



Nr sprawy: WZP.271.18.2024.E

Załącznik nr 1 – Opis przedmiotu zamówienia (zakres umowy)

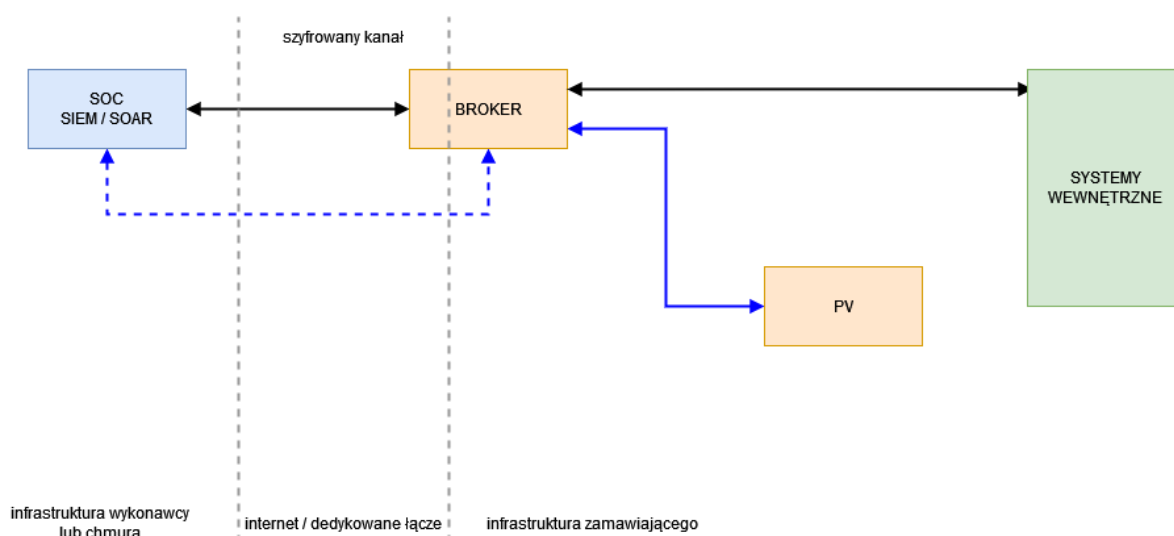
1) Założenia i wymagania ogólne

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), SOAR (Security Orchestration, Automation and Response), PV (Password Vault) lub rozwiązania hybrydowego łączącego funkcje narzędzi oraz brokera komunikacyjnego zapewniającego separację środowiska Wykonawcy i środowiska Zamawiającego.

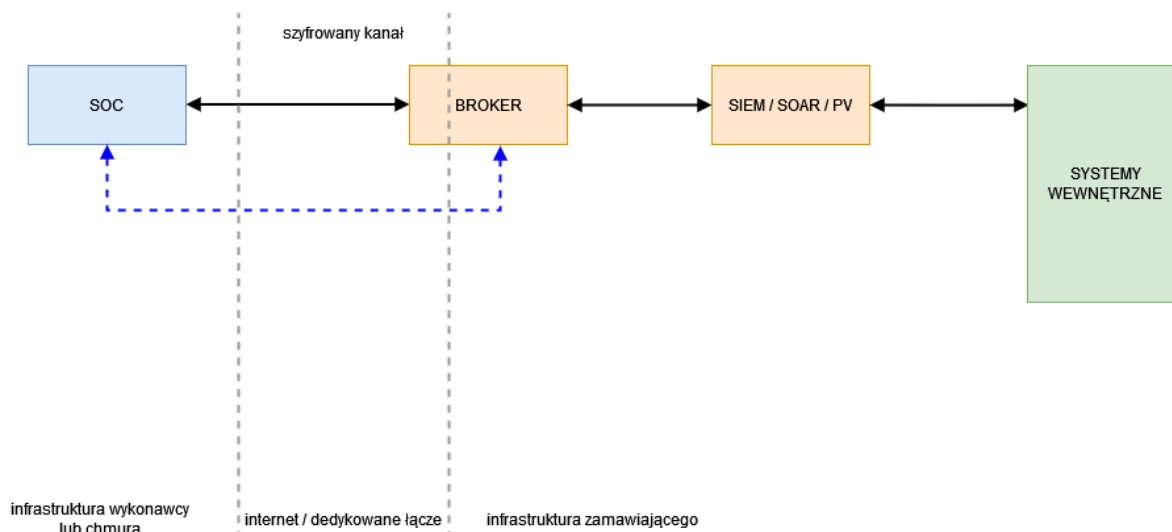
Usługa SOC musi spełniać wymagania opisane w poniższym dokumencie, a zaproponowane rozwiązanie musi posiadać architekturę jak na poniższych diagramach zgodnie z modelem 1 lub 2. Dopuszcza się dodanie innych rozwiązań dla zwiększenia bezpieczeństwa poniższych przepływów. Każde inne rozwiązanie dopuszczalne jest wyłącznie po uzyskaniu akceptacji Zamawiającego. Komunikacja między infrastrukturą Wykonawcy i Zamawiającego musi być szyfrowana. Wykonawca musi zapewnić niezawodną komunikację z infrastrukturą Zamawiającego. Dopuszcza się zastosowanie dedykowanego łącza do infrastruktury Zamawiającego o ile takim łączem dysponuje Wykonawca. Zamawiający dopuszcza uruchomienie usługi w chmurze zgodnie z modelem 1. W takim przypadku jednak cała usługa musi być umieszczona w Europejskim Obszarze Gospodarczym.

Rozwiązanie - model 1:





Rozwiązanie - model 2:



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 służącego do zbierania i korelacji logów z systemów Zamawiającego opisanych w załączniku nr 2 do umowy zgodnie ze specyfikacją opisaną w dokumencie przy zachowaniu harmonogramu i bez limitu reguł korelacyjnych
SOC-2	wdrożenie, uruchomienie i utrzymanie systemu klasy SOAR służącego do reagowania na incydenty raportowane przez system SIEM zgodnie ze specyfikacją opisaną w dokumencie przy zachowaniu harmonogramu i wraz z liczbą playbooków zgodną z ofertą Wykonawcy i akcji z nich wynikających; 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 kluczowe z punktu widzenia cyberbezpieczeństwa systemy, które należy monitorować, audyt przeprowadzony wraz z Zamawiającym musi wskazać również, którym systemom przypisany zostanie wysoki, średni i niski priorytet w zakresie czasu podłączenia do systemu SIEM; zamawiający może wyrazić zgodę na odstąpienie od integracji systemów o niskim priorytecie pod warunkiem, że Wykonawca przedstawi argumenty na brak wpływu rozwiązania na bezpieczeństwo Zamawiającego
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 wskazania zmian i optymalizacji w 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 każdego roku 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 pozwalającego na przechowywanie minimum 5000 poświadczeń i z dostępem dla minimum 3 administratorów Zamawiającego
SOC-7	wdrożenie oprogramowania pośredniczącego typu broker bez limitów związanych z użytkowaniem
SOC-8	Zamawiający dopuszcza rozwiązanie hybrydowe SIEM/SOAR/PV (Unified Security Operations Platform) przy założeniu jednak, że system hybrydowy spełnia wymagania dotyczące systemów SIEM, SOAR i PV opisane w dalszej części dokumentu, system hybrydowy może zostać posadowiony w infrastrukturze Wykonawcy lub chmurze publicznej z zastrzeżeniem, że system/moduł PV musi zostać zainstalowany w infrastrukturze Zamawiającego
SOC-9	<p>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</p> <p>Wykonawca zapewnia Zamawiającemu:</p> <ul style="list-style-type: none">• przekazywanie informacji o potencjalnych incydentach wypracowanym kanałem komunikacji• dostęp do konsoli monitorowania SIEM i konsoli SOAR / hybrydy 24/7/365 w uzgodnionym zakresie• obsługę zgłoszeń we własnym systemie ITSM wraz z jego utrzymaniem dla użytkowników i administratorów Zamawiającego• 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 Zamawiającego w wypełnianiu zaleceń wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa wraz z jej planowaną nowelizacją



SOC-10	<p>świadczenie usługi drugiej linii wsparcia SOC - L2, 8/5 w dni robocze w godzinach 8:00-16:00 z czasem reakcji 1 godzina</p> <p>Wykonawca zapewnia Zamawiającemu:</p> <ul style="list-style-type: none">• 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 incydemtem, pozyskanie dodatkowych danych niezbędnych do obsługi incydentu (z I linii wsparcia, z logów systemowych, ze źródeł zewnętrznych – CSIRT, użytkowników i innych)• proponowanie nowych reguł korelacyjnych i scenariuszy SIEM i playbooków (zautomatyzowanych reakcji na incydenty) SOAR do wdrożenia w systemie SIEM/SOAR/hybrydowym i propozycje optymalizacji aktualnie działających scenariuszy bezpieczeństwa• proponowanie rozszerzenia zakresu monitorowania o kolejne systemy teleinformatyczne Zamawiającego, przygotowywanie raportów dla Zamawiającego i jego dostawców• 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 Amerykańską Agencję Bezpieczeństwa (NSA)
SOC-11	<p>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</p> <p>Wykonawca zapewnia Zamawiającemu:</p> <ul style="list-style-type: none">• przygotowanie liczby playbooków, zgodnie z ofertą Wykonawcy, pozwalających na zautomatyzowane reagowanie na incydenty wykryte w systemach i infrastrukturze Zamawiającego wraz z ich bieżącą aktualizacją
SOC-12	<p>świadczenie usługi trzeciej linii wsparcia SOC - L3 w wymiarze rbh/rok, zgodnie z ofertą Wykonawcy (przy czym niewykorzystane roboczogodziny przechodzą na lata kolejne), 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; w przypadku nie zutilizowania rbh na zadania powyżej, Zamawiający może zlecić w ramach umowy</p>



	dodatkowe testy penetracyjne np. nowo wdrażanych systemów, doradztwo w zakresie architektury systemów i sieci, doradztwo w zakresie niezbędnych do wdrożenia dodatkowych zabezpieczeń, doradztwo w zakresie stosowania przepisów prawa związanych z cyberbezpieczeństwem (NIS2, KSC, KSC2, ustawa o działaniach antyterrorystycznych)
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 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 wykorzystania jej w oparciu o publiczne POC na ten temat lub gotowe exploity
SOC-14	wykonanie audytów podatności zgodnie z poniższymi wymaganiami <ul style="list-style-type: none">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)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
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 minimum 3h; w szkoleniu może uczestniczyć do 1600 pracowników Zamawiającego; Zamawiający dopuszcza szkolenie w wersji e-learningowej przy czy 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)
SOC-16	szkolenie online dla wskazanych maksymalnie 10 przedstawicieli najwyższego kierownictwa Zamawiającego z zakresu cyberhigieny, wymagań ustawy KSC i innych aktów prawnych związanych z cyberbezpieczeństwem, dobrych praktyk 1 raz w roku dla każdego pełnego roku trwania umowy czas trwania minimum 3h; szczegółowy zakres szkolenia ustalany każdorazowo z Zamawiającym
SOC-17	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 minimum 7h
SOC-18	<p>Raportowanie:</p> <ul style="list-style-type: none"> • 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, ransomware, 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-19	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-20	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
SOC-21	w przypadku konieczność zwiększenia wartości umowy aneksem, koszt roboczogodziny będzie ustalony na podstawie formularza ofertowego

3) Wymagania w zakresie wdrożenia, uruchomienia i utrzymania systemów klasy SIEM (Security Information and Event Management) i SOAR (Security Orchestration, Automation and Response) lub rozwiązania hybrydowego łączącego te funkcjonalności

Tabela 2 Wymagania w zakresie wdrożenia, uruchomienia i utrzymania systemów SIEM i SOAR/hybryda

Wymaganie	Opis
SISO-1	wdrożone systemy klasy SIEM i SOAR / rozwiązanie hybrydowe muszą być produktami komercyjnym, oferowanymi na rynku wraz ze wsparciem producenta rozwiązania; wyklucza się rozwiązania pozbawione wsparcia producenta
SISO-2	Wykonawca jest zobowiązany dostarczyć/posiadać wszystkie niezbędne licencje do uruchomienia systemów SIEM i SOAR / hybryda pozwalające na świadczenie usług na systemach, na czas trwania umowy, w tym licencje na bazę danych i inne niezbędne poza wymienionym w Załączniku nr 4 do umowy (model 1); w przypadku systemów instalowanych w infrastrukturze Zamawiającego dostarczone licencje muszą mieć charakter wieczysty (model 2) tak, aby Zamawiający mógł użytkować system po wygaśnięciu umowy z Wykonawcą
SISO-3	w przypadku licencji czasowych, po zakończeniu umowy, Zamawiający musi mieć możliwość pozyskania licencji na zaproponowany system SIEM i SOAR/ hybrydowy 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
SISO-4	system SIEM i SOAR / hybrydowy muszą umożliwić autoryzację użytkowników oraz precyzyjne nadawanie uprawnień dla administratorów i użytkowników oraz zapewniać pełną ich rozliczalność minimum w zakresie login/logoff, zmiana konfiguracji systemu, wykonane akcje; Zamawiający oczekuje minimum dostępu read-only dla systemu w modelu 1 oraz pełnego, rozliczalnego dostępu administracyjnego dla systemu w modelu 2
SISO-5	system klasy SIEM / rozwiązanie hybrydowe muszą pozwolić na zbieranie logów z systemów Zamawiającego, których klasy wymieniono w Załączniku nr 2 do umowy w tym w szczególności pozwolić na zbieranie informacji z końcówek i systemów klasy XDR, a w szczególności Bitdefender/Rapid7/TrendMicro oraz z urządzeń UTM, a w szczególności CheckPoint/Cisco/Fortinet/Paloalto/Sophos; system klasy SOAR / rozwiązanie hybrydowe musi umieć wykonywać akcje na końcówkach z wykorzystaniem wymienionych wyżej systemów XDR oraz urządzeń UTM
SISO-6	system SIEM / hybrydowy nie może ograniczać liczby równocześnie zalogowanych operatorów/użytkowników
SISO-7	system SIEM / hybrydowy musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healthcheck)
SISO-8	system SIEM / hybrydowy musi umożliwiać uwierzytelnienie oraz szyfrowanie połączenia między wszystkimi komponentami systemu
SISO-9	system SIEM / hybrydowy musi umożliwiać budowanie profili aktywności użytkowników oraz zasobów IT poprzez słowniki referencyjne i wykorzystywać je w regułach korelacyjnych i raportowaniu
SISO-10	Wykonawca musi dostosowywać na bieżąco reguły korelacyjne do zmieniającego się środowiska Zamawiającego tak, aby maksymalizować wykrywanie incydentów i minimalizować fałszywe alarmy
SISO-11	system SOAR / hybrydowy musi zapewniać możliwości orkiestracji i automatyzacji bezpieczeństwa oraz odpowiedzi na incydenty
SISO-12	Wykonawca musi dostosowywać na bieżąco playbooki do zmieniającego się środowiska Zamawiającego tak, aby maksymalizować automatyczną reakcję na incydenty
SISO-13	system SOAR musi natywnie integrować się z dostarczonym systemem klasy SIEM tj. producent oprogramowania SOAR musi oficjalnie wspierać integrację z dostarczonym rozwiązaniem SIEM lub musi stanowić jego część (rozwiązanie hybrydowe)
SISO-14	aktywności użytkowników systemu SOAR musi być śledzona i logowana na potrzeby ewentualnej analizy
SISO-15	system SOAR uruchomiony w modelu 1 nie może przechowywać haseł do systemów i urządzeń Zamawiającego
SISO-16	každorazowa 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 chyba, że Password Vault jest częścią rozwiązania hybrydowego



SISO-17	dostęp sieciowy systemu SOAR uruchomionego w modelu 1 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
SISO-18	Zamawiający nie dopuszcza bezpośrednich przejść sieciowych z systemu SOAR uruchomionego w modelu 1 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 wdrożenia, uruchomienia i utrzymania systemu klasy Password Vault

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

Wymaganie	Nazwa i Opis
PV-1	wdrożony system PV musi być produktem komercyjnym, oferowanym na rynku wraz ze wsparciem producenta rozwiązania; wyklucza się rozwiązania pozbawione wsparcia producenta; dopuszcza się rozwiązanie hybrydowe zintegrowane z rozwiązaniami SIEM i SOAR
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; dopuszcza się licencje wieczyste
PV-3	w przypadku licencji czasowych, 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 spełniającego 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
PV-7	system PV musi zapewnić pełną audytowalność użycia poświadczeń przez system SOAR oraz administratorów
PV-8	system musi zapewnić, aby pracownicy Wykonawcy nie mieli możliwości uzyskania dostępu do poświadczeń zapisanych w systemie

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

Tabela 4 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 systemów uruchamianych przez SOC w modelu 1 do systemów wewnętrznych Zamawiającego
BR-4	broker komunikacyjny ma zapewnić bezpieczną komunikację między infrastrukturą Wykonawcy a Zamawiającego, niedopuszczalny jest bezpośredni dostęp pracowników SOC w modelu 2 do systemów wewnętrznych Zamawiającego
BR-5	projekt rozwiązania Wykonawca przedstawi Zamawiającemu do akceptacji podczas etapu analizy i audytowania

6) 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 analizy i ankietyzacji związanej z infrastrukturą Zamawiającego pozwalającej w sposób optymalny świadczyć usługi cyberbezpieczeństwa – 1 miesiąc od dnia podpisania umowy. W czasie analizy i ankietyzacji zostaną ustalone priorytety (wysoki, średni, niski) podłączania systemów Zamawiającego do systemów SIEM i SOAR / hybrydowego.
 - 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 - 3 miesiące od podpisania umowy.
 - 4) Podłączenie do systemu SIEM systemów Zamawiającego określonych w Załączniku nr 2 do Umowy, będącym wykazem systemów i urządzeń Zamawiającego, o priorytecie wysoki - 3 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, o priorytecie średni - 4 miesiące 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 lub ich części zgodnie z wymaganiami OZP - 6 miesięcy od dnia podpisania umowy.
3. Uruchomienie usługi CTI w dla systemów SIEM/SOAR.



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

7) Parametry świadczenia usług – czasy maksymalne

Tabela 5 Parametry świadczenia usług - czasy maksymalne

Zadanie	Czas reakcji / podjęcia	Czas realizacji
SOC L1, całodobowe 24/7/365, podjęcie działań związanych z incydemem, 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 incydemem 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 incydemem i rozwiązanie incydentu w czasie realizacji	8h	40h

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