Nr sprawy: WZP.271.31.2024.B

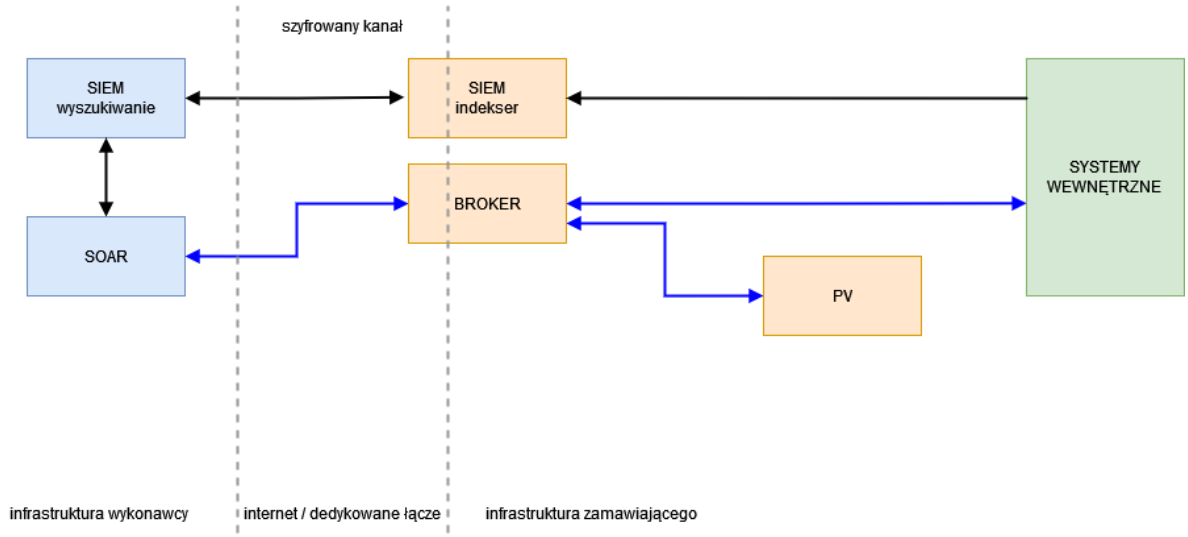
Załącznik nr 1 – Opis przedmiotu zamówienia (zakres umowy)

1) Założenia i wymagania ogólne

Chcąc wzmocnić odporność Urzędu Miasta Bydgoszczy na cyberataki Zamawiający zleca wykonanie usługi cyberbezpieczeństwa opartej o Security Operations Center (SOC) działający w reżimie 24h/7 dni w tygodniu, który będzie odpowiadał za realizację następujących zadań:

1) świadczenie usługi cyberbezpieczeństwa wraz z audytami bezpieczeństwa i testami penetracyjnymi, szkoleniami dla personelu Zamawiającego i raportowaniem,
2) wdrożenie, uruchomienie i utrzymanie systemu klasy SIEM (Security Information and Event Management),
3) wdrożenie, uruchomienie i utrzymanie systemu klasy SOAR (Security Orchestration, Automation and Response),
4) wdrożenie, uruchomienie i utrzymanie systemu klasy Password Vault,
5) wdrożenie, uruchomienie i utrzymanie systemu pełniącego rolę brokera komunikacyjnego.

Usługa SOC musi spełniać wymagania opisane w poniższym dokumencie, a zaproponowane rozwiązanie musi posiadać architekturę jak na poniższym diagramie. Dopuszcza się dodanie innych rozwiązań jak UTM, WAF dla zwiększenia bezpieczeństwa poniższych przepływów. Każde inne rozwiązanie dopuszczalne jest wyłącznie po uzyskaniu akceptacji zamawiającego. Komunikacja między infrastrukturą wykonawcy i zamawiającego musi być szyfrowana. Dopuszcza się zastosowanie dedykowanego łącza do infrastruktury zamawiającego o ile takim łączem dysponuje wykonawca. Cała usług uruchomiona jako usługa musi być umieszczona w Europejskim Obszarze Gospodarczym.



Poszczególne zadania muszą spełniać opisane poniżej wymagania oraz być wdrożone zgodnie z harmonogramem określonym w dokumencie.

2) Wymagania w zakresie świadczenia usługi cyberbezpieczeństwa

Tabela 1 Wymagania w zakresie świadczenia usługi cyberbezpieczeństwa

Wymaganie	Nazwa i Opis
SOC-1	wdrożenie, uruchomienie i utrzymanie systemu klasy SIEM zgodnie ze specyfikacją opisaną w dokumencie przy zachowaniu harmonogramu i bez limitu reguł korelacyjnych
SOC-2	wdrożenie, uruchomienie i utrzymanie systemu klasy SOAR zgodnie ze specyfikacją opisaną w dokumencie przy zachowaniu harmonogramu i wraz z liczbą playbooków zgodną z ofertą Wykonawcy i akcji z nich wynikające. Minimalna liczba playbooków to 20.
SOC-3	podłączenie do systemu SIEM systemów i urządzeń Zamawiającego opisanych w załączniku nr 2 do umowy zgodnie z opisanym tam zakresem monitorowania, w ramach wdrożenia wykonawca zobowiązany jest do przeprowadzenia audytu/ankietowania, które wskaże inne ważne z punktu widzenia cyberbezpieczeństwa systemy, które należy monitorować, dodatkowo, jeżeli audyt wskaże konieczność zastosowania rozwiązania WAF w zaproponowanej architekturze systemów SIEM/SOAR, to wykonawca zobowiązany jest skonfigurować urządzenie posiadane przez zamawiającego, audyt wskaże również, którym systemom przypisany zostanie wysoki, średni i niski priorytet w zakresie czasu podłączenia do systemu SIEM
SOC-4	wykonanie playbooków dla wdrożonego systemu SOAR zapewniającego zabezpieczenie systemów Zamawiającego opisanych w załączniku nr 2 do umowy z wykorzystaniem rozwiązań bezpieczeństwa stosowanych przez zamawiającego i opisanych w załączniku nr 3 w liczbie ___ (zgodnie z ofertą Wykonawcy), w ramach wdrożenia wykonawca zobowiązany jest do przeprowadzenia audytu/ankietowania, które wskaże inne ważne z punktu widzenia cyberbezpieczeństwa systemy, które należy objąć systemem SOAR, wykonawca zobowiązany jest również do konfiguracji wykorzystywanych urządzeń zamawiającego opisanych w załączniku nr 3 typu UTM, WAF, XDR, AV i innych w celu wykorzystania pełnego potencjału tych rozwiązań w ramach SOC
SOC-5	Zamawiający zakłada, że w ciągu trwania umowy do obsługi może zostać dołączonych kolejnych 30 systemów i/lub urządzeń
SOC-6	wdrożenie, uruchomienie i utrzymanie w infrastrukturze Zamawiającego opisanej w załączniku nr 4 do umowy systemu klasy Password Vault bez limitu na ilość poświadczeń przechowywanych i użytkowników systemu
SOC-7	wdrożenie oprogramowania pośredniczącego typu broker bez limitów związanych z użytkowaniem
SOC-8	wdrożenie oprogramowania typu indekser, służącego do normalizacji logów i parsowania oraz tworzenia indeksów umożliwiających szybkie wyszukiwanie
SOC-9	świadczenie usługi pierwszej linii wsparcia SOC - L1, całodobowe 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:

	• przekazywanie informacji o potencjalnych incydentach wypracowanym kanałem komunikacji • dostęp do konsoli monitorowania SIEM 24/7/365 w uzgodnionym zakresie • obsługę zgłoszeń w systemie ITSM wraz z jego utrzymaniem dla użytkowników i administratorów zamawiającego • dostęp do bazy wiedzy i rejestru konfiguracji, opisującego monitorowane systemy i urządzenia (CMDB), w ramach systemu ITSM • możliwość definiowania własnych reguł korelacyjnych SIEM • monitorowanie potencjalnych naruszeń bezpieczeństwa IT • przyjmowanie zgłoszeń o podejrzanych aktywnościach od personelu Zamawiającego • przeprowadzanie wstępnej analizy i eliminacji fałszywych alarmów • współpraca z II linią wsparcia SOC oraz z administratorami lokalnymi. • 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 Zamawiającym w wypełnianiu zaleceń wynikających z ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* wraz z jej planowaną nowelizacją
SOC-10	świadczenie usługi drugiej linii wsparcia SOC - L2, 8/5 w dni robocze w godzinach 8:00-16:00 z czasem reakcji 1 godzina Wykonawca zapewnia zamawiającemu: • przygotowanie z administratorami lokalnymi Zamawiającego scenariuszy reakcji na incydenty wynikające z reguł korelacyjnych • przygotowanie z administratorami lokalnymi Zamawiającego planów postępowania z incydentami • analiza zdarzeń i obsługa incydentów, zebranie informacji niezbędnych do poprawnego obsłużenia incydentu, weryfikacja poprawności i kompletności dostarczonych danych źródłowych • wydanie zaleceń i opracowanie scenariusza mitygacji zagrożenia wynikającego z incydentu oraz wsparcie administratorów IT przy realizacji przygotowanego scenariusza • opracowanie wniosków z incydentu, mających na celu ograniczenie możliwości powtórzenia się danego typu incydentu w przyszłości • Przygotowanie planu działania w celu ograniczenia strat związanych z incydentem, pozyskanie dodatkowych danych niezbędnych do obsługi incydentu (z I linii wsparcia, z logów systemowych, ze źródeł zewnętrznych – CSIRT, użytkowników i in.). • Proponowanie nowych reguł korelacyjnych i scenariuszy SIEM i playbooków (zautomatyzowanych reakcji na incydenty) SOAR do wdrożenia w systemie SIEM/SOAR i propozycje optymalizacji aktualnie działających scenariuszy bezpieczeństwa

	• Proponowanie rozszerzenia zakresu monitorowania o kolejne systemy teleinformatyczne zamawiającego, przygotowywanie raportów dla klienta • Wykonawca może w ramach usługi L2 uruchamiać okresowe testy podatności • Wykonawca może dokonywać niezautomatyzowanej analizy logów Zamawiającego w celu proaktywnego poszukiwania incydentów i zabezpieczenia materiałów po incydencie • 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 Amerykańska Agencja Bezpieczeństwa (NSA).
SOC-11	świadczenie usługi SOC L2 SOAR 24/7/365 z opracowanych w pełni automatycznych playbooków przy SLA – 15 minut czas reakcji polegającej na wsparciu w zakresie zautomatyzowanej reakcji na incydenty Wykonawca zapewnia zamawiającemu: • przygotowanie liczby playbooków, zgodnie z ofertą Wykonawcy, pozwalających na zautomatyzowane reagowanie na incydenty wykryte w systemach i infrastrukturze zamawiającego
SOC-12	świadczenie usługi trzeciej linii wsparcia SOC - L3 w wymiarze ___ rbh (zgodnie z ofertą Wykonawcy), z czasem reakcji 1 dzień roboczy, która obejmuje pomoc zdalną lub na miejscu w zakresie usunięcia skutków zaistniałego incydentu, rekomendacje w zakresie zachowania materiału dowodowego dla Zamawiającego wraz z pełną analizą powłamaniową, analizę złośliwego oprogramowania, testy penetracyjne, doradztwo w zakresie architektury systemów i sieci, doradztwo w zakresie stosowania przepisów prawa związanych z cyberbezpieczeństwem (NIS2, KSC, KSC2, ustawa o działaniach antyterrorystycznych). Minimalna liczba roboczogodzin to 80.
SOC-13	uruchomienie usługi CTI (Cyber Threat Intelligence) do wszystkich reguł SIEM i playbooków SOAR, w ramach których Zamawiający oczekuje wzbogacania danych w regułach SIEM i SOAR o wskaźniki IOC (Indicators of Compromise) pochodzące z CSIRT krajowych takich jak np. NASK, wymiana i synchronizacja tych danych powinna być zautomatyzowana, dodatkowo w wypadku stwierdzenia podatności aplikacji, bądź systemu Zamawiającego powinna zostać wykonana analiza ryzyka, pod kątem możliwości wykorzystania jej w oparciu o publiczne POC na ten temat lub gotowe exploity
SOC-14	audyt podatności • Wykonanie raportu podatności co 6 miesięcy w zakresie infrastruktury i stacji roboczych zamawiającego – raport musi obejmować całą infrastrukturę serwerową, w tym wirtualną, kluczowe urządzenia i stacje robocze wykorzystywane przez użytkowników zamawiającego • zarządzanie podatnościami w systemach i infrastrukturze Zamawiającego wraz z przekazywaniem na bieżąco rekomendacji z podziałem na podatności wysokiego ryzyka – koniczne do usunięcia (niemożliwe jest ich monitorowanie), średniego ryzyka (włączone do stałego monitorowania, ale

	generujące ryzyka), podatności niskiego ryzyka – bezpieczne w przypadku monitorowania
SOC-15	szkolenie online dla pracowników zamawiającego z zakresu cyberbezpieczeństwa zawierające informacje o współczesnych zagrożeniach, socjotechnice, phishingu, ransomware, DDOS, jak rozpoznać ataki, wskazanie dobrych nawyków zwiększających bezpieczeństwo w biurze i poza biurem oraz świadomość zagrożenia cyberatakami minimum 1 raz w roku dla każdego pełnego roku trwania umowy czas trwania 3h
SOC-16	szkolenie online dla wskazanych maksymalnie 10 administratorów i kadry IT zamawiającego z zakresu wykorzystywania zaproponowanych narzędzi, obserwowania i reakcji na incydenty, mitygowania podatności minimum 1 raz w roku dla każdego pełnego roku trwania umowy czas trwania 7h
SOC-17	Raportowanie: • każdorazowo przy wystąpieniu incydentu, który zwiera informacje o incydencie, wpływ na środowisko zamawiającego, sposoby mitygacji, • miesięczny raport w zakresie wykonywanej usługi, który zawiera listę zaobserwowanych zdarzeń w podziale na kategorie zdarzeń typu (DDoS, ransomeware, phishing, brute force, itp.) oraz wykorzystane zabezpieczenia • miesięczny raport zawierający informacje o stosunku zdarzeń false positive vs true positive z każdej reguły korelacyjnej wraz z rekomendacją ewentualnych zmian
SOC-18	na wniosek zamawiającego wyrażony 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 cyberbezpieczeństwa
SOC-19	niewykorzystane roboczogodziny mogą zostać przeznaczone na inne działania z zakresu cyberbezpieczeństwa o ile Wykonawca dysponuje/świadczy taką usługę, liczba roboczogodzin zostanie każdorazowo ustalona z Wykonawcą
SOC-20	w przypadku konieczność zwiększenia wartości umowy aneksem, koszt roboczogodziny będzie ustalony na podstawie formularza ofertowego

3) Wymagania w zakresie wdrożenia, uruchomienia i utrzymania systemu klasy SIEM (Security Information and Event Management)

Tabela 2 Wymagania w zakresie wdrożenia, uruchomienia i utrzymania klasy SIEM

Wymaganie	Opis
SIEM-1	wdrożony SIEM występuje/wystąpił na zestawieniu Magic Quadrant publikowanym przez przedsiębiorstwo analityczno-badawcze Gartnera dotyczącym Security Information and Event Management (SIEM) w czasie ostatnich 3 lat
SIEM-2	wykonawca jest zobowiązany dostarczyć wszystkie niezbędne licencje do uruchomienia systemu SIEM, na czas trwania umowy, w tym licencje na bazę danych i inne niezbędne poza wymienionym w Załączniku nr 4 do umowy
SIEM-3	po zakończeniu umowy Zamawiający musi mieć możliwość pozyskania licencji na zaproponowany system SIEM 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
SIEM-4	system SIEM nie może ograniczać liczby równocześnie zalogowanych operatorów/użytkowników
SIEM-5	system SIEM musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów – login/logoff, uruchamiane zapytania i zmiany konfiguracji systemu
SIEM-6	system SIEM musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healthcheck)
SIEM-7	system SIEM musi umożliwiać uwierzytelnienie oraz szyfrowanie połączenia między wszystkimi komponentami systemu

4) Wymagania w zakresie wdrożenia, uruchomienia i utrzymania systemu klasy SOAR (Security Orchestration, Automation and Response)

Tabela 3 Wymagania w zakresie wdrożenia, uruchomienia i utrzymania systemu klasy SOAR

Wymaganie	Nazwa i Opis
SOAR-1	wdrożony SOAR występuje/wystąpił na zestawieniu Magic Quadrant publikowanym przez przedsiębiorstwo analityczno-badawcze Gartnera dotyczącym rozwiązań Security Orchestration, Automation and Response (SOAR) w czasie ostatnich 3 lat
SOAR-2	wykonawca jest zobowiązany dostarczyć wszystkie niezbędne licencje do uruchomienia systemu SOAR, na czas trwania umowy, w tym licencje na bazę danych i inne niezbędne poza wymienionym w Załączniku nr 4 do umowy
SOAR-3	po zakończeniu umowy Zamawiający musi mieć możliwość pozyskania licencji na zaproponowany system SOAR 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
SOAR-4	system SOAR musi zapewniać możliwości orkiestracji i automatyzacji bezpieczeństwa oraz odpowiedzi na incydent
SOAR-5	system SOAR musi integrować się z dostarczonym systemem SIEM
SOAR-6	aktywności użytkowników systemu SOAR musi być śledzona i logowana na potrzeby ewentualnej analizy
SOAR-7	system SOAR nie może przechowywać haseł do systemów i urządzeń Zamawiającego
SOAR-8	każdorazowe potrzeba sięgnięcia przez system SOAR do aplikacji/systemu/urządzenia Zamawiającego musi wiązać się z uzyskaniem danego poświadczenia z Password Vault na czas niezbędny do wykonania akcji przez SOAR
SOAR-9	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
SOAR-10	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 za pomocą protokołów REST i HTTPS

5) Wymagania w zakresie wdrożenia, uruchomienia i utrzymania systemu klasy Password Vault

Tabela 4 Wymagania w zakresie wdrożenia, uruchomienia i utrzymania systemu klasy Password Vault

Wymaganie	Nazwa i Opis
PV-1	wdrożony PV występuje/wystąpił na zestawieniu Magic Quadrant publikowanym przez przedsiębiorstwo analityczno-badawcze Gartnera dotyczącym rozwiązań Privileged Access Management (PAM) w czasie ostatnich 3 lat
PV-2	wykonawca jest zobowiązany dostarczyć wszystkie niezbędne licencje do uruchomienia systemu PV, na czas trwania umowy, w tym licencje na bazę danych i inne niezbędne poza wymienionym w Załączniku nr 4 do umowy
PV-3	po zakończeniu umowy Zamawiający musi mieć możliwość pozyskania licencji na zaproponowany system 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
PV-4	administratorami systemu Password Vault (PV) muszą być pracownicy Zamawiającego
PV-5	system Password Vault (PV) ma zapewniać centralne przechowywanie, uzyskiwanie dostępu i dystrybucję poświadczeń służących do uwierzytelnienia takich jak: tokeny, hasła, certyfikaty, klucze szyfrowania
PV-6	system PV ma umożliwiać: bezpieczne wstrzykiwanie poświadczeń do aplikacji, synchronizowanie przepływów poświadczeń między systemem SOAR, a aplikacjami i urządzeniami Zamawiającego, ustawianie zasad wygasania i automatyzowanie przepływów pracy i rotacji dla poświadczeń
PV-7	system PV musi zapewnić pełną audytowalność użycia poświadczeń przez system SOAR
PV-8	uruchomienie systemu z PV powinno wiązać się z podaniem klucza prywatnego, który jest podzielony zgodnie ze schematem 2 z 5, który wymaga minimum podania dwóch części posiadanych przez dwóch różnych administratorów z pięciu, aby uruchomić system PV

6) Wymagania w zakresie wdrożenia, uruchomienia i utrzymania systemu pełniącego rolę brokera komunikacyjnego

Tabela 5 Wymagania w zakresie wdrożenia, uruchomienia i utrzymania systemu pełniącego rolę brokera komunikacyjnego

Wymaganie	Nazwa i Opis

BR-1	wykonawca jest zobowiązany dostarczyć wszystkie niezbędne licencje do uruchomienia brokera, na czas trwania umowy, w tym licencje na bazę danych i inne niezbędne poza wymienionym w Załączniku nr 4 do umowy
BR-2	po zakończeniu umowy Zamawiający musi 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 spełniające wymagania OPZ
BR-3	broker komunikacyjny ma zapewnić bezpieczną komunikację między infrastrukturą wykonawcy a zamawiającego, niedopuszczalny jest bezpośredni dostęp systemu SOAR do systemów wewnętrznych zamawiającego

7) Harmonogram

1. Wdrożenie wszystkich wymagań i funkcjonalności określonych Umową nastąpi w ciągu 8 miesięcy od dnia podpisania Umowy.
2. Czas ten dzieli się na następujące etapy:
    1) Przeprowadzenie wstępnej ankietyzacji związanej z infrastrukturą Zamawiającego pozwalającej w sposób optymalny świadczyć usługi cyberbezpieczeństa – 1 miesiące od dnia podpisania umowy. W czasie ankietyzacji zostaną ustalone priorytety (wysoki, średni, niski) podłączania systemów Zamawiającego do systemów SIEM i SOAR.
    2) Wdrożenie, uruchomienie i utrzymanie systemów SIEM, SOAR, Password Vault i brokera komunikacyjnego - 2 miesiące od dnia podpisania umowy.
    3) Podłączenie do systemu SOAR zabezpieczeń stosowanych przez Zamawiającego w celu automatycznej reakcji na incydenty - 2 miesiące od podpisania umowy.
    4) Podłączenie do systemu SIEM systemów Zamawiającego określonych w Załączniku nr 2 do Umowy będącym wykazem systemów i urządzeń Zamawiającego rozwiązań o priorytecie wysoki - 2 miesiące od dnia podpisania umowy.
    5) Podłączenie do systemu SIEM systemów Zamawiającego określonych w Załączniku nr 2 do Umowy będącym wykazem systemów i urządzeń Zamawiającego rozwiązań o priorytecie średni - 4 miesięcy od dnia podpisania umowy.
    6) Podłączenie do systemu SIEM systemów Zamawiającego określonych w Załączniku nr 2 do Umowy będącym wykazem systemów i urządzeń Zamawiającego rozwiązań o priorytecie niski - 4 miesiące od dnia podpisania umowy.
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 administratorów Zamawiającego (konkretny termin przeprowadzenia szkoleń określony zostanie w Harmonogramie szkoleń, po zawarciu umowy).

6. Wykonawca będzie przekazywał raporty z wykonanej usługi:
    1) każdorazowo przy wystąpieniu incydentu, który zwiera informacje o incydencie, wpływ na środowisko zamawiającego, sposoby mitygacji,
    2) raz w miesiącu raport w zakresie wykonywanej usługi, który zawiera listę zaobserwowanych zdarzeń w podziale na kategorie zdarzeń typu (DDoS, ransomeware, phishing, brute force, itp.) oraz wykorzystane zabezpieczenia,
    3) raz w miesiącu raport zawierający informacje o stosunku zdarzeń false positive vs true positive z każdej reguły korelacyjnej wraz z rekomendacją ewentualnych zmian.
7. Terminy i sposoby przekazania raportów zostaną ustalone między Wykonawcą a Zamawiającym.

8) Parametry świadczenia usług – czasy maksymalne

Tabela 6 Parametry świadczenia usług - czasy maksymalne

Zadanie	**Czas reakcji / podjęcia**	**Czas realizacji**
SOC L1, całodobowe 24/7/365, podjęcie działań związanych z incydentem, rozwiązanie incydentu polegające na zatrzymaniu zagrożenia lub przekazanie do SOC L2	30 minut	2h
SOC - L2, 8/5 w dni robocze w godzinach roboczych 8:00 – 16:00, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie reakcji	1h	8h
SOC L2 SOAR 24/7/365, zautomatyzowane podjęcie incydentu i aplikacja rozwiązania zatrzymującego zagrożenie w czasie realizacji	15 min	1h
SOC L3, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie reakcji	8h	40h