GÓRNOŚLĄSKIE
PRZEDSIĘBIORSTWO
WODOCIĄGÓW
SPÓŁKA AKCYJNA

ZAŁĄCZNIK NR 1 DO ZAPROSZENIA

GÓRNOŚLĄSKIE PRZEDSIĘBIORSTWO WODOCIĄGÓW SPÓŁKA AKCYJNA
ul. Wojewódzka 19, 40-026 Katowice

OPIS POTRZEB I WYMAGAŃ
(dalej „OPiW")

Dla postępowania na wykonanie zamówienia o nazwie:
„SOC – Security Operation Center"

Nr postępowania: **FZP/321/35/2023**

Zawartość OPiW:

POSTANOWIENIA OPISU POTRZEB I WYMAGAŃ
(OPiW)

ROZDZIAŁ I – ZAMAWIAJĄCY (INFORMACJE OGÓLNE)

Górnośląskie Przedsiębiorstwo Wodociągów S.A. 40-026 Katowice, ul. Wojewódzka 19, zarejestrowane w Sądzie Rejonowym Katowice-Wschód w Katowicach, Wydział VIII Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000247533, NIP 6340128788, REGON 271506695, wysokość kapitału zakładowego: 425 875 100,00zł, wpłacono w całości, posiadające status dużego przedsiębiorcy w rozumieniu art.4 pkt 6 ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (t.j. Dz.U.2023.711), tel.: +48 32 6038861, fax: +48 32 6038614, **http://www.gpw.katowice.pl**, zwane dalej „Zamawiającym".

ROZDZIAŁ II – ADRES STRONY INTERNETOWEJ, NA KTÓREJ UDOSTĘPNIONE ZOSTANĄ ZMIANY I WYJAŚNIENIA TREŚCI OPiW, A TAKŻE INNE DOKUMENTY ZAMÓWIENIA

1 Zamawiający udostępnia zmiany i wyjaśnienia treści OPiW, a także inne dokumenty zamówienia bezpośrednio związane z Postępowaniem o udzielenie zamówienia na stornie internetowej Zamawiającego, pod adresem: https://www.gpw.katowice.pl/przetargi/ogloszenia-o-zamowieniach

2 Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści OPiW lub Zaproszenia. Zamawiający jest zobowiązany udzielić wyjaśnień niezwłocznie, jednakże nie później niż na **2 dni** przed upływem terminu składania wniosków o dopuszczenie do udziału w Postępowaniu, o ile wniosek o wyjaśnienie treści OPiW lub Zaproszenia wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania wniosków o dopuszczenie do udziału w Postępowaniu. Wszelkie pytania dotyczące przedmiotu zamówienia należy składać:

– Pisemnie na adres: Górnośląskie Przedsiębiorstwo Wodociągów Spółka Akcyjna, ul. Wojewódzka 19, 40-026 Katowice, z dopiskiem: „Pytanie do postępowania SOC – Secutiry Operation Center nr postępowania FZP/321/35/2023"

lub

– w formie elektronicznej za pośrednictwem poczty elektronicznej na adres e-mail: zamowienia@gpw.katowice.pl

3 Treść pytań (bez ujawniania źródła) wraz z wyjaśnieniami, Zamawiającego, udostępni na swojej stronie internetowej pod adresem: https://www.gpw.katowice.pl/przetargi/ogloszenia-o-zamowieniach

4 Jeżeli wniosek o wyjaśnienie treści OPiW lub Zaproszenia wpłynął do Zamawiającego po upływie terminu, o którym mowa w ust. 2 powyżej lub dotyczy uprzednio udzielonych już wyjaśnień Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Przedłużenie terminu składania wniosków o dopuszczenie do udziału w Postępowaniu nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści OPiW lub Zaproszenia.

5 W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść OPiW lub Zaproszenia. Każda wprowadzona przez Zamawiającego zmiana staje się w takim przypadku częścią Zaproszenia. Jeśli w wyniku zmiany Zaproszenia niezbędny jest dodatkowy czas na wprowadzenie zmian we wnioskach o dopuszczenie do udziału w Postępowaniu, Zamawiający przedłuża termin składania wniosków o dopuszczenie do udziału w Postępowaniu.

ROZDZIAŁ III – OKREŚLENIE PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest:
Uruchomienie i realizacja usługi Security Operation Center (SOC) oraz wdrożenie narzędzi monitorowania sieci i systemów przemysłowych w Górnośląskim Przedsiębiorstwie Wodociągów S.A.

(CPV): 72720000-3 – Usługi w zakresie rozległej sieci komputerowej.

ROZDZIAŁ IV – TERMIN WYKONANIA ZAMÓWIENIA

Zamówienie należy zrealizować w terminie: **48 miesięcy od daty zawarcia Umowy**.

ROZDZIAŁ V – OPIS POTRZEB ZAMAWIAJĄCEGO I CECHY CHARAKTERYSTYCZNE DOSTAW STANOWIĄCYCH PRZEDMIOT ZAMÓWIENIA

1. Szczegółowy opis potrzeb Zamawiającego i cechy charakterystyczne przedmiotu zamówienia zawiera **Załącznik nr 1 do OPiW**. Szczegółowy opis wymagań Zamawiającego dotyczących realizacji zamówienia zawierają projektowane postanowienia umowy - **Załącznik nr 2 do OPiW**.

ROZDZIAŁ VI – MINIMALNE WYMAGANIA DOTYCZĄCE OPISU PRZEDMIOTU ZAMÓWIENIA LUB REALIZACJI ZAMÓWIENIA, NIEPODLEGAJĄCE NEGOCJACJOM, KTÓRE MUSZĄ SPEŁNIĆ WSZYSTKIE OFERTY

I. Zamawiający informuje, że wszystkie oferty muszą spełnić następujące wymagania niepodlegające negocjacjom:

1. Wymagania dla usługi SOC

1.1. Realizacja zadań SOC w zakresie :

1.1.1. monitoringu i wykrywania zdarzeń cyberbezpieczeństwa (potencjalnych incydentów z zakresu cyberbezpieczeństwa);

1.1.2. obsługi zdarzeń cyberbezpieczeństwa, zgodnie z (przygotowaną) instrukcją lub instrukcjami obsługi, w tym ich rejestrowanie, kategoryzację i priorytetyzację obsługi, analizowanie i korelowanie, kwalifikowanie i reagowanie;

1.1.3. raportowania zdarzeń cyberbezpieczeństwa;

1.1.4. obsługi zewnętrznego kanału komunikacji (email abuse) poza godzinami roboczymi.

1.2. Raportowanie w ramach usługi SOC, usługa podstawowa powinna być realizowane w następujących cyklach:

1.2.1. komunikacja bieżąca wynikająca ze scenariuszy obsługi zdarzeń;

1.2.2. raport dzienny z działania SOC usługa podstawowa (zautomatyzowany), obejmujący: liczbę obsłużonych zdarzeń (rozwiązanych i eskalowanych), krytyczność obsłużonych zdarzeń, informację o czasach podjęcia oraz rozwiązania/eskalowania zdarzeń;

1.2.3. raport miesięczny z działania SOC usługa podstawowa, w formie dokumentu podsumowującego pracę SOC usługa podstawowa zawierającego takie informacje jak: liczba obsłużonych zdarzeń (rozwiązanych i eskalowanych), krytyczność obsłużonych zdarzeń, czas wystąpienia zdarzenia, czas zamknięcia zdarzenia/eskalacji, status zdarzenia (otwarty, zamknięty, eskalowany), stan SLA (przekroczenia), powód przekroczenia;

1.3. Niezbędne zasoby, umiejętności i doświadczenie konieczne do obsługi zdarzeń i incydentów bezpieczeństwa oraz ich dokumentacji:

1.3.1. posiadanie własnego centrum SOC (Security Operations Center) zlokalizowanego w Polsce z wymaganym certyfikatem ISO 22301 ;

1.3.2. dysponowanie zespołem zdolnym do realizacji zadań usługi SOC - usługa podstawowa w trybie 24/7/365 – zbudowanym w oparciu o pracowników zatrudnionych przez dostawcę usługi przez cały okres realizacji zamówienia, posiadających zdolności techniczne oraz kompetencje zapewniające wykonanie zamówienia;

1.4. Zgodność usługi SOC z wymaganiami Ustawy o krajowym systemie cyberbezpieczeństwa oraz aktów powiązanych. (t.j. Dz.U.2023 poz.913)

2. **Dostarczenie funkcjonalności systemu SIEM w celu świadczenia usługi monitorowania**

2.1. Wykonawca dostarczy funkcjonalność systemu SIEM w modelu MSSP (Managed Security Service Provider) funkcjonującego we własnym data center (chmura prywatna) na terenie Polski.

2.2. System musi posiadać mechanizm przetrzymywania danych wraz z zaimplementowaną kompresja mająca możliwość kompresji danych na 10:1 . Funkcjonalność systemu pozwalać będzie na tworzenie różnych reguł korelacji na podstawie dowolnych danych otrzymanych z logów jak również zaimportowanych z innych źródeł zewnętrznych Zamawiającego pochodzących z sieci IT i OT.

2.3. Poszczególne komponenty systemu takie jak sondy, agregatory, serwery konektorów zainstalowane będą w sieci OT Zamawiającego na zwirtualizowanej lub fizycznej infrastrukturze Zamawiającego.

2.4. Agregowane zdarzenia z infrastruktury Zamawiającego będą przechowywane na przestrzeni dyskowej Wykonawcy przez co najmniej 12 miesięcy. Po tym czasie Wykonawca przekaże Zamawiającemu dane o których mowa powyżej, na odpowiednim co do pojemności nośniku, odpowiednio zabezpieczone hasłem w celu archiwizacji.

2.5. W przypadku nagłego zwiększenia ruchu danych w flow sieci lub logach monitorowanych źródeł system SIEM nie może odrzucać zwiększonego ruchu i monitorować go bez zakłóceń .

3. Usługa SOC ma być realizowana (w zakresie m.in. monitoringu i reakcji na incydenty bezpieczeństwa) w oparciu o zespół specjalistów, których kompetencje są potwierdzone certyfikatami wymienionymi w OPZ

4. Zakres świadczonej usługi:

4.1. Monitorowanie i obsługa incydentów

4.1.1. Monitorowanie zdarzeń w infrastrukturze Zamawiającego — czyli zbieranie, analizowanie oraz korelacje zdarzeń, które zachodzą w sieciach oraz systemach klienta Zamawiającego. Jako źródła zdarzeń oprócz systemów teleinformatycznych Zamawiającego, będą traktowane zgłoszenia użytkowników i administratorów Zamawiającego oraz przyjęte przez zamawiającego zgłoszenia incydentów otrzymane ze źródeł zewnętrznych (np. csirt.gov)

4.1.2. Wykrywanie zdarzeń oraz incydentów bezpieczeństwa,

4.1.3. Ocena wpływu zdarzenia oraz incydentu bezpieczeństwa OT na systemy Zamawiającego.

4.2. Usługa świadczona w trybie 24/7/365.

5. Dodatkowe wymagania szczegółowe:

5.1. Wykonawca zapewni dyżury oraz odpowiednią rotację zespołu SOC, zgodnie z przepisami prawa, gwarantującą jakość i ciągłość świadczonej usługi.

5.2. Wykonawca będzie zobowiązany do przygotowania okresowych rekomendacji zmian w środowisku informatycznym Zamawiającego, nie rzadziej niż 1 na miesiąc o ile takie rekomendacje wystąpią.

5.3. Wymagana jest całkowita separacja danych Zamawiającego od danych innych podmiotów, dla których Wykonawca również świadczy usługę SOC.

5.4. Licencja oprogramowania systemu monitorowania ma być licencją wieczystą z gwarancją bezpłatnej aktualizacji w okresie obowiązywania umowy, po tym okresie licencja nie wygasa
i może pracować bez obowiązku nabycia nowych aktualizacji systemu oraz sygnatur.

5.5. Wykonawca przed złożeniem oferty musi przeprowadzić wizje lokalne, a na etapie składania ofert przedstawić Zamawiającemu koncepcje zrealizowania wymagań opisanych w OPZ, na przykładzie 3 wskazanych obiektów

5.6. System musi zapewniać możliwość monitorowania sieci rozproszonej geograficznie.

5.7. Usługą ciągłego monitorowania należy objąć system telemetryczny działający w architekturze gwiazdy. Komunikację sieciową w obrębie systemu telemetrycznego należy monitorować w punkcie centralnym (lokalizacja Katowice).

5.8. Oprócz monitorowania komunikacji zastosowane rozwiązanie ma zabezpieczać komunikację pomiędzy serwerami a elementami systemu telemetrii rozproszonymi geograficznie.

II. O udzielenie Zamówienia mogą ubiegać się Wykonawcy, którzy potwierdzą – na Wniosku o dopuszczenie do udziału w postępowaniu (Załącznik nr 2 do Zaproszenia), że oferowane usługi, spełniają minimalne wymagania dotyczące opisu przedmiotu zamówienia lub realizacji zamówienia, niepodlegające negocjacjom.

ROZDZIAŁ VII – KRYTERIA OCENY OFERT, ICH WAGA ORAZ OPIS SPOSOBU DOKONYWANIA OCENY OFERT W RAMACH POSZCZEGÓLNYCH KRYTERIÓW

1. Przy wyborze oferty najkorzystniejszej, Zamawiający będzie się kierował następującym kryterium: **cena ofertowa z wagą 100 pkt.**

Każdy z Wykonawców otrzyma odpowiednią liczbę punktów (maksymalnie 100pkt), wyliczoną według następującego wzoru:

$$IP = \frac{Cn}{Cb} \times A$$

gdzie poszczególne litery oznaczają:

IP	liczba punktów,
Cn	cena ofertowa najniższa, spośród wszystkich rozpatrywanych i nieodrzuconych ofert
Cb	cena ofertowa oferty badanej (przeliczanej),
A	waga kryterium wyrażona w punktach – 100 pkt.

2. Liczba punktów zostanie zaokrąglona do dwóch miejsc po przecinku. Jeżeli trzecia cyfra po przecinku jest mniejsza niż 5 to przy zaokrągleniu druga cyfra nie ulega zmianie, a jeśli trzecia cyfra po przecinku jest równa 5 lub większa to druga cyfra zostanie zaokrąglona w górę.

3. Jeżeli została złożona oferta, dla każdej części zamówienia, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą o podatku od towarów i usług, dla celów zastosowania kryterium ceny Zamawiający dolicza do przestawionej w tej ofercie ceny kwotę podatku VAT, którą miałby obwiązek rozliczyć.

4. Jeżeli nie można, dla każdej części zamówienia, wybrać oferty najkorzystniejszej ze względu na to, że złożono dwie lub więcej ofert o takiej samej cenie Zamawiający wezwie Wykonawców do złożenia ofert dodatkowych przy czym ceny tych ofert nie mogą być wyższe niż w pierwotnie złożonej ofercie.

5. Oferta, dla każdej części zamówienia, która otrzyma najwyższą liczbę punktów, zostanie uznana za najkorzystniejszą.

ZAŁĄCZNIK NR 1 DO OPiW

OPIS PRZEDMIOTU ZAMÓWIENIA

„Uruchomienie i realizacja usługi SOC oraz wdrożenie narzędzi monitorowania sieci i systemów przemysłowych w Górnośląskim Przedsiębiorstwie Wodociągów S.A.”

I. Opis przedmiotu zamówienia

1. Przedmiot zamówienia.
   1.1. Przedmiotem zamówienia jest świadczenie przez Wykonawcę na rzecz Zamawiającego usług monitorowania incydentów bezpieczeństwa przez wyspecjalizowane Security Operations Center (SOC) tj. centrum bezpieczeństwa teleinformatycznego, które będzie wspierało Zamawiającego, jako operatora usługi kluczowej w spełnieniu wymogów ustawy o krajowym systemie cyberbezpieczeństwa w okresie obowiązywania umowy. W ramach usługi SOC Wykonawca wdroży wymagane narzędzia monitorowania sieci i systemów przemysłowych oraz zagwarantuje drogę komunikacji dla wdrażanych systemów z wszystkimi obiektami Zamawiającego przez cały okres realizacji umowy, lista obiektów ujęta została *w załączniku nr 1 pkt.1*. Usługa SOC obejmować ma główne obszary działania sieci przemysłowej, czyli:
      1.1.1. systemy telemetrii;
      1.1.2. systemy sterowania;
      1.1.3. systemy monitorowania pracy obiektów.
   1.2. W ramach świadczonych usług Wykonawca zapewni Zamawiającemu ciągłe monitorowanie i wykrywanie zagrożeń oraz analizę funkcjonowania w zakresie bezpieczeństwa systemów i infrastruktury OT. Usługa musi zapewniać szybką reakcję na incydenty, które mogą mieć negatywny wpływ na działalność Zamawiającego.
   1.3. W ramach usługi SOC dostarczy wszystkie niezbędne i wymagane licencje systemu ciągłego monitorowania klasy IDS (*Intrusion Detection System*) przeznaczonego do monitorowania sieci przemysłowych oraz wszelkie konieczne do realizacji zadania komponenty (serwery, sondy, bramy dostępowe, przemysłowe switche oraz jeżeli wymagane, przemysłowe routery dostępowe wykorzystujące komórkowe technologie bezprzewodowe, oparte o sieci operatorskie) wraz z pełnym wdrożeniem. Na potrzeby realizacji usługi i w okresie jej realizacji Wykonawca zapewni usługi telekomunikacyjne transmisji danych wraz wymaganymi urządzeniami sieciowymi. System monitorowania realizować ma ciągły monitoring sieci i systemów automatyki przemysłowej z uwzględnieniem:
      1.3.1. inwentaryzacji systemów;
      1.3.2. monitorowania zmian w architekturze i komunikacji logicznej;
      1.3.3. monitorowania ruchu w protokołach przemysłowych;
      1.3.4. wykrywania wrogich zachowań w rozproszonej sieci przemysłowej;
      1.3.5. obsługi realizowanej przez centralną konsolę zarządzania alarmami;
      1.3.6. możliwości realizacji zadania zarówno w architekturze rozproszonej jak i scentralizowanej.
   1.4. Szkolenia – w ramach zadania Wykonawca przeprowadzi wszelkie wymagane szkolenia z obsługi systemów oraz zdarzeń, a także będzie stanowił wsparcie dla zamawiającego w zakresie konsultacji mających na celu poprawę bezpieczeństwa objętych usługą systemów OT Zamawiającego.

Lista obiektów oraz szczegółowe informacje dotyczące obiektów oraz pozostałych wymagań stanowią *Załącznik nr 1* udostępniony po podpisaniu oświadczenia o zachowaniu poufności.

2. Ramy czasowe
   2.1. Szkolenie dla zespołu zamawiającego: co najmniej 2 tygodnie przed zakończeniem wdrożenia.
   2.2. Objęcie monitorowaniem wszystkich obiektów wyszczególnionych w Załączniku nr 1 pkt 1 : do 6 miesięcy od podpisania umowy.

II. Wymagania szczegółowe dla usługi SOC oraz wymagania funkcjonalne dla komponentów systemów monitorowania i komponentów zabezpieczeń.

1. Wymagania dla usługi SOC
   1.1. Realizacja zadań SOC w zakresie :
      1.1.1. monitoringu i wykrywania zdarzeń cyberbezpieczeństwa (potencjalnych incydentów z zakresu cyberbezpieczeństwa);
      1.1.2. obsługi zdarzeń cyberbezpieczeństwa, zgodnie z (przygotowaną) instrukcją lub instrukcjami obsługi, w tym ich rejestrowanie, kategoryzację i priorytetyzację obsługi, analizowanie i korelowanie, kwalifikowanie i reagowanie;
      1.1.3. raportowania zdarzeń cyberbezpieczeństwa;
      1.1.4. obsługi zewnętrznego kanału komunikacji (email abuse) poza godzinami roboczymi.
   1.2. Raportowanie w ramach usługi SOC, usługa podstawowa powinna być realizowane w następujących cyklach:
      1.2.1. komunikacja bieżąca wynikająca ze scenariuszy obsługi zdarzeń;
      1.2.2. raport dzienny z działania SOC usługa podstawowa (zautomatyzowany), obejmujący: liczbę obsłużonych zdarzeń (rozwiązanych i eskalowanych), krytyczność obsłużonych zdarzeń, informację o czasach podjęcia oraz rozwiązania/eskalowania zdarzeń;
      1.2.3. raport miesięczny z działania SOC usługa podstawowa, w formie dokumentu podsumowującego pracę SOC usługa podstawowa zawierającego takie informacje jak: liczba obsłużonych zdarzeń (rozwiązanych i eskalowanych), krytyczność obsłużonych zdarzeń, czas wystąpienia zdarzenia, czas zamknięcia zdarzenia/eskalacji, status zdarzenia (otwarty, zamknięty, eskalowany), stan SLA (przekroczenia), powód przekroczenia;
      1.2.4. spotkania komunikacyjno-koordynacyjne on-line przy wykorzystaniu aplikacji MS-Teams z wyznaczonym koordynatorem min. 1 raz w tygodniu;
      1.2.5. spotkania on-line przy wykorzystaniu aplikacji MS-Teams z wyznaczonym koordynatorem podsumowujące działalność min, 1 raz na kwartał.
   1.3. Niezbędne zasoby, umiejętności i doświadczenie konieczne do obsługi zdarzeń i incydentów bezpieczeństwa oraz ich dokumentacji:
      1.3.1. posiadanie własnego centrum SOC (Security Operations Center) zlokalizowanego w Polsce z wymaganym certyfikatem ISO 22301 ;
      1.3.2. dysponowanie zespołem zdolnym do realizacji zadań usługi SOC usługa podstawowa w trybie 24/7/365 – zbudowanym w oparciu o pracowników zatrudnionych przez dostawcę usługi przez cały okres realizacji zamówienia, posiadających zdolności techniczne oraz kompetencje (ujęte w pkt V. Referencje i certyfikaty) zapewniające wykonanie zamówienia;
      1.3.3. zapewnienie kanału kontaktowego (minimum telefon i skrzynka e-mail) z zespołem CSIRT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV) wskazanym przez Zamawiającego;
   1.4. Zgodność usługi SOC z wymaganiami Ustawy o krajowym systemie cyberbezpieczeństwa oraz aktów powiązanych.
   1.5. Przygotowywanie propozycji modyfikacji lub optymalizacji istniejących oraz wprowadzania za zgodą Zamawiającego nowych scenariuszy i reguł korelacyjnych w systemie SIEM.
   1.6. Przygotowywanie propozycji modyfikacji lub optymalizacji istniejących oraz wprowadzania za zgodą Zamawiającego nowych procedur operacyjnych obsługi zdarzeń.
2. SOC Usługa monitorowania i obsługi incydentów bezpieczeństwa
      2.1.1. Monitorowanie bezpieczeństwa w systemie SIEM zgodnie z uzgodnionymi między Wykonawcą i Zamawiającym procedurami i instrukcjami:
      2.1.2. Monitorowanie w trybie 24/7/365 wystąpień zdefiniowanych scenariuszy bezpieczeństwa zgodnie z procedurami uzgodnionymi z Zamawiającym. Monitorowanie realizowane jest w oparciu o konsolę systemu SIEM i zaimplementowane tam reguły korelacji zdarzeń;
      2.1.3. Identyfikacja zdarzenia, przeprowadzenie wstępnej analizy i eliminacja zdarzeń typu „false positive", zgodnie z procedurami reagowania uzgodnionymi z Zamawiającym;
      2.1.4. Obsługa zdarzeń wskazanych w procedurach monitorowania i reakcji, wykonanie przewidzianych w procedurach czynności, w tym selekcja i priorytetyzacja incydentów;

2.1.5. Notyfikacja do wyznaczonych osób po stronie Zamawiającego zgodnie z ustalonymi procedurami (utworzenie zapisów w systemie ticketowym dostawcy SOC);
2.1.6. Eskalacje podjęcia obsługi zdarzeń przez wskazane zespoły Zamawiającego;
2.1.7. Weryfikacja i obsługa zgłoszeń użytkowników dotyczących bezpieczeństwa spływających na dedykowaną kolejkę zgłoszeń w systemie ticketowym Zamawiającego. Zakres weryfikacji i obsługi zgłoszeń będzie zgodny z ustalonymi procedurami (w szczególności może on ograniczać się do priorytetyzacji zgłoszeń i przekierowania ich do odpowiednich służb po stronie Zamawiającego lub do wykonania innego zestawu określonych czynności przewidzianych w uzgodnionych procedurach i udostępnionych narzędziach);
2.1.8. Operatorzy SOC Wykonawcy podejmują inne czynności, zgodnie z dostarczonymi przez Zamawiającego procedurami postępowania (w szczególności informują wskazane służby Zamawiającego o wystąpieniu zdarzeń noszących znamiona incydentów bezpieczeństwa, które nie zostały objęte standardowymi procedurami reagowania);
2.1.9. Rejestracja incydentu w systemie ticketowym. Wykonawca ma zaproponować gotowy do użycia system oraz sparametryzować go na potrzeby procesu monitorowani z systemem SIEM;
2.1.10. Cykliczne, raz w miesiącu, raportowanie Zamawiającemu realizacji SLA umowy;
2.1.11. Cykliczne (miesięczne lub kwartalne) spotkania on0line, przeglądowe realizacji usług pomiędzy Zamawiającym i Wykonawcą;
2.1.12. Usługa realizowana będzie zdalnie, z siedziby SOC Wykonawcy;
2.1.13. SLA dla usługi podstawowej L1 – wykonawca zagwarantuje dostępność usługi – tryb 24/7/365 z czasem reakcji na wystąpienie incydentu bezpieczeństwa – 15 minut .
2.1.14. Wykrywanie nieautoryzowanego dostępu i uzyskania wyższych uprawnień w ramach prowadzonych analiz bezpieczeństwa na danych otrzymanych od Zamawiającego;
2.1.15. Identyfikacja pochodzenia zagrożenia i wszystkich podatnych / dotkniętych atakiem komponentów;
2.1.16. Wsparcie lokalnych administratorów w eliminacji pochodzenia incydentu;
2.1.17. Stałe utrzymanie i kalibracja narzędzi monitorowania, wzbogacanie ich o nowe sygnatury oraz usuwanie alertów typu false-positive
2.1.18. Analiza po włamaniowa i zabezpieczenie dowodów zdarzeń, informatyka śledcza oraz propozycja działań naprawczych po wykryciu incydentu bezpieczeństwa realizowana przez zespół CERT dostawcy usługi SOC posiadający wymagane w zapisach OPZ certyfikaty i kompetencje;
2.1.19. Możliwość skanowania podatności infrastruktury Zamawiającego z Internetu raz w tygodniu;
2.1.20. Możliwość skanowania podatności infrastruktury Zamawiającego z zewnątrz i wewnątrz sieci za pomocą dedykowanych narzędzi;
2.1.21. Monitorowanie ważności domen oraz certyfikatów SSL Zamawiającego;
2.1.22. Identyfikacja przypadków wycieku informacji o pracownikach Zamawiającego;
2.1.23. Informowanie o kampaniach phishingowych wykorzystujących markę Zamawiającego;
2.1.24. Monitorowanie reputacji adresów IP i domen Zamawiającego;
2.1.25. Comiesięczne podsumowanie najważniejszych alertów cyberbezpieczeństwa dla Zamawiającego w postaci raportu w formie elektronicznej uzgodnionej z Zamawiającym;
2.1.26. Materiały dotyczące budowania świadomości w zakresie cyberbezpieczeństwa dostarczane do Zamawiającego co najmniej raz w miesiącu w formie newslettera oraz raz w roku w formie raportu CERT.
2.1.27. SLA dla usługi rozszerzonej L2 wykonawca zagwarantuje dostępność usługi – tryb 8/5/251 z czasem reakcji na wystąpienie incydentu bezpieczeństwa – 120 minut.

3. Dostarczenie funkcjonalności systemu SIEM w celu świadczenia usługi monitorowania
   3.1. Wykonawca dostarczy funkcjonalność systemu SIEM w modelu MSSP (Managed Security Service Provider) funkcjonującego we własnym data center (chmura prywatna) na terenie Polski.
   3.2. Zaproponowane rozwiązania pozwolą na agregację logów z infrastruktury Zamawiającego poprzez umiejscowienie sond/serwerów zbierających dane w infrastrukturze Zamawiającego oraz

dostarczenie ich do centralnej jednostki systemu SIEM po stronie Wykonawcy. System SIEM pozwalać będzie na zaawansowaną korelację logów, ich przeszukiwanie, tworzenie różnych operacji dla wykrytych zdarzeń.

3.3. Dostawca usługi udostępnienia funkcjonalności SIEM powinien posiadać certyfikat ISO 27001 tym samym skutecznie chronić powierzone dane Zamawiającego do usługi dzięki efektywnie wdrożonemu i utrzymywanemu systemu zarządzania bezpieczeństwem informacji. Infrastruktura Dostawcy, na której będzie funkcjonował system SIEM, gromadzący dane Zamawiającego powinna być objęta certyfikacją ISO 22301 potwierdzającym posiadane procedury mające na celu zapewnienie bezpieczeństwa krytycznych procesów biznesowych.

3.4. System powinien posiadać mechanizm przetrzymywania danych wraz z zaimplementowaną kompresja mająca możliwość kompresji danych na 10:1 . Funkcjonalność systemu pozwalać będzie na tworzenie różnych reguł korelacji na podstawie dowolnych danych otrzymanych z logów jak również zaimportowanych z innych źródeł zewnętrznych Zamawiającego pochodzących z sieci IT i OT.

3.5. Poszczególne komponenty systemu takie jak sondy, agregatory, serwery konektorów zainstalowane będą w sieci OT Zamawiającego na zwirtualizowanej lub fizycznej infrastrukturze Zamawiającego.

3.6. Agregowane zdarzenia z infrastruktury Zamawiającego będą przechowywane na przestrzeni dyskowej Wykonawcy przez co najmniej 12 miesięcy. Po tym czasie Wykonawca przekaże Zamawiającemu dane o których mowa powyżej, na odpowiednim co do pojemności nośniku, odpowiednio zabezpieczone hasłem w celu archiwizacji.

3.7. Pełna administracja systemu SIEM oraz jego rozwój będą w gestii Wykonawcy z zachowaniem dostępności pełnej funkcjonalności systemu SIEM na poziomie 98% w skali miesiąca. Na potrzeby przeprowadzenia prac administracyjnych wyznaczone może zostać jedno miesięcznie stałe Okno Serwisowe o długości do [4] godzin w dniu i godzinach uzgodnionym z Zamawiającym;

3.8. Pojemność systemu SIEM będzie realizowana przez Wykonawcę w następującym zakresie:

3.8.1. System SIEM zostanie zintegrowany przez Wykonawcę z infrastrukturą Zamawiającego (źródła danych) w ilości ujętej *Załącznik nr 1 pkt. 5*.

3.8.2. Ilość EPS generowanych przez źródła Zamawiającego: do 1000 EPS. System dostawcy musi być elastycznie skalowany w przypadku wystąpienia dużo większej ilości EPS (do 1500 EPS).

3.8.3. Ilość GB danych generowanych przez Źródła Zamawiającego: do 30GB/dobę.

3.8.4. Ilość scenariuszy bezpieczeństwa przygotowanych i uzgodnionych z Zamawiającym – do 30 sztuk.

3.9. W przypadku nagłego zwiększenia ruchu danych w flow sieci lub logach monitorowanych źródeł system SIEM nie może odrzucać zwiększonego ruchu i monitorować go baz zakłóceń .

3.10. W przypadku potrzeby zwiększenia pojemności systemu rozwiązanie ma być gotowe do natychmiastowego zwiększenia parametrów pojemnościowych (bez przestoju pracy systemu).

3.11. W trakcie realizacji Umowy parametry pojemnościowe Systemu SIEM określone powyżej mogą ulegać zmianie na podstawie zrealizowanych Zamówień.

3.12. Źródła danych – infrastruktura sieci OT Zamawiającego podlegająca monitorowaniu pod kątem cyberbezpieczeństwa :

3.12.1. Serwery Windows;

3.12.2. Urządzenia sieciowe

3.12.3. System IDS z obiektów kluczowych oraz istotnych.

4. W trakcie realizacji usługi monitorowania lista rodzajów Źródeł danych i ich liczba mogą ulegać zmianie na podstawie zrealizowanych zamówień.
5. Usługa SOC ma być realizowana (w zakresie np.. monitoringu i reakcji na incydenty bezpieczeństwa) w oparciu o zespół specjalistów, których kompetencje są potwierdzone certyfikatami wymienionymi w rozdziale IV ust. 2.4. pkt 2.4.3. – 2.4.4. Zaproszenia do negocjacji.
6. Zakres świadczonej usługi:

6.1. Monitorowanie i obsługa incydentów

6.1.1. Monitorowanie zdarzeń w infrastrukturze Zamawiającego — czyli zbieranie, analizowanie oraz korelacje zdarzeń, które zachodzą w sieciach oraz systemach klienta Zamawiającego. Jako źródła zdarzeń oprócz systemów teleinformatycznych Zamawiającego, będą traktowane zgłoszenia użytkowników i administratorów Zamawiającego oraz przyjęte przez zamawiającego zgłoszenia incydentów otrzymane ze źródeł zewnętrznych (np. csirt.gov)

6.1.2. Wykrywanie zdarzeń lub incydentów bezpieczeństwa,

6.1.3. Ocena wpływu zdarzenia lub incydentu bezpieczeństwa OT na systemy Zamawiającego.

6.2. W ramach świadczonej usługi wykonawca weryfikuje, czy zdarzenie nie jest to fałszywym alarmem oraz grupuje wszystkie zdarzenia danego typu. Po analizie podejmuje działania zgodnie z procedurami.

6.3. Usługa świadczona w trybie 24/7/365.

7. Reakcja na incydenty

7.1. Reakcja na wykryte zdarzenie bezpieczeństwa poprzez przekazywanie do służb Zamawiającego zaleceń w zakresie sposobów eliminacji zagrożeń (w zakresie usuwania podatności, rekonfiguracji oraz innych działań, które mogą się przyczynić do eliminacji zagrożeń w ramach przyjętego SLA). Zalecenia muszą być dostosowane do możliwości oraz posiadanej przez Zamawiającego infrastruktury.

7.2. W ramach świadczonej usługi Wykonawca będzie cykliczne raz w miesiącu przekazywał Zamawiającemu biuletyny bezpieczeństwa w formie newslettera w zakresie istotnych zdarzeń, które mają miejsce zarówno w kraju jak i na świecie, a także udostępni „know how" w tym zakresie oraz w zakresie świadczonej usługi.

7.3. W ramach usługi dostępna będzie pula godzin konsultingowych na potrzeby analizy incydentów lub na żądanie w ilości do 24 godzin miesięcznie (np. w zakresie analizy malware'u oraz informatyki śledczej computer forensics). Niewykorzystane w danym miesiącu godziny będą przechodziły do wykorzystania na miesiące następne.

8. Dodatkowe wymagania szczegółowe:

8.1. Rolą SOC będzie ocena poziomu zagrożenia zdiagnozowanych incydentów, raportowanie o ich wystąpieniu i wydawaniu stosownych zaleceń. SOC będzie korelował informacje pochodzące z systemów Zamawiającego. Zakres analiz oraz sposób oceny zostanie dostosowany do potrzeb Zamawiającego podczas okresu wdrożenia usługi SOC.

8.2. Usługa będzie świadczona poprzez bezpieczne połączenie VPN Site2Site w technologii uzgodnionej z Zamawiającym na dostarczonych przez Wykonawcę łączach do wskazanych lokalizacji.

8.3. W ramach usługi Wykonawca musi zapewnić możliwość obsługi w zakresie tworzenia i zmiany reguł korelacyjnych, konfiguracji widoków, filtrów, zgodnie z uzgodnionym z Zamawiającym zakresem. Wykonawca zapewni ponadto Zamawiającemu dostęp do systemu korelacji zdarzeń wykorzystywanego w ramach świadczonej usługi.

8.4. Wykonawca w ramach usługi SOC będzie zgłaszał Zamawiającemu incydenty elektronicznie, za pomocą wiadomości e-mail na wskazany adres (adresy) oraz informował telefonicznie wyznaczoną osobę (osoby) do kontaktu ze strony Zamawiającego. Wykonawca zapewni ponadto Zamawiającemu dostęp do systemu ticketowego Wykonawcy, za pomocą którego będzie następowała obsługa incydentów bezpieczeństwa Zamawiającego w zakresie pełnego podglądu i obiegu incydentów zgodnie z założonym SLA.

8.5. Wykonawca zapewni dyżury oraz odpowiednią rotację zespołu SOC, zgodnie z przepisami prawa, gwarantującą jakość i ciągłość świadczonej usługi.

8.6. Wykonawca będzie zobowiązany do przygotowania okresowych rekomendacji zmian w środowisku informatycznym Zamawiającego, nie rzadziej niż 1 na miesiąc o ile takie rekomendacje wystąpią.

8.7. Wykonawca będzie przygotowywał okresowe, miesięczne raporty dotyczące świadczonej usługi w postaci elektronicznej na wskazany adres e-mail. Raport powinien zawierać informacje dotyczącą

ilości obsłużonych incydentów, czasów obsługi. Raport będzie dostarczany na wskazany e-mail, przez Zamawiającego.

8.8. Wykonawca będzie dokumentował i kontrolował działania oraz wykonanie prac za pomocą systemu obsługi zgłoszeń, w którym jest nadawana priorytetyzacja zadań oraz zamodelowany jest obieg informacji przez wszystkie linie ekspertów SOC.

8.9. W przypadku wystąpienia incydentu i zdiagnozowaniu konieczności wprowadzenia działań naprawczych w środowisku informatycznym Zamawiającego, Wykonawca musi zapewnić wsparcie ekspertów rekomendujących właściwe rozwiązanie, na żądanie Zamawiającego zgodnie z przyjętym SLA.

8.10. SOC będzie współpracował na bieżąco z Zamawiającym przy analizie incydentów w celu poprawienia efektywności oraz obniżenia ilości zgłaszanych fałszywych alarmów.

8.11. Wykonawca musi zapewniać retencję tj. przechowywanie danych zgłoszonych, czyli incydentów przez cały okres świadczenia usługi (dane przechowywane w bazie danych systemu będą dostępne dla funkcji agregacji, korelacji i detekcji). Zapewnienie przechowywania logów i danych historycznych umożliwi korelację zdarzeń z różnych źródeł w różnych okresach, a także zapewni dostęp do zdarzeń historycznych.

8.12. Zamawiający wymaga zapewnienia jak najmniejszej ingerencji w monitorowane systemy. Oznacza to możliwość zbierania logów bez konieczności instalacji dedykowanych agentów na źródłach danych urządzeń produkcyjnych, natomiast wykorzystanie zaimplementowanych już w systemach mechanizmów bez agentowych.

8.13. Wykaz rodzajów systemów, które będą źródłami do świadczenia usługi Załącznik nr 1 do przedmiotu zamówienia.

8.14. Przed zakończeniem świadczenia usługi Wykonawca zapewni trwałe usunięcie pod nadzorem Zamawiającego wszystkich danych Zamawiającego z elementów systemu używanych do świadczenia usługi SOC. Zamawiający będzie miał prawo do zachowania danych dotyczących jego systemów a zgromadzonych w systemie korelacji wykorzystywanym przez Wykonawcę w celu świadczenia usługi.

8.15. Wymagana jest całkowita separacja danych Zamawiającego od danych innych podmiotów, dla których Wykonawca również świadczy usługę SOC.

8.16. Wymagane jest umieszczenie elementów zbierających i korelujących logi w infrastrukturze Zamawiającego. Wykonawca będzie miał dostęp do systemu za pośrednictwem konsoli zarządzania oraz przy wykorzystaniu połączenia VPN. Logi źródłowe służące do świadczenia usługi będą przechowywane w infrastrukturze Zamawiającego.

8.17. Zamawiający wymaga przeszkolenia osób zaangażowanych po stronie zamawiającego zgodnie z zapisami pkt X.

III. System monitorowania

1. System monitorowania - założenia ogólne.

1.1. Licencja oprogramowania systemu monitorowania IDS ma być licencją wieczystą z gwarancją bezpłatnej aktualizacji w okresie obowiązywania umowy, po tym okresie licencja nie wygasa i może pracować bez obowiązku nabycia nowych aktualizacji systemu oraz sygnatur.

1.2. Wymaga się objęcia systemu sterowania rozwiązaniem do ciągłego monitorowania i wykrywania zagrożeń na podstawie pasywnej analizy ruchu sieciowego – IDS.

1.3. Identyfikacja niezgodności w ruchu sieciowym oraz wykrywanie zagrożeń musi być oparte o analizę pakietów oraz głęboką analizę pakietów (ang. Deep packet inspection - DPI) dla przemysłowych protokołów komunikacyjnych *Załącznik nr 1 pkt 2.*

1.4. Rozwiązanie do ciągłego monitorowania musi składać się z elementów pozwalających na zbudowanie elastycznej architektury umożliwiającej monitorowanie obiektów posiadających od kilkunastu do ponad stu urządzeń. Szczegółowe wymagania funkcjonalne dla elementów systemu monitorowania znajdują się w punkcie Wymagania dla systemu monitorowania w trybie ciągłym.

1.5. W skład systemu monitorowania powinny wchodzić:
   1.5.1. Centralna konsola IDS - system do prezentacji i zarządzania zdarzeniami zbieranymi z podrzędnych mu systemów/sensorów/sond systemu IDS – centralna konsola powinna być umieszczona w centrali spółki.
   1.5.2. Systemy IDS – autonomiczny element do analizy ruchu sieciowego i wykrywania incydentów, rozwiązanie pasywne działające na kopii ruchu sieciowego dostarczonego z portów mirror przełączników lub przez sondy IDS rozwiązanie ma być zainstalowane na obiektach kluczowych i istotnych *Załącznik nr 1 pkt. 1*.
   1.5.3. Sondy IDS – urządzenia służące do zbierania i agregowania ruchu z wielu portów mirror, kompresji tego ruchu i przesyłania go bezpiecznym tunelem do serwera IDS. Sonda IDS w razie potrzeby powinna być podłączona do rutera dostępowego zapewniającego bezpieczną transmisję lub być wyposażona w moduł LTE (w takim przypadku musi pełnić również rolę firewalla).
1.6. Zdarzenia identyfikowane przez system ciągłego monitorowania muszą być na bieżąco wysyłane do podmiotu świadczącego usługę SOC (wybranego w ramach niniejszego postępowania).
1.7. System ciągłego monitorowania IDS musi mieć funkcjonalność tworzenia cyfrowego obrazu sieci, który może być wykorzystany przez system automatyzujący analizę ryzyka.
1.8. Po stronie Wykonawcy jest zapewnienie bezprzewodowych usług transmisji danych lub zapewnienie innej bezpiecznej drogi przesyłania logów i/lub kopii ruchu z obiektów monitorowanych do systemów centralnego a następnie do SOC.
   1.8.1. Wykorzystywana sieć WAN ma służyć wyłącznie do zadań systemu monitorowania.
   1.8.2. Koszty utrzymania sieci WAN i transmisji danych w czasie trwania usługi ponosi Wykonawca.
   1.8.3. Należy zapewnić poufność i integralność przesyłanych danych poprzez zastosowanie technik zabezpieczających takich jak: wyłączny prywatny APN oraz VPN IPSec lub SSL VPN.
   1.8.4. Zastosowane karty SIM muszą mieć przypisane stałe adresy IP.
1.9. Systemem ciągłego monitorowania należy objąć obiekty w lokalizacjach w których działa przemysłowy system sterowania (ICS/OT) *Załącznik nr 1 pkt.1*.
1.10. Wykonawca przed złożeniem wniosku o dopuszczenie do udziału w postępowaniu musi przeprowadzić wizje lokalne, a na etapie składania ofert przedstawić Zamawiającemu koncepcje zrealizowania wymagań dla każdego z 3 obiektów będących przedmiotem wizji.
1.11. W przypadku gdy sieć obiektowa nie jest wyposażona w przełączniki LAN z funkcją port mirror (SPAN port) należy dostarczyć odpowiednie urządzenia sieciowe, a w koncepcji przedstawić sposób pozyskania kopii ruchu sieciowego do analizy lub w przypadku obiektów podstawowych wykorzystać np. funkcjonalność Sondy oraz doposażyć obiekt w odpowiednie rozwiązania Router LTE oraz karty SIM do komunikacji z wykorzystaniem sieci operatorskiej lub zapewnić inną drogę bezpiecznej transmisji danych.

IV. Wymagania szczegółowe dla systemu monitorowania w trybie ciągłym

Zamawiający oczekuje przedstawienia oferty wdrożenia systemu klasy IDS (Intrusion Detection System). System musi być pasywnym rozwiązaniem monitorowania bezpieczeństwa sieci i inwentaryzacji. System musi analizować kopię ruchu sieciowego dostarczoną z portów mirror/span przełączników sieciowych. System powinien współpracować z sondami i sensorami zdalnymi, a co za tym idzie umożliwiać monitorowanie sieci rozproszonej geograficznie. System powinien być rozwiązaniem programowym – niezależnym od platformy sprzętowej pochodzącej od konkretnego dostawcy. System musi umożliwiać wdrożenie jako maszyna wirtualna. System musi zapewniać wysoki poziom skalowalności umożliwiając monitorowanie małych obiektów (do 50 zasobów) jak również całych grup obiektów (powyżej 500 zasobów). System monitorowania najmniejszych obiektów powinien móc działać na standardowym komputerze przemysłowym 4 rdzenie CPU, do 16 GB RAM.

1. Wymagania główne
   1.1. System musi zapewniać możliwość monitorowania sieci rozproszonej geograficznie oraz współpracować z opcjonalnymi sondami sprzętowymi.

1.2. System musi umożliwiać bezpośrednie podłączenie do niego źródeł ruchu (kopia ruchu z portów mirror/SPAN).
1.3. System musi umożliwiać analizę zapisu ruchu sieciowego w postaci wgranych do systemu plików PCAP system powinien obsługiwać pliki o rozmiarze do 10 GB.
1.4. System musi dostarczać dane niezbędne do prowadzenia procesów Oceny Ryzyka (Risk Assesment) dla sieci ICS.
1.5. System musi dostarczać API, umożliwiające integrację aplikacji autorskich Zamawiającego z bazą danych rozwiązania.
1.6. System musi działać w trybie pasywnym (bez generowania dodatkowego ruchu w monitorowanej sieci), opcjonalnie system może zawierać lub współpracować z mechanizmem aktywnego odpytywania urządzeń (Active Polling).
1.7. System musi dostarczać funkcje audytu działań jego użytkowników i zapewniać możliwość przesyłania danych o tych akcjach za pomocą protokołu syslog.

2. Funkcje analityczne i wspierające analizę
2.1. System musi umożliwiać analizę danych zebranych w trakcie pracy.
2.2. Każdy zestaw danych prezentowanych przez system musi zapewniać:
2.2.1. Filtrowanie prezentowanych danych na podstawie zawartości wpisu, danych takich jak treść alarmu, adresy IP, MAC oraz metadanych takich jak np. godzina utworzenia.
2.2.2. Wszystkie dane tabelaryczne pozyskane z systemu powinny być eksportowane do formatów JSON, PDF i CSV, jak również możliwe do uzyskania za pomocą API.
2.2.3. Każdy wpis w zestawach danych dot. Zdarzeń (konsola alarmów) musi zapewniać możliwość uzyskania dokładniejszych informacji o przyczynie i urządzeniach biorących udział w komunikacji oraz dostęp do zapisów pakietów w formie plików PCAP.
2.3. System musi zapewnić możliwość utworzenia dowolnego raportu na podstawie zapytań do bazy danych oraz możliwość generowania raportu z całości okresu działania systemu a także powinien zapewniać możliwość przesyłania raportów okresowych za pomocą wiadomości e-mail.
2.4. System musi zapewniać prezentację wektorów ataku w formie graficznej na mapie.
2.5. System musi wspierać analizę ryzyka, przez umożliwienie tworzenia grup procesów biznesowych i określenie zasobów, od których procesy te zależą a także krytyczności procesów.
2.6. System musi wspierać analizę DPI dla protokołów przemysłowych ujętych w *załącznik nr 1 pkt. 2.*
2.7. System musi zapewnić możliwość dodawania komentarzy do alarmów oraz zapewnić możliwość definicji procedur postępowania dla kategorii alarmów (Playbook).
2.8. System musi zapewnić możliwość pobrania wszystkich plików PCAP powiązanych z alarmami wykrytymi przez system oraz zbierać pliki PCAP przez okres co najmniej 21 dni z całości ruchu.

3. Wykrywanie anomalii
3.1. System musi raportować wykryte anomalie w komunikacji sieciowej na warstwach 2, 3, 4, 7 modelu ISO/OSI.
3.2. System musi dostarczać sygnaturowy mechanizm detekcji z regułami dla środowiska przemysłowego, a także dostarczać sygnatury zagrożeń dla protokołów przemysłowych oraz sygnatury zagrożeń dla protokołów IT,
3.3. System musi dostarczać behawioralny mechanizm detekcji,
3.4. System musi przedstawiać rekomendacje dla wykrytych problemów wykrytych w sieci, zasobach i konfiguracji samego systemu monitorowania, w odniesieniu do norm lub dobrych praktyk stosowanych w sieciach OT,
3.5. System musi dostarczać mechanizm wspierający śledzenie postępów prac związanych z rekomendacjami np. oznaczenie zadań jako rozwiązane, otwarte/w trakcie analizy, ignorowane, odroczone.
3.6. System musi raportować zdarzenia inwentaryzacyjne takie jak wykrycie nowych zasobów w sieci, wykrycie nowych połączeń w sieci, wykrycie nowych adresów MAC, wykrycie prób komunikacji do sieci Internet, wykrycie zbyt długiej przerwy w komunikacji zasobu.
3.7. System musi raportować wykryte anomalie i zdarzenia bezpieczeństwa m.in.
3.7.1. podejrzenie ataku MitM (np. ARP Spoofing).
3.7.2. skanowanie portów i sieci.

3.7.3. zdarzenia wykryte przez silnik sygnaturowy w tym znane ataki sieciowe oraz znane charakterystyki ruchu złośliwego oprogramowania.
3.7.4. zdarzenia pasujące do zdefiniowanych przez administratora reguł zrealizowanych w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych które zostały wymienione w złączniku nr1).

3.8. System musi dostarczać dane o wykrytych anomaliach w postaci czytelnej centralnej konsoli alarmów.
3.8.1. Konsola alarmów musi czytelnie oddzielać alarmy aktywne (nowe) od przetworzonych (archiwalne).
3.8.2. Konsola alarmów musi dostarczać następujących informacji wadze zdarzenia (jego dotkliwość), dacie pierwszego wykrycia, dacie ostatniej modyfikacji, źródle ruchu oraz celu, a także wskazywać protokoły wykorzystane w komunikacji.

3.9. System musi umożliwiać raportowanie wykrycia dowolnego ruchu sieciowego o zadanej przez Zamawiającego charakterystyce w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych).

3.10. System musi analizować i prezentować anomalie protokołów przemysłowych m.in.:
3.10.1. nieautoryzowana komunikacja przemysłowa.
3.10.2. anomalie protokołów przemysłowych.
3.10.3. naruszenie zdefiniowanej polityki komunikacji przemysłowej.

4. Możliwości konfiguracji i modyfikacji zasad detekcji

4.1. System musi dostarczać niezbędnych danych do zrozumienia zasad działania reguł (Treść reguły, odniesienia do źródeł takich jak bazy CVE, Baza wiedzy Microsoft, Framework MITRE ATT&CK, itp.) oraz umożliwiać czytelny podgląd wszystkich reguł i ich wyjątków.

4.2. System musi umożliwiać modyfikację istniejących oraz tworzenie nowych sygnatur oraz umożliwiać włączanie i wyłączanie dowolnych sygnatur dla dowolnego komponentu systemu OT.

4.3. System musi umożliwiać modyfikację i tworzenie nowych wyjątków dla sygnatur na podstawie parametrów warstw 2, 3, 4, 7 modelu ISO/OSI bezpośrednio z konsoli alarmów po wystąpieniu zdarzenia, a także przed wystąpieniem zdarzenia oraz w trakcie okresu tworzenia wzorca ruchu sieciowego.

4.4. System w trybie nauki musi generować sugerowany wzorzec ruchu, który po przeglądzie i jego akceptacji utworzy automatycznie niezbędne wyjątki dla sygnatur.

4.5. System powinien zapewniać możliwość tworzenia nowych i modyfikację istniejących (bezczynny/detekcja/nauka) trybów pracy pozwalając włączać i wyłączać poszczególne silniki detekcji uruchomionych w poszczególnych trybach i dostosowywać ich konfigurację, w celu precyzyjnego określenia zachowania metod detekcji.

4.6. System musi umożliwiać prowadzenie działań proaktywnego wyszukiwania zagrożeń w sieci (Threat Hunting).

4.7. System w czasie pracy musi automatycznie w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych zgodnych z zapisami *pkt. 2 załącznik nr 1*) tworzyć sugestie detekcji, dotyczące zaobserwowanego ruchu, które operator może włączyć i dostosować aby wykorzystać je jako reguły dodatkowe wzbogacające detekcję sygnaturową.

4.8. System musi, za pomocą kreatora obecnego w GUI systemu, umożliwiać tworzenie własnych reguł detekcji, w celu wzbogacenia detekcji sygnaturowej, w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych zgodnie z *pkt. 2 załącznik nr 1*).

4.9. System musi umożliwiać przypisanie dowolnego dostępnego mechanizmu DPI do dowolnego portu TCP/UDP oraz umożliwiać tworzenie własnych modułów DPI dla protokołów autorskich.

4.10. System musi umożliwiać precyzyjne określenie zakresu adresacji sieci będącej siecią chronioną/monitorowaną (tzw. sieć domowa, ang. home net) oraz umożliwiać definicję zaufanych adresów IP spoza sieci chronionej.

4.11. System musi dostarczyć mechanizm ograniczenia wolumenu analizowanego ruchu przez filtrowanie ruchu przychodzącego np. na podstawie identyfikatora VLAN.

5. Funkcje Inwentaryzacyjne
   5.1. System musi zapewniać funkcje automatycznego wykrywania zasobów systemów automatyki i sterowania takich jak PLC, HMI, Serwer SCADA, OPC Serwer, Serwer Historian, Stacje operatorskie, stacje inżynierskie, Router i przypisywać im automatycznie określony typ oraz umożliwiać przypisywanie własnych typów dla urządzeń niezdefiniowanych przez producenta systemu.
   5.2. System musi inwentaryzować urządzenia komunikujące się z wykorzystaniem warstwy 2 ISO/OSI i wyższych oraz inwentaryzować urządzenia komunikujące się wyłącznie w warstwie 2 ISO/OSI (tj. nieposiadające adresu IP).
   5.3. System musi wykonywać pasywną identyfikację systemu operacyjnego (minimum rodziny systemów Microsoft Windows) urządzenia i jego wersji.
   5.4. System musi udostępniać dane o zinwentaryzowanych zasobach i połączeniach w formie tabelarycznej i umożliwiać eksportowanie tych danych do formatów co najmniej: JSON, CSV, PDF.
   5.5. System musi aktualizować zestawy danych o zasobach i połączeniach w trybie ciągłym. Jest to równoznaczne z odświeżaniem tych danych w tabelach i na mapie połączeń.
   5.6. System musi prezentować informacje o wykorzystywanych protokołach w połączeniach sieciowych w formie tabelarycznej i umożliwiać eksportowanie tych danych do formatów co najmniej: JSON, CSV, PDF.
   5.7. System musi prezentować informacje o wykorzystywanych protokołach w połączeniach sieciowych w formie graficznej na mapie i umożliwiać eksportowanie widoku do pliku graficznego PNG.
   5.8. System musi rozpoznawać automatycznie przypisanie urządzeń do stref (zones) według standardu IEC 62443 oraz rozpoznawać automatycznie kanały komunikacyjne (conduits) pomiędzy strefami zgodnie ze standardem IEC 62443.
   5.9. System musi określać producenta urządzenia na podstawie zebranych danych.
   5.10. System musi wykonywać analizę podatności na podstawie wykrytych lub podanych przez administratora wersji systemu operacyjnego.
   5.11. System powinien analizować wykorzystanie pasma przez każdy zasób i połączenie sieciowe.
   5.12. System musi umożliwiać dodawanie do karty urządzenia zdefiniowanych przez administratora kryteriów opisu danego zasobu/urządzenia, akcja ta powinna być dostępna globalnie dla urządzeń oraz lokalnie dla pojedynczego urządzenia. Systemu musi umożliwiać filtrowanie danych po stworzonych kryteriach oraz umożliwiać ich eksport do plików CSV, JSON, PDF. Dane te powinny być też dostępne w raporcie generowanym przez system.
   5.13. System musi zapewnić możliwość importu pliku w formacie minimum CSV, w celu wykonania wsadowej modyfikacji minimum nazwy, typu, producenta, każdego z wykrytych urządzeń.
   5.14. System musi umożliwiać grupowanie urządzeń w monitorowanej sieci w zależności od ich wpływu na poszczególne procesy biznesowe zachodzące w organizacji. Jedna grupa (proces biznesowy) może zawierać wiele urządzeń, a każde urządzenie może być członkiem wielu grup.
   5.15. System musi zapewnić możliwość modyfikacji wagi alarmów w zależności od krytyczności procesu biznesowego/typu urządzenia/indywidualnych wymogów urządzenia i właściciela systemu.
   5.16. System musi umożliwić edycję danych o producencie urządzenia, a także umożliwiać edycję nazw zasobów oraz dodawanie komentarzy do zasobów.
   5.17. System musi umożliwiać przypisanie więcej niż jednego adresu MAC do urządzenia, umożliwiając inwentaryzację klastrów systemów.
   5.18. System musi umożliwiać edycję danych o wykrytym systemie operacyjnym (w minimalnym wariancie dla MS Windows) wraz z informacjami o aktualizacjach nałożonych na ten system.
   5.19. System musi analizować i prezentować w karcie zasobu dodatkowe informacje w oparciu o analizę wykrytego ruchu protokołów ujętych w *pkt. 3 złączniku nr 1*.
   5.20. System musi analizować i prezentować przesyłane przez sieć komendy protokołów przemysłowych ujętych w *pkt. 2 załącznik 1*.

6. Interfejs oraz funkcje mapy.
   6.1. System musi dostarczać czytelnych informacji na temat istotnych zdarzeń zaobserwowanych w sieci (alarmów) oraz informacji o trybie pracy rozwiązania (bezczynny/detekcji/nauki).

6.2. System musi umożliwiać świadome przełączanie między trybami pracy wg. harmonogramu oraz ręcznie.
6.3. System musi dostarczać funkcje prezentowania zebranych danych o zasobach i ich połączeniach w postaci graficznej (Mapa połączeń), mapa musi być interaktywna, tj. umożliwiać uzyskanie szczegółowej informacji o prezentowanych na niej zasobach lub połączeniach (np. poprzez zaznaczenie urządzenia/połączenia kliknięciem)
6.4. Interfejs musi być w języku polskim.
6.5. Funkcja mapy musi wyświetlać schemat połączeń logicznych pomiędzy węzłami sieci oraz umożliwiać tworzenie własnych widoków w modelach: przepływu, PERA, zdefiniowanym przez użytkownika minimum zmieniając geometryczne rozłożenie obiektów na mapie.
6.6. Funkcja mapy musi umożliwiać wykorzystanie zdefiniowanych procesów biznesowych w celu stworzenia osobnych widoków mapy, ułatwiających analizę.
6.7. System musi prezentować na mapie fakt wykrycia routerów na trasie połączeń.
6.8. System musi prezentować na mapie kierunek komunikacji pomiędzy urządzeniami, a także wskazywać na mapie urządzenia zagrożone i dotknięte anomaliami.
6.9. System musi umożliwiać tworzenie własnych widoków mapy na podstawie grup procesów biznesowych lub z wykorzystaniem filtrowania zasobów (kluczem powinny być minimum adresy IP, adresy MAC, podsieci, producenci, cechy komunikacji jak np. komunikowanie się przez router lub lokalizacja poza siecią chronioną) oraz umożliwiać zapis widoku mapy do pliku graficznego.

7. Integracje
7.1. System musi umożliwiać integrację z dowolnym rozwiązaniem SIEM oraz wspierać przesyłanie danych za pomocą protokołu syslog w formatach CEF i LEEF.
7.2. System musi umożliwiać integrację z dowolnym rozwiązaniem kolejkowania pracy (np. ITSM) poprzez wysyłanie wiadomości e-mail.
7.3. System musi zapewniać granularną kontrolę przesyłanych danych protokołu syslog w zależności od: źródła powstawania komunikatów (silnika detekcji) oraz wagi komunikatu (krytyczność alarmu).
7.4. System musi umożliwiać przesłanie dowolnego zestawu informacji do dowolnej ilości odbiorców syslog, lub e-mail oraz umożliwiać tworzenie i przesyłanie za pomocą wiadomości e-mail raportów okresowych o wykrytych anomaliach i zdarzeniach, zawierające minimum adresy źródłowe i docelowe, daty wystąpienia alarmów i treści alarmów.
7.5. System musi integrować się jako odbiorca danych ze strumieni syslog, w celu wzbogacenia wewnętrznej bazy danych.
7.6. System musi integrować się z kolejkami workflow wybranych rozwiązań firewall, w celu przesyłania sugestii reguł firewalla, Lista rozwiązań stanowi *pkt 4. załącznik nr 1*.
7.7. System musi dostarczać API, dla integracji z dowolną aplikacją tworzoną w Organizacji.
7.8. System musi integrować się z usługą Active Directory w celu zarządzania kontami użytkowników systemu.
7.9. System powinien integrować się z rozwiązaniem RSA SecureID.
7.10. System może dostarczać lokalne zarządzanie kontami użytkowników.
7.11. System powinien dostarczać mechanizm zarządzania uprawnieniami użytkowników co najmniej dla trzech zdefiniowanych ról.

8. Kontrola poprawności działania systemu.
8.1. System musi zapewniać podgląd stanu systemu, w tym:
8.1.1. Użycie CPU.
8.1.2. Użycie pamięci RAM.
8.1.3. Wykorzystanie miejsca na dysku.
8.1.4. Wykorzystanie pasma na każdym z interfejsów.
8.2. System musi zapewniać możliwość monitorowania jego stanu za pomocą protokołu SNMP.
8.3. System powinien generować rekomendacje dotyczące stanu jego konfiguracji i bezpieczeństwa.

V. Wymagania dla centralnego systemu nadzoru nad alarmami

Zamawiający oczekuje przedstawienia oferty wdrożenia centralnego systemu nadzoru nad oferowanymi rozwiązaniami klasy NSM/IDS.

1. Wymagania główne:
   1.1. System musi być kompatybilny z wybranym przez Zamawiającego rozwiązaniem IDS/NSM.
   1.2. System musi zapewniać możliwość monitorowania sieci rozproszonej geograficznie.
   1.3. System musi umożliwiać tworzenie logicznych segmentów zawierających jeden lub więcej systemów NSM/IDS.
   1.4. System musi umożliwiać precyzyjne przydzielanie dostępu użytkowników z poziomem uprawnień Administrator/Ekspert/Analityk dla członków grupy odpowiedzialnej za konkretny obiekt:
      1.4.1. Indywidualnie dla każdego segmentu monitorującego konkretny obiekt
      1.4.2. Do każdej z grup segmentów monitorujących konkretne obiekty
      1.4.3. Globalnie do wszystkich segmentów
   1.5. System musi agregować dane z poszczególnych segmentów i przedstawiać je wyłącznie uprawnionym użytkownikom.
   1.6. System może prezentować dane z poszczególnych systemów w postaci mapy uwzględniającej ich rozmieszczenie geograficzne.
   1.7. System musi agregować dane sumaryczne dotyczące ilości alarmów, połączeń i zasobów
   1.8. System musi dostarczać czytelnych danych o alarmach wykrytych przez poszczególne silniki systemy IDS/NSM. Minimalnie system musi wskazywać alarmy cyberbezpieczeństwa i inwentaryzacji zasobów sieci.
   1.9. System musi umożliwiać scentralizowaną pracę z alarmami obecnymi w poszczególnych platformach IDS w tym:
      1.9.1. archiwizację alarmów,
      1.9.2. dodawanie komentarzy,
      1.9.3. tworzenie wyjątków,
      1.9.4. przegląd, sortowanie i filtrowanie alarmów.
   1.10. System musi umożliwiać scentralizowaną pracę z zasobami zinwentaryzowanymi na poszczególnych instancjach IDS.
   1.11. System musi dostarczać funkcje audytu działań jego użytkowników i zapewniać możliwość przesyłania danych o tych akcjach za pomocą protokołu syslog.
   1.12. System musi umożliwiać aktualizację oprogramowania na wszystkich rozwiązaniach IDS, będących pod kontrolą centralnego systemu zarządzani.
   1.13. System musi integrować się z usługą Active Directory w celu zarządzania kontami użytkowników systemu.
   1.14. System musi integrować się z rozwiązaniem RSA SecureID.
   1.15. System musi dostarczać lokalne zarządzanie kontami użytkowników.
   1.16. System musi dostarczać mechanizm zarządzania uprawnieniami użytkowników RBAC.
   1.17. System musi zapewniać podgląd stanu systemu, w tym:
      1.17.1. użycie CPU,
      1.17.2. użycie pamięci RAM,
      1.17.3. wykorzystanie miejsca na dysku,
      1.17.4. wykorzystanie pasma na każdym z interfejsów,
   1.18. System musi zapewniać możliwość monitorowania jego stanu za pomocą protokołu SNMP.

VI. Wymagania dla systemu zabezpieczenia telemetrii

1. Wymagania ogólne dla zabezpieczenia i monitorowania komunikacji w obrębie systemu telemetrycznego:
   1.1. Usługą ciągłego monitorowania należy objąć system telemetryczny działający w architekturze gwiazdy. Komunikację sieciową w obrębie systemu telemetrycznego należy monitorować w punkcie centralnym (lokalizacja Katowice).
   1.2. Oprócz monitorowania komunikacji zastosowane rozwiązanie ma zabezpieczać komunikację pomiędzy serwerami a elementami systemu telemetrii rozproszonymi geograficznie.
   1.3. Obudowa dostosowana do implementacji w szafie RACK 19”.

1.4. Urządzenie służące do monitorowania i zabezpieczenia komunikacji musi mieć funkcjonalność firewalla w celu filtrowania ruchu sieciowego z wykorzystaniem reguł opisujących dopuszczony ruch sieciowy za pomocą:
   1.4.1. Adresu IP źródła komunikacji;
   1.4.2. Źródłowego portu TCP lub UDP;
   1.4.3. Adresu IP celu;
   1.4.4. Docelowego portu TCP lub UDP;
   1.4.5. Protokołu warstwy aplikacyjnej;
   1.4.6. Harmonogramy czasowe.
1.5. Urządzenie musi mieć funkcjonalność routera i możliwość realizowania routingu w oparciu o:
   1.5.1. Reguły statyczne
   1.5.2. Protokoły dynamiczne: OSPF, RIP.
1.6. Urządzenie musi posiadać możliwość tworzenia reguł dla translacji adresów NAT i przekierowania portów PAT
1.7. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
1.8. Urządzenie musi posiadać możliwość filtrowania ruchu w trybie transparentnym dla wskazanych portów. Oznacza to możliwość egzekwowania wszystkich polityk firewalla dla portów zgrupowanych jako bridge (ta sama podsieć IP bez routingu).
1.9. Urządzenie musi tworzyć logi zarówno dla komunikacji dozwolonej jak i zablokowanej.
1.10. Urządzenie musi mieć wewnętrzną pamięć pozwalającą na zapis i przechowywanie logów lokalnie.
1.11. Urządzenie musi wysyłać logi za pomocą protokołu syslog do min. 3 określonych serwerów logów / SIEM przy jednoczesnym zdefiniowaniu:
   1.11.1. Protokołu i portu dla przekazywania logów,
   1.11.2. Kategorii (ang. Facility),
   1.11.3. Rodzaju logów przekazywanych, min: logi dot. połączeń, logi z firewalla, IPS/IDS, alarmy, dzienniki systemowe,
1.12. Urządzenie musi posiadać funkcjonalność IPS z możliwością przełączenia w tryb IDS czyli tylko monitorowania bez blokowania w przypadku wykrycia zagrożeń lub anomalii.
1.13. Wbudowany IPS/IDS musi być oparty o sygnatury wykrywające znane zagrożenia i ataki sieciowe.
1.14. Urządzenie musi zapewniać możliwość dodawania własnych sygnatur IPS.
1.15. Urządzenie musi być wyposażone w min. 12 miedzianych interfejsów Ethernet 10/100/1000 Mbps, z których każdy można dowolnie zdefiniować jako np. WAN, LAN, BRIDGE, MANAGEMENT lub DMZ.
1.16. Urządzenie musi mieć możliwość kreowania interfejsów VLAN oraz GRE.
1.17. Urządzenie musi umożliwiać tworzenie sieci VPN opartych o IPSec i SSL VPN.
1.18. Maksymalna liczba tuneli VPN IPSec – minimum 500.
1.19. Urządzenie ma być wyposażone w dysk SSD o pojemności powyżej 200 GB.
1.20. Obsługa interfejsów 802.11q (VLAN) – minimum 256.
1.21. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
1.22. Urządzenie nie może narzucać limitu na liczbę użytkowników.
1.23. Liczba reguł filtrowania – minimum 8 192.
1.24. Liczba tras statycznego routingu – minimum 2 048.
1.25. Skaner antywirusowy ma być dostarczany w ramach licencji.
1.26. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
1.27. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
1.28. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
1.29. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
1.30. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
   1.30.1. lokalną bazę użytkowników (wewnętrzny LDAP),
   1.30.2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),

1.30.3. usługę katalogową Microsoft Active Directory.

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

1.32. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:

1.32.1. SSL,

1.32.2. Radius,

1.32.3. Kerberos.

1.33. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.

1.34. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.

1.35. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

1.36. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

1.37. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa przez zaszyfrowany protokół HTTPS.

1.38. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.

1.39. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

1.40. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)

1.41. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.

1.42. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

1.43. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.

1.44. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:

1.44.1. manualnego eksportu do pliku w dowolnym momencie czasu,

1.44.2. automatycznego eksportu na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu.

1.45. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z dedykowanego serwera zarządzanego przez administratora.

1.46. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

1.47. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

1.48. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.

1.49. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego.

1.50. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.

1.51. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.

1.52. Możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji.

1.53. Okres wsparcia zgodnie z zapisami OPZ w zakresie wszystkich wymaganych licencji.

1.54. Gwarancja zgodnie z zapisami OPZ.

VII. Wymagania dla sond oraz wymagania dla urządzeń komunikacji (obiekt istotny i podstawowy)

1. Zaoferowane rozwiązanie ma zapewnić bezpieczną komunikację pomiędzy monitorowanymi obiektami a systemem centralnym oraz z SOC. W szczególności dla ***Obiektów Podstawowych*** (*pkt 1. w załącznik nr*

1) należy zapewnić przekazywanie z wykorzystaniem sondy zebranego ruchu sieciowego do analizy przez system IDS znajdujący się w ***Obiekcie Kluczowym***. Z kolei system IDS działający w ***Obiekcie Kluczowym*** w sposób bezpieczny ma komunikować się z systemem centralnym znajdującym się w centrali GPW w Katowicach, jednocześnie informacje o zdarzeniach mają za pomocą protokołu syslog być wysyłane do SOC. W ***Obiektach Istotnych*** mają zostać zainstalowane mniejsze / odpowiednio dobrane instancje systemu monitorowania IDS. Ma być zapewniona komunikacja tych systemów IDS z systemem centralnym znajdującym się w Katowicach oraz informacje o zdarzeniach mają za pomocą protokołu syslog być wysyłane do systemu centralnego oraz SOC.

2. Należy zapewnić również dwukierunkową bezpieczną komunikację pomiędzy systemem centralnym znajdującym się w Katowicach a SOC, tak aby SOC miał dostęp do graficznego interfejsu użytkownika tego systemu za pomocą protokołu https.
3. Do skomunikowania obiektów należy wykorzystać wydzielone rozwiązanie oparte o komunikację bezprzewodową wykorzystującą prywatny APN. Po stronie Dostawcy rozwiązania jest zapewnienie /dostarczenie, skonfigurowanie i uruchomienie odpowiednich urządzeń komunikacyjnych (sondy, routery LTE, etc.).
4. Sonda systemu IDS to urządzenie, którego zadaniem ma być przekazywanie kopii ruchu sieciowego z obiektów podstawowych do zlokalizowanego w obiekcie kluczowym serwera IDS.
   4.1. Wymagana funkcjonalność sondy dla obiektu kluczowego:
      4.1.1. Co najmniej 4 interfejsów Ethernet 10/100 Mbit/s.
      4.1.2. Co najmniej 2 interfejsy 100/1000 Mbit/s SFP.
      4.1.3. Interfejs komórkowy – modem 4G/LTE z możliwością obsługi dwóch kart SIM.
      4.1.4. Każdy z ww. interfejsów musi pełnić rolę interfejsu słuchającego kopii ruchu dostarczonej z portów SPAN / mirror przełączników lub rolę interfejsu wyjściowego łączącego sondę z serwerem IDS.
      4.1.5. Sonda ma mieć możliwość pracy jako switch lub router stanowiący element infrastruktury sieciowej obiektu – wtedy kopiowanie ruchu ma następować ze wskazanych portów na zdefiniowany port wyjściowy lub wskazany cel routingu dla tunelu GRE do systemu IDS lub Wykonawca zapewni w inny sposób spełnienie to wymagania.
      4.1.6. Zadaniem sondy jest agregowanie i tunelowanie monitorowanego ruchu sieciowego do systemu IDS.
      4.1.7. Komunikacja z portu wyjściowego sondy do serwera IDS ma być realizowana z wykorzystaniem tunelu GRE.
      4.1.8. Kopia ruchu przesyłana z sondy do IDS musi być kompresowana.
      4.1.9. Oprogramowanie sondy musi umożliwiać odfiltrowania na portach wejściowych ruchu (konkretnych adresów lub podsieci IP, portów źródłowych i docelowych oraz typu protokołu TCP/UDP), który nie będzie przesyłany do analizy.
      4.1.10. Sonda musi synchronizować czas z serwerem NTP.
   4.2. Sonda pozostałe wymagania
      4.2.1. Montaż na szynie DIN.
      4.2.2. Obudowa przemysłowa, IP 30.
      4.2.3. Chłodzenie konwekcyjne (brak wentylatorów).
      4.2.4. Zakres temperatur pracy: -25°C do 70°C.
      4.2.5. Zasilanie 48 VDC.
5. W ***Obiektach Podstawowych*** jest wymagane zapewnienie urządzenia posiadającego funkcjonalności przełącznika LAN i routera. Dopuszcza się wykorzystanie jednego urządzenia jako sondy i urządzenia komunikacyjnego z zachowaniem poniższych funkcjonalności:
   5.1. Wymagana funkcjonalność przełącznika/routera dla obiektu podstawowego:
      5.1.1. Co najmniej 8 interfejsów Ethernet 10/100 Mbit/s.
      5.1.2. Co najmniej 2 interfejsy 100/1000 Mbit/s SFP.
      5.1.3. Interfejs komórkowy – modem 4G/LTE z możliwością obsługi dwóch kart SIM.
   5.2. Funkcje sieciowe L2
      5.2.1. IEEE 802.1q VLAN
      5.2.2. DHCP klient, serwer, relay

5.2.3. Port mirror – kopiowanie ruchu z wszystkich portów na port monitorujący

5.3. Funkcje sieciowe L3

5.3.1. Routing statyczny

5.3.2. Routing dynamiczny OSPF, RIPv2

5.3.3. VRRP

5.3.4. NAT dynamiczny

5.3.5. NAT statyczny podsieć – podsieć

5.3.6. NAT statyczny IP – IP

5.3.7. Odczytywanie parametrów urządzenia poprzez SNMP

5.4. Kontrola dostępu

5.4.1. Listy dostępu ALC działające w warstwach L2, L3 i L4

5.4.2. Możliwość wyłączenia nieużywanych portów.

5.4.3. Uwierzytelnianie IEEE 802.1x na porcie.

5.4.4. Uwierzytelniające Proxy.

5.4.5. Ochrona dostępu do sterowników i urządzeń nieposiadających funkcji kontroli dostępu, użytkownik najpierw musi uwierzytelnić się na firewallu i potem otrzyma czasowy dostęp do konkretnego urządzenia za firewallem.

5.4.6. Logowanie aktywności użytkownika.

5.5. VPN

5.5.1. IPSec, obsługa certyfikatów X.509

5.5.2. IPSec, dynamiczna wymiana kluczy IKE

5.5.3. IPSec, szyfrowanie: AES, 3DES

5.5.4. L3 VPN GRE

5.5.5. OpenVPN SSL

5.5.6. DPI firewall - firewall realizujący głęboką analizę pakietów (DPI) dla protokołów co najmniej Modbus RTU, Modbus TCP, S7 TCP

5.6. Funkcje portów szeregowych

5.6.1. Transparentne tunelowanie

5.6.2. Brama dla protokołów Modbus RTU/Modbus TCP,

5.6.3. Serwer terminali szeregowych TCP/UDP

5.6.4. 2 porty szeregowe

5.6.5. Możliwość nasłuchiwania transmisji RS-232/485 i przekierowywanie jej do systemu IDS w celu analizy.

5.7. Pozostałe wymagania

5.7.1. Montaż na szynie DIN.

5.7.2. Obudowa przemysłowa, IP 30.

5.7.3. Chłodzenie konwekcyjne (brak wentylatorów).

5.7.4. Zakres temperatur pracy: -25°C do 70°C.

5.7.5. Zasilanie 48 VDC.

6. Do zapewnienia komunikacji z **Obiektów Istotnych** należy zastosować urządzenia komunikacyjne o następującej funkcjonalności:

6.1. Co najmniej 6 interfejsów Ethernet 10/100 Mbit/s.

6.2. Co najmniej 2 interfejsy 100/1000 Mbit/s SFP.

6.3. Interfejs komórkowy – modem 4G/LTE z możliwością obsługi dwóch kart SIM.

6.4. Urządzenie ma synchronizować czas z serwerem NTP.

6.5. Funkcje sieciowe L3:

6.5.1. Routing statyczny

6.5.2. Routing dynamiczny OSPF, RIPv2

6.5.3. VRRP

6.5.4. NAT dynamiczny

6.5.5. NAT statyczny podsieć – podsieć

6.5.6. NAT statyczny IP – IP

6.6. Kontrola dostępu:

6.6.1. Co najmniej listy dostępu ALC działające w warstwach L2, L3 i L4
6.6.2. Możliwość wyłączenia nieużywanych portów
6.6.3. Uwierzytelnianie IEEE 802.1x na porcie

6.7. VPN
6.7.1. IPSec, obsługa certyfikatów X.509
6.7.2. IPSec, dynamiczna wymiana kluczy IKE
6.7.3. IPSec, szyfrowanie: AES, 3DES
6.7.4. L3 VPN GRE
6.7.5. OpenVPN SSL

6.8. Pozostałe wymagania
6.8.1. Montaż na szynie DIN.
6.8.2. Obudowa przemysłowa, IP 30.
6.8.3. Chłodzenie konwekcyjne (brak wentylatorów).
6.8.4. Zakres temperatur pracy: -25°C do 70°C.
6.8.5. Zasilanie 48 VDC.

VIII. Wymagania dla urządzeń sieciowych i systemu zarządzania urządzeniami sieciowymi dla obiektu kluczowego.

1. System operacyjny przemysłowych urządzeń sieciowych (przełączników) powinien posiadać następujące funkcjonalności i możliwości:
   1.1. 802.1q Statyczny VLAN, VLAN tag, VLAN Q-in-Q (tunelowanie)
   1.2. 802.3x kontrola przepływu (Flow Control)
   1.3. IGMPv2/v3 snooping, IGMP querier, IGMP fast leave
   1.4. 802.1AB LLDP
   1.5. 802.1p Class of service
   1.6. Ograniczanie przepustowości portów (rate limiting, traffic shaping)
   1.7. Uwierzytelnianie lokalne i centralne (RADIUS, TACACS+)
   1.8. 802.1X kontrola dostępu (port access control)
   1.9. Uwierzytelnianie MAC, wykrywanie konfliktów IP/MAC
   1.10. Automatyczne wyłączanie nieużywanych portów
   1.11. NTP/SNTP (klient/serwer)
   1.12. 802.1d Spanning Tree Protocol (STP)
   1.13. 802.1w Rapid Spanning Tree Protocol (RSTP)
   1.14. Protokół ring
   1.15. SNMP v2c/3 (brak v1 lub możliwość wyłączenia)Syslog
   1.16. 802.1AX/802.3ad agregacja portów (statyczna i LACP)
   1.17. Statyczny i dynamiczny routing (RIPv2, OSPFv2, VRRPv2/3)
   1.18. Szyfrowane tunele VPN (klient i serwer) IPsec, SSL
   1.19. Routing multicast
   1.20. Tunelowanie GRE
   1.21. Zapora ogniowa (firewall) z inspekcją stanu
   1.22. Translacja adresów NAPT, NAT 1-TO-1 (wybrane adresy lub cała podsieć), proxy ARP
   1.23. Przekierowanie portów (port forwarding) IP Multinetting (kilka podsieci w jednym VLAN-ie)
   1.24. DSCP/ToS modification
   1.25. Port monitoring (mirroring) z możliwością wyboru rodzaju ruchu (in, out, in/out) z dowolnych portów
2. Pozostałe wymagania dla urządzeń sieciowych.
   2.1. Urządzenie w wykonaniu przemysłowym obudowa metalowa,
   2.2. Klasa szczelności IP30,
   2.3. Montaż na szynie DIN,
   2.4. Zakres temperatur pracy –25 to +70°C,
   2.5. MTBF wg MIL-HDBK-217-F co najmniej 500 000h
   2.6. Redundantne zasilanie (zasilanie z dwóch źródeł), zakres napięcia zasilającego 19 to 60 VDC.

2.7. Certyfikaty
2.7.1.IEC 62236-4, EN 50121-4,
2.7.2.EN 61000-6-1,EN 61000-6-2, EN 61000-6-3, EN 61000-6-4
2.8. Certyfikaty dot. Bezpieczeństwa UL 62368-1
2.9. Typ chłodzenia - bez wentylatorowy.

3. System do konfiguracji urządzeń i zarządzania siecią, wymagane funkcjonalności:
3.1. System musi umożliwiać skanowanie sieci w celu wykrycia urządzeń, zarówno z wykorzystaniem protokołu ICMP (ping) jak i innych/własnych rozwiązań pozwalających na odnalezienie urządzeń bez względu na ich adresy IP lub w ogóle nieposiadających adresu.
3.2. System musi umożliwiać wykrywanie topologii połączeń pomiędzy urządzeniami w oparciu o protokół LLDP
3.3. System musi umożliwiać obsługę SNMP w wersji v2 i v3
3.4. System musi umożliwiać szybki, uproszczony przydział adresów sieciowych.
3.5. System musi umożliwiać konfigurację nowych elementów sieci
3.6. System musi udostępniać łatwy dostęp do interfejsów administracyjnych urządzeń (WEB, CLI) z poziomu aplikacji monitorującej.
3.7. System musi umożliwiać monitorowanie i diagnostykę sieci, przynajmniej w zakresie wykrywania zaniku połączeń i zmian (rekonfiguracji) w topologii sieci.
3.8. System musi umożliwiać prezentację statystyk komunikacji na poszczególnych portach (status, prędkość, liczniki danych, błędy)
3.9. System musi umożliwiać prezentację wykrytych urządzeń i połączeń między nimi na schemacie topologii, z funkcją auto-rozmieszczenia i możliwością ręcznego wprowadzania zmian (dodawanie/usuwanie urządzeń, dodawanie/usuwanie połączeń, zmiana położenia, tworzenie grup). Możliwość filtrowania wyświetlanych na schemacie urządzeń w oparciu o: adres IP, domyślna brama, nazwa hosta, wersja firmware-u, rodzina/model, lokalizacja, status SNMP, odbierane pułapki SNMP
3.10. System musi umożliwiać wyświetlanie zdarzeń i alarmów odbieranych z urządzeń sieciowych (wbudowany serwer SNMP trap). Zdarzenia i alarmy powinny być przechowywane w aplikacji monitorującej z możliwością ich wyeksportowania.
3.11. System musi posiadać wbudowany serwer Syslog zbierający dane z dzienników urządzeń sieciowych z możliwością ich wyeksportowania.
3.12. System musi umożliwiać aktualizację firmware-u urządzeń, pojedynczo i zbiorczo
3.13. System musi umożliwiać Backup i odtwarzanie konfiguracji pojedynczych urządzeń i całej sieci
3.14. System musi umożliwiać budowanie kolejnych sieci (powielania) na podstawie utworzonego szablonu.
3.15. System musi umożliwiać automatyczne wykrywanie i alarmowanie zmian wprowadzonych do konfiguracji urządzeń z możliwością analizy/porównania z konfiguracją bazową
3.16. System musi posiadać wbudowana instrukcję obsługi zapewniająca dostęp do dokumentacji z poziomu aplikacji monitorującej.
3.17. System musi umożliwiać wymagane funkcjonalności z zakresu bezpieczeństwa takie jak:
3.17.1. Wykrywanie niezmienionych, domyślnych haseł
3.17.2. Możliwość zmiany haseł we wszystkich urządzeniach w systemie, pojedynczo i zbiorczo
3.17.3. Analizator mocy haseł
3.17.4. Możliwość stworzenia wzorca konfiguracji dla całej sieci
3.17.5. Identyfikacja adresów MAC urządzeń podłączonych do danego portu urządzenia
3.17.6. Konfiguracja filtrowania adresów MAC w oparciu o wykryte na poszczególnych portach urządzenia – tworzenie białej listy
3.17.7. Konfiguracja kontroli dostępu 802.1x
3.17.8. Konfiguracja ograniczeń dla przepustowości portów
3.17.9. Możliwość centralnego wykrywania i wyłączania nieużywanych portów na wybranych przełącznikach
3.17.10. Zabezpieczanie hasłem kopii bezpieczeństwa projektu

3.17.11. Wyłączenie usług zarządzających, które przesyłają dane otwartym tekstem (telnet i http)
3.17.12. Wykrywanie protokołów routingu OSPF i RIP, w których nie zastosowano sygnatur MD5-HMAC, możliwość skonfigurowanie tego zabezpieczenia
3.17.13. Kalkulator SHA256 dla plików z oprogramowaniem układowym (firmware)

3.18. Wymagania dodatkowe

3.18.1. Dla urządzeń sieciowych oraz systemu zarzadzania wymagana jest dostęp do bezpłatnych aktualizacji FW i SW przez cały okres użytkowania urządzeń przez zamawiającego.
3.18.2. Gwarancja min. 4 lat

IX. Serwis oraz wsparcie w zakresie zainstalowanych systemów.

Wraz z dostawą systemu powinno być zagwarantowane:

1. Wsparcie techniczne na okres obowiązywania umowy. Wsparcie powinno obejmować:
   a. Dostęp do najnowszych wersji oprogramowania;
   b. Pobieranie sygnatur dla podatności;
   c. Możliwość przedłużenia wsparcia dla systemu na okres dodatkowego roku po zakończeniu umowy;
   d. Dostęp do pomocy technicznej w dni robocze w godzinach 8:00- 16:00.

X. Szkolenia.

1. Wykonawca na własny koszt przeszkoli zespół zamawiającego (5 osób) z zakresu administracji oraz pracy z systemem. Szkolenie musi być przeprowadzone w języku polskim w oparciu o materiały szkoleniowe w języku polskim i trwać łącznie co najmniej 20 godzin. Koszty związane z przygotowaniem i przeprowadzeniem szkolenia pokrywa Wykonawca. Zamawiający wymaga by przedstawiciele zespołu automatyki mogli aktywnie uczestniczyć w procesie wdrożenia systemu i tym samym budować kompetencje.
2. Wykonawca na własny koszt przeszkoli zespół zamawiającego (5 osób) z zakresu administracji oraz pracy z systemem monitorowania oraz jego komponentami. Szkolenie musi być przeprowadzone w języku polskim w oparciu o materiały szkoleniowe w języku polskim i trwać łącznie co najmniej 40 godzin. Koszty związane z przygotowaniem i przeprowadzeniem szkolenia pokrywa Wykonawca. Zamawiający wymaga by przedstawiciele zespołu automatyki mogli aktywnie uczestniczyć w procesie wdrożenia systemu i tym samym budować kompetencje.
3. Ponadto Wykonawca przeprowadzi dla personelu odpowiedzialnego za systemy przemysłowe oraz dla personelu zamawiającego dwa szkolenia online budujące świadomość z zakresu bezpieczeństwa systemów OT/ICS.

XI. Warunki odbioru prac.

Odbiór prac będzie się odbywał poprzez protokół podpisany z obu stron

XII. Gwarancja

1. Wszystkie licencje i system (urządzenia) maja mieć zagwarantowane wsparcie na 4 lata od dnia uruchomienia usługi SOC.
2. Wszystkie urządzenia musza posiadać gwarancję na 4 lata liczoną od dnia uruchomienia usługi SOC.

MATERIAŁ POUFNY

Udostępniany na zasadach opisanych w Rozdziale III ust. 3 Zaproszenia do negocjacji

ZAŁĄCZNIK NR 2

PROJEKTOWANE POSTANOWIENIA
UMOWY WDROŻENIOWA ORAZ ZAKUPU SYSTEMU
(dalej jako**: „Umowa”**)

zawarta w dniu …… w Katowicach pomiędzy:

Górnośląskim Przedsiębiorstwem Wodociągów Spółką Akcyjną z siedzibą w Katowicach (40-026) przy ul. Wojewódzkiej 19, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem 000024753, której akta rejestrowe przechowuje Sąd Rejonowy Katowice-Wschód w Katowicach, Wydział VIII Gospodarczy Krajowego Rejestru Sądowego, posiadającą numer NIP 634 012 87 88 oraz REGON: 27150669500000, będącą podatnikiem VAT czynnym, wysokość kapitału zakładowego 425 875 100,00 zł. – opłacono w całości, posiadającą status dużego przedsiębiorstwa w rozumieniu art. 4 pkt 6 ustawy z dnia 08 marca 2013r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (t.j. Dz. U. 2023 poz. 711 z późn. zm.), reprezentowaną przez:

1. ……. …….
2. ……. ……..

zwaną dalej **„Zamawiającym"**

a

…….. prowadzącym działalność gospodarczą pod firmą „……” w ……. przy ul. ……., zarejestrowanym w Centralnej Ewidencji i Informacji o Działalności Gospodarczej, posiadającym numer NIP: ……, numerem REGON: ……., numer PESEL: ……., będącym podatnikiem VAT czynnym

lub

…….. wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS …….., której akta rejestrowe przechowuje Sąd Rejonowy ……., ……. Wydział Gospodarczy Krajowego Rejestru Sądowego, posiadającą numer NIP ……. oraz numer REGON ……, o kapitale zakładowym …….., będącą podatnikiem VAT czynnym, reprezentowaną przez:

1. …… …….
2. …… …….

uprawnionej/ych do samodzielnej/łącznej reprezentacji zgodnie z odpisem aktualnym Wykonawcy z rejestru przedsiębiorców Krajowego Rejestru Sądowego,
zwanym/ą dalej **„Wykonawcą”**,

zwanymi dalej łącznie **„Stronami”**, a każde z osobna **„Stroną”.**

Mając na uwadze, że celem niniejszej Umowy jest wdrożenie i świadczenie przez Wykonawcę we współpracy i na rzecz Zamawiającego przez okres …… usług monitorowania incydentów

bezpieczeństwa przez wyspecjalizowane Security Operations Center (SOC), tj. centrum bezpieczeństwa teleinformatycznego, które będzie wspierało Zamawiającego jako operatora usługi kluczowej w spełnieniu wymogów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U.2022.1863 t.j. z późn. zm.), dalej jako: „ustawa o krajowym systemie cyberbezpieczeństwa", Strony zgodnie oświadczają co następuje:

§1
Definicje

Strony postanawiają, że w dalszej części niniejszej Umowy oraz załącznikach do Umowy stanowiących jej integralną część stosować będą następujące definicje:

Awaria	Błąd lub wada powodujące utratę funkcjonalności Systemu, powodujący jego niewłaściwe działanie lub całkowite unieruchomienie, zidentyfikowany lub powstały w czasie eksploatacji Systemu.
Oprogramowanie	Oprogramowanie niezbędne do prawidłowej pracy systemu, które dzieli się na Oprogramowanie On Premise i Oprogramowanie SaaS.
Oprogramowanie On Premise	Oprogramowanie wskazane w Załączniku nr 9 będące oprogramowaniem zainstalowanym i utrzymywanym przez Wykonawcę na własnym sprzęcie (serwerze) Zamawiającego.
Oprogramowanie SaaS	Oprogramowanie wskazane w Załączniku nr 9 będące oprogramowaniem, z którego korzystanie odbywa się poprzez zapewnienie Zamawiającemu prawa do uzyskiwania dostępu i korzystania z Oprogramowania zainstalowanego na serwerach obsługiwanych przez Wykonawcę.
OPZ	Opis Przedmiotu Zamówienia
Licencja	Przysługujące Zamawiającemu w czasie obowiązywania umowy, niematerialne, niewyłączne i niezbywalne prawo do korzystania z Oprogramowania On Premise, w zakresie określonym w postanowieniach Umowy.
Personel Wykonawcy	Oznacza osoby delegowane przez Wykonawcę do wykonywania niniejszej Umowy, w skład których zespołów wchodzą osoby posiadające uprawnienia zgodne z tymi wskazanymi w szczegółowym Opisie Zamówienia.
Praca zdalna	Praca poprzez dostęp do Systemu lub jego części realizowana w inny sposób niż poprzez bezpośrednie fizyczne podłączenie do sieci informatycznej Zamawiającego w jego lokalizacji przez członka Personelu Wykonawcy. Praca zdalna winna zapewniać bezpieczeństwo i poufność danych przekazywanych do/i z systemów informatycznych Zamawiającego oraz być zgodna z obowiązującymi w tym zakresie u Zamawiającego procedurami.
Protokół Wykonania Usługi SOC	Dokument potwierdzający przez Zamawiającego poprawność świadczonych przez Wykonawcę Usług zgodnie z wzorem określonym w **Załączniku nr 4.**
Scenariusz	Scenariusz bezpieczeństwa w rozumieniu OPZ.

System	Rozwiązanie informatyczno-biznesowe, konfiguracja i parametryzacja, dostarczone przez Wykonawcę na podstawie Umowy, łącznie z Oprogramowaniem służące do stałego i ciągłego monitorowania zdarzeń w infrastrukturze Zamawiającego, (System zgłaszania i obsługi incydentów) przez co strony rozumieją zbieranie, analizowanie oraz korelację zdarzeń, które zachodzą w sieciach oraz systemach klienta Zamawiającego. Szczegółowy wykaz funkcjonalności, które powinien zawierać System zawarty jest w Szczegółowym OPZ.
Usługa SOC	Usługa polegająca na zapewnieniu, przy wykorzystaniu Systemu, stałego i ciągłego monitorowania zdarzeń w infrastrukturze Zamawiającego przez co strony rozumieją zbieranie, analizowanie oraz korelację zdarzeń, które zachodzą w sieciach oraz systemach Zamawiającego, a także wykrywanie zdarzeń lub incydentów bezpieczeństwa zagrożeń oraz analizę funkcjonowania w zakresie bezpieczeństwa systemów infrastruktury OT przez cały okres obowiązywania Umowy oraz ocena wpływu zdarzeń lub incydentu bezpieczeństwa OT na systemy Zamawiającego.
Utwory	Rezultaty prac Wykonawcy stanowiące utwory w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, powstałe w ramach realizacji Przedmiotu Umowy, z wyłączeniem Oprogramowania.
Wdrożenie	Wszelkie usługi, instalacje i czynności wykonane przez Wykonawcę i przez Zamawiającego w środowisku informatycznym Zamawiającego, bądź Wykonawcy (w przypadku Oprogramowania SaaS), tj. produkcyjnym, testowym, oraz na serwerach Zamawiającego mające na celu docelowe uruchomienie i nadanie poziomu odpowiedniej sprawności Systemu zapewniającego świadczenie Usługi SOC.
Wsparcie Techniczne Systemu	Usługa świadczona przez Wykonawcę na rzecz Zamawiającego dla zachowania ciągłości i prawidłowości świadczenia Usług, w tym Oprogramowania, na warunkach określonych w **Załączniku nr 2** do Umowy

§2
Przedmiot Umowy

1. Zamawiający powierza, a Wykonawca przyjmuje do wykonania Przedmiot Umowy, jakim jest Wdrożenie Oprogramowania i świadczenie przez Wykonawcę na rzecz Zamawiającego Usług SOC, tj. centrum bezpieczeństwa teleinformatycznego, które będzie wspierało Zamawiającego jako operatora usługi kluczowej w spełnieniu wymogów ustawy o krajowym systemie cyberbezpieczeństwa.
2. Przedmiot Umowy zostanie zrealizowany zgodnie z Umową, w tym z wymaganiami zawartymi w OPZ stanowiącym **Załącznik nr 1** do Umowy oraz Ofertą Wykonawcy stanowiącą **Załącznik nr 6** do Umowy, pod warunkiem że Oferta nie jest sprzeczna z warunkami umowy i OPZ. Zakres powyższego zadania obejmuje w szczególności:
   1) udostępnienie i Wdrożenie Oprogramowania (SaaS oraz On Premise), które zapewni stałe i ciągłe monitorowanie zdarzeń w infrastrukturze Zamawiającego przez co Strony rozumieją zbieranie, analizowanie oraz korelację zdarzeń, które zachodzą w sieciach oraz systemach Zamawiającego. Jako źródła zdarzeń oprócz systemów teleinformatycznych Zamawiającego będą traktowane zgłoszenia użytkowników i administratorów Zamawiającego oraz przyjęte przez Zamawiającego zgłoszenia incydentów otrzymane ze źródeł zewnętrznych;
   2) udostępnienie i Wdrożenie Oprogramowania (SaaS oraz On Premise), które zapewni wykrywanie zdarzeń lub incydentów bezpieczeństwa zagrożeń oraz analizę funkcjonowania w zakresie bezpieczeństwa systemów infrastruktury OT przez cały okres obowiązywania Umowy;

3) udostępnienie i Wdrożenie Oprogramowania (SaaS oraz On Premise), które zapewni ocenę wpływu zdarzeń lub incydentów bezpieczeństwa OT na systemy Zamawiającego;
4) Świadczenie usług SOC i Wsparcia Technicznego przez cały okres obowiązywania Umowy od dnia podpisania Protokołu Odbioru Końcowego Wdrożenia usługi SOC.

3. Przedmiot Umowy obejmuje realizację wszystkich czynności w celu zapewnienia wymaganych przez Zamawiającego funkcjonalności, zgodnie z Umową, w tym z OPZ.
4. Wykonawca oświadcza, że Przedmiot Umowy będzie zgodny z postanowieniami Umowy oraz że posiada odpowiednią wiedzę i doświadczenie oraz środki i urządzenia by wykonywać objęte Umową świadczenia oraz że wykona je z zachowaniem należytej zawodowej staranności, a także w zgodzie z obowiązującymi przepisami, zaś podejmowane przez niego działania oraz Oprogramowanie i System, którym dysponuje i który udostępnia Zamawiającemu są zgodne z wymogami zawartymi w ustawie o krajowym systemie cyberbezpieczeństwa. Wykonawca oświadcza, że jeśli wykonanie Umowy będzie wymagało dostępu do informacji niejawnych, to Wykonawca będzie spełniał wszelkie wymagania związane z dostępem oraz ochroną informacji niejawnych o odpowiedniej klauzuli.
5. Zamawiający udostępni Wykonawcy swoją Infrastrukturę systemową w szczególności zaś swoje serwery oraz macierz dyskową. Parametry sprzętu udostępnionego będą stanowić **Załącznik nr 11**. Wykonawca oświadcza, że sprzęt udostępniony jest wystarczający dla wykonania Przedmiotu Umowy, zaś jego ewentualne uzupełnienie obciąża Wykonawcę i nie będzie wpływać na wysokość Wynagrodzenia. Na sprzęcie udostępnionym Wykonawca będzie mógł przechowywać część danych niezbędnych do prawidłowego wykonywania Umowy, w szczególności zaś informacje gromadzone przez System, a związane z monitorowaniem i wykrywaniem zagrożeń będące Oprogramowaniem On Premise. Dodatkowo Zamawiający, w zakresie urządzeń serwerowych za które jest odpowiedzialny zapewni możliwość bezpiecznego, zdalnego połączenia z Systemem w celu przeprowadzenia czynności serwisowych i instalacyjnych pod warunkiem zapewnienia ze strony Wykonawcy bezpieczeństwa i poufności przekazywanych danych do/i z systemów informatycznych Zamawiającego. Zdalny dostęp do infrastruktury Zamawiającego jest możliwy jedynie przy spełnieniu przez Wykonawcę warunków zawartych w wewnętrznych politykach Zamawiającego, definiujących tę kwestię, które to polityki Wykonawca zobowiązuje się przestrzegać.
6. Wykonawca zobowiązuje się na moment zakończenia Umowy udostępnić do importu wszystkie dane Zamawiającego znajdujące się w Systemie niezależnie od ich usytuowania (tj. tego czy znajdują się na Serwerach Zamawiającego czy też Wykonawcy), tj. wykaz urządzeń, konfiguracje, polityki, logi, raporty, lokalizacje.
7. Wykonawca, w ramach realizacji Przedmiotu Umowy przeprowadzi szkolenia dla osób zaangażowanych po stronie Zamawiającego.
8. Szkolenia będą przeprowadzone zdalnie poprzez uzgodniony z Zamawiającym komunikator, w języku polskim, a Wykonawca zapewni materiały szkoleniowe w języku polskim w formie elektronicznej dla wszystkich przedstawicieli Zamawiającego biorących udział w szkoleniu. Szkolenie zostanie zorganizowane dla maksymalnie 5 osób. W przypadku gdy przedstawiciele Zamawiającego nie będą mogli wziąć udziału w przeprowadzonym szkoleniu, Strony każdorazowo ustalą termin dodatkowego szkolenia.
9. W ramach wynagrodzenia określonego w § 4 ust. 1 Umowy, Wykonawca poniesie wszelkie koszty związane z przygotowaniem i przeprowadzeniem szkolenia, o którym mowa w ust. 8 powyżej.
10. Odbycie szkolenia przez wskazanych przez Zamawiającego pracowników Zamawiającego, będzie potwierdzone certyfikatem wystawionym przez Wykonawcę.

§3

Terminy obowiązywania Umowy

1. Wykonawca zobowiązany jest do Wdrożenia Systemu w infrastrukturze teleinformatycznej Zamawiającego i rozpoczęcia świadczenia Usługi SOC, w tym przeprowadzenia szkoleń i dostarczenia dokumentacji szkoleniowej wskazanej w § 2 ust. 8 Umowy w terminie 6 miesięcy od dnia podpisania Umowy. Strony przewidują możliwość wydłużenia wyżej wymienionego terminu na podstawie oświadczenia Zamawiającego. Oświadczenie w tym zakresie może złożyć Kierownik Projektu Zamawiającego. Zamawiający może złożyć oświadczenie gdy przyczyna wydłużenia terminu wykonania prac leży po jego stronie. Prace mogą zostać wydłużone maksymalnie o cztery tygodnie.
2. Zakończenie realizacji Przedmiotu Umowy w zakresie Wdrożenia Systemu określonego w § 2 ust. 1 Umowy, zostanie potwierdzone podpisaniem Protokołu Końcowego Odbioru Systemu, którego wzór stanowi **Załącznik nr 3** do Umowy.
3. Umowa wchodzi w życie w dniu podpisania i obowiązuje przez 48 miesięcy.
4. Za termin zakończenia realizacji Przedmiotu Umowy w zakresie świadczenia Usługi SOC oraz Usługi Wsparcia Technicznego Systemu przyjmuje się datę podpisania Protokołu Końcowego Odbioru Usług SOC oraz Wsparcia Technicznego Systemu, którego wzór stanowi **Załącznik nr 12** do Umowy.

§ 4

Wynagrodzenie

1. Za należyte wykonanie całości świadczeń składających się na Przedmiot Umowy, w tym za Wdrożenie, świadczenie Usługi SOC, świadczenie Usługi Wsparcia Technicznego, udzielenie licencji na Oprogramowanie oraz przeniesienie praw autorskich do Utworów, Zamawiający zapłaci Wykonawcy miesięczne wynagrodzenie ryczałtowe w łącznej wysokości:
   a) …… PLN netto (słownie: ……)
   b) …… PLN brutto (słownie:……).
2. Wynagrodzenie płatne będzie w 48 równych częściach. Płatności będą dokonywane w okresach miesięcznych w kwocie:
   a) …… PLN netto (słownie: ……)
   b) ……. PLN brutto (słownie:……)
3. Wynagrodzenie ryczałtowe, określone w ust. 1 powyżej, stanowi całkowite i zupełne wynagrodzenie należne Wykonawcy oraz pokrywa wszelkie ryzyko i koszty poniesione przez Wykonawcę, jak również wynagrodzenie z tytułu świadczonych przez Zamawiającego usług. Żadne niedoszacowanie, pominięcie, brak rozpoznania warunków realizacji nie może być podstawą do żądania zmiany składników wynagrodzenia ustalonych w Umowie.
4. Strony zgodnie przyznają, iż wynagrodzenie wskazane w ust. 1 powyżej obejmuje również wynagrodzenie z tytułu Wdrożenia Systemu oraz wynagrodzenia za przeniesienie praw autorskich i udzielenia licencji na podstawie niniejszej Umowy.
5. Wynagrodzenie zostanie powiększone o podatek VAT w obowiązującej stawce.
6. Wynagrodzenie Wykonawcy płatne będzie w terminie 30 dni od daty wystawienia faktury. Wykonawca zobowiąże się doręczyć fakturę nie później niż w terminie 7 dni od jej wystawienia a uchybienie temu terminowi spowoduje odpowiednie wydłużenie terminu zapłaty o każdy dzień uchybienia. Podstawą do wystawienia faktury jest podpisany przez obie Strony właściwy Protokół Wykonania Usługi SOC i Usługi Wsparcia Technicznego.
7. Wynagrodzenie płatne będzie na rachunek bankowy Wykonawcy, wskazany w fakturze. Terminem zapłaty jest dzień obciążenia rachunku bankowego Zamawiającego wymaganą należnością.
8. Wykonawca ma obowiązek wskazywania numeru Umowy na fakturze.
   Strony Oświadczają, że są zarejestrowanymi, czynnymi podatnikami podatku od towarów i usług, uprawnionymi do wystawiania i otrzymywania faktur.

9. Zamawiający zastrzega sobie prawo do dokonywania zapłaty stosując mechanizm podzielonej płatności (split payment).
10. Rachunek rozliczeniowy wskazany przez Wykonawcę na fakturze musi występować na tzw. białej liście podatników VAT. W przypadku, gdy rachunek rozliczeniowy nie będzie widniał na białej liście podatników VAT, Zamawiający uprawniony będzie do wstrzymania płatności do czasu wskazania przez Wykonawcę odpowiedniego rachunku. W takim przypadku Wykonawca nie będzie uprawniony do naliczenia odsetek za opóźnienie.
11. W przypadku naliczenia przez Zamawiającego kar umownych zgodnie z § 16 Umowy, Zamawiający zastrzega sobie prawo do potrącenia kwoty naliczonych kar umownych bezpośrednio z zafakturowanej kwoty należnej Wykonawcy z tytułu wykonania Przedmiotu Umowy, na podstawie stosownej noty wystawionej przez Zamawiającego, na co Wykonawca wyraża bezwarunkową zgodę.
    Zamawiający oświadcza, że zezwala na przesyłanie drogą elektroniczną faktur wystawianych przez Wykonawcę zgodnie z obowiązującymi przepisami ustawy z 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. U. z 2022 r. poz. 931 t.j. z późn. zm.), w formacie PDF w związku z realizacją niniejszej Umowy. W formacie PDF będą wystawiane i przesyłane drogą elektroniczną również faktury korygujące i duplikaty faktur oraz noty.
12. Wykonawca uprawniony jest do przesyłania Zamawiającemu wystawionych przez siebie faktur elektronicznych (faktury, faktury korygujące) oraz not wraz z dołączonymi do nich załącznikami w postaci jednolitego pliku PDF na adres mailowy Zamawiającego: ……

§5
Obowiązki Stron

1. W ramach wykonywania Przedmiotu Umowy, o którym mowa w § 2 Umowy, Wykonawca zobowiązany jest w szczególności do:
    1) wykonania Przedmiotu Umowy z należytą starannością, przy zachowaniu zasad współczesnej wiedzy technicznej i zgodnie z obowiązującymi przepisami prawa w szczególności zaś w zgodzie z wymogami zawartymi w ustawie o krajowym systemie cyberbezpieczeństwa,
    2) dołożenia należytej staranności w celu zapewnienia rozwiązań optymalnych, w szczególności ze względu na niezawodność, wydajność i ergonomię zgodne z oczekiwaniami Zamawiającego,
    3) bieżącego konsultowania prac z Zamawiającym w celu uzyskania akceptacji przez Zamawiającego wszelkich prac na wszystkich etapach realizacji Przedmiotu Umowy,
    4) współpracy z Zamawiającym w celu przekazania wiedzy na temat Systemu, polegającej w szczególności na udzielaniu Zamawiającemu wszelkich informacji,
    5) całkowitej separacji danych Zamawiającego od danych innych podmiotów, dla których Wykonawca również świadczy usługi SOC,
    6) przestrzegania przepisów bhp i ppoż. oraz obowiązujących procedur i instrukcji dotyczących zasad zapewnienia bezpieczeństwa oraz podporządkowywania się wszelkim poleceniom służb Zamawiającego w tym zakresie. W przypadku stwierdzenia przez Zamawiającego niestosowania się Wykonawcy do obowiązujących przepisów lub procedur lub zarządzeń, o których mowa w niniejszym punkcie, Zamawiający ma prawo odstąpić od Umowy lub ją wypowiedzieć z zachowaniem prawa do kary umownej, o której mowa w § 16 ust. 2 Umowy,
    7) poniesienia pełnej odpowiedzialności z tytułu szkód, które zostały spowodowane przez Wykonawcę lub przez którekolwiek osoby realizujące Umowy w jego imieniu i na jego rzecz oraz za działania lub zaniechania osób, którym zlecił zadania w zakresie realizacji Umowy jak za swoje własne działania lub zaniechania,
    8) przeszkolenia wyznaczonych pracowników Zamawiającego,

9) przygotowywania okresowych, miesięcznych raportów dotyczących świadczonej usługi w postaci elektronicznej na wskazany adres e-mail. Raport powinien zawierać informację dotyczącą ilości obsłużonych incydentów, czasów obsługi. Raport będzie dostarczany na wskazany przez Zamawiającego adres e-mail.

10) dokumentowania i kontrolowania działania oraz wykonanie prac za pomocą systemu obsługi zgłoszeń, w którym jest nadawana priorytetyzacja incydentów oraz zamodelowany jest obieg informacji przez wszystkie linie ekspertów SOC.

2. Zamawiający oświadcza, że dołoży wszelkich niezbędnych starań zmierzających do umożliwienia Wykonawcy sprawnego wykonywania postanowień niniejszej Umowy, w szczególności poprzez zapewnienie niezawodnej infrastruktury sprzętowej o parametrach określonych w **Załączniku nr 11**, odpowiednich warunków technicznych i organizacyjnych realizacji Przedmiotu Umowy, terminowego realizowania postanowień i zobowiązań oraz oddelegowanie do prac związanych z realizacją Umowy niezbędnej liczby kompetentnych pracowników.

3. Zamawiający zobowiązany jest do zapewnienia niezbędnego współdziałania przy wykonywaniu Umowy przez Wykonawcę, a w szczególności:

1) zapewnienia infrastruktury sprzętowej wyspecyfikowanej w **Załączniku nr 11**, koniecznej do instalacji Oprogramowania On Premise i wdrożenia objętego Umową Systemu oraz świadczenia Usługi SOC,

2) zapewnienia udziału w pracach wdrożeniowych przedstawicieli Zamawiającego w uzgodnionym wymiarze czasowym, o kompetencjach umożliwiających wykonanie powierzonych prac,

3) opiniowania, weryfikacji i akceptacji rezultatów prac wykonywanych przez Wykonawcę zgodnie z przyjętymi procedurami, podejmowania decyzji w zakresie wymaganych funkcjonalności Systemu.

4. W przypadku, gdy w trakcie realizacji Przedmiotu Umowy zajdzie konieczność uzyskania wglądu w dane użytkowników Systemu, Zamawiający może umożliwić Wykonawcy dostęp do elementów systemu zawierających dane osobowe pod warunkiem podpisania pomiędzy stronami umowy o powierzeniu przetwarzania danych osobowych.

§ 6
Zarządzanie projektem

1. W celu należytego wykonania Przedmiotu Umowy, Strony powołują Kierowników Projektu w osobach:

1) po stronie Zamawiającego — ……..
tel.: ……., kom.: ……, email: ……

2) po stronie Wykonawcy — ……..
tel.: ……., kom.: ……, email: ……..

2. Obowiązkami Kierowników Projektu jest:

1) zapewnienie odpowiedniego wsparcia dla realizacji Przedmiotu Umowy,

2) zapewnienie odpowiednich zasobów do realizacji Przedmiotu Umowy,

3) nadzór nad realizacją Przedmiotu Umowy oraz bieżące zarządzanie postępem prac oraz sposobem wykonywania Usługi SOC i usługi Wsparcia Technicznego Usługi SOC i Systemu

4) podpisywanie wszystkich dokumentów niestanowiących aneksów do Umowy.

3. Każda ze Stron może zmienić swojego Kierownika Projektu, z zastrzeżeniem, że zmiana taka nie jest podstawą do zmiany Harmonogramu Prac. Zmiana przez Strony Kierownika Projektu nie jest zmianą Umowy i nie wymaga podpisania aneksu. Zmiana przez Strony Kierownika Projektu jest skuteczna względem drugiej Strony od chwili otrzymania stosownego pisemnego zawiadomienia. Zawiadomienie o osobie nowego Kierownika Projektu winno być podpisane przez osoby umocowane do reprezentowania Strony.

§ 7

Kontrola jakości

1. Zamawiający ma prawo do bieżącej weryfikacji jakości świadczonych przez Wykonawcę prac przez własnych specjalistów lub z wykorzystaniem konsultantów zewnętrznych.
2. Weryfikacja, o której mowa w ust. 1 będzie prowadzona w sposób, który nie będzie negatywnie wpływał na wykonywanie przez Wykonawcę jego obowiązków wynikających z Umowy.
3. W trakcie kontroli postępu prac, Wykonawca zobowiązany jest do udzielania Zamawiającemu wszelkich niezbędnych informacji oraz wyjaśnień w zakresie realizacji Przedmiotu Umowy.
4. W przypadku stwierdzenia usterek lub/i wystąpienia Awarii, Wykonawca zobowiązany jest do ich usunięcia w terminie nie dłuższym niż [•]. Zamawiający jest uprawniony do zgłoszenia usterek/Awarii na następujący adres e-mail [•].

§ 8

Odbiory

1. Wykonanie postanowień Umowy zostanie potwierdzone przez Strony podpisaniem następujących dokumentów:
   1) Protokół Odbioru Końcowego Systemu, którego wzór stanowi **Załącznik nr 3** do Umowy,
   2) Protokół Wykonania Usługi SOC i Usługi Wsparcia Technicznego, którego wzór stanowi **Załącznik nr 4** do Umowy, podpisywany przez Strony co miesiąc i będący potwierdzeniem prawidłowego wykonywania ww. usług a także przekazania i wdrożenia Scenariuszy.
2. Przed przystąpieniem do odbioru, Wykonawca jest zobowiązany do umożliwienia Zamawiającemu wraz z Wykonawcą przeprowadzenia testów akceptacyjnych, dotyczących wdrażanego Systemu. Wykonawca zobowiązany jest do powiadomienia Zamawiającego w formie pisemnej o gotowości przystąpienia do testów, na co najmniej 3 (trzy) dni robocze przed zamierzonym rozpoczęciem testów.
3. W ramach testów akceptacyjnych, o których mowa w ust. 2 Wykonawca przygotuje Scenariusze testowe do potwierdzenia prawidłowości wdrożenia oprogramowania. Przygotowane przez Wykonawcę Scenariusze testowe będą wymagały akceptacji Zamawiającego. W przypadku uwag do Scenariuszy Testowych zgłaszanych przez Zamawiającego Wykonawca dokona stosownych zmian. Wszelkie zmiany w Scenariuszach dokonywane na podstawie niniejszego ustępu nie wpływają na terminy wykonania Prac określone w Umowie.
4. Ostateczne potwierdzenie działania Systemu nastąpi po uruchomieniu w środowisku produkcyjnym tj. docelowym miejscu pracy, co zostanie potwierdzone Protokołem Odbioru końcowego Systemu stanowiącego **Załącznik nr 3** do Umowy.
5. W przypadku zastrzeżeń Zamawiającego do Przedmiotu Umowy, bierze się pod uwagę daty przedstawienia go ponownie do odbioru po usunięciu przyczyn zastrzeżeń. W takim przypadku Zamawiający będzie uprawniony do odmowy odbioru końcowego do czasu usunięcia wszystkich zgłoszonych uchybień oraz zastrzeżeń.
6. Przyjęcie przez Zamawiającego wyników prac Wykonawcy nie zwalnia Wykonawcy z odpowiedzialności za wady tych wyników prac ani z odpowiedzialności za szkody wynikłe z ich wadliwości stwierdzonej później, w zakresie przewidzianym postanowieniami Umowy.

§ 9
Prawa Autorskie

1. Wykonawca przenosi, w ramach wynagrodzenia wskazanego w § 4 ust. 1, na Zamawiającego całość majątkowych praw autorskich do utworów powstałych w związku z wykonywaniem niniejszej Umowy i niebędących oprogramowaniem wraz z podpisaniem właściwego protokołu odbioru. Przeniesienie praw autorskich, o których mowa w niniejszym ustępie nastąpi bez ograniczeń terytorialnych i czasowych w odniesieniu do Utworów niebędących programami komputerowymi – w szczególności na następujących polach eksploatacji:
   a) W zakresie utrwalania i zwielokrotniania – w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie (w tym wprowadzanie do pamięci komputera, zwielokrotnianie techniką drukarską, reprograficzną lub cyfrową, w tym m.in. poprzez CD-ROM-y, DVD, taśmy magnetyczne, nośniki magnetooptyczne, poprzez inne urządzenia elektroniczne, w tym tzw. papier elektroniczny), również w zakresie, w którym zwielokrotnianie jest niezbędne dla wprowadzania, wyświetlania, stosowania, zwielokrotniania, przekazywania i przechowywania,
   b) w zakresie obrotu oryginałem każdego z Utworów albo egzemplarzami, na których utrwalono którykolwiek z Utworów – wprowadzania do obrotu, zbywania, najmu, użyczania, dzierżawy lub udostępniania w dowolny inny sposób oryginału lub kopii,
   c) w zakresie rozpowszechniania każdego z Utworów w sposób inny niż określony w lit. b) powyżej – publicznego wykonania, wystawienia, wyświetlenia, odtworzenia oraz nadawania i remitowania w dowolny sposób i za pomocą dowolnej techniki, a także publicznego udostępniania któregokolwiek Utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym, niezależnie od rodzaju i wielkości widowni, w tym m.in. poprzez:
      i. udostępnianie go w sieci Internet,
      ii. nadanie za pomocą wizji i fonii przewodowej i bezprzewodowej przez stację naziemną, za pośrednictwem satelity (sygnał kodowany i niekodowany), analogowo i cyfrowo, TV, telewizję na telefonii komórkowej, telewizję w Internecie, w sieciach wszelkiego rodzaju telefonii i videofonii, w tym stacjonarnej i komórkowej, w sieci telewizyjnej w sklepach, wraz z prawem do retransmisji w ramach platform cyfrowych lub w sieciach kablowych,
      iii. wprowadzanie do pamięci komputera, do sieci komputerowej, internetowej i/lub multimedialnej, do baz danych, udostępnienie i rozpowszechnienie za pośrednictwem sieci komputerowych,
      w tym Internetu, intranetu i extranetu,
      iv. wprowadzania dowolnych zmian do dowolnych Utworów, oraz wykonywania ich opracowań;
      v. wykonywanie i zezwalanie na wykonywanie przez osoby trzecie opracowań, w tym przeróbek i adaptacji Utworów,
      vi. wykorzystanie, zwielokrotnianie, wprowadzania do obrotu i rozpowszechnianie Utworów na polach eksploatacji, które zastąpią powyższe pola eksploatacji wraz z postępem technicznym.

2. W ramach wynagrodzenia wskazanego w § 4 ust. 1 Umowy, Wykonawca w odniesieniu do wszystkich Utworów będących Oprogramowaniem, co do których nieprzeniesiono na Zamawiającego praw autorskich udziela Zamawiającemu na czas nieokreślony (licencja wieczysta) licencji w zakresie utrwalania, zwielokrotniania i modyfikowania obejmującej: trwałe lub czasowe zwielokrotnianie programów komputerowych w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie; w zakresie, w którym dla wprowadzenia, wyświetlenia, stosowania, przekazywania i przechowywania programu komputerowego niezbędne jest jego zwielokrotnienie, czynności te nie wymagają zgody uprawnionego.

§ 10

SLA

1. Zasady utrzymania przez Wykonawcę odpowiedniego poziomu usług w zakresie poszczególnych Linii Serwisowych są określone w **Załączniku nr 2** do niniejszej Umowy – Warunkach Usługi SOC i Wsparcia technicznego.
2. W celu realizacji zgłoszenia, Zamawiający jest zobowiązany do przesłania stosownego „Formularza zgłoszenia Problemu".

§ 11

Gwarancja

1. Wykonawca udziela gwarancji na okres …… lat oraz oświadcza, że dostarczane usługi i produkty będące Przedmiotem Umowy będą objęte gwarancją producenta oraz wsparciem technicznym producenta (które może być realizowane także przez podmioty autoryzowane przez producenta).
2. Okres gwarancji o którym mowa w ust. 1 powyżej liczony jest od podpisania bez zastrzeżeń Protokołu Odbioru Końcowego wdrożenia usługi SOC.

§ 12

Cesje i podwykonawcy

1. Wykonawca nie może dokonać cesji praw i obowiązków wynikających z niniejszej Umowy, bez uprzedniej pisemnej zgody Zamawiającego pod rygorem nieważności.
2. Wykonawca może powierzyć wykonanie zobowiązań wynikających z niniejszej Umowy osobom trzecim, po uprzednim poinformowaniu o tym Zamawiającego i pod warunkiem, że Zamawiający nie zgłosi w tym zakresie sprzeciwu w terminie 30 dni od daty doręczenia mu zawiadomienia. Powyższe nie dotyczy możliwości wykorzystywania serwerów innych niż te wskazane w **Załączniku nr 10** do Umowy, pod rygorem prawa odstąpienia lub wypowiedzenia Umowy przez Zamawiającego, z przyczyn leżących po stronie Wykonawcy, z zachowaniem przez Zamawiającego prawa do naliczenia kary umownej zgodnie z § 16 ust. 2 Umowy. W każdym przypadku zobowiązania mogą być powierzone wyłącznie podmiotowi spełniającemu wszelkie kryteria wynikające z Umowy dla Wykonawcy. Powyższy zapis dotyczy również dalszych podwykonawców.

§ 13

Wypowiedzenie i Odstąpienie od Umowy

1. Zamawiającemu przysługuje prawo do wypowiedzenia Umowy ze skutkiem natychmiastowym, w przypadku istotnego naruszenia przez Wykonawcę zobowiązań wynikających z Umowy, a w szczególności niewykonywania lub nienależytego wykonywania prac składających się na Przedmiot Umowy i nieusunięcia danego naruszenia w ciągu 5 dni kalendarzowych od otrzymania przez Wykonawcę pisemnego zawiadomienia określającego naruszenie.
2. Wykonawcy przysługuje prawo do wypowiedzenia Umowy w przypadku gdy Zamawiający pozostaje w zwłoce z zapłatą wymagalnego świadczenia co najmniej 30 dni.
3. Odstąpienie lub wypowiedzenie Umowy pozostaje bez wpływu na obowiązek zachowania poufności wskazany w Umowie oraz prawo Zamawiającego do żądania od Wykonawcy zapłaty kar umownych.
4. Oświadczenie o wypowiedzeniu Umowy ze skutkiem natychmiastowym bądź o odstąpieniu od umowy, powinno nastąpić na piśmie pod rygorem nieważności.
5. Po złożeniu oświadczenia o odstąpieniu od Umowy przez Zamawiającego, Wykonawca zobowiązuje się do podjęcia niezwłocznie działań prowadzących do szybkiego i uporządkowanego zakończenia zadań, jednak nie dłużej niż w ciągu 30 dni od odstąpienia od Umowy, zaś w odniesieniu do szeregu obowiązków wskazanych w **Załączniku nr 7** do momentu potwierdzenia wykonania Obowiązku; w razie niepodjęcia przedmiotowych czynności Zamawiający będzie traktował zachowanie Wykonawcy jako działanie ze szkodą dla Zamawiającego.

6. Strony ustalają, że odstąpienie od Umowy będzie wywoływało wyłącznie skutki na przyszłość zaś ewentualne odstąpienie od Umowy nie będzie obejmowało części Umowy już wykonanej. W tym zakresie Strony ustalają, że ich świadczenia miały charakter ekwiwalentny i nie zgłaszają względem siebie żadnych roszczeń z tego tytułu, z zastrzeżeniem postanowień odmiennych niniejszej Umowy.

§ 14

Zabezpieczenie należytego wykonania umowy

1. W celu zabezpieczenia roszczeń Zamawiającego z tytułu niewykonania lub nienależytego wykonania umowy Wykonawca zobowiązuje się do złożenia Zamawiającemu, nie później niż w dniu zawarcia Umowy, bezwarunkową, nieodwołalną i płatną na pierwsze pisemne żądanie Zamawiającego Gwarancję Bankową lub Gwarancję Ubezpieczeniową lub nieoprocentowaną kaucję pieniężną („**kaucja**") w wysokości 5 % ryczałtowego wynagrodzenia netto (całości zadania), wskazanego w § 4 ust.1 lit. a) Umowy. Treść, jak i wystawca Gwarancji bankowej/ubezpieczeniowej podlega akceptacji Zamawiającego.
2. W przypadku zabezpieczenia w formie kaucji, będzie ona nieoprocentowana i zostanie zwrócona Wykonawcy w wartości nominalnej bez odsetek- w przypadku skorzystania z zabezpieczenia, kwota zostanie pomniejszona o sumę odpowiadającą wysokości roszczeń Zamawiającego. Kaucja zostanie wpłacona na konto bankowe Zamawiającego nr …… z podaniem tytułu: „Zabezpieczenie Należytego Wykonania Umowy nr xxxx". Ponadto nie później niż w dniu podpisania Umowy Wykonawca przekaże Zamawiającemu dowód wpłaty kaucji.
3. W przypadku, gdy Wykonawca nie złoży lub nie uzupełni Zabezpieczenia Należytego Wykonania Umowy lub nie przekaże dowodu wpłaty lub uzupełnienia kaucji w terminie określonym odpowiednio w ust. 1, 2 powyżej lub ust. 4 poniżej, Zamawiający będzie miał prawo do wypowiedzenia Umowy w trybie natychmiastowym, z zachowaniem prawa do kary umownej, o której mowa w § 16 ust. 2 Umowy.
4. Zamawiający ma prawo do potrącenia z zabezpieczenia należytego wykonania Umowy wszelkich kwot należnych od Wykonawcy w tym kar umownych, odsetek i odszkodowań, jakie powstaną w wyniku realizacji Umowy, na co Wykonawca wyraża bezwarunkową zgodę. W przypadku potrącenia przez Zamawiającego wypłaty z Zabezpieczenia Należytego Wykonania Umowy, Wykonawca zobowiązuje się uzupełnić jego kwotę do wysokości określonej w ust. 1 powyżej, w terminie 14 dni kalendarzowych od daty dokonania przez Zamawiającego wypłaty, o której mowa w powyższym zdaniu. Ponadto w przypadku Zabezpieczenia Należytego Wykonania Umowy w formie kaucji, Wykonawca przekaże Zamawiającemu, w terminie 14 dni od wypłaty z zabezpieczenia w formie kaucji, dowód uzupełnienia kaucji. Dowód uzupełnienia kaucji powinien zawierać adnotację, że wpłata stanowi uzupełnienie istniejącego Zabezpieczenia Należytego Wykonania Umowy.
5. Jeżeli zmianie ulegnie określony w § 3 Umowy termin obowiązywania Umowy, a Zabezpieczenie Należytego Wykonania Umowy wniesione będzie w innej formie niż kaucja, to Wykonawca będzie samodzielnie i na własny koszt, bez odrębnego wezwania do przedłużenia ważności zabezpieczenia aż do czasu jego zwrotu zgodnie z ust. 7 poniżej. W przypadku Zabezpieczenia Należytego Wykonania Umowy wniesionego w innej formie niż pieniężna, jego przedłużenie będzie następowało najpóźniej w terminie 14 dni kalendarzowych przed upływem ważności poprzedniego Zabezpieczenia Należytego Wykonania Umowy, tak, aby była zachowana ciągłość zabezpieczenia.
6. Wszelkie koszty dotyczące Zabezpieczenia Należytego Wykonania Umowy ponosi Wykonawca.
7. Zwolnienie Zabezpieczenia Należytego Wykonania Umowy nastąpi na pisemny wniosek Wykonawcy w terminie 30 dni od daty podpisania przez Strony Protokołu końcowego Wykonania Usługi SOC i Usługi Wsparcia Technicznego za ostatni okres świadczenia usługi i nie wcześniej, niż po zaspokojeniu się przez Zamawiającego z Zabezpieczenia Należytego Wykonania Umowy ewentualnych zobowiązań Wykonawcy względem Zamawiającego.
8. Wszelkie koszty dotyczące wniesienia, utrzymania, zwrotu zabezpieczenia należytego wykonania Umowy ponosi Wykonawca.

9. Każda zmiana zabezpieczenia należytego wykonania Umowy będzie podlegała wcześniejszej akceptacji Zamawiającego co do treści takiego zabezpieczenia oraz jego wystawcy.

§ 15

Ubezpieczenie

1. Wykonawca przedstawi Zamawiającemu w dniu podpisania Umowy potwierdzoną za zgodność z oryginałem kopię polisy ubezpieczeniowej od odpowiedzialności cywilnej kontraktowej i deliktowej, z sumą ubezpieczeniową nie niższą niż 1.200.000,00 PLN obejmującą:
   1) szkody w mieniu stanowiącym przedmiot wykonywanych prac, udostępnionym, przekazanym itp. przez Zamawiającego w celu wykonania usługi z limitem nie mniejszym niż ……PLN,
   2) szkody powstałe po wykonaniu usługi wynikłej z jej wadliwego wykonania,
   3) szkody wyrządzone przez podwykonawców. W przypadku korzystania z ich usług przy realizacji Umowy z limitem nie mniejszym niż suma ubezpieczeniowa,
   4) czyste straty finansowe z limitem nie mniejszym niż ……PLN,

   wraz z potwierdzeniem opłaty składki ubezpieczeniowej. Wykonawca oświadcza, że będzie posiadać ubezpieczenie, o którym mowa w powyższym zdaniu, do końca okresu obowiązywania umowy, a także w okresie obowiązywania gwarancji.
2. Wykonawca zobowiązany jest przedstawić Zamawiającemu, na co najmniej 7 dni przed upływem okresu ubezpieczenia następną polisę/polisy ubezpieczeniową spełniającą wymagania określone w ust. 1 powyżej, zapewniającą ciągłości ochrony, jeżeli przedstawiona polisa/polisy nie obejmuje całego okresu obowiązywania Umowy.
3. Do polisy ubezpieczeniowej, o której mowa w ust. 1 powyżej, Wykonawca dołączy warunki ubezpieczenia oraz kopie dowodów opłaty składki ubezpieczeniowej.
4. Ewentualne szkody niepokryte z polis ubezpieczeniowych Wykonawcy, lub których polisa ubezpieczeniowa nie uwzględnia, zostaną pokryte we własnym zakresie bezpośrednio przez Wykonawcę, na co Wykonawca wyrażą bezwarunkowa zgodę.

§ 16

Kary umowne i odpowiedzialność

1. W przypadku niewykonania lub nienależytego wykonania Umowy przez Wykonawcę, Zamawiający będzie uprawniony do obciążenia Wykonawcy następującymi karami umownymi:
   1) w przypadku zwłoki w realizacji Przedmiotu Umowy, w stosunku do końcowego terminu realizacji Przedmiotu Umowy określonego w § 3 ust. 1 Umowy w wysokości **0,10** % ryczałtowego wynagrodzenia netto, o którym mowa w § 4 ust. 1 lit. a) Umowy za każdy dzień zwłoki,
   2) w przypadku zwłoki w zakresie dostarczenia Scenariuszy testowych, zgodnie z harmonogramem określonym w OPZ w wysokości **0,05** % ryczałtowego wynagrodzenia netto, o którym mowa w § 4 ust. 1 lit. a) Umowy za każdy dzień zwłoki,
   3) za niedotrzymanie przez Wykonawcę Czasu reakcji na Incydent w ramach I Linii Serwisowej, opisanym w **Załączniku nr 2** do Umowy, w wysokości **200,00** PLN (słownie: dwieście złotych) za każde rozpoczęte 15 minut zwłoki,
   4) za niedotrzymanie przez Wykonawcę Czasu przygotowania zgłoszenia do właściwego CSIRT GOV od wykrycia Incydentu zakwalifikowanego jako poważny w ramach II Linii Serwisowej określonej w **Załączniku nr 2** do Umowy, w wysokości **2.000,00** PLN (słownie: dwa tysiące złotych) za każdą rozpoczętą 1 godzinę zwłoki,
   5) za niedotrzymanie przez Wykonawcę Czasu przygotowania zaleceń modyfikacji konfiguracji oraz innych działań wpływających na podwyższenie bezpieczeństwa do wdrożenia przez administratorów Zamawiającego w ramach II Linii Serwisowej określonej w **Załączniku nr 2**

do Umowy, w wysokości **500,00** PLN (słownie: pięćset złotych) za każde rozpoczęte 24 godziny zwłoki,

6) za niedotrzymanie przez Wykonawcę maksymalnego Czasu przyjęcia zadania do realizacji w ramach IIII Linii Serwisowej określonej w **Załączniku nr 2** do Umowy, w wysokości **500,00** PLN (słownie: pięćset złotych) za każdy dzień zwłoki,
7) w przypadku zwłoki we wniesieniu, przedłużeniu lub uzupełnieniu Zabezpieczenia Należytego Wykonania Umowy w formie gwarancji bankowej/ubezpieczeniowej, zgodnie z terminem, o którym mowa w § 14 ust. 1, 4 i 5 Umowy, a w przypadku kaucji nieprzedstawienia dowodu wpłaty lub uzupełnienia kaucji, zgodnie z terminem, o którym mowa w §14 ust. 2 i 4 Umowy - w wysokości **200,00** PLN (słownie: dwieście złotych) za każdy dzień zwłoki,
8) w przypadku zwłoki w usunięciu usterki/Awarii względem terminu wskazanego w §7 ust. 4 Umowy w wysokości 0,25 % ryczałtowego wynagrodzenia netto, o którym mowa w § 4 ust. 1 lit. a) Umowy za każdy dzień zwłoki,
9) za każdorazowe naruszenie zakazu zatrudniania pracowników Zamawiającego przy realizacji Przedmiotu Umowy, o którym mowa w § 5 ust. 1 pkt 8) Umowy, Zamawiający ma prawo naliczyć Wykonawcy kary umowne w wysokości **5.000,00** PLN (słownie: pięć tysięcy złotych),
10) Za każdorazowe naruszenie przez Wykonawcę obowiązków określonych w Exit Plan, Zamawiający ma prawo naliczyć kary umowne w wysokości **1.000,00** PLN (słownie: tysiąc złotych) za każdy przypadek naruszenia,
11) Zamawiający ma prawo naliczyć kary umowne za niedochowanie – zgodnie z **Załącznikiem 2** – poziomu Dostępności:
   - w przypadku Dostępności poniżej 98 % zgodnie z SLA - **2%** wartości abonamentu miesięcznego za każdy rozpoczęty punkt procentowy obniżenia Dostępności,
   - w przypadku naruszenia przez daną Stronę zobowiązania do zachowania poufności, o którym mowa w § 18 Umowy w wysokości **10.000,00** PLN (słownie: dziesięć tysięcy złotych) za każde z naruszeń.

2. Jeżeli Zamawiający odstąpi od Umowy lub ją wypowie z przyczyn leżących po stronie Wykonawcy, wówczas Zamawiający będzie uprawniony do naliczenia Wykonawcy kary umownej w wysokości **10** % łącznej wartości umowy netto, o której mowa w § 4 ust. 1 lit. a) Umowy.
3. Jeżeli Wykonawca odstąpi od Umowy lub ją wypowie z przyczyn leżących po stronie Wykonawcy, wówczas Zamawiający będzie uprawniony do naliczenia Wykonawcy kary umownej w wysokości **10** % łącznej wartości umowy netto, o której mowa w § 4 ust. 1 lit. a) Umowy.
4. Jeżeli Zamawiający odstąpi od Umowy lub ją wypowie z przyczyn leżących po stronie Zamawiającego, wówczas Wykonawca będzie uprawniony do naliczenia Zamawiającemu kary umownej w wysokości **10** % łącznej wartości umowy netto, o której mowa w § 4 ust. 1 lit. a) Umowy.
5. W przypadku obciążenia Wykonawcy karami umownymi, o których mowa w niniejszym paragrafie, Zamawiający wystawi Wykonawcy stosowne noty, płatne w terminie 14 dni kalendarzowych od daty jej wystawienia. Kary umowne mogą być bezpośrednio wypłacone z Zabezpieczenia Należytego Wykonania Umowy lub potrącone z wynagrodzenia Wykonawcy, na co Wykonawca wyraża bezwarunkową zgodę.
6. Zapłata kary umownej za opóźnienie nie zwalnia Wykonawcy z obowiązku dokończenia prac będących Przedmiotem Umowy.
7. Zamawiający zastrzega sobie prawo dochodzenia odszkodowania od Wykonawcy na zasadach ogólnych Kodeksu Cywilnego niezależnie od naliczonych kar umownych.
8. Maksymalna łączna kwota kar umownych nie może przekroczyć 30% ryczałtowego wynagrodzenia netto, określonego w § 4 ust. 1 lit. a) Umowy. Kara umowna z tytułu odstąpienia od Umowy może być naliczana łącznie z karami umownymi z tytułu zwłoki.

§ 17
Siła wyższa

1. Strony niniejszej umowy nie będą ponosiły odpowiedzialności, jeżeli wykonanie któregokolwiek z jego zobowiązań wynikających z niniejszej umowy zostanie opóźnione lub nie dojdzie do skutku z powodu zaistnienia siły wyższej.
2. Przez siłę wyższą strony rozumieją – zdarzenie, którego wystąpienie jest niezależne od stron i niemożliwe do przewidzenia przez strony i dotyczy: wojny na terenie RP, klęski żywiołowej, ataku terrorystycznego. Celem doprecyzowania Strony wskazują, iż agresja zbrojna Rosji na Ukrainę lub też skutki rzeczonych okoliczności nie stanowią siły wyższej w rozumieniu niniejszego paragrafu.
3. Każda ze stron jest zobowiązana do niezwłocznego zawiadomienia drugiej ze stron o zajściu przypadku siły wyższej, o ile druga strona nie wskaże inaczej na piśmie. Strona, która dokonała zawiadomienia będzie kontynuowała wykonanie swoich obowiązków wynikających z umowy w takim zakresie w jakim to jest możliwe, jak również musi podjąć wszelkie alternatywne działania zmierzające do wykonania umowy, których podjęcia nie wstrzymuje zdarzenie siły wyższej.
4. W przypadku ustania siły wyższej strony niezwłocznie przystąpią do realizacji swoich obowiązków, chyba że wykonanie zamówienia nie będzie leżało w interesie Zamawiającego.
5. Wykonawca oświadcza, że jest świadom ograniczeń i skutków jakie na dzień podpisania umowy spowodowała agresja zbrojna Rosji na Ukrainę i uwzględnił te ograniczenia i skutki podpisując niniejszą umowę.

§18
Informacje poufne i ochrona danych osobowych

1. Strony zobowiązują się do nieujawniania osobom trzecim informacji stanowiących tajemnicę przedsiębiorstwa, uzyskanych w związku z realizacją zadań objętych Umową, chyba że uzyskają pisemną zgodę drugiej Strony w każdym konkretnym przypadku. Strony ustalają, że osobami trzecimi w rozumieniu niniejszego paragrafu nie są spółki wobec których Strona umowy jest spółką dominującą w rozumieniu przepisów kodeksu spółek handlowych.
2. Przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zborze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności — art. 11 ust. 2 Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jednolity Dz. U. z 2022 r. poz.1233 t.j.).
3. W celu uniknięcia wątpliwości strony przyjmują, iż wszelkie dane, dokumenty lub materiały, niezależnie od ich postaci, udostępnione Wykonawcy przez Zamawiającego będą traktowane jako informacje stanowiące tajemnicę przedsiębiorstwa Zamawiającego, o ile Zamawiający nie zastrzeże, że nie zawierają takich informacji.
4. Strony zobowiązują się do ochrony i zachowania w tajemnicy wszelkich, uzyskanych w trakcie współpracy informacji stanowiących tajemnicy przedsiębiorstwa Strony przekazującej informację, niezależnie od formy przekazania tych informacji, w trakcie trwania Umowy oraz przez okres 25 lat od daty udostępnienia danej informacji.
5. Strony zobowiązują się podjąć wszelkie niezbędne kroki dla zapewnienia, że żadna z osób otrzymujących informacje, o których mowa w ust. 1 i ust. 2 powyżej, nie ujawni tych informacji ani ich źródła, zarówno w całości, jak i w części, osobom trzecim bez uzyskania uprzednio wyraźnego upoważnienia na piśmie od Strony ujawniającej.
6. Wykonawca zobowiązuje się ujawnić informacje jedynie tym pracownikom, którzy muszą mieć do nich dostęp dla celów realizacji zadań wynikających z Przedmiotu Umowy.

7. Wykonawca zobowiązuje się nie kopiować, nie powielać ani w jakikolwiek sposób nie rozpowszechniać jakiejkolwiek części określonych informacji z wyjątkiem uzasadnionej potrzeby i tylko do celów związanych z zakresem współpracy, po uprzednim uzyskaniu pisemnej zgody od zamawiającego.
8. Zakaz o którym mowa w ust. 1 oraz ust. 2 powyżej nie dotyczy informacji:
   1) które znajdowały się w nieograniczonym posiadaniu Stron przed otrzymaniem ich od drugiej Strony;
   2) które są powszechnie znane lub zostaną podane przez Zamawiającego do publicznej wiadomości;
   3) które Strona mogła otrzymać od osoby trzeciej bez powiadomienia o stosownych ograniczeniach, co do ich używania lub ujawnienia;
   4) co do których dana Strona jest w stanie udowodnić, ze to informacje zostały przez nią opracowane niezależnie od ich otrzymania.
9. Zobowiązanie do poufności, o którym mowa powyżej, trwa 25 lat od daty przekazania informacji. Strony odpowiadają za zachowanie poufności przez swoich pracowników, pełnomocników oraz osoby działające w ich imieniu.
10. Strona otrzymująca Informacje Poufne na pisemne wezwanie wystosowane przez Stronę ujawniającą Informację Poufną, zobowiązuje się do niezwłocznego zwrotu wszystkich informacji utrwalonych w formie pisanej oraz ich kopii, także utrwalonych na nośnikach elektronicznych, przy czym - w odniesieniu do informacji elektronicznie utrwalonych — wystarczy, jeżeli Strona otrzymująca Informację Poufną oświadczy, że zostały one trwale usunięte.
11. Wszystkie osoby uczestniczące w realizacji Umowy z ramienia Wykonawcy są zobowiązane do podpisania „Zobowiązania do zachowania w tajemnicy informacji stanowiących tajemnicy przedsiębiorstwa ZAMAWIAJĄCY oraz przestrzegania zasad postępowania z nimi". Wzór zobowiązania stanowi **Załącznik nr 5** do Umowy
12. Ujawnienie informacji stanowiących tajemnicę przedsiębiorstwa Stronu ujawniającej Informację Poufną wymagane zgodnie z obowiązującym prawem, orzeczeniem sądowym lub decyzją administracyjną uprawnionego organu administracji państwowej nie podlega powyższym ograniczeniom. Ujawnienie informacji stanowiących tajemnicę handlową lub tajemnicę przedsiębiorstwa, wymagane zgodnie z obowiązującym prawem, orzeczeniem sądowym lub decyzją administracyjną uprawnionego organu administracji państwowej nie podlega powyższym ograniczeniom.
13. Strony zobowiązują się do przestrzegania przepisów o ochronie danych osobowych w tym Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz aktów służących jego wykonaniu m.in. ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U.2019.1781 t.j).
14. W związku z koniecznymi uzyskania przez Wykonawcę dostępu do danych osobowych, których administratorem jest Zamawiający, Strony zawrą odrębną umowę o powierzenie przetwarzania danych osobowych, zgodnie z wzorem opisanym w **Załączniku nr 8** do Umowy, jednocześnie z podpisaniem niniejszej Umowy.
15. Wykonawca zobowiązuje się do wykonania prac wyłącznie z wykorzystaniem personelu i sprzętu, który uzyska akceptację Zamawiającego.
16. Wykonawca zobowiązuje się, że jego wszystkie serwery, które będą przetwarzać dane przekazywane przez Zamawiającego będą znajdować się na terytorium Unii Europejskiej. Szczegółowy wykaz usytuowania serwerów Wykonawcy stanowi **Załącznik nr 10** do Umowy.
17. Wykonawca najpóźniej w dniu podpisania umowy zobowiązany jest przekazać Zamawiającemu pisemny wykaz serwerów o których mowa w ust. 16 powyżej.

§ 19
Postanowienia końcowe

1. W zakresie wszelkich sporów wynikłych z niewykonania lub nienależytego wykonywania postanowień Umowy spory rozstrzygane są przez Sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
2. W sprawach nieuregulowanych niniejszą umowę stosuje się polskie przepisy, a w szczególności ustawę z dnia z dnia 23 kwietnia 1964 r. kodeks cywilny (Dz.U.2022.1360 t.j. z późn. zm.), ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U.2022.2509 t.j.), ustawę z dnia 30 czerwca 2000 r. prawo własności przemysłowej (Dz.U.2023.1170 t.j. z późn. zm.).
3. Z zastrzeżeniem odmiennych postanowień Umowy, wszelkie zmiany warunków niniejszej Umowy wymagają pisemnej zgody obu Stron w formie aneksu do Umowy pod rygorem nieważności.
4. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach w tym jeden dla Wykonawcy i jeden dla Zamawiającego.
5. Załączniki stanowią integralną część niniejszej Umowy.

Załączniki do Umowy:

Załącznik nr 1 — Opis przedmiotu zamówienia;
Załącznik nr 2 — Warunki świadczenia usługi SOC i wsparcia technicznego systemu;
Załącznik nr 3 — Protokół odbioru końcowego wdrożenia usługi SOC;
Załącznik nr 4 — Miesięczny Protokół Wykonania Usługi SOC i Wsparcia Systemu;
Załącznik nr 5 — Lista osób zobowiązanych do zachowania w tajemnicy informacji stanowiących tajemnicę przedsiębiorstwa Zamawiającego oraz do przestrzegania zasad postępowania z nimi;
Załącznik nr 6 — Oferta ostateczna Wykonawcy;
Załącznik nr 7 — Exit Plan;
Załącznik nr 8 — Umowa powierzenia przetwarzania danych osobowych;
Załącznik nr 9 — wykaz Oprogramowania On Premise oraz Oprogramowania SaaS;
Załącznik nr 10 — wykaz miejsc w których znajdują się serwery przetwarzających dane przekazywane na podstawie Umowy;
Załącznik nr 11 — Końcowy protokół wykonania usługi SOC i wsparcia technicznego systemu

WYKONAWCA **ZAMAWIAJĄCY**

---------- ----------

ZAŁĄCZNIK NR 1 DO UMOWY

OPIS PRZEDMIOTU ZAMÓWIENIA

„Uruchomienie i realizacja usługi SOC oraz wdrożenie narzędzi monitorowania sieci i systemów przemysłowych w Górnośląskim Przedsiębiorstwie Wodociągów S.A.”

I. Opis przedmiotu zamówienia

1. Przedmiot zamówienia.
   1.1. Przedmiotem zamówienia jest świadczenie przez Wykonawcę na rzecz Zamawiającego usług monitorowania incydentów bezpieczeństwa przez wyspecjalizowane Security Operations Center (SOC) tj. centrum bezpieczeństwa teleinformatycznego, które będzie wspierało Zamawiającego, jako operatora usługi kluczowej w spełnieniu wymogów ustawy o krajowym systemie cyberbezpieczeństwa w okresie obowiązywania umowy. W ramach usługi SOC Wykonawca wdroży wymagane narzędzia monitorowania sieci i systemów przemysłowych oraz zagwarantuje drogę komunikacji dla wdrażanych systemów z wszystkimi obiektami Zamawiającego przez cały okres realizacji umowy, lista obiektów ujęta została *w załączniku nr 1 pkt.1*. Usługa SOC obejmować ma główne obszary działania sieci przemysłowej, czyli:
      1.1.1. systemy telemetrii;
      1.1.2. systemy sterowania;
      1.1.3. systemy monitorowania pracy obiektów.
   1.2. W ramach świadczonych usług Wykonawca zapewni Zamawiającemu ciągłe monitorowanie i wykrywanie zagrożeń oraz analizę funkcjonowania w zakresie bezpieczeństwa systemów i infrastruktury OT. Usługa musi zapewniać szybką reakcję na incydenty, które mogą mieć negatywny wpływ na działalność Zamawiającego.
   1.3. W ramach usługi SOC dostarczy wszystkie niezbędne i wymagane licencje systemu ciągłego monitorowania klasy IDS (*Intrusion Detection System*) przeznaczonego do monitorowania sieci przemysłowych oraz wszelkie konieczne do realizacji zadania komponenty (serwery, sondy, bramy dostępowe, przemysłowe switche oraz jeżeli wymagane, przemysłowe routery dostępowe wykorzystujące komórkowe technologie bezprzewodowe, oparte o sieci operatorskie) wraz z pełnym wdrożeniem. Na potrzeby realizacji usługi i w okresie jej realizacji Wykonawca zapewni usługi telekomunikacyjne transmisji danych wraz wymaganymi urządzeniami sieciowymi. System monitorowania realizować ma ciągły monitoring sieci i systemów automatyki przemysłowej z uwzględnieniem:
      1.3.1. inwentaryzacji systemów;
      1.3.2. monitorowania zmian w architekturze i komunikacji logicznej;
      1.3.3. monitorowania ruchu w protokołach przemysłowych;
      1.3.4. wykrywania wrogich zachowań w rozproszonej sieci przemysłowej;
      1.3.5. obsługi realizowanej przez centralną konsolę zarządzania alarmami;
      1.3.6. możliwości realizacji zadania zarówno w architekturze rozproszonej jak i scentralizowanej.
   1.4. Szkolenia – w ramach zadania Wykonawca przeprowadzi wszelkie wymagane szkolenia z obsługi systemów oraz zdarzeń, a także będzie stanowił wsparcie dla zamawiającego w zakresie konsultacji mających na celu poprawę bezpieczeństwa objętych usługą systemów OT Zamawiającego.

Lista obiektów oraz szczegółowe informacje dotyczące obiektów oraz pozostałych wymagań stanowią *Załącznik nr 1* udostępniony po podpisaniu oświadczenia o zachowaniu poufności.

2. Ramy czasowe
   2.1. Szkolenie dla zespołu zamawiającego: co najmniej 2 tygodnie przed zakończeniem wdrożenia.
   2.2. Objęcie monitorowaniem wszystkich obiektów wyszczególnionych w Załączniku nr 1 pkt 1 : do 6 miesięcy od podpisania umowy.

II. Wymagania szczegółowe dla usługi SOC oraz wymagania funkcjonalne dla komponentów systemów monitorowania i komponentów zabezpieczeń.

1. Wymagania dla usługi SOC
   1.1. Realizacja zadań SOC w zakresie :
      1.1.1. monitoringu i wykrywania zdarzeń cyberbezpieczeństwa (potencjalnych incydentów z zakresu cyberbezpieczeństwa);
      1.1.2. obsługi zdarzeń cyberbezpieczeństwa, zgodnie z (przygotowaną) instrukcją lub instrukcjami obsługi, w tym ich rejestrowanie, kategoryzację i priorytetyzację obsługi, analizowanie i korelowanie, kwalifikowanie i reagowanie;
      1.1.3. raportowania zdarzeń cyberbezpieczeństwa;
      1.1.4. obsługi zewnętrznego kanału komunikacji (email abuse) poza godzinami roboczymi.
   1.2. Raportowanie w ramach usługi SOC, usługa podstawowa powinna być realizowane w następujących cyklach:
      1.2.1. komunikacja bieżąca wynikająca ze scenariuszy obsługi zdarzeń;
      1.2.2. raport dzienny z działania SOC usługa podstawowa (zautomatyzowany), obejmujący: liczbę obsłużonych zdarzeń (rozwiązanych i eskalowanych), krytyczność obsłużonych zdarzeń, informację o czasach podjęcia oraz rozwiązania/eskalowania zdarzeń;
      1.2.3. raport miesięczny z działania SOC usługa podstawowa, w formie dokumentu podsumowującego pracę SOC usługa podstawowa zawierającego takie informacje jak: liczba obsłużonych zdarzeń (rozwiązanych i eskalowanych), krytyczność obsłużonych zdarzeń, czas wystąpienia zdarzenia, czas zamknięcia zdarzenia/eskalacji, status zdarzenia (otwarty, zamknięty, eskalowany), stan SLA (przekroczenia), powód przekroczenia;
      1.2.4. spotkania komunikacyjno-koordynacyjne on-line przy wykorzystaniu aplikacji MS-Teams z wyznaczonym koordynatorem min. 1 raz w tygodniu;
      1.2.5. spotkania on-line przy wykorzystaniu aplikacji MS-Teams z wyznaczonym koordynatorem podsumowujące działalność min, 1 raz na kwartał.
   1.3. Niezbędne zasoby, umiejętności i doświadczenie konieczne do obsługi zdarzeń i incydentów bezpieczeństwa oraz ich dokumentacji:
      1.3.1. posiadanie własnego centrum SOC (Security Operations Center) zlokalizowanego w Polsce z wymaganym certyfikatem ISO 22301 ;
      1.3.2. dysponowanie zespołem zdolnym do realizacji zadań usługi SOC usługa podstawowa w trybie 24/7/365 – zbudowanym w oparciu o pracowników zatrudnionych przez dostawcę usługi przez cały okres realizacji zamówienia, posiadających zdolności techniczne oraz kompetencje (ujęte w pkt V. Referencje i certyfikaty) zapewniające wykonanie zamówienia;
      1.3.3. zapewnienie kanału kontaktowego (minimum telefon i skrzynka e-mail) z zespołem CSIRT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV) wskazanym przez Zamawiającego;
   1.4. Zgodność usługi SOC z wymaganiami Ustawy o krajowym systemie cyberbezpieczeństwa oraz aktów powiązanych.
   1.5. Przygotowywanie propozycji modyfikacji lub optymalizacji istniejących oraz wprowadzania za zgodą Zamawiającego nowych scenariuszy i reguł korelacyjnych w systemie SIEM.
   1.6. Przygotowywanie propozycji modyfikacji lub optymalizacji istniejących oraz wprowadzania za zgodą Zamawiającego nowych procedur operacyjnych obsługi zdarzeń.
2. SOC Usługa monitorowania i obsługi incydentów bezpieczeństwa
      2.1.1. Monitorowanie bezpieczeństwa w systemie SIEM zgodnie z uzgodnionymi między Wykonawcą i Zamawiającym procedurami i instrukcjami:
      2.1.2. Monitorowanie w trybie 24/7/365 wystąpień zdefiniowanych scenariuszy bezpieczeństwa zgodnie z procedurami uzgodnionymi z Zamawiającym. Monitorowanie realizowane jest w oparciu o konsolę systemu SIEM i zaimplementowane tam reguły korelacji zdarzeń;
      2.1.3. Identyfikacja zdarzenia, przeprowadzenie wstępnej analizy i eliminacja zdarzeń typu „false positive", zgodnie z procedurami reagowania uzgodnionymi z Zamawiającym;
      2.1.4. Obsługa zdarzeń wskazanych w procedurach monitorowania i reakcji, wykonanie przewidzianych w procedurach czynności, w tym selekcja i priorytetyzacja incydentów;

2.1.5. Notyfikacja do wyznaczonych osób po stronie Zamawiającego zgodnie z ustalonymi procedurami (utworzenie zapisów w systemie ticketowym dostawcy SOC);
2.1.6. Eskalacje podjęcia obsługi zdarzeń przez wskazane zespoły Zamawiającego;
2.1.7. Weryfikacja i obsługa zgłoszeń użytkowników dotyczących bezpieczeństwa spływających na dedykowaną kolejkę zgłoszeń w systemie ticketowym Zamawiającego. Zakres weryfikacji i obsługi zgłoszeń będzie zgodny z ustalonymi procedurami (w szczególności może on ograniczać się do priorytetyzacji zgłoszeń i przekierowania ich do odpowiednich służb po stronie Zamawiającego lub do wykonania innego zestawu określonych czynności przewidzianych w uzgodnionych procedurach i udostępnionych narzędziach);
2.1.8. Operatorzy SOC Wykonawcy podejmują inne czynności, zgodnie z dostarczonymi przez Zamawiającego procedurami postępowania (w szczególności informują wskazane służby Zamawiającego o wystąpieniu zdarzeń noszących znamiona incydentów bezpieczeństwa, które nie zostały objęte standardowymi procedurami reagowania);
2.1.9. Rejestracja incydentu w systemie ticketowym. Wykonawca ma zaproponować gotowy do użycia system oraz sparametryzować go na potrzeby procesu monitorowani z systemem SIEM;
2.1.10. Cykliczne, raz w miesiącu, raportowanie Zamawiającemu realizacji SLA umowy;
2.1.11. Cykliczne (miesięczne lub kwartalne) spotkania on0line, przeglądowe realizacji usług pomiędzy Zamawiającym i Wykonawcą;
2.1.12. Usługa realizowana będzie zdalnie, z siedziby SOC Wykonawcy;
2.1.13. SLA dla usługi podstawowej L1 – wykonawca zagwarantuje dostępność usługi – tryb 24/7/365 z czasem reakcji na wystąpienie incydentu bezpieczeństwa – 15 minut .
2.1.14. Wykrywanie nieautoryzowanego dostępu i uzyskania wyższych uprawnień w ramach prowadzonych analiz bezpieczeństwa na danych otrzymanych od Zamawiającego;
2.1.15. Identyfikacja pochodzenia zagrożenia i wszystkich podatnych / dotkniętych atakiem komponentów;
2.1.16. Wsparcie lokalnych administratorów w eliminacji pochodzenia incydentu;
2.1.17. Stałe utrzymanie i kalibracja narzędzi monitorowania, wzbogacanie ich o nowe sygnatury oraz usuwanie alertów typu false-positive
2.1.18. Analiza po włamaniowa i zabezpieczenie dowodów zdarzeń, informatyka śledcza oraz propozycja działań naprawczych po wykryciu incydentu bezpieczeństwa realizowana przez zespół CERT dostawcy usługi SOC posiadający wymagane w zapisach OPZ certyfikaty i kompetencje;
2.1.19. Możliwość skanowania podatności infrastruktury Zamawiającego z Internetu raz w tygodniu;
2.1.20. Możliwość skanowania podatności infrastruktury Zamawiającego z zewnątrz i wewnątrz sieci za pomocą dedykowanych narzędzi;
2.1.21. Monitorowanie ważności domen oraz certyfikatów SSL Zamawiającego;
2.1.22. Identyfikacja przypadków wycieku informacji o pracownikach Zamawiającego;
2.1.23. Informowanie o kampaniach phishingowych wykorzystujących markę Zamawiającego;
2.1.24. Monitorowanie reputacji adresów IP i domen Zamawiającego;
2.1.25. Comiesięczne podsumowanie najważniejszych alertów cyberbezpieczeństwa dla Zamawiającego w postaci raportu w formie elektronicznej uzgodnionej z Zamawiającym;
2.1.26. Materiały dotyczące budowania świadomości w zakresie cyberbezpieczeństwa dostarczane do Zamawiającego co najmniej raz w miesiącu w formie newslettera oraz raz w roku w formie raportu CERT.
2.1.27. SLA dla usługi rozszerzonej L2 wykonawca zagwarantuje dostępność usługi – tryb 8/5/251 z czasem reakcji na wystąpienie incydentu bezpieczeństwa – 120 minut.

3. Dostarczenie funkcjonalności systemu SIEM w celu świadczenia usługi monitorowania
   3.1. Wykonawca dostarczy funkcjonalność systemu SIEM w modelu MSSP (Managed Security Service Provider) funkcjonującego we własnym data center (chmura prywatna) na terenie Polski.
   3.2. Zaproponowane rozwiązania pozwolą na agregację logów z infrastruktury Zamawiającego poprzez umiejscowienie sond/serwerów zbierających dane w infrastrukturze Zamawiającego oraz dostarczenie ich do centralnej jednostki systemu SIEM po stronie Wykonawcy. System SIEM

pozwalać będzie na zaawansowaną korelację logów, ich przeszukiwanie, tworzenie różnych operacji dla wykrytych zdarzeń.

3.3. Dostawca usługi udostępnienia funkcjonalności SIEM powinien posiadać certyfikat ISO 27001 tym samym skutecznie chronić powierzone dane Zamawiającego do usługi dzięki efektywnie wdrożonemu i utrzymywanemu systemu zarządzania bezpieczeństwem informacji. Infrastruktura Dostawcy, na której będzie funkcjonował system SIEM, gromadzący dane Zamawiającego powinna być objęta certyfikacją ISO 22301 potwierdzającym posiadane procedury mające na celu zapewnienie bezpieczeństwa krytycznych procesów biznesowych.

3.4. System powinien posiadać mechanizm przetrzymywania danych wraz z zaimplementowaną kompresja mająca możliwość kompresji danych na 10:1 . Funkcjonalność systemu pozwalać będzie na tworzenie różnych reguł korelacji na podstawie dowolnych danych otrzymanych z logów jak również zaimportowanych z innych źródeł zewnętrznych Zamawiającego pochodzących z sieci IT i OT.

3.5. Poszczególne komponenty systemu takie jak sondy, agregatory, serwery konektorów zainstalowane będą w sieci OT Zamawiającego na zwirtualizowanej lub fizycznej infrastrukturze Zamawiającego.

3.6. Agregowane zdarzenia z infrastruktury Zamawiającego będą przechowywane na przestrzeni dyskowej Wykonawcy przez co najmniej 12 miesięcy. Po tym czasie Wykonawca przekaże Zamawiającemu dane o których mowa powyżej, na odpowiednim co do pojemności nośniku, odpowiednio zabezpieczone hasłem w celu archiwizacji.

3.7. Pełna administracja systemu SIEM oraz jego rozwój będą w gestii Wykonawcy z zachowaniem dostępności pełnej funkcjonalności systemu SIEM na poziomie 98% w skali miesiąca. Na potrzeby przeprowadzenia prac administracyjnych wyznaczone może zostać jedno miesięcznie stałe Okno Serwisowe o długości do [4] godzin w dniu i godzinach uzgodnionym z Zamawiającym;

3.8. Pojemność systemu SIEM będzie realizowana przez Wykonawcę w następującym zakresie:

3.8.1. System SIEM zostanie zintegrowany przez Wykonawcę z infrastrukturą Zamawiającego (źródła danych) w ilości ujętej *Załącznik nr 1 pkt. 5*.

3.8.2. Ilość EPS generowanych przez źródła Zamawiającego: do 1000 EPS. System dostawcy musi być elastycznie skalowany w przypadku wystąpienia dużo większej ilości EPS (do 1500 EPS).

3.8.3. Ilość GB danych generowanych przez Źródła Zamawiającego: do 30GB/dobę.

3.8.4. Ilość scenariuszy bezpieczeństwa przygotowanych i uzgodnionych z Zamawiającym – do 30 sztuk.

3.9. W przypadku nagłego zwiększenia ruchu danych w flow sieci lub logach monitorowanych źródeł system SIEM nie może odrzucać zwiększonego ruchu i monitorować go baz zakłóceń .

3.10. W przypadku potrzeby zwiększenia pojemności systemu rozwiązanie ma być gotowe do natychmiastowego zwiększenia parametrów pojemnościowych (bez przestoju pracy systemu).

3.11. W trakcie realizacji Umowy parametry pojemnościowe Systemu SIEM określone powyżej mogą ulegać zmianie na podstawie zrealizowanych Zamówień.

3.12. Źródła danych – infrastruktura sieci OT Zamawiającego podlegająca monitorowaniu pod kątem cyberbezpieczeństwa :

3.12.1. Serwery Windows;

3.12.2. Urządzenia sieciowe

3.12.3. System IDS z obiektów kluczowych oraz istotnych.

4. W trakcie realizacji usługi monitorowania lista rodzajów Źródeł danych i ich liczba mogą ulegać zmianie na podstawie zrealizowanych zamówień.
5. Usługa SOC ma być realizowana (w zakresie np.. monitoringu i reakcji na incydenty bezpieczeństwa) w oparciu o zespół specjalistów, których kompetencje są potwierdzone certyfikatami wymienionymi w rozdziale IV ust. 2.4. pkt 2.4.3. – 2.4.4. Zaproszenia do negocjacji.
6. Zakres świadczonej usługi:
   6.1. Monitorowanie i obsługa incydentów

6.1.1. Monitorowanie zdarzeń w infrastrukturze Zamawiającego — czyli zbieranie, analizowanie oraz korelacje zdarzeń, które zachodzą w sieciach oraz systemach klienta Zamawiającego. Jako źródła zdarzeń oprócz systemów teleinformatycznych Zamawiającego, będą traktowane zgłoszenia użytkowników i administratorów Zamawiającego oraz przyjęte przez zamawiającego zgłoszenia incydentów otrzymane ze źródeł zewnętrznych (np. csirt.gov)

6.1.2. Wykrywanie zdarzeń lub incydentów bezpieczeństwa,

6.1.3. Ocena wpływu zdarzenia lub incydentu bezpieczeństwa OT na systemy Zamawiającego.

6.2. W ramach świadczonej usługi wykonawca weryfikuje, czy zdarzenie nie jest to fałszywym alarmem oraz grupuje wszystkie zdarzenia danego typu. Po analizie podejmuje działania zgodnie z procedurami.

6.3. Usługa świadczona w trybie 24/7/365.

7. Reakcja na incydenty

7.1. Reakcja na wykryte zdarzenie bezpieczeństwa poprzez przekazywanie do służb Zamawiającego zaleceń w zakresie sposobów eliminacji zagrożeń (w zakresie usuwania podatności, rekonfiguracji oraz innych działań, które mogą się przyczynić do eliminacji zagrożeń w ramach przyjętego SLA). Zalecenia muszą być dostosowane do możliwości oraz posiadanej przez Zamawiającego infrastruktury.

7.2. W ramach świadczonej usługi Wykonawca będzie cykliczne raz w miesiącu przekazywał Zamawiającemu biuletyny bezpieczeństwa w formie newslettera w zakresie istotnych zdarzeń, które mają miejsce zarówno w kraju jak i na świecie, a także udostępni „know how" w tym zakresie oraz w zakresie świadczonej usługi.

7.3. W ramach usługi dostępna będzie pula godzin konsultingowych na potrzeby analizy incydentów lub na żądanie w ilości do 24 godzin miesięcznie (np. w zakresie analizy malware'u oraz informatyki śledczej computer forensics). Niewykorzystane w danym miesiącu godziny będą przechodziły do wykorzystania na miesiące następne.

8. Dodatkowe wymagania szczegółowe:

8.1. Rolą SOC będzie ocena poziomu zagrożenia zdiagnozowanych incydentów, raportowanie o ich wystąpieniu i wydawaniu stosownych zaleceń. SOC będzie korelował informacje pochodzące z systemów Zamawiającego. Zakres analiz oraz sposób oceny zostanie dostosowany do potrzeb Zamawiającego podczas okresu wdrożenia usługi SOC.

8.2. Usługa będzie świadczona poprzez bezpieczne połączenie VPN Site2Site w technologii uzgodnionej z Zamawiającym na dostarczonych przez Wykonawcę łączach do wskazanych lokalizacji.

8.3. W ramach usługi Wykonawca musi zapewnić możliwość obsługi w zakresie tworzenia i zmiany reguł korelacyjnych, konfiguracji widoków, filtrów, zgodnie z uzgodnionym z Zamawiającym zakresem. Wykonawca zapewni ponadto Zamawiającemu dostęp do systemu korelacji zdarzeń wykorzystywanego w ramach świadczonej usługi.

8.4. Wykonawca w ramach usługi SOC będzie zgłaszał Zamawiającemu incydenty elektronicznie, za pomocą wiadomości e-mail na wskazany adres (adresy) oraz informował telefonicznie wyznaczoną osobę (osoby) do kontaktu ze strony Zamawiającego. Wykonawca zapewni ponadto Zamawiającemu dostęp do systemu ticketowego Wykonawcy, za pomocą którego będzie następowała obsługa incydentów bezpieczeństwa Zamawiającego w zakresie pełnego podglądu i obiegu incydentów zgodnie z założonym SLA.

8.5. Wykonawca zapewni dyżury oraz odpowiednią rotację zespołu SOC, zgodnie z przepisami prawa, gwarantującą jakość i ciągłość świadczonej usługi.

8.6. Wykonawca będzie zobowiązany do przygotowania okresowych rekomendacji zmian w środowisku informatycznym Zamawiającego, nie rzadziej niż 1 na miesiąc o ile takie rekomendacje wystąpią.

8.7. Wykonawca będzie przygotowywał okresowe, miesięczne raporty dotyczące świadczonej usługi w postaci elektronicznej na wskazany adres e-mail. Raport powinien zawierać informacje dotyczącą

ilości obsłużonych incydentów, czasów obsługi. Raport będzie dostarczany na wskazany e-mail, przez Zamawiającego.

8.8. Wykonawca będzie dokumentował i kontrolował działania oraz wykonanie prac za pomocą systemu obsługi zgłoszeń, w którym jest nadawana priorytetyzacja zadań oraz zamodelowany jest obieg informacji przez wszystkie linie ekspertów SOC.

8.9. W przypadku wystąpienia incydentu i zdiagnozowaniu konieczności wprowadzenia działań naprawczych w środowisku informatycznym Zamawiającego, Wykonawca musi zapewnić wsparcie ekspertów rekomendujących właściwe rozwiązanie, na żądanie Zamawiającego zgodnie z przyjętym SLA.

8.10. SOC będzie współpracował na bieżąco z Zamawiającym przy analizie incydentów w celu poprawienia efektywności oraz obniżenia ilości zgłaszanych fałszywych alarmów.

8.11. Wykonawca musi zapewniać retencję tj. przechowywanie danych zgłoszonych, czyli incydentów przez cały okres świadczenia usługi (dane przechowywane w bazie danych systemu będą dostępne dla funkcji agregacji, korelacji i detekcji). Zapewnienie przechowywania logów i danych historycznych umożliwi korelację zdarzeń z różnych źródeł w różnych okresach, a także zapewni dostęp do zdarzeń historycznych.

8.12. Zamawiający wymaga zapewnienia jak najmniejszej ingerencji w monitorowane systemy. Oznacza to możliwość zbierania logów bez konieczności instalacji dedykowanych agentów na źródłach danych urządzeń produkcyjnych, natomiast wykorzystanie zaimplementowanych już w systemach mechanizmów bez agentowych.

8.13. Wykaz rodzajów systemów, które będą źródłami do świadczenia usługi Załącznik nr 1 do przedmiotu zamówienia.

8.14. Przed zakończeniem świadczenia usługi Wykonawca zapewni trwałe usunięcie pod nadzorem Zamawiającego wszystkich danych Zamawiającego z elementów systemu używanych do świadczenia usługi SOC. Zamawiający będzie miał prawo do zachowania danych dotyczących jego systemów a zgromadzonych w systemie korelacji wykorzystywanym przez Wykonawcę w celu świadczenia usługi.

8.15. Wymagana jest całkowita separacja danych Zamawiającego od danych innych podmiotów, dla których Wykonawca również świadczy usługę SOC.

8.16. Wymagane jest umieszczenie elementów zbierających i korelujących logi w infrastrukturze Zamawiającego. Wykonawca będzie miał dostęp do systemu za pośrednictwem konsoli zarządzania oraz przy wykorzystaniu połączenia VPN. Logi źródłowe służące do świadczenia usługi będą przechowywane w infrastrukturze Zamawiającego.

8.17. Zamawiający wymaga przeszkolenia osób zaangażowanych po stronie zamawiającego zgodnie z zapisami pkt X.

III. System monitorowania

1. System monitorowania - założenia ogólne.

1.1. Licencja oprogramowania systemu monitorowania IDS ma być licencją wieczystą z gwarancją bezpłatnej aktualizacji w okresie obowiązywania umowy, po tym okresie licencja nie wygasa i może pracować bez obowiązku nabycia nowych aktualizacji systemu oraz sygnatur.

1.2. Wymaga się objęcia systemu sterowania rozwiązaniem do ciągłego monitorowania i wykrywania zagrożeń na podstawie pasywnej analizy ruchu sieciowego – IDS.

1.3. Identyfikacja niezgodności w ruchu sieciowym oraz wykrywanie zagrożeń musi być oparte o analizę pakietów oraz głęboką analizę pakietów (ang. Deep packet inspection - DPI) dla przemysłowych protokołów komunikacyjnych *Załącznik nr 1 pkt 2.*

1.4. Rozwiązanie do ciągłego monitorowania musi składać się z elementów pozwalających na zbudowanie elastycznej architektury umożliwiającej monitorowanie obiektów posiadających od kilkunastu do ponad stu urządzeń. Szczegółowe wymagania funkcjonalne dla elementów systemu monitorowania znajdują się w punkcie Wymagania dla systemu monitorowania w trybie ciągłym.

1.5. W skład systemu monitorowania powinny wchodzić:
   1.5.1. Centralna konsola IDS - system do prezentacji i zarządzania zdarzeniami zbieranymi z podrzędnych mu systemów/sensorów/sond systemu IDS – centralna konsola powinna być umieszczona w centrali spółki.
   1.5.2. Systemy IDS – autonomiczny element do analizy ruchu sieciowego i wykrywania incydentów, rozwiązanie pasywne działające na kopii ruchu sieciowego dostarczonego z portów mirror przełączników lub przez sondy IDS rozwiązanie ma być zainstalowane na obiektach kluczowych i istotnych *Załącznik nr 1 pkt. 1*.
   1.5.3. Sondy IDS – urządzenia służące do zbierania i agregowania ruchu z wielu portów mirror, kompresji tego ruchu i przesyłania go bezpiecznym tunelem do serwera IDS. Sonda IDS w razie potrzeby powinna być podłączona do rutera dostępowego zapewniającego bezpieczną transmisję lub być wyposażona w moduł LTE (w takim przypadku musi pełnić również rolę firewalla).
1.6. Zdarzenia identyfikowane przez system ciągłego monitorowania muszą być na bieżąco wysyłane do podmiotu świadczącego usługę SOC (wybranego w ramach niniejszego postępowania).
1.7. System ciągłego monitorowania IDS musi mieć funkcjonalność tworzenia cyfrowego obrazu sieci, który może być wykorzystany przez system automatyzujący analizę ryzyka.
1.8. Po stronie Wykonawcy jest zapewnienie bezprzewodowych usług transmisji danych lub zapewnienie innej bezpiecznej drogi przesyłania logów i/lub kopii ruchu z obiektów monitorowanych do systemów centralnego a następnie do SOC.
   1.8.1. Wykorzystywana sieć WAN ma służyć wyłącznie do zadań systemu monitorowania.
   1.8.2. Koszty utrzymania sieci WAN i transmisji danych w czasie trwania usługi ponosi Wykonawca.
   1.8.3. Należy zapewnić poufność i integralność przesyłanych danych poprzez zastosowanie technik zabezpieczających takich jak: wyłączny prywatny APN oraz VPN IPSec lub SSL VPN.
   1.8.4. Zastosowane karty SIM muszą mieć przypisane stałe adresy IP.
1.9. Systemem ciągłego monitorowania należy objąć obiekty w lokalizacjach w których działa przemysłowy system sterowania (ICS/OT) *Załącznik nr 1 pkt.1*.
1.10. Wykonawca przed złożeniem wniosku o dopuszczenie do udziału w postępowaniu musi przeprowadzić wizje lokalne, a na etapie składania ofert przedstawić Zamawiającemu koncepcje zrealizowania wymagań dla każdego z 3 obiektów będących przedmiotem wizji.
1.11. W przypadku gdy sieć obiektowa nie jest wyposażona w przełączniki LAN z funkcją port mirror (SPAN port) należy dostarczyć odpowiednie urządzenia sieciowe, a w koncepcji przedstawić sposób pozyskania kopii ruchu sieciowego do analizy lub w przypadku obiektów podstawowych wykorzystać np. funkcjonalność Sondy oraz doposażyć obiekt w odpowiednie rozwiązania Router LTE oraz karty SIM do komunikacji z wykorzystaniem sieci operatorskiej lub zapewnić inną drogę bezpiecznej transmisji danych.

IV. Wymagania szczegółowe dla systemu monitorowania w trybie ciągłym

Zamawiający oczekuje przedstawienia oferty wdrożenia systemu klasy IDS (Intrusion Detection System). System musi być pasywnym rozwiązaniem monitorowania bezpieczeństwa sieci i inwentaryzacji. System musi analizować kopię ruchu sieciowego dostarczoną z portów mirror/span przełączników sieciowych. System powinien współpracować z sondami i sensorami zdalnymi, a co za tym idzie umożliwiać monitorowanie sieci rozproszonej geograficznie. System powinien być rozwiązaniem programowym – niezależnym od platformy sprzętowej pochodzącej od konkretnego dostawcy. System musi umożliwiać wdrożenie jako maszyna wirtualna. System musi zapewniać wysoki poziom skalowalności umożliwiając monitorowanie małych obiektów (do 50 zasobów) jak również całych grup obiektów (powyżej 500 zasobów). System monitorowania najmniejszych obiektów powinien móc działać na standardowym komputerze przemysłowym 4 rdzenie CPU, do 16 GB RAM.

1. Wymagania główne
   1.1. System musi zapewniać możliwość monitorowania sieci rozproszonej geograficznie oraz współpracować z opcjonalnymi sondami sprzętowymi.

1.2. System musi umożliwiać bezpośrednie podłączenie do niego źródeł ruchu (kopia ruchu z portów mirror/SPAN).
1.3. System musi umożliwiać analizę zapisu ruchu sieciowego w postaci wgranych do systemu plików PCAP system powinien obsługiwać pliki o rozmiarze do 10 GB.
1.4. System musi dostarczać dane niezbędne do prowadzenia procesów Oceny Ryzyka (Risk Assesment) dla sieci ICS.
1.5. System musi dostarczać API, umożliwiające integrację aplikacji autorskich Zamawiającego z bazą danych rozwiązania.
1.6. System musi działać w trybie pasywnym (bez generowania dodatkowego ruchu w monitorowanej sieci), opcjonalnie system może zawierać lub współpracować z mechanizmem aktywnego odpytywania urządzeń (Active Polling).
1.7. System musi dostarczać funkcje audytu działań jego użytkowników i zapewniać możliwość przesyłania danych o tych akcjach za pomocą protokołu syslog.

2. Funkcje analityczne i wspierające analizę
2.1. System musi umożliwiać analizę danych zebranych w trakcie pracy.
2.2. Każdy zestaw danych prezentowanych przez system musi zapewniać:
2.2.1. Filtrowanie prezentowanych danych na podstawie zawartości wpisu, danych takich jak treść alarmu, adresy IP, MAC oraz metadanych takich jak np. godzina utworzenia.
2.2.2. Wszystkie dane tabelaryczne pozyskane z systemu powinny być eksportowane do formatów JSON, PDF i CSV, jak również możliwe do uzyskania za pomocą API.
2.2.3. Każdy wpis w zestawach danych dot. Zdarzeń (konsola alarmów) musi zapewniać możliwość uzyskania dokładniejszych informacji o przyczynie i urządzeniach biorących udział w komunikacji oraz dostęp do zapisów pakietów w formie plików PCAP.
2.3. System musi zapewnić możliwość utworzenia dowolnego raportu na podstawie zapytań do bazy danych oraz możliwość generowania raportu z całości okresu działania systemu a także powinien zapewniać możliwość przesyłania raportów okresowych za pomocą wiadomości e-mail.
2.4. System musi zapewniać prezentację wektorów ataku w formie graficznej na mapie.
2.5. System musi wspierać analizę ryzyka, przez umożliwienie tworzenia grup procesów biznesowych i określenie zasobów, od których procesy te zależą a także krytyczności procesów.
2.6. System musi wspierać analizę DPI dla protokołów przemysłowych ujętych w *załącznik nr 1 pkt. 2.*
2.7. System musi zapewnić możliwość dodawania komentarzy do alarmów oraz zapewnić możliwość definicji procedur postępowania dla kategorii alarmów (Playbook).
2.8. System musi zapewnić możliwość pobrania wszystkich plików PCAP powiązanych z alarmami wykrytymi przez system oraz zbierać pliki PCAP przez okres co najmniej 21 dni z całości ruchu.

3. Wykrywanie anomalii
3.1. System musi raportować wykryte anomalie w komunikacji sieciowej na warstwach 2, 3, 4, 7 modelu ISO/OSI.
3.2. System musi dostarczać sygnaturowy mechanizm detekcji z regułami dla środowiska przemysłowego, a także dostarczać sygnatury zagrożeń dla protokołów przemysłowych oraz sygnatury zagrożeń dla protokołów IT,
3.3. System musi dostarczać behawioralny mechanizm detekcji,
3.4. System musi przedstawiać rekomendacje dla wykrytych problemów wykrytych w sieci, zasobach i konfiguracji samego systemu monitorowania, w odniesieniu do norm lub dobrych praktyk stosowanych w sieciach OT,
3.5. System musi dostarczać mechanizm wspierający śledzenie postępów prac związanych z rekomendacjami np. oznaczenie zadań jako rozwiązane, otwarte/w trakcie analizy, ignorowane, odroczone.
3.6. System musi raportować zdarzenia inwentaryzacyjne takie jak wykrycie nowych zasobów w sieci, wykrycie nowych połączeń w sieci, wykrycie nowych adresów MAC, wykrycie prób komunikacji do sieci Internet, wykrycie zbyt długiej przerwy w komunikacji zasobu.
3.7. System musi raportować wykryte anomalie i zdarzenia bezpieczeństwa m.in.
3.7.1. podejrzenie ataku MitM (np. ARP Spoofing).

3.7.2. skanowanie portów i sieci.
3.7.3. zdarzenia wykryte przez silnik sygnaturowy w tym znane ataki sieciowe oraz znane charakterystyki ruchu złośliwego oprogramowania.
3.7.4. zdarzenia pasujące do zdefiniowanych przez administratora reguł zrealizowanych w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych które zostały wymienione w złączniku nr1).

3.8. System musi dostarczać dane o wykrytych anomaliach w postaci czytelnej centralnej konsoli alarmów.
3.8.1. Konsola alarmów musi czytelnie oddzielać alarmy aktywne (nowe) od przetworzonych (archiwalne).
3.8.2. Konsola alarmów musi dostarczać następujących informacji wadze zdarzenia (jego dotkliwość), dacie pierwszego wykrycia, dacie ostatniej modyfikacji, źródle ruchu oraz celu, a także wskazywać protokoły wykorzystane w komunikacji.

3.9. System musi umożliwiać raportowanie wykrycia dowolnego ruchu sieciowego o zadanej przez Zamawiającego charakterystyce w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych).

3.10. System musi analizować i prezentować anomalie protokołów przemysłowych m.in.:
3.10.1. nieautoryzowana komunikacja przemysłowa.
3.10.2. anomalie protokołów przemysłowych.
3.10.3. naruszenie zdefiniowanej polityki komunikacji przemysłowej.

4. Możliwości konfiguracji i modyfikacji zasad detekcji

4.1. System musi dostarczać niezbędnych danych do zrozumienia zasad działania reguł (Treść reguły, odniesienia do źródeł takich jak bazy CVE, Baza wiedzy Microsoft, Framework MITRE ATT&CK, itp.) oraz umożliwiać czytelny podgląd wszystkich reguł i ich wyjątków.

4.2. System musi umożliwiać modyfikację istniejących oraz tworzenie nowych sygnatur oraz umożliwiać włączanie i wyłączanie dowolnych sygnatur dla dowolnego komponentu systemu OT.

4.3. System musi umożliwiać modyfikację i tworzenie nowych wyjątków dla sygnatur na podstawie parametrów warstw 2, 3, 4, 7 modelu ISO/OSI bezpośrednio z konsoli alarmów po wystąpieniu zdarzenia, a także przed wystąpieniem zdarzenia oraz w trakcie okresu tworzenia wzorca ruchu sieciowego.

4.4. System w trybie nauki musi generować sugerowany wzorzec ruchu, który po przeglądzie i jego akceptacji utworzy automatycznie niezbędne wyjątki dla sygnatur.

4.5. System powinien zapewniać możliwość tworzenia nowych i modyfikację istniejących (bezczynny/detekcja/nauka) trybów pracy pozwalając włączać i wyłączać poszczególne silniki detekcji uruchomionych w poszczególnych trybach i dostosowywać ich konfigurację, w celu precyzyjnego określenia zachowania metod detekcji.

4.6. System musi umożliwiać prowadzenie działań proaktywnego wyszukiwania zagrożeń w sieci (Threat Hunting).

4.7. System w czasie pracy musi automatycznie w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych zgodnych z zapisami *pkt. 2 załącznik nr 1*) tworzyć sugestie detekcji, dotyczące zaobserwowanego ruchu, które operator może włączyć i dostosować aby wykorzystać je jako reguły dodatkowe wzbogacające detekcję sygnaturową.

4.8. System musi, za pomocą kreatora obecnego w GUI systemu, umożliwiać tworzenie własnych reguł detekcji, w celu wzbogacenia detekcji sygnaturowej, w oparciu o parametry warstw L2 (np. adresy MAC, VLANy), L3 (np. adresy IP, protokół transportowy), L4 (np. porty TCP/UDP) oraz L7 (cechy szczególne, wykrywane przez DPI dla protokołów przemysłowych zgodnie z *pkt. 2 załącznik nr 1*).

4.9. System musi umożliwiać przypisanie dowolnego dostępnego mechanizmu DPI do dowolnego portu TCP/UDP oraz umożliwiać tworzenie własnych modułów DPI dla protokołów autorskich.

4.10. System musi umożliwiać precyzyjne określenie zakresu adresacji sieci będącej siecią chronioną/monitorowaną (tzw. sieć domowa, ang. home net) oraz umożliwiać definicję zaufanych adresów IP spoza sieci chronionej.
4.11. System musi dostarczyć mechanizm ograniczenia wolumenu analizowanego ruchu przez filtrowanie ruchu przychodzącego np. na podstawie identyfikatora VLAN.

5. Funkcje Inwentaryzacyjne
5.1. System musi zapewniać funkcje automatycznego wykrywania zasobów systemów automatyki i sterowania takich jak PLC, HMI, Serwer SCADA, OPC Serwer, Serwer Historian, Stacje operatorskie, stacje inżynierskie, Router i przypisywać im automatycznie określony typ oraz umożliwiać przypisywanie własnych typów dla urządzeń niezdefiniowanych przez producenta systemu.
5.2. System musi inwentaryzować urządzenia komunikujące się z wykorzystaniem warstwy 2 ISO/OSI i wyższych oraz inwentaryzować urządzenia komunikujące się wyłącznie w warstwie 2 ISO/OSI (tj. nieposiadające adresu IP).
5.3. System musi wykonywać pasywną identyfikację systemu operacyjnego (minimum rodziny systemów Microsoft Windows) urządzenia i jego wersji.
5.4. System musi udostępniać dane o zinwentaryzowanych zasobach i połączeniach w formie tabelarycznej i umożliwiać eksportowanie tych danych do formatów co najmniej: JSON, CSV, PDF.
5.5. System musi aktualizować zestawy danych o zasobach i połączeniach w trybie ciągłym. Jest to równoznaczne z odświeżaniem tych danych w tabelach i na mapie połączeń.
5.6. System musi prezentować informacje o wykorzystywanych protokołach w połączeniach sieciowych w formie tabelarycznej i umożliwiać eksportowanie tych danych do formatów co najmniej: JSON, CSV, PDF.
5.7. System musi prezentować informacje o wykorzystywanych protokołach w połączeniach sieciowych w formie graficznej na mapie i umożliwiać eksportowanie widoku do pliku graficznego PNG.
5.8. System musi rozpoznawać automatycznie przypisanie urządzeń do stref (zones) według standardu IEC 62443 oraz rozpoznawać automatycznie kanały komunikacyjne (conduits) pomiędzy strefami zgodnie ze standardem IEC 62443.
5.9. System musi określać producenta urządzenia na podstawie zebranych danych.
5.10. System musi wykonywać analizę podatności na podstawie wykrytych lub podanych przez administratora wersji systemu operacyjnego.
5.11. System powinien analizować wykorzystanie pasma przez każdy zasób i połączenie sieciowe.
5.12. System musi umożliwiać dodawanie do karty urządzenia zdefiniowanych przez administratora kryteriów opisu danego zasobu/urządzenia, akcja ta powinna być dostępna globalnie dla urządzeń oraz lokalnie dla pojedynczego urządzenia. Systemu musi umożliwiać filtrowanie danych po stworzonych kryteriach oraz umożliwiać ich eksport do plików CSV, JSON, PDF. Dane te powinny być też dostępne w raporcie generowanym przez system.
5.13. System musi zapewnić możliwość importu pliku w formacie minimum CSV, w celu wykonania wsadowej modyfikacji minimum nazwy, typu, producenta, każdego z wykrytych urządzeń.
5.14. System musi umożliwiać grupowanie urządzeń w monitorowanej sieci w zależności od ich wpływu na poszczególne procesy biznesowe zachodzące w organizacji. Jedna grupa (proces biznesowy) może zawierać wiele urządzeń, a każde urządzenie może być członkiem wielu grup.
5.15. System musi zapewnić możliwość modyfikacji wagi alarmów w zależności od krytyczności procesu biznesowego/typu urządzenia/indywidualnych wymogów urządzenia i właściciela systemu.
5.16. System musi umożliwić edycję danych o producencie urządzenia, a także umożliwiać edycję nazw zasobów oraz dodawanie komentarzy do zasobów.
5.17. System musi umożliwiać przypisanie więcej niż jednego adresu MAC do urządzenia, umożliwiając inwentaryzację klastrów systemów.
5.18. System musi umożliwiać edycję danych o wykrytym systemie operacyjnym (w minimalnym wariancie dla MS Windows) wraz z informacjami o aktualizacjach nałożonych na ten system.
5.19. System musi analizować i prezentować w karcie zasobu dodatkowe informacje w oparciu o analizę wykrytego ruchu protokołów ujętych w *pkt. 3 złączniku nr 1*.
5.20. System musi analizować i prezentować przesyłane przez sieć komendy protokołów przemysłowych ujętych w *pkt. 2 załącznik 1*.

6. Interfejs oraz funkcje mapy.
   6.1. System musi dostarczać czytelnych informacji na temat istotnych zdarzeń zaobserwowanych w sieci (alarmów) oraz informacji o trybie pracy rozwiązania (bezczynny/detekcji/nauki).
   6.2. System musi umożliwiać świadome przełączanie między trybami pracy wg. harmonogramu oraz ręcznie.
   6.3. System musi dostarczać funkcje prezentowania zebranych danych o zasobach i ich połączeniach w postaci graficznej (Mapa połączeń), mapa musi być interaktywna, tj. umożliwiać uzyskanie szczegółowej informacji o prezentowanych na niej zasobach lub połączeniach (np. poprzez zaznaczenie urządzenia/połączenia kliknięciem)
   6.4. Interfejs musi być w języku polskim.
   6.5. Funkcja mapy musi wyświetlać schemat połączeń logicznych pomiędzy węzłami sieci oraz umożliwiać tworzenie własnych widoków w modelach: przepływu, PERA, zdefiniowanym przez użytkownika minimum zmieniając geometryczne rozłożenie obiektów na mapie.
   6.6. Funkcja mapy musi umożliwiać wykorzystanie zdefiniowanych procesów biznesowych w celu stworzenia osobnych widoków mapy, ułatwiających analizę.
   6.7. System musi prezentować na mapie fakt wykrycia routerów na trasie połączeń.
   6.8. System musi prezentować na mapie kierunek komunikacji pomiędzy urządzeniami, a także wskazywać na mapie urządzenia zagrożone i dotknięte anomaliami.
   6.9. System musi umożliwiać tworzenie własnych widoków mapy na podstawie grup procesów biznesowych lub z wykorzystaniem filtrowania zasobów (kluczem powinny być minimum adresy IP, adresy MAC, podsieci, producenci, cechy komunikacji jak np. komunikowanie się przez router lub lokalizacja poza siecią chronioną) oraz umożliwiać zapis widoku mapy do pliku graficznego.
7. Integracje
   7.1. System musi umożliwiać integrację z dowolnym rozwiązaniem SIEM oraz wspierać przesyłanie danych za pomocą protokołu syslog w formatach CEF i LEEF.
   7.2. System musi umożliwiać integrację z dowolnym rozwiązaniem kolejkowania pracy (np. ITSM) poprzez wysyłanie wiadomości e-mail.
   7.3. System musi zapewniać granularną kontrolę przesyłanych danych protokołu syslog w zależności od: źródła powstawania komunikatów (silnika detekcji) oraz wagi komunikatu (krytyczność alarmu).
   7.4. System musi umożliwiać przesłanie dowolnego zestawu informacji do dowolnej ilości odbiorców syslog, lub e-mail oraz umożliwiać tworzenie i przesyłanie za pomocą wiadomości e-mail raportów okresowych o wykrytych anomaliach i zdarzeniach, zawierające minimum adresy źródłowe i docelowe, daty wystąpienia alarmów i treści alarmów.
   7.5. System musi integrować się jako odbiorca danych ze strumieni syslog, w celu wzbogacenia wewnętrznej bazy danych.
   7.6. System musi integrować się z kolejkami workflow wybranych rozwiązań firewall, w celu przesyłania sugestii reguł firewalla, Lista rozwiązań stanowi *pkt 4. załącznik nr 1*.
   7.7. System musi dostarczać API, dla integracji z dowolną aplikacją tworzoną w Organizacji.
   7.8. System musi integrować się z usługą Active Directory w celu zarządzania kontami użytkowników systemu.
   7.9. System powinien integrować się z rozwiązaniem RSA SecureID.
   7.10. System może dostarczać lokalne zarządzanie kontami użytkowników.
   7.11. System powinien dostarczać mechanizm zarządzania uprawnieniami użytkowników co najmniej dla trzech zdefiniowanych ról.
8. Kontrola poprawności działania systemu.
   8.1. System musi zapewniać podgląd stanu systemu, w tym:
      8.1.1. Użycie CPU.
      8.1.2. Użycie pamięci RAM.
      8.1.3. Wykorzystanie miejsca na dysku.
      8.1.4. Wykorzystanie pasma na każdym z interfejsów.
   8.2. System musi zapewniać możliwość monitorowania jego stanu za pomocą protokołu SNMP.
   8.3. System powinien generować rekomendacje dotyczące stanu jego konfiguracji i bezpieczeństwa.

V. Wymagania dla centralnego systemu nadzoru nad alarmami

Zamawiający oczekuje przedstawienia oferty wdrożenia centralnego systemu nadzoru nad oferowanymi rozwiązaniami klasy NSM/IDS.

1. Wymagania główne:
   1.1. System musi być kompatybilny z wybranym przez Zamawiającego rozwiązaniem IDS/NSM.
   1.2. System musi zapewniać możliwość monitorowania sieci rozproszonej geograficznie.
   1.3. System musi umożliwiać tworzenie logicznych segmentów zawierających jeden lub więcej systemów NSM/IDS.
   1.4. System musi umożliwiać precyzyjne przydzielanie dostępu użytkowników z poziomem uprawnień Administrator/Ekspert/Analityk dla członków grupy odpowiedzialnej za konkretny obiekt:
      1.4.1. Indywidualnie dla każdego segmentu monitorującego konkretny obiekt
      1.4.2. Do każdej z grup segmentów monitorujących konkretne obiekty
      1.4.3. Globalnie do wszystkich segmentów
   1.5. System musi agregować dane z poszczególnych segmentów i przedstawiać je wyłącznie uprawnionym użytkownikom.
   1.6. System może prezentować dane z poszczególnych systemów w postaci mapy uwzględniającej ich rozmieszczenie geograficzne.
   1.7. System musi agregować dane sumaryczne dotyczące ilości alarmów, połączeń i zasobów
   1.8. System musi dostarczać czytelnych danych o alarmach wykrytych przez poszczególne silniki systemy IDS/NSM. Minimalnie system musi wskazywać alarmy cyberbezpieczeństwa i inwentaryzacji zasobów sieci.
   1.9. System musi umożliwiać scentralizowaną pracę z alarmami obecnymi w poszczególnych platformach IDS w tym:
      1.9.1. archiwizację alarmów,
      1.9.2. dodawanie komentarzy,
      1.9.3. tworzenie wyjątków,
      1.9.4. przegląd, sortowanie i filtrowanie alarmów.
   1.10. System musi umożliwiać scentralizowaną pracę z zasobami zinwentaryzowanymi na poszczególnych instancjach IDS.
   1.11. System musi dostarczać funkcje audytu działań jego użytkowników i zapewniać możliwość przesyłania danych o tych akcjach za pomocą protokołu syslog.
   1.12. System musi umożliwiać aktualizację oprogramowania na wszystkich rozwiązaniach IDS, będących pod kontrolą centralnego systemu zarządzani.
   1.13. System musi integrować się z usługą Active Directory w celu zarządzania kontami użytkowników systemu.
   1.14. System musi integrować się z rozwiązaniem RSA SecureID.
   1.15. System musi dostarczać lokalne zarządzanie kontami użytkowników.
   1.16. System musi dostarczać mechanizm zarządzania uprawnieniami użytkowników RBAC.
   1.17. System musi zapewniać podgląd stanu systemu, w tym:
      1.17.1. użycie CPU,
      1.17.2. użycie pamięci RAM,
      1.17.3. wykorzystanie miejsca na dysku,
      1.17.4. wykorzystanie pasma na każdym z interfejsów,
   1.18. System musi zapewniać możliwość monitorowania jego stanu za pomocą protokołu SNMP.

VI. Wymagania dla systemu zabezpieczenia telemetrii

1. Wymagania ogólne dla zabezpieczenia i monitorowania komunikacji w obrębie systemu telemetrycznego:
   1.1. Usługą ciągłego monitorowania należy objąć system telemetryczny działający w architekturze gwiazdy. Komunikację sieciową w obrębie systemu telemetrycznego należy monitorować w punkcie centralnym (lokalizacja Katowice).
   1.2. Oprócz monitorowania komunikacji zastosowane rozwiązanie ma zabezpieczać komunikację pomiędzy serwerami a elementami systemu telemetrii rozproszonymi geograficznie.

1.3. Obudowa dostosowana do implementacji w szafie RACK 19”.
1.4. Urządzenie służące do monitorowania i zabezpieczenia komunikacji musi mieć funkcjonalność firewalla w celu filtrowania ruchu sieciowego z wykorzystaniem reguł opisujących dopuszczony ruch sieciowy za pomocą:
  1.4.1. Adresu IP źródła komunikacji;
  1.4.2. Źródłowego portu TCP lub UDP;
  1.4.3. Adresu IP celu;
  1.4.4. Docelowego portu TCP lub UDP;
  1.4.5. Protokołu warstwy aplikacyjnej;
  1.4.6. Harmonogramy czasowe.
1.5. Urządzenie musi mieć funkcjonalność routera i możliwość realizowania routingu w oparciu o:
  1.5.1. Reguły statyczne
  1.5.2. Protokoły dynamiczne: OSPF, RIP.
1.6. Urządzenie musi posiadać możliwość tworzenia reguł dla translacji adresów NAT i przekierowania portów PAT
1.7. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
1.8. Urządzenie musi posiadać możliwość filtrowania ruchu w trybie transparentnym dla wskazanych portów. Oznacza to możliwość egzekwowania wszystkich polityk firewalla dla portów zgrupowanych jako bridge (ta sama podsieć IP bez routingu).
1.9. Urządzenie musi tworzyć logi zarówno dla komunikacji dozwolonej jak i zablokowanej.
1.10. Urządzenie musi mieć wewnętrzną pamięć pozwalającą na zapis i przechowywanie logów lokalnie.
1.11. Urządzenie musi wysyłać logi za pomocą protokołu syslog do min. 3 określonych serwerów logów / SIEM przy jednoczesnym zdefiniowaniu:
  1.11.1. Protokołu i portu dla przekazywania logów,
  1.11.2. Kategorii (ang. Facility),
  1.11.3. Rodzaju logów przekazywanych, min: logi dot. połączeń, logi z firewalla, IPS/IDS, alarmy, dzienniki systemowe,
1.12. Urządzenie musi posiadać funkcjonalność IPS z możliwością przełączenia w tryb IDS czyli tylko monitorowania bez blokowania w przypadku wykrycia zagrożeń lub anomalii.
1.13. Wbudowany IPS/IDS musi być oparty o sygnatury wykrywające znane zagrożenia i ataki sieciowe.
1.14. Urządzenie musi zapewniać możliwość dodawania własnych sygnatur IPS.
1.15. Urządzenie musi być wyposażone w min. 12 miedzianych interfejsów Ethernet 10/100/1000 Mbps, z których każdy można dowolnie zdefiniować jako np. WAN, LAN, BRIDGE, MANAGEMENT lub DMZ.
1.16. Urządzenie musi mieć możliwość kreowania interfejsów VLAN oraz GRE.
1.17. Urządzenie musi umożliwiać tworzenie sieci VPN opartych o IPSec i SSL VPN.
1.18. Maksymalna liczba tuneli VPN IPSec – minimum 500.
1.19. Urządzenie ma być wyposażone w dysk SSD o pojemności powyżej 200 GB.
1.20. Obsługa interfejsów 802.11q (VLAN) – minimum 256.
1.21. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
1.22. Urządzenie nie może narzucać limitu na liczbę użytkowników.
1.23. Liczba reguł filtrowania – minimum 8 192.
1.24. Liczba tras statycznego routingu – minimum 2 048.
1.25. Skaner antywirusowy ma być dostarczany w ramach licencji.
1.26. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
1.27. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
1.28. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
1.29. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
1.30. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
  1.30.1. lokalną bazę użytkowników (wewnętrzny LDAP),

1.30.2. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
1.30.3. usługę katalogową Microsoft Active Directory.
1.31. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
1.32. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
1.32.1. SSL,
1.32.2. Radius,
1.32.3. Kerberos.
1.33. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
1.34. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
1.35. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
1.36. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
1.37. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa przez zaszyfrowany protokół HTTPS.
1.38. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
1.39. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
1.40. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
1.41. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
1.42. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
1.43. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
1.44. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
1.44.1. manualnego eksportu do pliku w dowolnym momencie czasu,
1.44.2. automatycznego eksportu na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu.
1.45. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z dedykowanego serwera zarządzanego przez administratora.
1.46. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
1.47. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
1.48. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
1.49. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego.
1.50. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
1.51. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
1.52. Możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji.
1.53. Okres wsparcia zgodnie z zapisami OPZ w zakresie wszystkich wymaganych licencji.
1.54. Gwarancja zgodnie z zapisami OPZ.

VII. Wymagania dla sond oraz wymagania dla urządzeń komunikacji (obiekt istotny i podstawowy)

7. Zaoferowane rozwiązanie ma zapewnić bezpieczną komunikację pomiędzy monitorowanymi obiektami a systemem centralnym oraz z SOC. W szczególności dla ***Obiektów Podstawowych*** (*pkt 1. w załącznik nr 1*) należy zapewnić przekazywanie z wykorzystaniem sondy zebranego ruchu sieciowego do analizy przez system IDS znajdujący się w ***Obiekcie Kluczowym***. Z kolei system IDS działający w ***Obiekcie Kluczowym*** w sposób bezpieczny ma komunikować się z systemem centralnym znajdującym się w centrali GPW w Katowicach, jednocześnie informacje o zdarzeniach mają za pomocą protokołu syslog być wysyłane do SOC. W ***Obiektach Istotnych*** mają zostać zainstalowane mniejsze / odpowiednio dobrane instancje systemu monitorowania IDS. Ma być zapewniona komunikacja tych systemów IDS z systemem centralnym znajdującym się w Katowicach oraz informacje o zdarzeniach mają za pomocą protokołu syslog być wysyłane do systemu centralnego oraz SOC.
8. Należy zapewnić również dwukierunkową bezpieczną komunikację pomiędzy systemem centralnym znajdującym się w Katowicach a SOC, tak aby SOC miał dostęp do graficznego interfejsu użytkownika tego systemu za pomocą protokołu https.
9. Do skomunikowania obiektów należy wykorzystać wydzielone rozwiązanie oparte o komunikację bezprzewodową wykorzystującą prywatny APN. Po stronie Dostawcy rozwiązania jest zapewnienie /dostarczenie, skonfigurowanie i uruchomienie odpowiednich urządzeń komunikacyjnych (sondy, routery LTE, etc.).
10. Sonda systemu IDS to urządzenie, którego zadaniem ma być przekazywanie kopii ruchu sieciowego z obiektów podstawowych do zlokalizowanego w obiekcie kluczowym serwera IDS.
    10.1. Wymagana funkcjonalność sondy dla obiektu kluczowego:
        10.1.1. Co najmniej 4 interfejsów Ethernet 10/100 Mbit/s.
        10.1.2. Co najmniej 2 interfejsy 100/1000 Mbit/s SFP.
        10.1.3. Interfejs komórkowy – modem 4G/LTE z możliwością obsługi dwóch kart SIM.
        10.1.4. Każdy z ww. interfejsów musi pełnić rolę interfejsu słuchającego kopii ruchu dostarczonej z portów SPAN / mirror przełączników lub rolę interfejsu wyjściowego łączącego sondę z serwerem IDS.
        10.1.5. Sonda ma mieć możliwość pracy jako switch lub router stanowiący element infrastruktury sieciowej obiektu – wtedy kopiowanie ruchu ma następować ze wskazanych portów na zdefiniowany port wyjściowy lub wskazany cel routingu dla tunelu GRE do systemu IDS lub Wykonawca zapewni w inny sposób spełnienie to wymagania.
        10.1.6. Zadaniem sondy jest agregowanie i tunelowanie monitorowanego ruchu sieciowego do systemu IDS.
        10.1.7. Komunikacja z portu wyjściowego sondy do serwera IDS ma być realizowana z wykorzystaniem tunelu GRE.
        10.1.8. Kopia ruchu przesyłana z sondy do IDS musi być kompresowana.
        10.1.9. Oprogramowanie sondy musi umożliwiać odfiltrowania na portach wejściowych ruchu (konkretnych adresów lub podsieci IP, portów źródłowych i docelowych oraz typu protokołu TCP/UDP), który nie będzie przesyłany do analizy.
        10.1.10. Sonda musi synchronizować czas z serwerem NTP.
    10.2. Sonda pozostałe wymagania
        10.2.1. Montaż na szynie DIN.
        10.2.2. Obudowa przemysłowa, IP 30.
        10.2.3. Chłodzenie konwekcyjne (brak wentylatorów).
        10.2.4. Zakres temperatur pracy: -25°C do 70°C.
        10.2.5. Zasilanie 48 VDC.
11. W ***Obiektach Podstawowych*** jest wymagane zapewnienie urządzenia posiadającego funkcjonalności przełącznika LAN i routera. Dopuszcza się wykorzystanie jednego urządzenia jako sondy i urządzenia komunikacyjnego z zachowaniem poniższych funkcjonalności:
    11.1. Wymagana funkcjonalność przełącznika/routera dla obiektu podstawowego:
        11.1.1. Co najmniej 8 interfejsów Ethernet 10/100 Mbit/s.
        11.1.2. Co najmniej 2 interfejsy 100/1000 Mbit/s SFP.

11.1.3. Interfejs komórkowy – modem 4G/LTE z możliwością obsługi dwóch kart SIM.

11.2. Funkcje sieciowe L2

11.2.1. IEEE 802.1q VLAN

11.2.2. DHCP klient, serwer, relay

11.2.3. Port mirror – kopiowanie ruchu z wszystkich portów na port monitorujący

11.3. Funkcje sieciowe L3

11.3.1. Routing statyczny

11.3.2. Routing dynamiczny OSPF, RIPv2

11.3.3. VRRP

11.3.4. NAT dynamiczny

11.3.5. NAT statyczny podsieć – podsieć

11.3.6. NAT statyczny IP – IP

11.3.7. Odczytywanie parametrów urządzenia poprzez SNMP

11.4. Kontrola dostępu

11.4.1. Listy dostępu ALC działające w warstwach L2, L3 i L4

11.4.2. Możliwość wyłączenia nieużywanych portów.

11.4.3. Uwierzytelnianie IEEE 802.1x na porcie.

11.4.4. Uwierzytelniające Proxy.

11.4.5. Ochrona dostępu do sterowników i urządzeń nieposiadających funkcji kontroli dostępu, użytkownik najpierw musi uwierzytelnić się na firewallu i potem otrzyma czasowy dostęp do konkretnego urządzenia za firewallem.

11.4.6. Logowanie aktywności użytkownika.

11.5. VPN

11.5.1. IPSec, obsługa certyfikatów X.509

11.5.2. IPSec, dynamiczna wymiana kluczy IKE

11.5.3. IPSec, szyfrowanie: AES, 3DES

11.5.4. L3 VPN GRE

11.5.5. OpenVPN SSL

11.5.6. DPI firewall - firewall realizujący głęboką analizę pakietów (DPI) dla protokołów co najmniej Modbus RTU, Modbus TCP, S7 TCP

11.6. Funkcje portów szeregowych

11.6.1. Transparentne tunelowanie

11.6.2. Brama dla protokołów Modbus RTU/Modbus TCP,

11.6.3. Serwer terminali szeregowych TCP/UDP

11.6.4. 2 porty szeregowe

11.6.5. Możliwość nasłuchiwania transmisji RS-232/485 i przekierowywanie jej do systemu IDS w celu analizy.

11.7. Pozostałe wymagania

11.7.1. Montaż na szynie DIN.

11.7.2. Obudowa przemysłowa, IP 30.

11.7.3. Chłodzenie konwekcyjne (brak wentylatorów).

11.7.4. Zakres temperatur pracy: -25°C do 70°C.

11.7.5. Zasilanie 48 VDC.

12. Do zapewnienia komunikacji z **Obiektów Istotnych** należy zastosować urządzenia komunikacyjne o następującej funkcjonalności:

12.1. Co najmniej 6 interfejsów Ethernet 10/100 Mbit/s.

12.2. Co najmniej 2 interfejsy 100/1000 Mbit/s SFP.

12.3. Interfejs komórkowy – modem 4G/LTE z możliwością obsługi dwóch kart SIM.

12.4. Urządzenie ma synchronizować czas z serwerem NTP.

12.5. Funkcje sieciowe L3:

12.5.1. Routing statyczny

12.5.2. Routing dynamiczny OSPF, RIPv2

12.5.3. VRRP

12.5.4. NAT dynamiczny
12.5.5. NAT statyczny podsieć – podsieć
12.5.6. NAT statyczny IP – IP
12.6. Kontrola dostępu:
12.6.1. Co najmniej listy dostępu ALC działające w warstwach L2, L3 i L4
12.6.2. Możliwość wyłączenia nieużywanych portów
12.6.3. Uwierzytelnianie IEEE 802.1x na porcie
12.7. VPN
12.7.1. IPSec, obsługa certyfikatów X.509
12.7.2. IPSec, dynamiczna wymiana kluczy IKE
12.7.3. IPSec, szyfrowanie: AES, 3DES
12.7.4. L3 VPN GRE
12.7.5. OpenVPN SSL
12.8. Pozostałe wymagania
12.8.1. Montaż na szynie DIN.
12.8.2. Obudowa przemysłowa, IP 30.
12.8.3. Chłodzenie konwekcyjne (brak wentylatorów).
12.8.4. Zakres temperatur pracy: -25°C do 70°C.
12.8.5. Zasilanie 48 VDC.

VIII. Wymagania dla urządzeń sieciowych i systemu zarządzania urządzeniami sieciowymi dla obiektu kluczowego.

4. System operacyjny przemysłowych urządzeń sieciowych (przełączników) powinien posiadać następujące funkcjonalności i możliwości:
4.1. 802.1q Statyczny VLAN, VLAN tag, VLAN Q-in-Q (tunelowanie)
4.2. 802.3x kontrola przepływu (Flow Control)
4.3. IGMPv2/v3 snooping, IGMP querier, IGMP fast leave
4.4. 802.1AB LLDP
4.5. 802.1p Class of service
4.6. Ograniczanie przepustowości portów (rate limiting, traffic shaping)
4.7. Uwierzytelnianie lokalne i centralne (RADIUS, TACACS+)
4.8. 802.1X kontrola dostępu (port access control)
4.9. Uwierzytelnianie MAC, wykrywanie konfliktów IP/MAC
4.10. Automatyczne wyłączanie nieużywanych portów
4.11. NTP/SNTP (klient/serwer)
4.12. 802.1d Spanning Tree Protocol (STP)
4.13. 802.1w Rapid Spanning Tree Protocol (RSTP)
4.14. Protokół ring
4.15. SNMP v2c/3 (brak v1 lub możliwość wyłączenia)Syslog
4.16. 802.1AX/802.3ad agregacja portów (statyczna i LACP)
4.17. Statyczny i dynamiczny routing (RIPv2, OSPFv2, VRRPv2/3)
4.18. Szyfrowane tunele VPN (klient i serwer) IPsec, SSL
4.19. Routing multicast
4.20. Tunelowanie GRE
4.21. Zapora ogniowa (firewall) z inspekcją stanu
4.22. Translacja adresów NAPT, NAT 1-TO-1 (wybrane adresy lub cała podsieć), proxy ARP
4.23. Przekierowanie portów (port forwarding) IP Multinetting (kilka podsieci w jednym VLAN-ie)
4.24. DSCP/ToS modification
4.25. Port monitoring (mirroring) z możliwością wyboru rodzaju ruchu (in, out, in/out) z dowolnych portów
5. Pozostałe wymagania dla urządzeń sieciowych.
5.1. Urządzenie w wykonaniu przemysłowym obudowa metalowa,
5.2. Klasa szczelności IP30,

5.3. Montaż na szynie DIN,
5.4. Zakres temperatur pracy –25 to +70°C,
5.5. MTBF wg MIL-HDBK-217-F co najmniej 500 000h
5.6. Redundantne zasilanie (zasilanie z dwóch źródeł), zakres napięcia zasilającego 19 to 60 VDC.
5.7. Certyfikaty
5.7.1.IEC 62236-4, EN 50121-4,
5.7.2.EN 61000-6-1,EN 61000-6-2, EN 61000-6-3, EN 61000-6-4
5.8. Certyfikaty dot. Bezpieczeństwa UL 62368-1
5.9. Typ chłodzenia - bez wentylatorowy.

6. System do konfiguracji urządzeń i zarządzania siecią, wymagane funkcjonalności:
6.1. System musi umożliwiać skanowanie sieci w celu wykrycia urządzeń, zarówno z wykorzystaniem protokołu ICMP (ping) jak i innych/własnych rozwiązań pozwalających na odnalezienie urządzeń bez względu na ich adresy IP lub w ogóle nieposiadających adresu.
6.2. System musi umożliwiać wykrywanie topologii połączeń pomiędzy urządzeniami w oparciu o protokół LLDP
6.3. System musi umożliwiać obsługę SNMP w wersji v2 i v3
6.4. System musi umożliwiać szybki, uproszczony przydział adresów sieciowych.
6.5. System musi umożliwiać konfigurację nowych elementów sieci
6.6. System musi udostępniać łatwy dostęp do interfejsów administracyjnych urządzeń (WEB, CLI) z poziomu aplikacji monitorującej.
6.7. System musi umożliwiać monitorowanie i diagnostykę sieci, przynajmniej w zakresie wykrywania zaniku połączeń i zmian (rekonfiguracji) w topologii sieci.
6.8. System musi umożliwiać prezentację statystyk komunikacji na poszczególnych portach (status, prędkość, liczniki danych, błędy)
6.9. System musi umożliwiać prezentację wykrytych urządzeń i połączeń między nimi na schemacie topologii, z funkcją auto-rozmieszczenia i możliwością ręcznego wprowadzania zmian (dodawanie/usuwanie urządzeń, dodawanie/usuwanie połączeń, zmiana położenia, tworzenie grup). Możliwość filtrowania wyświetlanych na schemacie urządzeń w oparciu o: adres IP, domyślna brama, nazwa hosta, wersja firmware-u, rodzina/model, lokalizacja, status SNMP, odbierane pułapki SNMP
6.10. System musi umożliwiać wyświetlanie zdarzeń i alarmów odbieranych z urządzeń sieciowych (wbudowany serwer SNMP trap). Zdarzenia i alarmy powinny być przechowywane w aplikacji monitorującej z możliwością ich wyeksportowania.
6.11. System musi posiadać wbudowany serwer Syslog zbierający dane z dzienników urządzeń sieciowych z możliwością ich wyeksportowania.
6.12. System musi umożliwiać aktualizację firmware-u urządzeń, pojedynczo i zbiorczo
6.13. System musi umożliwiać Backup i odtwarzanie konfiguracji pojedynczych urządzeń i całej sieci
6.14. System musi umożliwiać budowanie kolejnych sieci (powielania) na podstawie utworzonego szablonu.
6.15. System musi umożliwiać automatyczne wykrywanie i alarmowanie zmian wprowadzonych do konfiguracji urządzeń z możliwością analizy/porównania z konfiguracją bazową
6.16. System musi posiadać wbudowana instrukcję obsługi zapewniająca dostęp do dokumentacji z poziomu aplikacji monitorującej.
6.17. System musi umożliwiać wymagane funkcjonalności z zakresu bezpieczeństwa takie jak:
6.17.1. Wykrywanie niezmienionych, domyślnych haseł
6.17.2. Możliwość zmiany haseł we wszystkich urządzeniach w systemie, pojedynczo i zbiorczo
6.17.3. Analizator mocy haseł
6.17.4. Możliwość stworzenia wzorca konfiguracji dla całej sieci
6.17.5. Identyfikacja adresów MAC urządzeń podłączonych do danego portu urządzenia
6.17.6. Konfiguracja filtrowania adresów MAC w oparciu o wykryte na poszczególnych portach urządzenia – tworzenie białej listy
6.17.7. Konfiguracja kontroli dostępu 802.1x
6.17.8. Konfiguracja ograniczeń dla przepustowości portów

6.17.9. Możliwość centralnego wykrywania i wyłączania nieużywanych portów na wybranych przełącznikach
6.17.10. Zabezpieczanie hasłem kopii bezpieczeństwa projektu
6.17.11. Wyłączenie usług zarządzających, które przesyłają dane otwartym tekstem (telnet i http)
6.17.12. Wykrywanie protokołów routingu OSPF i RIP, w których nie zastosowano sygnatur MD5-HMAC, możliwość skonfigurowanie tego zabezpieczenia
6.17.13. Kalkulator SHA256 dla plików z oprogramowaniem układowym (firmware)

6.18. Wymagania dodatkowe

6.18.1. Dla urządzeń sieciowych oraz systemu zarzadzania wymagana jest dostęp do bezpłatnych aktualizacji FW i SW przez cały okres użytkowania urządzeń przez zamawiającego.
6.18.2. Gwarancja min. 4 lat

X. Serwis oraz wsparcie w zakresie zainstalowanych systemów.

Wraz z dostawą systemu powinno być zagwarantowane:

2. Wsparcie techniczne na okres obowiązywania umowy. Wsparcie powinno obejmować:
   b. Dostęp do najnowszych wersji oprogramowania;
   c. Pobieranie sygnatur dla podatności;
   d. Możliwość przedłużenia wsparcia dla systemu na okres dodatkowego roku po zakończeniu umowy;
   e. Dostęp do pomocy technicznej w dni robocze w godzinach 8:00- 16:00.

XI. Szkolenia.

2. Wykonawca na własny koszt przeszkoli zespół zamawiającego (5 osób) z zakresu administracji oraz pracy z systemem. Szkolenie musi być przeprowadzone w języku polskim w oparciu o materiały szkoleniowe w języku polskim i trwać łącznie co najmniej 20 godzin. Koszty związane z przygotowaniem i przeprowadzeniem szkolenia pokrywa Wykonawca. Zamawiający wymaga by przedstawiciele zespołu automatyki mogli aktywnie uczestniczyć w procesie wdrożenia systemu i tym samym budować kompetencje.
3. Wykonawca na własny koszt przeszkoli zespół zamawiającego (5 osób) z zakresu administracji oraz pracy z systemem monitorowania oraz jego komponentami. Szkolenie musi być przeprowadzone w języku polskim w oparciu o materiały szkoleniowe w języku polskim i trwać łącznie co najmniej 40 godzin. Koszty związane z przygotowaniem i przeprowadzeniem szkolenia pokrywa Wykonawca. Zamawiający wymaga by przedstawiciele zespołu automatyki mogli aktywnie uczestniczyć w procesie wdrożenia systemu i tym samym budować kompetencje.
4. Ponadto Wykonawca przeprowadzi dla personelu odpowiedzialnego za systemy przemysłowe oraz dla personelu zamawiającego dwa szkolenia online budujące świadomość z zakresu bezpieczeństwa systemów OT/ICS.

XII. Warunki odbioru prac.

Odbiór prac będzie się odbywał poprzez protokół podpisany z obu stron

XIII. Gwarancja

2. Wszystkie licencje i system (urządzenia) maja mieć zagwarantowane wsparcie na 4 lata od dnia uruchomienia usługi SOC.
3. Wszystkie urządzenia musza posiadać gwarancję na 4 lata liczoną od dnia uruchomienia usługi SOC.

MATERIAŁ POUFNY

Udostępniany na zasadach opisanych w Rozdziale III ust. 3 Zaproszenia do negocjacji

ZAŁĄCZNIK NR 2 DO UMOWY

WARUNKI ŚWIADCZENIA USŁUGI SOC I WSPARCIA TECHNICZNEGO SYSTEMU

w ramach realizacji Umowy nr xxx

na usługi monitorowania incydentów bezpieczeństwa przez wyspecjalizowane Security Operations Center (SOC)

Art. 1 Definicje

Wyrazy i zwroty użyte w Warunkach świadczenia usługi SOC i Wsparcia Technicznego mają takie samo znaczenie, jakie przypisano im w Umowie, a niżej wymienione nazwy i zwroty należy rozumieć jak następuje:

1. **I Linia Serwisowa** - Zespół wyspecjalizowany w obsłudze zgłoszeń incydentów, monitoringu stanu bezpieczeństwa OT, selekcji i priorytetyzacji incydentów. W celu świadczenia usługi Wykonawca będzie korelował logi z urządzeń Zamawiającego. Wykonawca zastosuje ponadto przy świadczeniu usługi system rejestracji incydentów (system ticketowania), który będzie wspomagał proces obiegu i rozwiązywania incydentów. Zespół będzie świadczył swoje usługi w trybie 24/7/365.
2. **II Linia Serwisowa** - zespół odpowiedzialny za obszar zarządzania platformami systemowymi dostarczonymi przez wykonawcę w ramach świadczonej usługi oraz za zarządzanie incydentami z tego obszaru. Specjaliści pracujący w zespole muszą mieć kompetencje w zakresie administrowania systemami (sieciowymi oraz bezpieczeństwa), które posiada w swojej infrastrukturze Zamawiający.
3. **III Linia Serwisowa** - zespół ekspertów specjalizujących się w wykrywaniu zaawansowanych technik ataku i najbardziej skomplikowanych zagrożeń, w tym:
   a. ekspertów posiadających kompetencje w zakresie analizy szkodliwego oprogramowania (analizy malware);
   b. ekspertów posiadających kompetencje w zabezpieczaniu teleinformatycznych śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania;
   c. ekspertów posiadających wysokie kompetencje w identyfikowaniu zagrożeń w odniesieniu do systemów informatycznych.
4. **CSIRT GOV** - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
5. **Incydent** - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
6. **Incydent krytyczny** - incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT GOV;
7. **Incydent poważny** - incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;
8. **Incydent istotny** - incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej "rozporządzeniem wykonawczym 2018/151";
9. **Dostępność** - oznacza okres, w którym nie występowały utrudnienia w zakresie świadczenia Usług I, II i III Linii Serwisowej.
10. **Zarządzanie incydentem** - obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;
11. **Zarządzanie ryzykiem** - skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka.

Art. 2 Warunki świadczenia Wsparcia Technicznego Systemu

1. Wykonawca w ramach świadczenia Wsparcia Technicznego Systemu, w związku z wynagrodzeniem ryczałtowym otrzymywanym na podstawie Umowy musi zapewnić utrzymanie ciągłości świadczonych przez siebie Usług.
2. Wykonawca w ramach usługi Wsparcia Technicznego Systemu zobowiązany jest do:
   1) Konsultacji technicznych polegających na udzielaniu wszelkiej pomocy merytorycznej Zamawiającemu, osobiście, lub za pośrednictwem telefonu, poczty elektronicznej.
   2) Przeglądów konserwacyjnych Systemu zapewniających prawidłowe świadczenie Usług przez Wykonawcę.
   3) W ramach świadczonych Usług wykonawca zapewni odpowiedni poziom świadczonych przez siebie usług i zapewni, że
      a) **w ramach I linii Serwisowej-** czas reakcji na incydent będzie nie dłuższy niż 15 minut od daty wykrycia incydentu,
      b) **w ramach II linii Serwisowej**
         - wykonawca zapewni przygotowanie zgłoszenia do właściwego csirt.gov w terminie 12 godzin od wykrycia incydentu zakwalifikowanego jako poważny. Ostatecznej kwalifikacji incydentu jako poważny dokonuje Zamawiający,
         - wykonawca rozpocznie niezwłoczne działania w zakresie zaleceń modyfikacji konfiguracji oraz innych działań wpływających na podwyższenie bezpieczeństwa do wdrożenia przez administratorów Zamawiającego – maksymalny czas przygotowania i przekazania zaleceń to 24 godziny robocze (w godzinach pracy II linii),
      c) **w ramach III linii Serwisowej** – maksymalny czas przyjęcia zadania do realizacji – następny dzień roboczy.

Art. 3 Zasady możliwości zgłaszania Incydentów

Wykonawca, niezależnie od możliwości zgłaszania Incydentów, wynikającej z działania Systemu będzie obsługiwał incydenty przekazywane przez Zamawiającego poprzez następujące metody kontaktu:

1) Telefonicznie na numer: ……. (jeden dedykowany numer telefonu),
2) Mailem na adres: ..... (jeden dedykowany adres e-mail).

Art. 4 Poziom utrzymania

1. Wykonawca, w ramach usługi SOC i Wsparcia Technicznego, zobowiązany jest do zapewnienia możliwości świadczenia Usług SOC w każdy dzień kalendarzowy.
2. Wykonawca zobowiązuje się do zapewnienia Dostępności Usług I linii wsparcia na poziomie **98 %** czasu mierzonego w skali miesiąca.
3. Z zastrzeżeniem ust. 2 Wnioskodawca zapewnia ciągłość w zakresie świadczonych przez siebie Usług nieprzerwanie 24 godziny na dobę przez 7 dni w tygodniu z wyłączeniem Okien Serwisowych.
4. Wszystkie planowane prace konserwacyjne i administracyjne wymagające wstrzymania świadczenia Usług będą realizowane przez Wykonawcę w ramach Okien Serwisowych. Zamawiający wyraża zgodę na przerwę w zakresie świadczonych na jego rzecz Usług, skutkujące w szczególności utratą możliwości świadczenia Usług, na okres uzgodnionych przez Strony Okien Serwisowych.
5. Strony niniejszym:
   3) uzgadniają jedno miesięcznie stałe Okno Serwisowe o długości do [6] godzin w godzinach [23.30] do [5.30] w dniu uzgodnionym z Zamawiającym;
   4) dopuszczają możliwość uzgodnienia dodatkowych Okien Serwisowych, o ile wymagać tego będzie charakter koniecznych do przeprowadzenia prac konserwacyjnych i administracyjnych. Dla swej ważności uzgodnienia takie muszą zawsze być dokonywane przez Kierowników Projektów lub innych upoważnionych przedstawicieli Stron w postaci

listu e-mail wysłanego przez Kierownika Projektu lub innego upoważnionego przedstawiciela Stron

6. Zamawiający zostanie poinformowany przez Wykonawcę o początku Okna Serwisowego, o którym mowa powyżej dnia poprzedzającego Okno Serwisowe do godziny ……... Powyższe ustalenie dotyczące początku Okna Serwisowego będzie obowiązywało do czasu określenia nowego początku Okna Serwisowego.
7. Na czas realizacji prac w Oknach Serwisowych Wykonawca zapewni alternatywne sposoby świadczenia Usług w ramach wszystkich trzech Linii Serwisowych.
8. W przypadku wykonania prac/usług dodatkowych nieobjęte Umową, Wykonawca zobowiązany będzie do uprzedniego przesłania oferty w formie pisemnej lub e-mail obejmującej usługi dodatkowe. Akceptacja przez Zamawiającego oferty obejmującej usługi dodatkowe następować będzie w formie pisemnej lub e-mail, przy czym brak odpowiedzi nie oznacza akceptacji oferty. W przypadku wykonania przez Wykonawcę prac lub usług nieobjętych niniejszą umową bez wcześniejszej akceptacji przez Zamawiającego oferty dotyczącej prac/usług dodatkowych, Wykonawca nie może żądać zapłaty za wykonane, niezgłoszone prace/usługi dodatkowe.

ZAŁĄCZNIK NR 3 DO UMOWY

Protokół Odbioru Końcowego wdrożenia usługi SOC

<table>
<tr><td colspan="2">Przedmiot odbioru:
Raport zawierający zakres zrealizowanych zadań w ramach Umowy nr ……</td></tr>
<tr><td colspan="2">Podstawa wykonania: Umowa ……</td></tr>
<tr><td>Zamawiający:
……</td><td>Wykonawca:
……</td></tr>
<tr><td colspan="2">prawniony Przedstawiciel Zamawiającego, Pan/Pani ……..…..….. stwierdza, że prace objęte przedmiotem odbioru wykonano zgodnie z Umową w dn. …….. r. Zamawiający nie zgłasza kolejnych zastrzeżeń i akceptuje sposób wprowadzenia uwag oraz wyjaśnienia Wykonawcy.
lub
prawniony Przedstawiciel Zamawiającego, Pan/Pani …….……..…….. stwierdza, że prace objęte przedmiotem odbioru wykonano niezgodnie z Umową. Zamawiający zgłasza następujące zastrzeżenia:
……
…….
do czasu ich usunięcia nie akceptuje sposobu wykonania prac objętych przedmiotem odbioru oraz wyjaśnień Wykonawcy. Zamawiający wyznacza termin […] do ponownego przedłożenia prac objętych przedmiotem odbioru uwzględniających powyższe zastrzeżenia.</td></tr>
<tr><td colspan="2">Niniejszy Protokół stanowi podstawę/nie stanowi podstawy* do wystawienia przez Wykonawcę faktury – zgodnie z Umową.</td></tr>
<tr><td>Zamawiający

….....</td><td>Wykonawca

……</td></tr>
<tr><td colspan="2">Protokół sporządzono w 2 jednobrzmiących egzemplarzach – po jednym egzemplarzu dla Zamawiającego i Wykonawcy.</td></tr>
</table>

ZAŁĄCZNIK NR 4 DO UMOWY

MIESIĘCZNY PROTOKÓŁ WYKONANIA USŁUGI SOC i WSPARCIA TECHNICZNEGO SYSTEMU

W ramach realizacji Umowy nr …… z dnia …… r.

Strony potwierdzają co następuje:

- wykonanie usługi **Security Operation Center (SOC)** w okresie od …… do ……..

Uwagi Wykonawcy:

……
……

Uwagi Zamawiającego:

……
……

W ramach świadczonej usługi, przez cały okres jej świadczenia którego dotyczy niniejszy protokół, Wykonawca dostarczył i wdrożył oraz zastosował przy świadczeniu Usługi SOC ……. scenariusze bezpieczeństwa
Podpisanie protokołu przez Strony stanowi/nie stanowi[1] podstawy do wystawienia przez Wykonawcę faktury w kwocie określonej w Umowie za okresowe świadczenie usługi SOC.

Podpisanie protokołu przez Strony stanowi/nie stanowi podstawy zwolnienia Zabezpieczenia Należytego Wykonania Umowy zgodnie z Umową.

Protokół został sporządzony w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Zamawiający	Wykonawca
….....	……
Miejsce, data	Miejsce, data

[1] Niepotrzebne skreślić

ZAŁĄCZNIK NR 5 DO UMOWY

Lista osób zobowiązanych do zachowania w tajemnicy informacji stanowiących tajemnicę przedsiębiorstwa Zamawiającego oraz do przestrzegania zasad postępowania z nimi

ZAŁĄCZNIK NR 6 DO UMOWY

Oferta ostateczna Wykonawcy

ZAŁĄCZNIK NR 7 DO UMOWY

EXIT PLAN

Art. 1 Zasady ogólne

1. Wykonawca w ramach Exit Planu będzie realizował wszystkie niezbędne prace mające na celu sprawne przeniesienie zarządzania Usługą SOC przez Zamawiającego bądź przez nowego Wykonawcę w sposób zapobiegający jakimkolwiek przerwom lub zakłóceniom świadczenia Usługi, w celu zachowania ciągłości działania usług świadczonych przez nowy System świadczący usługi analogiczne do usług Wykonawcy.
2. Prace przypisane do Exit Planu będą podlegały ocenie Zamawiającego.
3. Exit Plan uważany jest za zakończony, jeżeli Zamawiający pozytywnie go zweryfikuje i pisemnie poświadczy jego pomyślne zakończenie.

Art. 2 obowiązki Wykonawcy

1. Wykonawca przeprowadzi transfer wiedzy oraz migrację wszelkich danych uzyskanych w związku ze świadczeniem Usług SOC do Zamawiającego lub osoby trzeciej wskazanej przez Zamawiającego w zakresie. Zakres danych i informacji przekazanych musi nastąpić w formie i zakresie umożliwiającym samodzielną kontynuację działań związanych z utrzymaniem ciągłości działania SOC po wygaśnięciu Umowy;
2. Niezależnie od dalej idących postanowień Umowy, w tym paragrafów regulujących prawa własności intelektualnej, Zamawiający jest uprawniony do samodzielnego wykorzystania lub do przekazania osobie trzeciej, w celu zapewnienia ciągłości działania SOC, wszelkich Produktów, dokumentów, prezentacji, rezultatów prac Wykonawcy otrzymanych w ramach realizacji Umowy oraz wszelkiej innej dokumentacji.
3. W zakresie jakichkolwiek utworów dostarczonych przez Wykonawcę w ramach Usług Utrzymania mają zastosowanie postanowienia paragrafów regulujących prawa własności intelektualnej. Zamawiający nabywa – odpowiednio – prawa majątkowe lub licencje do utworów dostarczonych w ramach Usług Utrzymania.
4. Łączny wymiar usług związanych z przekazaniem Usług Utrzymania nie przekroczy 40 godzin roboczych.

Art. 3 Wynagrodzenie dotyczące Exit Planu, odbiór

1. Wynagrodzenie z tytułu wykonania zobowiązań Wykonawcy przewidzianych w niniejszym Załączniku Umowy jest zawarte w ramach wynagrodzenia opisanego w § 4 Umowy. Strony zgodnie potwierdzają, że z tytułu realizacji powyższych zobowiązań Wykonawca nie jest uprawniony do żądania zapłaty żadnego dodatkowego wynagrodzenia przez Zamawiającego.
2. Po stwierdzeniu przez Zamawiającego, że Wykonawca wypełnił wszystkie obowiązki określone w pkt 2 niniejszego Exit Planu Strony poświadczą ten fakt, w formie pisemnej pod rygorem nieważności.

ZAŁĄCZNIK NR 8 DO UMOWY

WZÓR Umowy powierzenia
przetwarzania danych osobowych

zawarta w Katowicach w dniu …… 202… roku pomiędzy:

Górnośląskim Przedsiębiorstwem Wodociągów Spółką Akcyjną z siedzibą przy ul. Wojewódzkiej 19, 40 – 026 Katowice, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowym Katowice - Wschód, Wydział VIII Gospodarczy Krajowego Rejestru Sądowego pod numerem 0000247533, posługującą się NIP 634 012 87 88, numerem REGON 271506695, będącą podatnikiem VAT czynnym, o kapitale zakładowym 425 875 100,00 zł, opłaconym w całości, posiadającą status dużego przedsiębiorcy w rozumieniu regulacji art. 4 pkt 6 ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (tj. Dz.U. z 2020 r. poz. 935 z późn. zm.), reprezentowaną przez:

……..
……..

(dalej: **„Administrator”**),

a

(dalej: **„Podmiot przetwarzający "**),

zwanymi dalej łącznie „**Stronami**”, a każdą z osobna „**Stroną**”.

§ 1.
Przedmiot Umowy

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w zakresie i celu objętym umową z dnia …….. (zwanej dalej „Umową główną”).
2. Administrator oświadcza, że jest administratorem powierzanych danych osobowych w zakresie określonym w Umowie głównej w rozumieniu przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (rozporządzenie ogólne o ochronie danych, dalej „**RODO**”) i przetwarza powierzane dane osobowe zgodnie z obowiązującymi przepisami prawa.

§ 2.
Zakres i cel przetwarzania danych osobowych

1. Podmiot przetwarzający może przetwarzać dane osobowe udostępnione przez Administratora wyłącznie w zakresie i w celu określonym w niniejszej Umowie powierzenia bądź Umowie głównej w zgodzie z art. 28 RODO.

2. Dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu wykonania przez Podmiot przetwarzający czynności w zakresie ……..
3. Zakres przetwarzania obejmuje następujące dane osobowe osób fizycznych: ……..
4. Poprzez przetwarzanie danych w rozumieniu RODO rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie; rzeczone operacje będą wykonywane zarówno na zbiorach manualnych, jak i w systemach teleinformatycznych.

§ 3.

Obowiązki stron

1. Administrator zobowiązuje się realizować obowiązki informacyjne wobec podmiotów, których dane powierza Przetwarzającemu, w szczególności informować o prawach wynikających z RODO w związku z przetwarzaniem danych osobowych.
2. Podmiot przetwarzający jest zobowiązany do przestrzegania przepisów RODO.
3. Podmiot przetwarzający oświadcza, że przed rozpoczęciem przetwarzania danych przyjmie środki techniczne i organizacyjne mające na celu należyte zabezpieczenie powierzonych danych osobowych stosownie do przepisów, o których mowa w art. 32 RODO.
4. Podmiot przetwarzający przetwarza dane osobowe wyłącznie w sposób określony w Umowie lub na udokumentowane polecenie Administratora, chyba że obowiązek przetwarzania nakłada na niego prawo Unii Europejskiej lub prawo polskie; w takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
5. Podmiot przetwarzający zobowiązuje się do przetwarzania danych zgodnie z Umową, przepisami prawa powszechnie obowiązującego, a w szczególności do:
   1) zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych osobowych,
   2) przetwarzania danych osobowych z uwzględnieniem odpowiednich do zagrożeń oraz kategorii danych objętych ochroną rozwiązań, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
   3) podejmowania wszelkich środków wymaganych na mocy art. 32 RODO, w tym w szczególności:
      a) uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Podmiot przetwarzający wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku,
      b) Podmiot przetwarzający oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,

c) Podmiot przetwarzający podejmuje działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia Administratora lub Podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie dla Administratora, chyba że wymaga tego od niej prawo Unii Europejskiej lub prawo krajowe;

4) prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz środki podjęte na podstawie niniejszego paragrafu;
5) powołania Inspektora Ochrony Danych w przypadku, gdy taki obowiązek wynika z RODO;
6) udostępnienia Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w artykule 28 RODO;
7) umożliwienia audytorowi upoważnionemu przez Administratora, Inspektorowi Ochrony Danych Osobowych powołanemu przez Administratora przeprowadzania audytów, inspekcji i kontroli dokonywanych czynności przetwarzania dokonywanego na podstawie Umowy.

6. Podmiot przetwarzający po zakończeniu przetwarzania danych zobowiązany jest do niezwłocznego usunięcia powierzonych mu danych. Na życzenie Administratora, Podmiot przetwarzający ma obowiązek przedstawić w terminie 7 dni pisemny protokół potwierdzający fakt zniszczenia/usunięcia danych osobowych.
7. Podmiot przetwarzający nie może powierzyć wykonania zadań wynikających z Umowy osobie trzeciej bez uprzedniej zgody Administratora wyrażonej na piśmie, która określać będzie szczegółowe warunki powierzenia.
8. Jeżeli do wykonania w imieniu Administratora konkretnych czynności przetwarzania Podmiot przetwarzający będzie korzystał z usług innego podmiotu przetwarzającego (dalej w umowie zwanego: "subprocesorem"), Podmiot przetwarzający nałoży na subprocesora te same obowiązki dotyczące ochrony danych osobowych jak obowiązki Podmiotu przetwarzającego określone w Umowie. Jeżeli subprocesor nie wywiąże się ze spoczywających na nim obowiązkach ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków subprocesora spoczywa na Podmiocie przetwarzającym.
9. Podmiot przetwarzający przekaże Administratorowi na wezwanie kopię dokumentów wykazujących spełnianie wymogów dotyczących przetwarzania danych osobowych nałożonych prawem.

§ 4.
Uprawnienia informacyjne i kontrola wykonywania Umowy

1. Administratorowi przysługuje prawo kierowania zapytań do Podmiotu przetwarzającego w zakresie prawidłowości wykonania przez Podmiot przetwarzający obowiązków dotyczących zabezpieczenia powierzonych mu na podstawie Umowy danych.
2. Podmiot przetwarzający zobowiązuje się udzielić odpowiedzi na zapytanie, o którym mowa w ust. 1, w terminie 7 dni od daty wpłynięcia zapytania.
3. W przypadku stwierdzenia jakiejkolwiek sytuacji stanowiącej naruszenie lub mogącej stanowić naruszenie bezpieczeństwa danych osobowych Podmiot przetwarzający zobowiązany jest niezwłocznie:
   a) ustalić przyczynę naruszenia,
   b) podjąć wszelkie czynności mające na celu usunięcie naruszenia i zabezpieczenie danych osobowych w sposób należyty przed dalszymi naruszeniami,

c) zebrać wszystkie możliwe dane i dokumenty, które mogą pomóc w ustaleniu okoliczności naruszenia i przeciwdziałaniu podobnym naruszeniom w przyszłości,
d) spełnić wszelkie inne przewidziane prawem obowiązki nałożone na podmioty przetwarzające dane osobowe, w tym, jeżeli jest to wymagane prawem, dokonać zgłoszenia naruszenia do właściwego organu państwowego.

4. Podmiot przetwarzający zobowiązuje się niezwłocznie zawiadomić Administratora o:
   a) o wszystkich naruszeniach lub uzasadnionych podejrzeniach naruszenia ochrony danych osobowych, o których mowa w ust. 3,
   b) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba że zakaz zawiadomienia wynika z przepisów prawa, a w szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia,
   c) każdym nieupoważnionym dostępie do danych osobowych,
   d) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.
5. Administrator ma prawo do kontroli sposobu wykonywania Umowy poprzez przeprowadzenie, zapowiedzianych na 7 dni wcześniej, kontroli dotyczących przetwarzania danych osobowych dokonywanego przez Podmiot przetwarzający oraz żądania składania przez niego pisemnych wyjaśnień.
6. W przypadku wystąpienia sytuacji określonych w §4 ust. 3, Administrator będzie miał prawo dokonać kontroli bez konieczności zachowania terminu, o których mowa w §4 ust 5.
7. Na zakończenie kontroli, o których mowa w ust. 5 i 6, przedstawiciel Administratora sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu Stron. Podmiot przetwarzający może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez Strony.
8. Podmiot przetwarzający zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych, pod rygorem wypowiedzenia umowy, o której mowa w §1 ust. 1 Umowy.

§ 5.
Dostęp do danych oraz upoważniania przetwarzania danych

1. Dostęp do powierzonych danych osobowych mogą posiadać tylko osoby, którym Podmiot przetwarzający nadał upoważnienia do przetwarzania danych.
2. Podmiot przetwarzający zobowiązuje się do prowadzenia rejestru osób upoważnionych do przetwarzania danych. Na żądanie Administratora, Podmiot przetwarzający niezwłocznie udostępni aktualny rejestr osób upoważnionych do przetwarzania powierzonych danych.
3. Podmiot przetwarzający zobowiązuje się zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru danych oraz komu są przekazywane.
4. Podmiot przetwarzający oświadcza, że każda osoba, w tym pracownik etatowy, osoba świadcząca czynności na podstawie umów cywilnoprawnych, inne osoby pracujące na rzecz Podmiotu przetwarzającego, która zostanie dopuszczona do przetwarzania powierzonych przez Administratora danych osobowych zostanie zobowiązana do zachowania wszelkich informacji dotyczących tych danych w tajemnicy. Tajemnica ta obejmuje również wszelkie informacje dotyczące sposobów zabezpieczenia powierzonych do przetwarzania danych osobowych.

§ 6.
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za przetwarzanie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. Odpowiedzialność, o której mowa w ust. 1, obejmuje także odpowiedzialność Podmiotu przetwarzającego za działania subprocesorów, o których mowa w §3 ust. 8 Umowy.
3. W przypadku naruszenia przez Podmiot przetwarzający przepisów prawa powszechnie obowiązującego lub niniejszej Umowy, w następstwie czego Administrator zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny albo jakąkolwiek inną karą, Podmiot przetwarzający zobowiązuje się pokryć poniesioną z tego tytułu szkodę.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność względem osób trzecich i jest zobowiązany do naprawienia szkody powstałej w związku z niezgodnym z prawem lub postanowieniami Umowy przetwarzaniem danych osobowych.
5. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez polski organ nadzorczy. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

§ 7.
Wynagrodzenie

Z tytułu wykonywania usług objętych Umową powierzenia Stronom nie przysługuje odrębne wynagrodzenie poza określonym w § 4 Umowy głównej.

§ 8.
Wejście w życie Umowy i jej rozwiązanie

1. Umowa wchodzi w życie z chwilą podpisania przez Strony.
2. Umowa zostaje zawarta na czas obowiązywania Umowy głównej.
3. Administrator ma prawo rozwiązać Umowę w trybie natychmiastowym na podstawie złożonego przez siebie na piśmie oświadczenia, gdy Podmiot przetwarzający:
   a) przetwarza dane osobowe w sposób niezgodny z Umową,
   b) powierzył przetwarzanie danych osobowych innym podmiotom bez zgody Administratora,
   c) nie zaprzestanie niewłaściwego przetwarzania danych osobowych, pomimo wezwania do takiego zaprzestania,
   d) zawiadomi o swojej niezdolności do dalszego wykonywania Umowy.
4. Podmiot przetwarzający usunie powierzone mu dane osobowe oraz poinformuje Administratora o usunięciu danych osobowych, a także przedstawi protokół usunięcia danych osobowych, niezwłocznie, a najpóźniej w terminie 7 dni:
   a) po wykonaniu usług określonych w § 1 ust. 6 Umowy głównej albo

b) po rozwiązaniu Umowy powierzenia,
którekolwiek nastąpi wcześniej.

§ 9.

Postanowienia końcowe

1. Podmiot przetwarzający wyznacza jako swojego przedstawiciela ……., który jest upoważniony do zarządzania i nadzorowania w jego imieniu Umową powierzenia, odbioru dokumentów wskazanych w § 1 ust. 6 i 7 Umowy głównej oraz bezpośrednich kontaktów z Administratorem. Podmiotowi przetwarzającemu przysługuje prawo do zmiany przedstawiciela. O dokonaniu zmiany przedstawiciela Podmiot przetwarzający powiadomi na piśmie Administratora.
2. W przypadku rozbieżności postanowień Umowy powierzenia i jakiegokolwiek innego dokumentu, postanowienia niniejszej Umowy powierzenia będą miały walor rozstrzygający w stosunku do Stron niniejszej Umowy powierzenia, z zastrzeżeniem późniejszych zmian bezwzględnie obowiązujących przepisów prawa.
3. Jeżeli jakiekolwiek postanowienie Umowy powierzenia jest lub stanie się nieważne w całości lub części, nie będzie to miało wpływu na ważność pozostałych postanowień Umowy powierzenia. W takim przypadku Strony zastąpią nieważne postanowienie ważnym postanowieniem, które będzie odpowiadało w jak najbliższym zakresie celowi nieważnego postanowienia.
4. Wszelkie spory związane z zawarciem lub wykonaniem Umowy powierzenia Strony zgodnie poddają pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby Administratora.
5. Wszelkie zmiany lub uzupełnienia Umowy powierzenia wymagają zachowania formy pisemnej pod rygorem nieważności.
6. W sprawach nieuregulowanych niniejszą umową mają zastosowania przepisy RODO oraz przepisy ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz.U. 1964 nr 16 poz. 93 z późn. zm.) oraz Ustawy o ochronie danych osobowych (Dz.U. 2018 poz. 1000 z późn. zm.).
7. Umowa powierzenia została zawarta w dwóch egzemplarzach po jednym dla każdej ze Stron.

W imieniu i na rzecz Administratora

W imieniu i na rzecz
podmiotu przetwarzającego

ZAŁĄCZNIK NR 9 DO UMOWY

Wykaz Oprogramowania On Premise oraz Oprogramowania SaaS

ZAŁĄCZNIK NR 10 DO UMOWY

Wykaz miejsc w których znajdują się serwery przetwarzających dane przekazywane na podstawie Umowy

ZAŁĄCZNIK NR 11 DO UMOWY

KOŃCOWY PROTOKÓŁ WYKONANIA USŁUGI SOC i WSPARCIA TECHNICZNEGO SYSTEMU

W ramach realizacji Umowy nr …… z dnia ……. r.

Strony potwierdzają co następuje:

- wykonanie usługi **Security Operation Center (SOC)** w okresie od …… do ……

Uwagi Wykonawcy:

……
……

Uwagi Zamawiającego:

……
……

W ramach świadczonej usługi, przez cały okres jej świadczenia którego dotyczy niniejszy protokół, Wykonawca dostarczył i wdrożył oraz zastosował przy świadczeniu Usługi SOC ……. scenariusze bezpieczeństwa
Protokół został sporządzony w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Zamawiający	Wykonawca
….....	……
Miejsce, data	Miejsce, data