**OPIS PRZEDMIOTU ZAMÓWIENIA – część jawna**

**„Dostarczenie, integracja, dostosowanie do potrzeb infrastruktury Zamawiającego oraz produkcyjne uruchomienie oprogramowania na potrzeby Centrum Nadzoru Bezpieczeństwa Teleinformatycznego (ang. SOC – Security Operations Center) dla Śląskiej Sieci Metropolitalnej Sp. z o.o.”**

**Podstawowe wymogi funkcjonalno – użytkowe związane z uruchomieniem Centrum Nadzoru Bezpieczeństwa Teleinformatycznego (ang. SOC – Security Operations Center)   
na potrzeby Śląskiej Sieci Metropolitalnej Sp. z o.o.**

**Cel zadania:**

Celem głównym jest dostarczenie, wdrożenie i produkcyjne uruchomienie oprogramowania typu SIEM (ang. Security Information and Event Management) pozwalającego na prowadzenia ciągłego, stałego nadzoru nad bezpieczeństwem informacji i systemów cyfrowych istotnych z punktu widzenia ciągłości działania, poufności i integralności danych Śląskiej Sieci Metropolitalnej Sp z. o.o. Zakres zamówienia obejmuje także przeprowadzenie szkoleń dla personelu własnego Zamawiającego, zarówno w zakresie użytkowania dostarczonego oprogramowania, jak i możliwości dalszej jego rozbudowy oraz prowadzenia ciągłego procesu dostosowywania do zmieniających się w miarę upływu czasu, potrzeb. Istotną część niniejszego zamówienia stanowi obowiązek dostosowania przez Wykonawcę dostarczonego oprogramowania do potrzeb i infrastruktury Zamawiającego, zarówno pod kątem akwizycji i normalizacji danych wejściowych, jak i reguł korelacji i raportowania wyników ich przetwarzania, w szczególności pod kątem detekcji występujących zagrożeń.

Zamawiający informuje, iż w ramach realizacji celu głównego zadania Wykonawca zobowiązany będzie do skutecznego objęcia nadzorem bezpieczeństwa zarówno infrastruktury biurowej Śląskiej Sieci Metropolitalnej, jak i infrastruktury serwerowo-usługowej Centrum Przetwarzania Danych (chmura prywatna Data Center SSM). Istotnym z punktu widzenia Zamawiającego zagadnieniem jest dostarczenie systemu skalowalnego, umożliwiającego przyszłą rozbudowę.

Celem dodatkowym zadania, w przypadku podjęcia przez Zamawiającego decyzji o poszerzeniu zakresu przedmiotu umowy (prawo opcji) będzie objęcie zakresem funkcjonowania dostarczonego systemu także, dodatkowo, jednego z Kontrahentów Śląskiej Sieci Metropolitalnej Sp. z o.o., wraz   
z całością posiadanej przezeń infrastruktury teleinformatycznej. W tym przypadku również istotną częścią udzielonego zamówienia będzie obowiązek dostosowania przez Wykonawcę dostarczonego oprogramowania do potrzeb i infrastruktury Kontrahenta Śląskiej Sieci Metropolitalnej, zarówno pod kątem akwizycji i normalizacji danych wejściowych, jak i reguł korelacji i raportowania wyników ich przetwarzania, w szczególności pod kątem detekcji występujących zagrożeń. Zamawiający przewiduje, iż Kontrahent objęty zostać powinien wdrożeniem w ramach funkcjonowania tego samego systemu, który uruchomiono na potrzeby Zamawiającego w ramach realizacji celu głównego zadania.

Zamawiający informuje niniejszym, iż jest Operatorem Telekomunikacyjnym świadczącym usługi na potrzeby samorządu Miasta Gliwice. W związku z charakterem pracy Administracji Publicznej zakłada się, iż całość zastosowanego rozwiązania funkcjonować musi w infrastrukturze własnej Śląskiej Sieci Metropolitalnej. Nie dopuszcza się rozwiązań zlokalizowanych w chmurze, wymagających przesyłu  
lub przechowywania informacji objętych ochroną poza infrastrukturą znajdującą się pod bezpośrednią kontrolą Zamawiającego. Całość zadań operacyjnych, związanych z obsługą uruchomionego systemu wykonywana musi być docelowo siłami własnymi Śląskiej Sieci Metropolitalnej. Nie dopuszcza   
się zastosowania modelu bezpieczeństwo jako usługa, realizowanego w całości lub w części przez zewnętrznego Wykonawcę, pozostającego poza bezpośrednią kontrolą administracji Publicznej Miasta Gliwice. Istotną, z punktu widzenia Zamawiającego, funkcjonalnością dostarczonego rozwiązania będzie możliwość raportowania statusu poszczególnych zdarzeń, sporządzania okresowych raportów sumarycznych oraz zabezpieczania materiału dowodowego na potrzeby ewentualnych przyszłych postępowań, typowo obejmujących okres czasu wykraczający poza zakres retencji danych czasu rzeczywistego (praca na danych archiwalnych, lub danych stanowiących materiał zabezpieczony   
w ramach obsługi incydentu).

Zamawiający zakłada wykorzystanie, w trakcie wdrożenie prowadzonego przez Wykonawcę, jako źródeł danych dla systemu minimum mechanizmów Active Directory, EDR i/lub XDR, logów urządzeń sieciowych, w tym urządzeń bezpieczeństwa sieci, kopii informacji o ruchu sieciowym w formie Flowstream lub informacji pochodzących z systemów ADS (Anomaly Detection System) i/lub NDR (Network Detection and Response), logów systemów serwerowych i ich hipernadzorców,   
oraz informacji pochodzących bezpośrednio ze stacji końcowych użytkowników i serwerów (kolekcja przy użyciu agenta systemowego lub natywnych mechanizmów kolekcji logów, wbudowanych   
w system operacyjny).

# **Przedmiotem zamówienia są następujące elementy:**

**(Szczegóły dostępne są w części niejawnej OPZ)**

1. Dostarczenie licencji oprogramowania klasy SIEM (jeżeli zaoferowane rozwiązanie takowych wymaga).
2. Instalacja oprogramowania w infrastrukturze Zamawiającego.
3. Dostosowanie oprogramowania do szczegółowych wymagań Zamawiającego.
4. Świadczenie wsparcia wdrożeniowego w co najmniej następującym zakresie:
   1. Przygotowanie projektu technicznego wdrożenia,
   2. Instalacja i konfiguracja systemu oraz oprogramowania systemowego niezbędnego   
      do funkcjonowania systemu na wszystkich komponentach,
   3. Konfiguracja ustawień systemu,
   4. Asysta przy instalacji i konfiguracji agentów systemu,
   5. Asysta przy konfiguracji rejestracji zdarzeń i generowania logów dla wszystkich źródeł,
   6. Jeśli to konieczne, stworzenie mechanizmów pobierania logów, ich parsowania i klasyfikacji dla wszystkich wymaganych przez Zamawiającego źródeł niestandardowych,
   7. Optymalizacja zbieranych danych,
   8. Analiza środowiska i potrzeb Zamawiającego w zakresie zagrożeń i możliwości detekcji zdarzeń bezpieczeństwa. Przygotowanie listy scenariuszy do implementacji na etapie wdrożenia systemu SIEM,
   9. Budowa bazy zasobów i tożsamości niezbędnej dla prawidłowej korelacji zdarzeń bezpieczeństwa,
   10. Wdrożenie co najmniej pięciu przykładowych scenariuszy bezpieczeństwa wybranych wspólnie z Zamawiającym,
   11. Wykonanie dokumentacji powykonawczej zawierającej uaktualnione informacje z projektu technicznego uzupełnione o procedury, scenariusze i dane istotne, powstałe w czasie prowadzonego wdrożenia,
5. Zapewnienie usługi wsparcia technicznego i usług związanych z usuwaniem ewentualnych usterek systemu (świadczenia gwarancyjne).
6. Organizacja szkoleń dla personelu technicznego Zamawiającego, w tym zarówno szkoleń własnych przeprowadzonych przez Wykonawcę, jak i certyfikowanych szkoleń zakończonych możliwością uzyskania dokumentu stanowiącego dowód kompetencji.
7. Prowadzenie konsultacji w formie treningu przy pracy, których celem będzie zwiększanie kompetencji personelu technicznego Zamawiającego pod kątem produkcyjnej obsługi dostarczonego rozwiązania, oraz ewentualnej przyszłej jego rozbudowy.

**Etapy wdrożenia:**

Zamawiający wymaga realizacji przedmiotu zamówienia w trzech następujących etapach:

1. Etap 1 – realizacja do 31.12.2024 r.
   1. Przygotowanie dokumentacji projektowo-wdrożeniowej;
   2. Dostarczenie, instalacja i konfiguracja oprogramowania SIEM na sprzęcie Zamawiającego;
   3. Integracja z istniejącymi komponentami infrastruktury Zamawiającego w zakresie systemów bezpieczeństwa i nadzoru IT – parsery, scenariusze;
   4. Uruchomienie produkcyjne dostarczonego rozwiązania na potrzeby Centrum Nadzoru Bezpieczeństwa SOC Zamawiającego;
   5. szkolenie pracowników Zamawiającego w zakresie użytkowania dostarczonego rozwiązania, zakończone wydaniem certyfikatu kompetencji wydanego przez dostawcę (6 osób);
   6. Szkolenie pracowników Zamawiającego w trybie „training on the job” w zakresie bieżącego uruchamiania i dostosowywania dostarczonego produktu;
   7. Przygotowanie dokumentacji powdrożeniowej.
2. Etap 2 – realizacja od 01.01.2025 r. do końca trwania umowy
3. wsparcie dostarczonego produktu w zakresie bieżącego utrzymania;
4. 200 roboczogodzin (RBH) do wykorzystania przez Zamawiającego w zakresie bieżącego dostosowywania produktu do potrzeb Zamawiającego z uwzględnieniem bieżącego szkolenia pracowników Zamawiającego w trybie „*training on the job*”   
   w zakresie dokonywanych zmian i obsługi dostarczonego rozwiązania.
5. Etap 3 – etap ten jest związany z realizacją zadań wynikających ze skorzystania Zamawiającego z „prawa opcji” - termin realizacji tych zadań musi zamknąć się do końca okresu obowiązywania umowy. Zamawiający poinformuje wykonawcę o zamiarze skorzystania z prawa opcji najpóźniej na 3 miesiące przed zakończeniem terminu obowiązywania umowy. Zakres etapu 3 stanowią:
   1. dostarczenie dodatkowych licencji oprogramowania dla integracji z monitorowaną przez Zamawiającego infrastrukturą podmiotu zewnętrznego (zgodnie z tabelą opisaną w części niejawnej OPZ);
   2. szkolenie pracowników Zamawiającego w zakresie użytkowania i administrowania dostarczonym rozwiązaniem, zakończone możliwością uzyskania certyfikatu kompetencji wydanego przez producenta rozwiązania;
   3. do 200 roboczogodzin (RBH) do wykorzystania przez Zamawiającego w zakresie bieżącego dostosowywania produktu do potrzeb Zamawiającego (w tym m. in. personalizacja, rekonfiguracja bazowych ustawień oraz dostosowanie do objęcia nadzorem nowych elementów infrastruktury) z uwzględnieniem bieżącego szkolenia osób wskazanych przez Zamawiającego w trybie „training on the job” w zakresie dokonywanych zmian i obsługi dostarczonego rozwiązania.

Zamawiający zastrzega sobie prawo do swobodnego określenia zakresu „prawa opcji” jednak   
w ilościach nie wyższych jak zdeklarowane powyżej.