Opis przedmiotu zamówienia

Świadczenie usługi centrum operacji bezpieczeństwa

Przedmiot zamówienia dotyczy realizacji projektu pn.: „Cyberbezpieczny Rząd – Ministerstwo Rodziny, Pracy i Polityki Społecznej”, którego celem jest poprawa cyberbezpieczeństwa w Ministerstwie Rodziny, Pracy i Polityki Społecznej (MRPiPS) poprzez realizacje przedsięwzięć z obszaru organizacyjnego, kompetencyjnego i technicznego, współfinansowanego przez Unię Europejską w ramach programu Krajowy Plan Odbudowy i Zwiększania Odporności, w konkursie grantowym pn. „Cyberbezpieczny Rząd”.

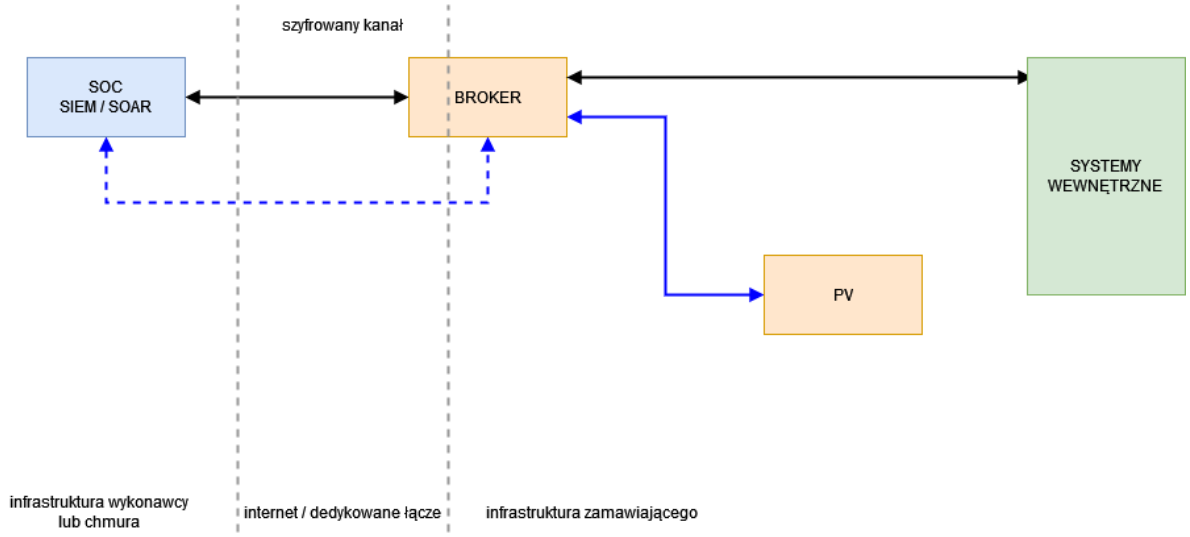
Przedmiot zamówienia

1. Założenia i wymagania ogólne
   1) W celu wzmocnienia odporności Ministerstwa Rodziny, Pracy i Polityki Społecznej na cyberataki, Zamawiający zleca świadczenie usług zarządzanych w zakresie cyberbezpieczeństwa, opartych o centrum operacji bezpieczeństwa (SOC – Security Operations Center) działające całodobowo – 24 godziny na dobę, 7 dni w tygodniu, przez cały rok (tryb 24/7/365) – które będzie odpowiadało za realizację działań związanych z zarządzaniem ryzykiem w cyberbezpieczeństwie, w tym:
      a) świadczenie usługi cyberbezpieczeństwa wraz z audytami bezpieczeństwa i testami penetracyjnymi, szkoleniami dla personelu Zamawiającego i raportowaniem,
      b) uruchomienie i utrzymanie systemów SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response) i PV (Password Vault) lub rozwiązania łączącego funkcjonalności tych systemów oraz brokera komunikacyjnego zapewniającego separację środowiska Wykonawcy i środowiska Zamawiającego;
   2) Usługa SOC powinna spełniać wymagania opisane w niniejszym dokumencie, a zaproponowane rozwiązanie powinno posiadać architekturę jak na Rys. 1. Dopuszcza się dodanie innych rozwiązań dla zwiększenia bezpieczeństwa poniższych przepływów, ale każde inne rozwiązanie dopuszczalne jest wyłącznie po uzyskaniu akceptacji Zamawiającego. Komunikacja między infrastrukturą Wykonawcy i Zamawiającego powinna być szyfrowana. Wykonawca powinien zapewnić niezawodną komunikację z infrastrukturą Zamawiającego. Dopuszcza się zastosowanie dedykowanego łącza do infrastruktury Zamawiającego, jeśli Wykonawca dysponuje takim łączem. Zamawiający dopuszcza uruchomienie usługi w chmurze, pod warunkiem że cała usługa będzie umieszczona w Europejskim Obszarze Gospodarczym;
   3) Raporty zawierające informacje na temat podatności lub incydentów, dotyczące infrastruktury Zamawiającego oraz raporty miesięczne będą przekazywane przez Wykonawcę w sposób bezpieczny, jako informacje wymagające szczególnej ochrony o charakterze niejawnym.
2. Wymagania w zakresie świadczenia usługi SOC
   1) uruchomienie i utrzymanie systemu SIEM służącego do zbierania i korelacji logów ze źródeł Zamawiającego (900 serwerów Windows/Linux, 100 urządzeń sieciowych, 1000 stacji roboczych użytkowników), zgodnie ze specyfikacją opisaną w dokumencie, przy zachowaniu harmonogramu i bez limitu reguł korelacyjnych;
   2) uruchomienie i utrzymanie systemu SOAR służącego do reagowania na incydenty raportowane przez system SIEM, zgodnie ze specyfikacją opisaną w dokumencie, przy zachowaniu

harmonogramu, bez limitu zautomatyzowanych reakcji na incydenty (playbooków) i akcji z nich wynikających;

3) przeprowadzenie audytu i analizy infrastruktury Zamawiającego określających systemy kluczowe dla cyberbezpieczeństwa w celu ich monitorowania oraz priorytetyzacja systemów ze względu na termin ich podłączenia do systemu SIEM;
4) podłączenie do systemu SIEM systemów i urządzeń Zamawiającego;

Rys. 1 Schemat architektury rozwiązania




5) wykonanie playbooków dla uruchomionego systemu SOAR zapewniającego zabezpieczenie systemów Zamawiającego, z wykorzystaniem rozwiązań bezpieczeństwa stosowanych przez Zamawiającego (UTM, WAF, AV+EDR, AD, IPS/IDS, system antyspamowy, QRadar); w ramach wdrożenia Wykonawca zobowiązany jest do przeprowadzenia audytu, wskazującego inne, ważne z punktu widzenia cyberbezpieczeństwa systemy, które należy objąć systemem SOAR; Wykonawca zobowiązany jest również do wskazania zmian i optymalizacji w konfiguracji wykorzystywanych urządzeń bezpieczeństwa Zamawiającego, w celu wykorzystania pełnego potencjału tych rozwiązań w ramach usługi SOC;
6) Zamawiający zakłada, że w ciągu każdego roku trwania umowy do obsługi może zostać dołączonych kolejnych 30 źródeł logów;
7) uruchomienie i utrzymanie w infrastrukturze Zamawiającego systemu PV pozwalającego na przechowywanie co najmniej 5000 poświadczeń i z dostępem dla co najmniej 3 administratorów Zamawiającego;
8) wdrożenie oprogramowania pośredniczącego broker bez limitów związanych z jego użytkowaniem;
9) Zamawiający dopuszcza zastosowanie rozwiązania łączącego funkcjonalności uruchamianych i utrzymywanych systemów, pod warunkiem że rozwiązanie to spełnia wymagania dotyczące poszczególnych systemów, opisane w dalszej części dokumentu.
10) świadczenie usługi pierwszej linii wsparcia (SOC-L1), w trybie 24/7/365, monitorowanie infrastruktury i systemów IT, korelacja zdarzeń, identyfikacja zdarzeń potencjalnie niebezpiecznych, wykrywanie i informowanie o incydentach, z czasem reakcji 30 minut; Wykonawca zapewnia Zamawiającemu:
    a) przekazywanie informacji o potencjalnych incydentach wypracowanym kanałem komunikacji,

b) dostęp do monitorowania SIEM i SOAR w trybie 24/7/365, w uzgodnionym zakresie,
c) obsługę zgłoszeń we własnym systemie ITSM wraz z jego utrzymaniem dla użytkowników i administratorów Zamawiającego,
d) możliwość definiowania własnych reguł korelacyjnych SIEM,
e) monitorowanie potencjalnych naruszeń bezpieczeństwa IT,
f) przyjmowanie zgłoszeń o podejrzanych aktywnościach od personelu Zamawiającego,
g) przeprowadzanie wstępnej analizy i eliminacji fałszywych alertów,
h) współpracę z drugą linią wsparcia oraz z administratorami lokalnymi,
i) przekazywanie uzgodnionych informacji o incydentach do CSIRT NASK i wypełnianie w imieniu Zamawiającego obowiązków wynikających z ustawy z dnia 10 czerwca 2016 r. *o działaniach antyterrorystycznych* w zakresie stopni alarmowych CRP i monitorowania systemów informatycznych oraz wsparcie Zamawiającego w wypełnianiu zaleceń wynikających z ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* wraz z jej planowaną nowelizacją;

11) świadczenie usługi drugiej linii wsparcia (SOC-L2), w dni robocze, w godzinach 8:00-16:00, przy czym działania niezakończone do godz. 16:00 są kontynuowane od godz. 8:00 w następnym dniu roboczym (tryb 8/5), z czasem reakcji 60 minut;
Wykonawca zapewnia Zamawiającemu:
a) przygotowanie z administratorami lokalnymi Zamawiającego scenariuszy reakcji na incydenty, wynikające z reguł korelacyjnych,
b) przygotowanie z administratorami lokalnymi Zamawiającego planów postępowania z incydentami,
c) analizę zdarzeń i obsługę incydentów, zebranie informacji niezbędnych do poprawnego obsłużenia incydentu, weryfikację poprawności i kompletności dostarczonych danych źródłowych,
d) wydanie zaleceń i opracowanie scenariusza mitygacji ryzyka wynikającego z incydentu oraz wsparcie administratorów IT przy realizacji przygotowanego scenariusza,
e) opracowanie wniosków z incydentu, mających na celu ograniczenie możliwości powtórzenia się danego typu incydentu w przyszłości,
f) przygotowanie planu działania w celu ograniczenia strat związanych z incydentem, pozyskanie dodatkowych danych niezbędnych do obsługi incydentu (z SOC-L1, z logów systemowych, ze źródeł zewnętrznych, takich jak CSIRT, użytkowników i innych),
g) proponowanie nowych reguł korelacyjnych i scenariuszy SIEM oraz playbooków SOAR do wdrożenia w systemie SIEM/SOAR i propozycje optymalizacji aktualnie działających scenariuszy bezpieczeństwa,
h) proponowanie rozszerzenia zakresu monitorowania o kolejne systemy teleinformatyczne Zamawiającego, przygotowywanie raportów dla Zamawiającego i jego dostawców,
i) Wykonawca może w ramach usługi SOC-L2 uruchamiać okresowe testy podatności,
j) Wykonawca może dokonywać niezautomatyzowanej analizy logów Zamawiającego w celu proaktywnego poszukiwania incydentów i zabezpieczenia materiałów po incydencie,
k) wydawanie rekomendacji w zakresie poprawy bezpieczeństwa systemów i infrastruktury Zamawiającego, a w szczególności możliwości wdrożenia rozwiązań bezpieczeństwa zgodnych z metodyką DiD – Defense-in-Depth opracowaną przez Amerykańską Agencję Bezpieczeństwa (NSA);

12) świadczenie usługi SOC-L2 SOAR 24/7/365 z opracowanych playbooków, przy czasie reakcji 15 minut, polegającej na wsparciu w zakresie zautomatyzowanej reakcji na incydenty; Wykonawca zapewnia Zamawiającemu przygotowanie liczby playbooków, pozwalającej

na zautomatyzowane reagowanie na incydenty wykryte w systemach i infrastrukturze Zamawiającego wraz z ich bieżącą aktualizacją;

13) świadczenie usługi trzeciej linii wsparcia (SOC-L3) w wymiarze 120 rbh/rok (przy czym niewykorzystane roboczogodziny przechodzą na lata kolejne), z czasem reakcji 8 godzin, która obejmuje:
    a) pomoc zdalną lub na miejscu w zakresie usunięcia skutków zaistniałego incydentu,
    b) rekomendacje w zakresie zachowania materiału dowodowego dla Zamawiającego wraz z pełną analizą powłamaniową,
    c) analizę złośliwego oprogramowania;
14) w przypadku niewykorzystania roboczogodzin na zadania SOC-L3, Zamawiający może zlecić w ramach umowy:
    a) dodatkowe testy penetracyjne np. nowo wdrażanych systemów,
    b) doradztwo w zakresie architektury systemów i sieci,
    c) doradztwo w zakresie niezbędnych do wdrożenia dodatkowych zabezpieczeń,
    d) doradztwo w zakresie stosowania przepisów prawa związanych z cyberbezpieczeństwem (dyrektywa NIS2, ustawa o KSC, ustawa o działaniach antyterrorystycznych);
15) uruchomienie usługi CTI do wszystkich reguł SIEM i playbooków SOAR, w ramach której Zamawiający oczekuje wzbogacania danych w regułach SIEM i playbookach SOAR o wskaźniki naruszenia (IoC – Indicators of Compromise) pochodzące z CSIRT krajowych, takich jak CSIRT-NASK lub CERT dostawcy wdrożonego rozwiązania; wymiana i synchronizacja tych danych powinna być zautomatyzowana, dodatkowo, w wypadku stwierdzenia podatności aplikacji, bądź systemów Zamawiającego, powinna zostać wykonana analiza ryzyka, pod kątem możliwości ich wykorzystania w oparciu o publiczne PoC lub gotowe exploity;
16) wykonanie audytów podatności zgodnie z poniższymi wymaganiami:
    a) wykonanie audytu i raportu podatności co 6 miesięcy w zakresie infrastruktury zewnętrznej Zamawiającego (do 30 publicznych adresów IP) oraz co 12 miesięcy w zakresie infrastruktury wewnętrznej i stacji roboczych Zamawiającego – raporty muszą obejmować całą infrastrukturę serwerową, w tym wirtualną, kluczowe urządzenia i stacje robocze wykorzystywane przez użytkowników Zamawiającego (zakres infrastruktury kluczowej i kluczowych stacji roboczych zostanie ustalony w czasie wstępnego audytu),
    b) zarządzanie podatnościami w systemach i infrastrukturze Zamawiającego wraz z przekazywaniem na bieżąco rekomendacji z podziałem na podatności wysokiego ryzyka – konieczne do usunięcia (niemożliwe jest ich monitorowanie i zabezpieczenie systemów), średniego ryzyka (włączone do stałego monitorowania, ale generujące ryzyka), podatności niskiego ryzyka – bezpieczne w przypadku monitorowania;
17) szkolenie online dla pracowników Zamawiającego z zakresu cyberbezpieczeństwa – zawierające informacje o współczesnych zagrożeniach, socjotechnice, phishingu, ransomware, DDOS, malware, jak rozpoznać ataki, wskazanie dobrych nawyków zwiększających bezpieczeństwo w biurze i poza biurem oraz świadomość zagrożenia cyberatakami – co najmniej 1 raz w roku dla każdego pełnego roku trwania umowy, czas trwania co najmniej 3 godziny; w szkoleniu może uczestniczyć do 1000 pracowników Zamawiającego; Zamawiający dopuszcza szkolenie w wersji e-learningowej, przy czym w przypadku wersji e-learningowej platformę do szkoleń wraz z treściami zapewnia Wykonawca – Wykonawca zobowiązany jest w takim przypadku do udostępnienia indywidualnych kont dla szacowanej liczby pracowników Zamawiającego wraz z dostarczeniem raportu dotyczącego przeszkolonych osób po zakończeniu szkolenia; w przypadku szkolenia online grupa pracowników zostanie

ograniczona w sposób umożliwiający przeszkolenie osób kluczowych (liderów systemów informatycznych, kierownictwa);

18) szkolenie online dla wskazanych maksymalnie 10 przedstawicieli najwyższego kierownictwa Zamawiającego z zakresu cyberhigieny, wymagań ustawy o KSC i innych aktów prawnych związanych z cyberbezpieczeństwem, dobrych praktyk – raz w roku dla każdego pełnego roku trwania umowy, czas trwania co najmniej 3 godziny; szczegółowy zakres szkolenia ustalany będzie każdorazowo z Zamawiającym;
19) szkolenie online dla wskazanych maksymalnie 10 administratorów i kadry IT Zamawiającego z zakresu wykorzystywania zaproponowanych narzędzi, obserwowania i reakcji na incydenty, mitygowania podatności – co najmniej raz w roku dla każdego pełnego roku trwania umowy, czas trwania co najmniej 7 godzin;
20) Raportowanie:
    a) każdorazowo przy wystąpieniu incydentu – raport, który zawiera informacje o incydencie, wpływ na środowisko Zamawiającego, sposoby mitygacji,
    b) miesięczny raport w zakresie wykonywanej usługi, który zawiera listę zaobserwowanych zdarzeń w podziale na kategorie zdarzeń (DDoS, ransomware, phishing, brute force, itp.) oraz wykorzystane zabezpieczenia,
    c) miesięczny raport zawierający informacje o stosunku zdarzeń będących fałszywymi alertami do alertów prawidłowych (*false positive vs true positive*) z każdej reguły korelacyjnej wraz z rekomendacją ewentualnych zmian;
21) na każde żądanie Zamawiającego wyrażone w czasie trwania umowy, przekazanie Zamawiającemu reguł korelacyjnych w standardzie Sigma Rules opartym o YAML, scenariuszy działań i playbooków pozwalających na wykorzystanie przez innego dostawcę usług zarządzanych w zakresie cyberbezpieczeństwa;
22) działania SOC-L3, ich zakres i niezbędna liczba roboczogodzin wymagają każdorazowej akceptacji Zamawiającego, chyba że incydent wymaga natychmiastowej reakcji w godzinach niedostępności Zamawiającego; w takim przypadku Zamawiający wymaga szczegółowego raportu wraz z uzasadnieniem wykorzystanych roboczogodzin;
23) w przypadku konieczności zwiększenia wartości umowy aneksem, koszt roboczogodziny będzie ustalony na podstawie formularza ofertowego.

3. Wymagania w zakresie uruchomienia i utrzymania systemów SIEM i SOAR lub rozwiązania łączącego funkcjonalności tych systemów
    1) wdrożone systemy SIEM/SOAR muszą być produktami komercyjnymi, oferowanymi na rynku wraz ze wsparciem producenta rozwiązania; wyklucza się rozwiązania pozbawione wsparcia producenta;
    2) Wykonawca jest zobowiązany dostarczyć/posiadać wszystkie niezbędne licencje do uruchomienia systemów SIEM/SOAR pozwalające na świadczenie usług, na czas trwania umowy, w tym licencje na bazę danych i inne niezbędne;
    3) w przypadku licencji czasowych, po zakończeniu umowy, Zamawiający powinien mieć możliwość pozyskania licencji na zaproponowany system SIEM/SOAR na wolnym rynku (od innego dostawcy) – w przypadku gdyby podczas zbliżania się końca umowy systemy lub ich elementy nie były dostępne na rynku, Wykonawca zobowiązuje się do zaproponowania innego rozwiązania dostępnego na rynku i spełniającego wymagania OPZ;
    4) systemy SIEM/SOAR muszą umożliwić autoryzację użytkowników oraz precyzyjne nadawanie uprawnień dla administratorów i użytkowników oraz zapewniać pełną ich rozliczalność

co najmniej w zakresie: login/logoff, zmiana konfiguracji systemu, wykonane akcje; Zamawiający oczekuje dostępu co najmniej read-only do systemów;

5) system SIEM powinien:
   a) pozwolić na zbieranie logów z systemów Zamawiającego, w tym pozwolić na zbieranie informacji z końcówek i systemów EDR, w szczególności ESET oraz z urządzeń UTM, w szczególności Cisco/Fortinet/Palo Alto;
   b) umożliwiać liczbę równocześnie zalogowanych operatorów/użytkowników bez ograniczeń;
   c) posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healthcheck);
   d) umożliwiać uwierzytelnienie oraz szyfrowanie połączenia między wszystkimi komponentami systemu;
   e) umożliwiać budowanie profili aktywności użytkowników oraz zasobów IT poprzez słowniki referencyjne i wykorzystywać je w regułach korelacyjnych i raportowaniu;
6) Wykonawca powinien dostosowywać na bieżąco reguły korelacyjne do zmieniającego się środowiska Zamawiającego, tak aby maksymalizować wykrywanie incydentów i minimalizować fałszywe alerty;
7) system SOAR powinien:
   a) móc wykonywać akcje na końcówkach z wykorzystaniem wymienionych wyżej systemów EDR oraz urządzeń UTM,
   b) zapewniać możliwości orkiestracji i automatyzacji bezpieczeństwa oraz odpowiedzi na incydenty,
   c) natywnie integrować się z dostarczonym systemem SIEM, tj. producent oprogramowania SOAR powinien oficjalnie wspierać integrację z dostarczanym rozwiązaniem SIEM, lub powinien stanowić jego część;
8) Wykonawca powinien dostosowywać na bieżąco playbooki do zmieniającego się środowiska Zamawiającego, tak aby maksymalizować automatyczną reakcję na incydenty;
9) aktywność użytkowników systemu SOAR powinna być śledzona i logowana na potrzeby ewentualnej analizy;
10) system SOAR nie może przechowywać haseł do systemów i urządzeń Zamawiającego;
11) każdorazowa potrzeba sięgnięcia przez system SOAR do aplikacji / systemu / urządzenia Zamawiającego powinna wiązać się z uzyskaniem danego poświadczenia z PV na czas niezbędny do wykonania akcji przez SOAR;
12) dostęp sieciowy systemu SOAR do aplikacji / systemów / urządzeń Zamawiającego powinien odbywać się przez oprogramowanie pośredniczące zainstalowane w środowisku Zamawiającego, które umożliwi komunikację sieciową między wewnętrznymi sieciami Zamawiającego, a systemem SOAR;
13) Zamawiający nie dopuszcza bezpośrednich przejść sieciowych z systemu SOAR do wewnętrznych sieci Zamawiającego, a jedynie przez oprogramowanie pośredniczące, które pracując jako broker powinno umożliwiać ten dostęp i przekazywać odpowiedzi z sieci Zamawiającego do systemu SOAR.

4. Wymagania w zakresie uruchomienia i utrzymania systemu PV
   1) wdrożony PV powinien być produktem komercyjnym, oferowanym na rynku wraz ze wsparciem producenta rozwiązania; wyklucza się rozwiązania pozbawione wsparcia producenta;
   2) Wykonawca jest zobowiązany dostarczyć wszystkie niezbędne licencje do uruchomienia PV, na czas trwania umowy, w tym licencje na bazę danych i inne niezbędne; dopuszcza się licencje wieczyste;

3) w przypadku licencji czasowych, po zakończeniu umowy Zamawiający powinien mieć możliwość pozyskania licencji na zaproponowany PV na wolnym rynku (od innego dostawcy) – w przypadku gdyby podczas zbliżania się końca umowy system lub jego elementy nie były dostępne na rynku, Wykonawca zobowiązuje się do zaproponowania innego rozwiązania dostępnego na rynku i spełniające wymagania OPZ;
4) administratorami PV muszą być pracownicy Zamawiającego;
5) PV ma zapewniać centralne przechowywanie, uzyskiwanie dostępu i dystrybucję poświadczeń służących do uwierzytelnienia, takich jak: tokeny, hasła, certyfikaty, klucze szyfrowania;
6) PV ma umożliwiać:
   a) bezpieczne wstrzykiwanie poświadczeń do aplikacji,
   b) synchronizowanie przepływów poświadczeń między systemem SOAR a aplikacjami i urządzeniami Zamawiającego;
7) PV powinien zapewnić:
   a) pełną rozliczalność użycia poświadczeń przez system SOAR oraz administratorów;
   b) aby pracownicy Wykonawcy nie mieli możliwości uzyskania dostępu do poświadczeń zapisanych w systemie.

5. Wymagania w zakresie uruchomienia i utrzymania systemu pełniącego rolę brokera komunikacyjnego
   1) Wykonawca jest zobowiązany dostarczyć wszystkie niezbędne licencje do uruchomienia brokera, na czas trwania umowy, w tym licencje na bazę danych i inne niezbędne;
   2) po zakończeniu umowy Zamawiający powinien mieć możliwość pozyskania licencji na zaproponowanego brokera komunikacyjnego na wolnym rynku (od innego dostawcy) – w przypadku gdyby podczas zbliżania się końca umowy system lub jego elementy nie były dostępne na rynku, Wykonawca zobowiązuje się do zaproponowania innego rozwiązania dostępnego na rynku i spełniającego wymagania OPZ;
   3) broker komunikacyjny ma zapewnić bezpieczną komunikację między infrastrukturą Wykonawcy a Zamawiającego, niedopuszczalny jest bezpośredni dostęp systemów uruchamianych przez SOC do systemów wewnętrznych Zamawiającego;
   4) projekt rozwiązania Wykonawca przedstawi Zamawiającemu do akceptacji podczas etapu audytowania i analizy.
6. Harmonogram
   1) Wdrożenie wszystkich wymagań i funkcjonalności określonych umową nastąpi w ciągu 6 miesięcy od dnia zawarcia umowy;
   2) Czas ten dzieli się na następujące etapy:
      a) przeprowadzenie audytu i analizy infrastruktury Zamawiającego ustalających systemy kluczowe oraz priorytety systemów (wysoki, średni, niski) podłączanych do systemów SIEM/SOAR – 1 miesiąc od dnia zawarcia umowy,
      b) uruchomienie systemów SIEM/SOAR, PV i brokera komunikacyjnego – 2 miesiące od dnia zawarcia umowy,
      c) podłączenie do systemu SOAR zabezpieczeń stosowanych przez Zamawiającego w celu automatycznej reakcji na incydenty – 3 miesiące od dnia zawarcia umowy,
      d) podłączenie do systemu SIEM systemów Zamawiającego o priorytecie wysoki – 3 miesiące od dnia zawarcia umowy,
      e) podłączenie do systemu SIEM systemów Zamawiającego o priorytecie średni – 4 miesiące od dnia zawarcia umowy,
      f) podłączenie do systemu SIEM systemów Zamawiającego o priorytecie niski lub ich części zgodnie z wymaganiami OPZ – 5 miesięcy od dnia zawarcia umowy;

g) uruchomienie usługi CTI dla systemów SIEM/SOAR;

3) W czasie trwania umowy Wykonawca będzie doskonalił wspólnie z Zamawiającym systemy bezpieczeństwa i reguły automatycznej reakcji na incydenty, tak aby maksymalnie wzmocnić bezpieczeństwo Zamawiającego;
4) Przynajmniej raz w roku Wykonawca przeprowadzi szkolenie dla personelu Zamawiającego (konkretny termin przeprowadzenia szkoleń określony zostanie w Harmonogramie szkoleń, po zawarciu umowy);
5) Przynajmniej raz w roku Wykonawca przeprowadzi szkolenie dla najwyższego kierownictwa Zamawiającego (konkretny termin przeprowadzenia szkoleń określony zostanie w Harmonogramie szkoleń, po zawarciu umowy);
6) Przynajmniej raz w roku Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego (konkretny termin przeprowadzenia szkoleń określony zostanie w Harmonogramie szkoleń, po zawarciu umowy);
7) Wykonawca będzie przekazywał raporty z wykonanej usługi zgodnie z pkt 2.20;
8) Terminy i sposoby przekazania raportów zostaną ustalone między Wykonawcą a Zamawiającym.
9) Terminy audytów podatności zostaną ustalone z Zamawiającym.
10) Działania dodatkowe w ramach roboczogodzin zostaną każdorazowo ustalone między Wykonawcą a Zamawiającym zgodnie z wymaganiami OPZ.

7. Parametry świadczenia usług – czasy maksymalne

| **Zadanie** | **Tryb pracy** | **Czas reakcji** | **Czas realizacji** |
|---|---|---|---|
| SOC-L1, podjęcie działań związanych z incydentem, rozwiązanie incydentu polegające na zatrzymaniu zagrożenia lub przekazanie do SOC-L2 | 24/7/365 (całodobowo) | 30 min | 2 godz. |
| SOC-L2, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie realizacji lub przekazanie do SOC-L3 | 8/5 – w dni robocze, w godzinach pracy 8:00 – 16:00 | 60 min | 8 godz. |
| SOC-L2 SOAR, zautomatyzowane podjęcie incydentu i aplikacja rozwiązania zatrzymującego zagrożenie w czasie realizacji | 24/7/365 (całodobowo) | 15 min | 1 godz. |
| SOC-L3, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie realizacji | wg potrzeby | 8 godz. | 40 godz. |

**Zamawiający zastrzega sobie prawo do wykonania audytu w siedzibie Wykonawcy lub przeprowadzenia testów potwierdzających świadczenie usług na wskazanym poziomie.**