. zdefiniowanie jego tytułu,

c. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,

d. możliwość ograniczenia cyklu do dni powszednich,

e. określenie daty przesłania pierwszego raportu,

f. określenie okresu przez jaki będą one przesyłane, poprzez:

- zdefiniowanie daty końcowej,
- bez daty końcowej,
- określenie liczby raportów,

g. określenie odbiorców raportu.

96. System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard'u", tj. dostosowywać zakres i prezentacje danych do potrzeb zalogowanego użytkownika.

97. System musi pozwalać na tworzenie dedykowanych dashboard'ów obejmujących:

a. zestaw wykresów dla bieżącego użytkownika,

b. zestaw wykresów dla wybranego użytkownika,

c. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu,

d. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC (Security Operations Center).

98. System musi zapewniać zestaw predefiniowanych dashboard'ów obejmujących następujące wykresy:

a. wykres przedstawiający status klasyfikacji zdarzeń, który uwzględnia:

- ilość zdarzeń nowych i niesklasyfikowanych,
- ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa,
- ilość zdarzeń sklasyfikowanych jako fałszywe alarmy,

b. wykres przedstawiający skale zagrożeń, który uwzględnia:

- ilość zasobów krytycznych na których są obsługiwane zdarzenia,
- ilość zasobów niekrytycznych na których są obsługiwane zdarzenia,

c. wykres przedstawiający źródła zagrożeń, który uwzględnia:

- ilość nowych zdarzeń dotyczących użytkowników,
- ilość podjętych zdarzeń dotyczących użytkowników,
- ilość nowych zdarzeń dotyczących zasobów,
- ilość podjętych zdarzeń dotyczących zasobów,

d. wykres przedstawiający poziom zagrożeń, który uwzględnia:

- ilość nowych zdarzeń w podziale na priorytety,
- ilość podjętych zdarzeń w podziale na priorytety,

e. wykres przedstawiający czas obsługi zagrożeń, który uwzględnia:

- ilość zdarzeń zarejestrowanych w bieżącym dniu,
- ilość zdarzeń zarejestrowanych w ostatnim tygodniu,

- ilość zdarzeń zarejestrowanych w ostatnim miesiącu,
- ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu,

f. wykres przedstawiający zagrożone usługi, który uwzględnia:

- ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia,
- ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia,

g. wykres przedstawiający zagrożone dane, który uwzględnia:

- ilość nowych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
- ilość podjętych zdarzeń dotyczących zasobów krytycznych, przetwarzających sklasyfikowane informacje,
- ilość nowych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,
- ilość podjętych zdarzeń dotyczących pozostałych zasobów, przetwarzających sklasyfikowane informacje,

h. wykres przedstawiający skale podatności, który uwzględnia:

- ilość zasobów krytycznych na których są obsługiwane podatności,
- ilość zasobów niekrytycznych na których są obsługiwane podatności,

i. wykres przedstawiający czas obsługi podatności, który uwzględnia:

- ilość podatności zarejestrowanych w bieżącym dniu,
- ilość podatności zarejestrowanych w ostatnim tygodniu,
- ilość podatności zarejestrowanych w ostatnim miesiącu,
- ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu,

j. wykres przedstawiający wagę podatności, który uwzględnia:

- ilość nowych podatności w podziale na priorytety,
- ilość podjętych podatności w podziale na priorytety,

99. Nawigacja w ramach „Dashboard'u" musi wspierać opcję typu „Drill down" w następującym zakresie:

a. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,

b. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,

c. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,

d. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,

e. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres,

f. „kliknięcie" wartości prezentowanej na wykresie, dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem, pozwalającym pokazać te same wartości których dotyczy wykres.

100. Rozwiązanie może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.

101. Rozwiązanie musi zapewniać elastyczną i skalowalną architekturę, której rozbudowa nie będzie wymagała zakupu dodatkowych licencji, zapewniając tym samym możliwość wydzielania następujących warstw funkcjonalnych zwanych dalej kolektorami, do instalacji na osobnych serwerach bądź maszynach wirtualnych:

a. kolektor parsujący;

b. kolektor logów;

c. kolektor korelacyjny;

d. kolektor zdarzeń;

e. kolektor sztucznej inteligencji;

f. kolektor reakcyjny;

g. kolektor kontrolujący.

102. Kolektor parsujący powinien być odpowiedzialny za odbieranie i parsowanie logów a następnie ich przesyłanie zarówno postaci surowej jak i sparsowanej do odpowiednich kolektorów logów, zgodnie z regułami ich przekierowania zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym. Pojedynczy kolektor parsujący musi zapewniać wydajność co najmniej 20 tysięcy zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

103. Kolektor logów powinien być odpowiedzialny za przechowywanie logów zarówno w postaci surowej jak i sparsowanej oraz przechowywać pliki indeksów. Logi muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu). Pojedynczy kolektor logów powinien mieć wydajność co najmniej 10 tyś zdarzeń na sekundę w trybie ciągłym oraz posiadać bufor do obsługi natłoku w rozmiarze miliona zdarzeń.

104. Kolektor korelujący powinien umożliwiać korelację logów oraz ich agregację zgodnie z regułami korelacyjnymi zdefiniowanymi w jednym miejscu dla wszystkich kolektorów w interfejsie graficznym.

105. Kolektor zdarzeń powinien umożliwiać składowanie zdarzeń stanowiących wyniki korelacji oraz umożliwiać ponowne wykorzystanie tych zdarzeń w kolejnych regułach umożliwiając tym korelację zależności pomiędzy nimi. Zdarzenia muszą być przechowywane w postaci skompresowanej oraz kolektor musi zapewnić mechanizmy zabezpieczające je przed nieautoryzowaną modyfikacją (np.: Certyfikat cyfrowy czy funkcja skrótu).

106. Kolektor sztucznej inteligencji powinien zawierać wiedzę pozyskaną ze środowiska obejmującą zarówno linię trendu zachowania użytkowników oraz zasobów obejmujące mechanizmy uczenia maszynowego jak i algorytmy sztucznej inteligencji pozwalające na wypracowanie nowej wiedzy wynikającej z korelacji wyników wiedzy wypracowanej poprzez inne metody.

107. Kolektor reakcyjny musi umożliwiać automatyczną reakcję na wykryte zagrożenia, która nie będzie wymagała żadnej interakcji ze strony użytkownika, chyba że taka będzie dodatkowo zdefiniowana. W celu automatyzacji reakcji musi posiadać funkcjonalność systemu PAM lub być z nim dostarczony w celu przechowywania danych uwierzytelniających oraz kluczy API potrzebnych do automatyzacji reakcji.

108. Architektura rozwiązania musi w pełni wspierać konfigurację niezawodnościową, zapewniającą zarówno pełną redundancję w zakresie, odbierania logów i ich przechowywania, korelacji oraz reakcji na zagrożenia jak i możliwość zastosowania konfiguracji o ograniczonej redundancji do najważniejszych dla zamawiającego źródeł danych.

109. Konfiguracja niezawodnościowa musi wspierać możliwość zastosowania stosu kolektorów zastępczych które zostaną uruchomione w przypadku awarii stosu podstawowego, przy czym wszystkie one muszę być zarządzane centralnie z poziomu tej samej konsoli co kolektory podstawowe.

110. Kolektory muszą mieć zapewnione mechanizmy automatycznej aktualizacji zarówno w zakresie parserów czy reguł korelacyjnych jak i wersji oprogramowania, przy czym aktualizacja musi odbywać się z poziomu centralnego systemu zarządzania.

111. Rozwiązanie musi zapewnić konsole do aktualizacji pozwalającą na wybór dodatkowych pakietów reguł czy parserów udostępnianych w ramach aktywnego wsparcia producenta w formie usługi, każda aktualizacja musi wspierać mechanizm wersjonowania pozwalający zarówno aktualizację jaki i przywracanie poprzednich wersji reguł i parserów.

112. Rozwiązanie musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych lub maszyn fizycznych z nowymi typami kolektorów, przy czym dodawanie nowych komponentów nie może wiązać się z koniecznością zakupu nowej licencji, ani posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej.

113. Skalowanie przez dodawanie nowych kolektorów musi zwiększać wydajność rozwiązania zgodnie z wartościami zadeklarowanymi przez producenta, przykładowo dwa kolektory logów muszą zapewnić dwukrotną wydajność rozwiązania, czyli minimum 20 tyś zdarzeń na sekundę. Przy czym całe rozwiązanie nie może ograniczać ilość zastosowanych kolektorów.

114. Rozwiązanie nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)

115. Poszczególne kolektory zdarzeń oraz logów muszą zapewniać przechowywanie danych zarówno na maszynach wirtualnych jak i na dyskach sieciowych.

116. Kolektor logów musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych.

117. Rozwiązanie przechowywanie logów oraz zdarzeń nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP lub autorskie rozwiązanie producenta.

118. Rozwiązanie musi zapewniać możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania oraz możliwość zbudowania struktury rozproszonej, zapewniającej większą wydajność zapisu i wyszukiwania.

119. Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, raportów, konfiguracji, bazy CMDB oraz innych ustrukturyzowanych informacji.

120. Rozwiązanie musi zapewniać możliwość automatycznego budowania kontekstu poprzez wykrywanie urządzeń oraz komputerów mających swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB).

121. Wymagane jest, aby kolektor odpowiedzialny za parsowanie pozwalał na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania.

122. Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów

123. Tworzenie własnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)

124. Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI).

125. Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:

a. zdolność do definiowania wzorców które powtarzają się jako zmienne;

b. zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych;

c. zdolność do testowania poszczególnych funkcji;

d. zdolność do przekształcania danych w trakcie ich parsowania.

126. Rozwiązanie SIEM/SOAR musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:

a. centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej;

b. możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows;

c. możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application;

d. zdolność do monitorowania integralności plików;

e. zdolność do monitorowania rejestru systemowego;

f. zdolność do monitorowania urządzeń zewnętrznych (removable devices);

g. agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM.SOAR w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS;

h. musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu;

i. musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS;

j. musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu.

127. System musi mieć możliwość realizacji funkcjonalności UEBA (User Entity Behaviour Analysis) zarówno w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar.

128. Rozwiązanie musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI

129. System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń.

130. Rozwiązanie musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data).

131. System musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi

132. System musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np.VirusTotal.

133. System musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK dla standardowego zbioru wbudowanych reguł.

134. Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji.

135. Rozwiązanie musi mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system) oraz mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów.

136. System musi wpierać mechanizmy typu Machine Learning w oparciu o zgromadzone zdarzenia. Musi być możliwe użycie przynajmniej 4 różnych rodzajów mechanizmów Machine Learning wraz z możliwością ich ręcznego wybrania oraz działania w trybie automatycznym. W wyniku działania opisanych mechanizmów Machine Learning system SIEM/SOAR ma tworzyć model bazowy zachowania oraz umożliwiać wykrycie odchyleń i anomalii od niego. Zadania Machine Learning mają mieć możliwość dystrybuowania ich pomiędzy elementy warstwy korelującej i/lub zarządzającej. Mechanizmy Machine Learning mają również umożliwiać wsparcie dla podejmowania decyzji przy rozwiązywaniu incydentów w systemie SIEM/SOAR.

137. W związku z tym, że obsługa systemu ma objąć także użytkowników nieposługujących się biegle językiem angielskim, interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski. Pliki tłumaczące interfejs na język polski muszą zostać wgrane w trakcie wdrożenia systemu, przed jego zakończeniem.

138. Zamawiający na obecnym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie.

139. Produkt musi umożliwiać równoczesną pracę co najmniej 5 operatorów oraz obsługiwać min. 150 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerem i sprzętem wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.

140. System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.

141. Usługa SOC musi być świadczona całodobowo (24/7/365) w oparciu o system bezpieczeństwa SIEM/SOAR, który powinien znajdować się na dedykowanym środowisku wysokiej dostępności HA w profesjonalnym Data Center spełniający minimum wymogi TIER III i znajdujący się na terenie Unii Europejskiej.

142. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016 lub nowszych), Redhat/Oracle Linux (minimum 7.x).

143. Dostarczone rozwiązanie musi być objęte wsparciem producenta lub producentów przez okres 36 miesięcy. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego).

144. Wykonawca musi zapewnić usługę obejmującą proces aktualizacji oprogramowania oraz kontekstu systemu (dotyczy to zwłaszcza bazy reguł korelacyjnych, bazy parserów, bazy dostępnych aktualizacji). Dostęp do centralnej usługi aktualizacyjnej ma pozwalać na automatycznie wyświetlanie i pobieranie z poziomu interfejsu systemu dostępnych aktualizacji. Dla

pobranych w procesie aktualizacji reguł oraz parserów musi być dostępne wersjonowanie, pozwalające uruchomić nową wersję reguły korelacyjnej oraz parsera z poziomu interfejsu systemu. Automatyczne wersjonowanie ma umożliwiać wczytanie starszej wersji reguły lub parsera, a zmiana reguł i parserów musi być możliwa z poziomu graficznego systemu.

145. Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu lub systemów. Szkolenie ma zostać przeprowadzone dla maksymalnie 1 osoby i muszą być zakończone przyznaniem certyfikatu, potwierdzającego wspomniane umiejętności wydanym przez producenta systemu/ systemów. Szkolenia mogą odbyć się w formie zdalnej.

146. System rozszerzonej detekcji i reagowania powinien posiadać następujące cechy i funkcjonalności

a. Powinien posiadać możliwość instalacji agenta na systemach: - Windows 10 i nowsze,

- Windows Server 2016 i nowsze. Agent umożliwia: zbieranie logów ze stacji końcowej/serwera do modułu SIEM/SOAR, dodawania i wyłączanie reguł zapory sieciowej na stacji końcowej/serwerze, zawieszanie i odwieszanie procesu na stacji końcowej/serwerze. Dodatkowo zapewnia mechanizm do instalacji oraz zarządzania konfiguracją narzędzia Microsoft Sysmon na stacjach końcowych/serwerach, w celu rozszerzenia logów systemowych o aktywność procesów, plików oraz rejestrów.

b. System powinien być wyposażony w serwer aplikacji udostępniający konsolę graficzną dla operatorów oraz sterujący działaniem orkiestratora oraz kontrolera

c. System powinien posiadać Orkiestrator służący do wykonania akcji na innych systemach niż komputery, na których zainstalowany jest agent, np.: zablokowanie ruchu wychodzącego na Firewall dla hosta, na którym zainstalowany jest agent służy do zarządzania agentami i jest odpowiedzialny zarówno za ich monitorowanie, aktualizację oraz zlecanie im zadań, np.: izolacja procesu czy izolacja sieciowa

d. Agent powinien wzbogacać analizę zdarzeń na nim występujących o pełne dane telemetryczne.

e. System powinien posiadać centralny kontroler zarządzający agentami oraz monitorujący ich pracę

f. System powinien posiadać mechanizm wykrywania zagrożeń zgodny z taktykami i technikami Mitre Att&ck™

g. System powinien umożliwiać wykrywanie zagrożeń na komputerze na bazie wielu wskaźników naruszeń bezpieczeństwa (IoC)

h. System powinien umożliwiać centralną korelację zdarzeń z komputera względem innych zdarzeń (sieć, chmura, Threat Intel)

i. System powinien być wyposażony w mechanizmy uczenia maszynowego obejmujące analizę behawioralną komputera oraz jego użytkownika

j. System powinien posiadać wiele algorytmów wykrywania anomalii oraz profilowania komputera i jego użytkownika

k. System powinien umożliwiać rozszerzoną analizę behawioralną użytkownika komputera względem pracy innych użytkowników

l. System powinien umożliwiać kontrolę aplikacji zainstalowanych na stacjach roboczych i serwerach

m. System powinien umożliwiać kontrolę podatności, zgodności oraz zainstalowanych poprawek

n. System powinien mieć możliwość zaawansowanej analizy zdalnej np.: uruchomione procesy czy połączenia sieciowe

o. System powinien posiadać mechanizmy automatyzujące reakcję na komputerze z poziomu agenta, np.: wstrzymanie procesu, blokada portu

p. System powinien posiadać funkcjonalność dostosowania reakcji na zagrożenia w zależności od rodzajów zagrożeń (konfigurowalne playbooki)

q. System musi być wyposażony w autonomiczny mechanizm oceny ryzyka dla wykrytych zagrożeń

r. System powinien umożliwiać zarządzanie zgodnością (Compliance): KSC/KRI/GDRP

s. System powinien posiadać panel do zarządzania incydentami oraz podatnościami wsparty playbookami

t. System powinien posiadać przejrzyste dashbordy z możliwości drążenia danych oraz wizualizacji zagrożeń

u. System powinien posiadać możliwości powiadamiania o zagrożeniach poprzez e-mail, sms

147. Rozwiązanie musi posiadać możliwość instalacji agentów telemetrii dla systemów Windows.

148. Licencja na agentów telemetrii musi obejmować wszystkie źródła logów liczonych jako komputery oraz serwery wykorzystywane w organizacji.

149. Pełen zakres funkcjonalności agenta telemetrii musi być dostępny z poziomu centralnej konsoli zarządzania.

150. Agent telemetrii powinien być w pełni kontrolowany za pośrednictwem playbooków, umożliwiając wykonywanie akcji izolacji oraz blokowania na podstawie warunków związanych z analizowanymi zdarzeniami.

151. Agent telemetrii powinien umożliwiać blokowanie na poziomie jądra systemu (kernela)

152. Agent telemetrii powinien obsługiwać tryb komunikacji jednostronnej, w którym nie otwiera żadnych portów, a jedynie sam inicjuje połączenia z konsolą zarządzającą.

153. Agent telemetrii musi przesyłać do konsoli centralnej pełen zakres telemetrii, obejmujący m.in. połączenia sieciowe, modyfikacje rejestrów, uruchamianie procesów i komend oraz dostęp do plików, w celu korelacji danych.

154. Rozwiązanie musi posiadać możliwość instalacji agentów telemetrii dla systemów Windows.

155. System umożliwia stworzenie kompletnych w zasoby informacji rejestrów spełniających wymogi art. 30 RODO m. in. rejestru czynności oraz rejestru kategorii czynności przetwarzania zawierających informacje dotyczące przede wszystkim:

- celu/kategorii przetwarzania

- związku z procesem,

- określenia kategorii danych wraz z kategorią osób, których dane są przetwarzane

- oznaczenia podstawy prawnej oraz wymaganej zgody na przetwarzanie danych

- określenia źródła danych

- informacją na temat retencji danych / planowanego terminu usunięcia

- wskazania systemów i oprogramowania do przetwarzania danych wraz z określeniem ich zabezpieczeń

- określenia zastosowanych środków bezpieczeństwa - organizacyjnych i technicznych i wielu innych istotnych z punktu widzenia właściwej ochrony dla przetwarzanych danych osobowych.

156. System umożliwia ewidencjonowanie umów powierzenia przetwarzania danych osobowych zarówno dla danych, których użytkownik jest Administratorem jak i Procesorem.

157. System umożliwia prowadzenie rejestru udostępnień danych osobowych wraz z określeniem wszystkich stosownych, wymaganych przepisami prawa informacji na temat udostępnień.

158. System pozwala na nadawanie upoważnień dla osób przetwarzających dane osobowe w sposób indywidualny jak i zbiorczy. Ponadto dzięki wbudowanemu elektronicznemu obiegowi dokumentów (workflow) proces nadawania i akceptacji upoważnień jest w pełni zautomatyzowany.

159. System maksymalnie usprawnia proces inwentaryzacji obszarów przetwarzania danych osobowych poprzez wyszukiwanie systemów IT przetwarzających tego typu dane jak również grup i kategorii danych osobowych.

160. System wyznacza dostępne zabezpieczenia techniczne w odniesieniu do potencjalnych źródeł zagrożenia dla systemów IT przetwarzających dane osobowe

161. System automatycznie wykonuje analizę ryzyka danych osobowych w odniesieniu do zagrożeń natury informatycznej oraz wykonuje ocenę skutków dla ochrony danych dla trzech głównych ryzyk: ryzyka utraty poufności, integralności oraz dostępności danych osobowych.

162. Analiza ryzyka obejmuje również aspekty nie informatyczne i jest wyliczana zgodnie z wytycznymi opisanymi standardem ISO 29134.

163. System wykonuje analizę ryzyka dla przetwarzanych danych osobowych wraz z określeniem zarówno zagrożeń jak i konsekwencji na jakie narażone są osoby fizyczne z związku z przetwarzaniem ich danych osobowych.

164. System umożliwia szacowanie ryzyka od momentu wdrażania organizacyjnych i technicznych środków bezpieczeństwa przez cały proces przetwarzania danych osobowych w organizacji. Cały proces monitorowania poziomu zagrożeń oraz zapewniania rozliczalności w odniesieniu do zastosowanych zabezpieczeń jest więc procesem ciągłym i na bieżąco dostrajanym.

165. System zapewnia spełnienie wymagań formalno-prawnych dotyczących raportowania naruszeń bezpieczeństwa danych osobowych zgodnie z art. 33 pkt 5 RODO umożliwiając w pełni automatyczne generowanie „Raportu naruszenia ochrony danych osobowych dla organu nadzorczego” łącznie z wyznaczeniem możliwych konsekwencji naruszenia bezpieczeństwa

166. System automatyzuje wykonywanie oceny skutków dla ochrony danych osobowych wraz z automatycznym generowaniem raportów w obszarze analizy ryzyka cyberzagrożeń (art. 35 RODO)

167. System umożliwia rejestrację zgłoszeń incydentów dotyczących danych osobowych związanych ze zbiorami danych osobowych, jednostkami organizacyjnymi, osobami, lokalizacjami oraz zasobami informatycznymi.

168. System umożliwia obsługę incydentów związanych z przetwarzaniem danych osobowych zapewniając możliwość automatycznego ich wykrywania na podstawie logów z systemów informatycznych biorących udział w ich przetwarzaniu. System umożliwia dostrojenie reguł wykrywania zarówno w kontekście informacji pozyskanych z logów jak i parametrów elektronicznej dokumentacji związanej z ich przetwarzaniem. Dedykowana obsługa pozwala na automatyczne przydzielenie zespołu obsługi do incydentu, dotyczącego zasobu przetwarzającego dane osobowe oraz uruchomieniu adekwatnego scenariusza obsługi, np.: dla konsekwencji wycieku danych osobowych.

169. System zapewnia możliwość rejestracji i obsługi wniosków i roszczeń klientów związanych z przetwarzaniem danych osobowych np.: żądanie usunięcia czy sprostowania danych osobowych oraz żądanie otrzymania kopii tych danych.

170. System umożliwia drukowanie prowadzonych rejestrów czynności przetwarzania/kategorii czynności przetwarzania, rejestrów powierzeń oraz udostępnień ja również pojedynczych rekordów z wymienionych rejestrów.

171. System pozwala opracowywać plany postępowania z ryzykiem wraz z określeniem terminowości, ustanowieniem poszczególnych zadań, przypisaniem zespołów obsługi oraz pełną ich rozliczalnością.

172. System pozwala na przechowywanie dokumentów dotyczących systemu ochrony danych osobowych umożliwiając użytkownikom śledzenie zmian w dokumentach, informowanie o zmianach oraz pełnym nadzorem nad dostępem do dokumentów.

173. System powinien posiadać wbudowanego asystenta AI, który wspiera operatora w obsłudze zdarzeń oraz zarządzaniu podatnościami.

174. Asystent AI musi umożliwiać integrację z lokalnymi oraz publicznie dostępnymi modelami językowymi (LLM).

175. Asystent AI powinien działać kontekstowo, z możliwością przypisania odpowiednich promptów do każdego kontekstu.

176. Asystent AI powinien oferować dedykowane tryby działania, obejmujące co najmniej obsługę incydentów, zarządzanie podatnościami, przeglądanie logów, analizę zdarzeń korelacyjnych oraz tworzenie nowych parserów

177. Asystent AI musi być wyposażony w edytor promptów, umożliwiający ich edycję oraz tworzenie nowych.

178. Prompty powinny być wersjonowane i możliwe do pobrania z portalu producenta.

179. Asystent AI musi być dostępny w trybie ciągłym oraz dynamicznie przełączać kontekst w zależności od wykorzystywanych funkcjonalności.

180. Szkolenie ma obejmować zarządzenie i administrację wdrożonym systemem SIEM/SOAR.

181. Zamawiający wymaga, aby w trakcie warsztatów realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym systemem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych.

182. Warsztaty muszą obejmować co najmniej poniższe zagadnienia:

- Wstęp do zarządzania logami,

- Specyfika dostarczonego oprogramowania SIEM/SOAR – wymagania, architektura oraz różnice w wersjach oprogramowania,

- Instalacja i konfiguracja ogólnych ustawień dostarczonego oprogramowania SIEM/SOAR,

- Zbieranie logów, czyli konfiguracja metod pozyskiwania dzienników zdarzeń,

- Przetwarzanie dzienników zdarzeń, czyli tworzenie strumieni logów, ich parsowanie oraz filtrowanie,

- Wizualizacja logów, czyli tworzenie czytelnych zestawień tabelarycznych i graficznych,

- Konfiguracja alertów i powiadomień,

- Administracja i utrzymanie dostarczonego oprogramowania SIEM/SOAR,

- forma praktycznych przykładów użycia dostarczonego oprogramowania SIEM/SOAR.

XXVI. Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa

Lp.	Nazwa podzespołu/ parametry	Opis minimalnych wymagań

1.	UPS	UPS fabrycznie nowy, nie powystawowy, nierekondycjonowany, nie poleasingowy, nie będący przedmiotem prezentacji - rok produkcji nie starszy niż: 2026.
2.	Ilość	1 szt.
1	Obudowa	Typu Rack 19”
2.	Topologia	Line-interactive
3.	Moc skuteczna / Moc pozorna	Min. 2700 W / 3000 VA
4.	Interfejs komunikacyjny	- 1 x 10/100/1000 Base-T (Komunikacja i zarządzanie) - 1 x USB
5.	Gniazda wyjściowe	IEC 320 C13 - 8 szt. IEC 320 C19 - 1 szt. RJ-45 USB
6.	Kable	- 1 x kabel komunikacyjny do UPS (2 metry) - 1 x kabel zasilający do UPS’a (2 metry) - 4 x kabel umożliwiający podłączenie zasilania od UPSa do sprzętu serwerowego
7.	Oprogramowanie i zarządzanie	Do UPSa musi być dołączone oprogramowanie (z wymaganą licencją, jeśli jest niezbędna) umożliwiające konfigurację bezpiecznego wyłączenia serwera po zaniku zasilania. Oprogramowanie musi działać na systemie operacyjnym Microsoft Windows Server 2025.
8.	Zabezpieczenia	Przeciwzwarciowe Przeciążeniowe Przeciwprzepięciowe Termiczne Zabezpieczenie przed przeładowaniem
9.	Sygnalizacja pracy	Wyświetlacz LCD Diody LED Dźwiękowa
10.	Dodatkowe wymogi	Zimny start Automatyczna regulacja napięcia (AVR) Wyłącznik obwodu z możliwością resetu Powiadomienie o rozłączeniu akumulatora Alarmy dźwiękowe Automatyczny test Wbudowany wyświetlacz LCD Funkcja awaryjnego wyłączania zasilania EPO (Emergency Power Off) Inteligentny Slot UPS musi zostać dostarczony wraz z oryginalnymi bateriami.
11.	Gwarancja	Minimum 24 miesiące na UPS oraz baterie.

XXVII. Profesjonalna usługa wdrożenia urządzenia UPS do produktów i rozwiązań z zakresu cyberbezpieczeństwa

Wykonawca jest zobowiązany do dostarczenia, montażu, instalacji, konfiguracji oraz wdrożenia do produkcji **systemu zasilania awaryjnego UPS** zapewniającego ciągłość pracy kluczowej infrastruktury serwerowej, sieciowej i teleinformatycznej Zamawiającego w przypadku zaniku zasilania podstawowego.

1. Dostawa sprzętu i komponentów

- Dostarczenie fabrycznie nowych urządzeń UPS zgodnych ze specyfikacją techniczną zawartą w OPZ (
- Zapewnienie wszystkich niezbędnych komponentów: baterie, moduły dodatkowe, karty komunikacyjne, kable zasilające oraz akcesoria montażowe.
- Dostarczenie wymaganych licencji na oprogramowanie zarządzania UPS (jeśli dotyczy).

2. Montaż i instalacja fizyczna

- Transport i wniesienie urządzeń UPS oraz szaf bateryjnych do serwerowni Zamawiającego.
- Profesjonalny montaż UPS-ów w szafach rack 19”
- Montaż i podłączenie baterii zgodnie z instrukcją producenta oraz normami bezpieczeństwa przeciwpożarowego.
- Podłączenie zasilania wejściowego
- Wykonanie okablowania wyjściowego UPS do listew zasilających PDU lub bezpośrednio do urządzeń

- Oznaczenie wszystkich obwodów

3. Konfiguracja i uruchomienie

- Konfiguracja parametrów pracy UPS
- Instalacja i konfiguracja kart komunikacyjnych
- Konfiguracja automatycznego shutdown serwerów Windows Server.
- Włączenie i konfiguracja funkcji testu baterii oraz kalibracji.
- Aktualizacja firmware'u UPS do najnowszej wersji zalecanej przez producenta.

4. Integracja z infrastrukturą Zamawiającego

- Konfiguracja powiadomień alarmowych (awaria zasilania, niski poziom baterii, przegrzanie, bypass aktywny itp.).

5. Testy i odbiór

- Przeprowadzenie kompleksowych testów systemu UPS, w tym:
  - Test pracy na baterii (autonomia przy pełnym obciążeniu)
  - Test przełączania
  - Test komunikacji i powiadomień alarmowych
  - Test automatycznego shutdown serwerów i maszyn wirtualnych
- Pomiar rzeczywistego czasu podtrzymania oraz obciążenia.
- Sporządzenie szczegółowych protokołów testowych wraz z wynikami pomiarów.
- Usunięcie wszystkich usterek wykrytych podczas testów.
- Ostateczny odbiór techniczny systemu UPS przez Zamawiającego.

6. Dokumentacja

- Przygotowanie kompletnej dokumentacji powdrożeniowej zawierającej:
  - Schemat instalacji i okablowania UPS
  - Parametry konfiguracyjne UPS
  - Procedury postępowania w przypadku awarii zasilania
  - Instrukcje obsługi i konserwacji
  - Karty gwarancyjne oraz spis numerów seryjnych

Wykonawca zobowiązany jest wykonać wszystkie prace zgodnie z normami, zaleceniami producenta UPS oraz zasadami bezpieczeństwa pożarowego i elektrycznego, tak aby system zasilania awaryjnego gwarantował wysoką niezawodność i ciągłość działania kluczowej infrastruktury IT.

XXVIII. Klucze sprzętowe U2F

Klucz sprzętowy	
Nazwa	Klucze sprzętowe U2F kompatybilne z oferowanym oprogramowaniem antywirusowym
Ilość	30 szt.
Interfejs:	USB Typu-A
Specyfikacje kryptograficzne:	• RSA 2048, • RSA 4096 (PGP), • ECC P-256, • ECC P-384, • ECC P-521
Certyfikaty	• FIDO Universal 2nd Factor (U2F), • FIDO2, • IP68, • FIDO L2
Wbudowane moduły:	NFC
Gwarancja:	Minimum 24 miesiące w systemie DoorToDoor.

XXIX. Wdrożenia Klucze Sprzętowe U2F

Wykonawca jest zobowiązany do dostarczenia, konfiguracji oraz wdrożenia do produkcji systemu wieloskładnikowego uwierzytelniania (MFA) z wykorzystaniem **kluczy sprzętowych U2F/FIDO2** jako jednego z głównych mechanizmów wzmacniania bezpieczeństwa dostępu do systemów Zamawiającego.

1. Dostawa kluczy sprzętowych

- Dostarczenie fabrycznie nowych kluczy sprzętowych zgodnych ze standardami **FIDO2** oraz **U2F**
- Zapewnienie kluczy w ilości określonej w OPZ
- Dostarczenie kluczy w wersjach obsługujących interfejsy USB-A oraz NFC

2. Integracja z systemami uwierzytelniania

- Integracja kluczy sprzętowych FIDO2/U2F z systemem wieloskładnikowego uwierzytelniania
- Integracja z **Active Directory Domain Services**

3. Konfiguracja i wdrożenie MFA

- Wdrożenie polityki **MFA obowiązkowego** dla wszystkich kont uprzywilejowanych
- Konfiguracja zasad rejestracji kluczy sprzętowych

4. Dystrybucja i aktywacja kluczy

- Przygotowanie procedury wydawania i aktywacji kluczy sprzętowych dla użytkowników.
- Rejestracja kluczy w systemach uwierzytelniania (Active Directory + ESET PROTECT).

5. Testy i weryfikacja

- Przeprowadzenie testów funkcjonalnych MFA z wykorzystaniem kluczy sprzętowych we wszystkich zintegrowanych systemach.
- Testy scenariuszy awaryjnych
- Sporządzenie protokołów testowych z wynikami.
- Usunięcie wszystkich usterek wykrytych podczas testów.
- Ostateczny odbiór techniczny wdrożenia kluczy sprzętowych przez Zamawiającego.

6. Dokumentacja

- Przygotowanie kompletnej dokumentacji powdrożeniowej zawierającej:
  - Procedurę rejestracji i wydawania kluczy sprzętowych
  - Konfigurację polityk MFA w Active Directory i systemie wieloskładnikowego uwierzytelniania
  - Listę zintegrowanych systemów
  - Instrukcje dla użytkowników i administratorów
  - Procedury postępowania w przypadku utraty lub uszkodzenia klucza

Wykonawca zobowiązany jest wykonać wszystkie prace zgodnie z najlepszymi praktykami F, tak aby wdrożenie kluczy sprzętowych U2F/FIDO2 znacząco podniosło poziom odporności środowiska na ataki phishingowe i przejęcie kont uprzywilejowanych.

XXX. Szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa.

Lp.	Element konfiguracji	Opis wymagań technicznych
1	Wysokość	Wysokość - 42U
2	Wyposażenie	Szafa wyposażona w zdejmowane drzwi przednie i tylne zamykane na klucz, zdejmowane panele boczne. Drzwi przednie perforowane, zamykane na klamkę z kluczykiem, z przewodem uziemiającym. Możliwość zmiany drzwi przednich – prawe/lewe. Drzwi tylne perforowane, zamykane na klamkę z kluczykiem. Słupki pionowe – regulowana głębokość instalacji w szafie, otwory montażowe numerowane w pozycjach U.

		Kółka transportowe oraz nóżki poziomujące w miejscu docelowej instalacji.
3	Wymiary	Minimalna głębokość: 120 cm Minimalna szerokość: 80 cm Minimalna wysokość: 2000 cm
4	Obciążenie	Możliwe obciążenie - 800kg
5	Wymagane normy	1) Zgodność z normami EIA-310
6	Listwy zasilające	Dwie listwy zasilające 19", 9 gniazd, z wyłącznikiem i zabezpieczeniem 1,8 m wtyk C14, gniazda CEE 7/5.
7	Wyposażenie dodatkowe dla szafy	4 x wentylator 2 x organizator kabli 19" 1U szczotkowy, 1 x organizator kabli 19" 1U grzebieniowy
8	Gwarancja	3 lata gwarancji producenta

XXXI. Audyt bezpieczeństwa IT i OT w którym wykonane zostaną: Testy bezpieczeństwa, audyt cyberbezpieczeństwa sieci,

Przedmiot zamówienia:

Przedmiotem zamówienia jest przeprowadzenie kompleksowego audytu bezpieczeństwa środowisk teleinformatycznych (IT) oraz środowisk technologii operacyjnej (OT) Zamawiającego, w celu oceny poziomu bezpieczeństwa, identyfikacji podatności, luk organizacyjnych i technicznych oraz określenia ryzyk cybernetycznych wpływających na ciągłość działania procesów biznesowych i technologicznych.

Audyt obejmuje zarówno aspekty techniczne, organizacyjne, jak i proceduralne, ze szczególnym uwzględnieniem systemów automatyki przemysłowej oraz ich integracji z infrastrukturą IT. W ramach przedmiotu zamówienia Wykonawca wykona dla obszaru IT i OT Testy bezpieczeństwa, audyt cyberbezpieczeństwa sieci, Testy bezpieczeństwa infrastruktury sieciowej, Testy bezpieczeństwa serwisów internetowych, Testy bezpieczeństwa aplikacji

Zakres przedmiotu zamówienia:

1) Audyt środowiska IT obejmuje w szczególności:
   a. analizę architektury infrastruktury IT;
   b. ocenę konfiguracji:
      i. systemów operacyjnych,
      ii. serwerów i stacji roboczych,
      iii. urządzeń sieciowych,
      iv. systemów bezpieczeństwa (firewall, IDS/IPS, EDR/XDR, WAF);
   c. ocenę zarządzania tożsamością i dostępami (IAM);
   d. analizę bezpieczeństwa aplikacji i baz danych (na poziomie konfiguracyjnym);
   e. weryfikację procesów:
      i. zarządzania podatnościami,
      ii. zarządzania aktualizacjami,
      iii. kopii zapasowych i odtwarzania danych;
   f. ocenę odporności na incydenty cyberbezpieczeństwa.
   g. Identyfikację usług otwartych portów dostępnych z sieci publicznej (internet) i przeprowadzanie testów bezpieczeństwa tych usług.
   h. przeprowadzenie testów bezpieczeństwa wykrytych usług wewnątrz sieci pod kątem znanych luk (CVE), błędów konfiguracji oraz podatności na ataki

2) Audyt środowiska OT obejmuje w szczególności:
   a. inwentaryzację i klasyfikację zasobów OT;
   b. ocenę architektury sieci przemysłowej i segmentacji IT/OT;
   c. analizę bezpieczeństwa systemów;
   d. ocenę bezpieczeństwa komunikacji i protokołów przemysłowych (m.in. Modbus, OPC, Profinet, EtherNet/IP);

e. ocenę mechanizmów kontroli dostępu do systemów OT;
f. analizę zarządzania zmianą i aktualizacjami w środowiskach OT;
g. ocenę odporności systemów OT na zagrożenia cybernetyczne.

Audyt IT/ OT powinien być realizowany w sposób nieinwazyjny, z zachowaniem ciągłości działania infrastruktury i bezpieczeństwa procesów technologicznych.

W ramach audytu Wykonawca przeprowadzi również:

a) ocenę polityk bezpieczeństwa informacji;
b) ocenę procedur reagowania na incydenty IT i OT;
c) Ocena planów ciągłości działania i odtwarzania po awarii
d) analizę podziału ról i odpowiedzialności w zakresie cyberbezpieczeństwa;
e) ocenę świadomości bezpieczeństwa personelu (na podstawie wywiadów);
f) weryfikację zgodności z wymaganiami prawnymi i regulacyjnymi.

Wykonawca dostarczy:

a) raport końcowy z audytu IT i OT zawierający:
   i. opis aktualnego stanu bezpieczeństwa,
   ii. zidentyfikowane podatności i niezgodności,
   iii. ocenę ryzyka (wraz z poziomami ryzyka),
   iv. rekomendacje działań korygujących i doskonalących;