Załącznik nr 1 do Informacji	Opis przedmiotu zamówienia

Subskrypcja systemu SIEM wraz z wdrożeniem

Przedmiotem zamówienia jest subskrypcja systemu SIEM (zwanego dalej systemem) wraz z wdrożeniem, który będzie spełniał wymagania konfiguracyjne i parametrowe zgodne z poniższą tabelą:

LP.	PARAMETRY I FUNKCJE	WYMAGANIA
1.	Wymagania ogólne	- dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), którego celem jest gromadzenie i korelacja zdarzeń systemowych (w tym zdarzeń bezpieczeństwa), przesyłanych lub pobieranych z innych systemów i urządzeń teleinformatycznych; - oprogramowanie zostanie dostarczone w formie subskrypcji (na minimum 2 lata od dnia podpisania ostatecznego protokołu odbioru - zakończenie wdrożenia) w ramach której Wykonawca zapewnieni gwarancję w trakcie trwania subskrypcji oraz licencje dla liczby urządzeń określonych w niniejszym opisie; - niedopuszczalne są rozwiązania darmowe/open source oraz rozwiązania składające się z wielu osobnych modułów różnych producentów, dodatkowo wszystkie komponenty muszą być w wersji produkcyjnej; - konsola systemu musi być dostarczona w postaci SaaS; - system musi posiadać graficzny interfejs użytkownika, który będzie możliwy do uruchomienia przez przeglądarki internetowe minimum Chrome, Firefox, Edge, Safari - bez konieczności instalowania dodatkowego oprogramowania; - system musi działać zachowując wszystkie funkcje w modelu chmurowym. Konsola systemu musi być hostowana na platformie m. in. AWS, GCP lub MS Azure; - system musi mieć możliwość zbierania danych poprzez dostarczone przez producenta kolektory danych;

		- komunikacja pomiędzy konsolą systemu a kolektorami i agentami musi być zabezpieczona z wykorzystaniem protokołu TLS; - system musi zawierać technologie „deception" służącą do wykrywania złośliwych użytkowników i działań poprzez rozwiązania typu Honeypot;
2.	Wymagania dotyczące specyfikacji pod kątem infrastruktury Zamawiającego	- system musi mieć możliwość zbierania danych ze środowisk chmurowych oraz on-premise; - system musi umożliwić obsługę minimum 250 źródeł zdarzeń/logów (sprzęt oraz systemy posiadane w infrastrukturze Zamawiającego); - system musi mieć możliwość zbierania danych ze stacji końcowych poprzez oprogramowanie agenta działającego co najmniej na systemach z rodzin: Microsoft Windows Desktop i Microsoft Windows Server – systemy posiadane przez Zamawiającego.
3.	Wymagania dodatkowe	- system musi posiadać wsparcie techniczne producenta; - system musi być dystrybuowany poprzez oficjalny kanał dystrybucji producenta oferowanego systemu; - rozwiązanie musi być zgodne co najmniej ze standardami GDPR - (Rozporządzenie 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).
4.	Użytkownicy	- system powinien być dostarczony w wersji umożliwiającej jednoczesną pracę na konsoli systemu co najmniej 10-ciu użytkownikom w oparciu o indywidualne konta dostępowe; - możliwe nadawanie różnych uprawnień dla poszczególnych użytkowników w oparciu o RBAC; - użytkownicy muszą uwierzytelniać się bezpośrednio w konsoli systemu, system musi zapewniać funkcjonalność uwierzytelniania wieloskładnikowego co najmniej poprzez: Okta, SMS, Google Authenticator.
5.	Detekcja ataków i zagrożeń dotyczących	- system musi mieć możliwość wykrywania zagrożeń w oparciu o reguły; - system musi dodatkowo obsługiwać reguły out-of-the-box, reguły powinny mieć możliwość modyfikacji w oparciu o znane zachowania atakujących;

	aplikacji/ systemów Zamawiającego	- system musi wspierać funkcjonalność File Integrity Monitoring (monitorowanie integralności plików), musi mieć możliwość audytowania plików na stacjach końcowych oraz wykrywania modyfikacji krytycznych plików i folderów; - system musi monitorować co najmniej wymienione poniżej typy plików: • .bat • .cfg • .conf • .config • .dll • .exe • .ini • .sys
6.	Zbieranie logów z aplikacji/ systemów Zamawiającego	System musi wspierać pobieranie danych co najmniej z następujących środowisk: • AWS CloudTrail • Box.com • Duo Security • Google Apps • Office 365 • Okta.com • Centrify • OneLogin • Microsoft Azure - system posiada interfejs/protokół umożliwiający zaczytanie danych z platformy co najmniej: • AWS CloudTrial • Box.com • Duo Security • Google Apps • Office 365 • Okta - system musi zbierać dane co najmniej z technologii wymienionych poniżej: • Firewall o Barracuda Firewall o Cisco ASA Firewall + VPN

		○ Cisco Meraki ○ Check Point ○ Clavister W20 ○ Fortinet Firewall ○ Juniper Netscreen ○ Juniper Junos OS ○ Palo Alto ○ Palo Alto Networks WildFire ○ pfSense Firewall ○ SonicWALL ○ Sophos Firewall ○ Stonesoft Firewall ○ WatchGuard XTM • IDS/IPS ○ Corero IPS ○ Dell iSensor ○ McAfee IDS ○ Metaflows IDS ○ Security Onion ○ Snort IDS ○ Sourcefire 3D • EDR/XDR ○ Carbon Black EDR ○ Crowdstrike Falcon ○ Cyberreason ○ Palo Alto Cortex XDR ○ Microsoft Defender ATP
7.	Monitorowanie aktywności użytkowników aplikacji/ systemów Zamawiającego	- oprogramowanie agenta instalowane na stacjach końcowych musi zapewniać wgląd w aktywność ich procesów – klienckich jak i serwerowych; - oprogramowanie agenta musi przechwytywać zdarzenia o aktywności procesów na stacji w czasie rzeczywistym; - system musi mieć możliwość identyfikacji unikalnych i rzadkich procesów uruchamianych w środowisku zamawiającego; - system musi mieć możliwość analizy zachowania atakującego poprzez reguły behawioralne zawierające różnorodne możliwości detekcji; - system musi dostarczać gotowe reguły analizy zachowania użytkowników UBA oraz zachowania atakującego;

		- reguły UBA i zachowań atakującego muszą być automatycznie aktualizowane przez producenta, częstotliwość aktualizacji powinna opierać się na identyfikacji nowych zagrożeń, testowaniu ich wykrywalności, a następnie wypychaniu do platformy.
8.	Monitorowanie urządzeń sieciowych Zamawiającego	- monitorowanie logów z ruchu sieciowego z widocznością na poziomie użytych protokołów, portów oraz aplikacji.
9.	Integracja z systemami monitorowania posiadanych przez Zamawiającego	- integracja z systemami monitorowania logów; - integracja z systemami monitorowania aplikacji; - integracja z systemami monitorowania chmury.
10.	Wykrywanie nieautoryzowanego dostępu do aplikacji/ systemów Zamawiającego	- system musi mieć możliwość mapowania taktyk oraz technik atakującego na matrycę MITRE ATT&CK.
11.	Moduł obsługi incydentów	- system musi dostarczyć możliwości analizy incydentów poprzez konsolę chmurową; - moduł obsługi incydentów systemu musi zawierać osobną sekcję służącą do analizy incydentów w monitorowanym środowisku. W ramach procesu każdy incydent przyjmuje odpowiedni status, np.: otwarty, poddany analizie, zamknięty itp. - moduł obsługi incydentów systemu musi być wyposażony w mechanizm automatycznego powiadamiania wskazanych adresatów o nowych incydentach; - system musi mieć możliwość wizualizacji incydentów na osi czasu; - system musi mieć możliwość dostarczania w incydencie co najmniej informacji o hostach, kontach, użytkownikach i dokładnym czasie wystąpienia zdarzenia;

		- administrator musi mieć możliwość tworzenia notatek dotyczących danego incydentu, notatki muszą być tworzone i przechowywane w ramach konsoli systemu.
12.	Integracja z innymi systemami Zamawiającego	- System musi wspierać możliwość zbierania danych z co najmniej wymienionych poniżej technologii: • Active Directory • LDAP • Firewall • Antivirus • IDS/IPS • DHCP • DNS • Web proxy
13.	Powiadomienia i alerty	- alerty behawioralne muszą być domyślnie włączone; - system musi umożliwiać automatyczne generowanie alertu jeśli w środowisku klienta wykryje parametr zgodny z dostarczonymi przez producenta IoC (Indicators of Compromise) -; - system musi wspierać możliwość tworzenia niestandardowych alertów; - system musi mieć możliwość automatycznego powiadamiania użytkowników o znaczących zagrożeniach za pośrednictwem wiadomości email;
14.	Reguły korelacji	- system musi mieć możliwość śledzenia i analizowania zagrożeń w postaci zunifikowanych incydentów; - system musi koncentrować się na zachowaniu, a nie statycznych wskaźnikach zagrożeń dostarczając kontekst incydentu; - silnik UBA musi mieć możliwości automatycznego korelowania adresów IP z logów typu „raw data” wraz z powiązanymi z nimi nazwami hostów i użytkownikami; - producent musi dostarczać do systemu dane Threat Intelligence stale aktualizowane i analizowane przez grupy badawcze producenta. Producent musi dostarczać co najmniej dane o złośliwych procesach, adresach IP, domenach i adresach URL.
15.	Raporty i dane	- dostarczona licencja musi zapewniać przechowywanie danych zebranych przez system przez okres co najmniej 12 miesięcy;

		System musi umożliwiać: - przechowywanie danych bez konieczności używania sprzętu zewnętrznego; - izolowanie danych każdego z klientów wewnątrz jego własnej instancji w indywidualnej bazie danych uniemożliwiając innym klientom dostęp do bazy użytkowników; - prezentację danych w postaci dostosowanego dashboardu przez administratora/użytkownika; - wizualizację danych w specjalnej sekcji „Dashboard". Musi mieć możliwość wyświetlania co najmniej informacji o statystykach, użytkownikach, incydentach i hostach; - dostarczanie gotowych pulpitów do wizualizacji danych jak i umożliwiać Zamawiającemu tworzenie własnych niestandardowych pulpitów; - tworzenie raportów z niestandardowych pulpitów zbudowanych z prekonfigurowanych kart, które można dopasowywać wedle potrzeb zamawiającego; - tworzenie raportów jednorazowo jak i wg. skonfigurowanego harmonogramu; - eksportowanie danych na temat użytkowników, hostów i logów bezpośrednio z konsoli systemu; - przetwarzanie danych strukturalnych co najmniej w formatach STIX i CSV; - wyszukiwanie danych co najmniej poprzez Regex, String, KeyValue oraz Keyword; - wysyłanie raportów o alertach do wszystkich subskrybowanych w systemie kont; - eksportowanie poszczególnych raportów co najmniej w formacie PDF; - raporty na żądanie w oparciu o zapytanie i dane z logów, uwzględniające: a) automatyczne generowanie raportów w oparciu o interwały czasowe; b) wybór zakresu czasowego: możliwość wyboru zakresu czasowego dla raportu; c) dostępny eksport danych do formatów co najmniej: PDF lub CSV; d) wykresy i diagramy ułatwiające wizualizację i analizę danych;

16.	Parser logów systemów	- zbieranie logów i proces normalizacji (parsowania): realizowany z użyciem kolektorów dostarczanych przez producenta. - normalizacja logów z różnych źródeł do jednolitego formatu, na podstawie którego może odbywać się dalsze przetwarzanie oraz wyszukiwanie danych, system musi posiadać predefiniowany zestaw reguł normalizacji logów dla źródeł logów min. dla: urządzeń sieciowych, systemów bezpieczeństwa, Windows, Active Directory; - skalowalność – możliwe rozbudowanie do obsługiwania dużych ilości logów z różnych źródeł w czasie rzeczywistym.

Ponadto, Wykonawca zobowiązany jest spełnić poniższe wymagania.

1. Zapewnić wdrożenie systemu uwzględniając całą infrastrukturę i konfigurację poszczególnych systemów Zamawiającego.
2. Przez wdrożenie Zamawiający rozumie:
   1) sporządzenie i przedstawienie przez Wykonawcę, w terminie 7 dni roboczych (dzień roboczy – poniedziałek-piątek z wyłączenie dni ustawowo wolnych od pracy) od dnia podpisania umowy projektu wdrożenia systemu i oraz uzyskanie dla niego akceptacji Zamawiającego. W ramach projektu technicznego wdrożenia Wykonawca jest zobowiązany załączyć plan testów użytkowych/funkcjonalnych, przy czym:
      a) testy użytkowe/funkcjonalne będą przeprowadzane przez Wykonawcę pod nadzorem administratorów systemu (użytkownicy końcowi),
      b) testy użytkowe/funkcjonalne obejmować będą badania polegające na:
         - potwierdzeniu czy poprawnie działa całość systemu lub jego wybrany komponent poprzez uruchomienie danego procesu biznesowego i zweryfikowanie czy dane wyjściowe są zgodne z oczekiwanymi wynikami,
         - sprawdzeniu poprawnego działania mechanizmów rejestrowania (logowania) stanu komponentów systemu i braku błędów krytycznych w logach,
         - sprawdzeniu integracji systemu SIEM z istniejącymi systemami bezpieczeństwa i monitorowania, weryfikacja poprawności konfiguracji i funkcji integracyjnych, np. wysyłanie alertów do systemów zarządzania zdarzeniami lub zabezpieczeniami,
      c) testy wydajnościowe systemu: Wykonawca zaproponuje i wykona zestaw testów obciążeniowych weryfikujących poprawne zachowanie systemu w normalnych warunkach pracy jak i pod okresowo zwiększonym obciążeniem.

   Zamawiający jest uprawniony do wprowadzenia zmian do ww. projektu w terminie 3 dni roboczych od dnia przedstawienie przez Wykonawcę projektu do akceptacji. Brak informacji o zmianach w ww. terminie oznacza akceptację projektu przez Zamawiającego. W przypadku wprowadzenia zamian, Wykonawca jest zobowiązany zrealizować przedmiot zamówienia

zgodnie ze zmianami zaproponowanymi przez Zamawiającego. W przypadku gdy, proponowane przez Zamawiającego zmiany miałyby niekorzystnie wpłynąć na infrastrukturę informatyczną Zamawiającego, Wykonawca jest zobowiązany w terminie 2 dni roboczych od otrzymania informacji o zmianach, poinformować o tych zagrożeniach Zamawiającego. Jeżeli pomimo otrzymania ww. informacji Zamawiający potwierdzi realizację przedmiotu zamówienia zgodnie z ww. zmianami (w całości lub części), Wykonawca wykona przedmiot zamówienia z uwzględnieniem tych zmian. W przypadku gdy w wyniku realizacji ww. procesu nastąpi zmiana projektu Wykonawca zaktualizuje projekt i dostarczy go do Zamawiającego w terminie 2 dni roboczych od dnia uzyskania potwierdzenia realizacji przedmiotu zamówienia zgodnie z ww. zmianami.

2) dostarczenie licencji na oprogramowanie systemu;
3) przygotowanie infrastruktury Zamawiającego do instalacji systemu – w tym konfiguracja poszczególnych źródeł logów do nadawania zdarzeń/przepływów sieciowych do systemu;
4) instalacja i konfiguracja niezbędnego oprogramowania oraz serwerów wirtualnych jeżeli są wymagane;
5) instalacja systemu;
6) aktywacja licencji;
7) aktualizacja oprogramowania – najnowsza wersja oprogramowania dostępna na dzień instalacji;
8) konfiguracja systemu i uzyskanie akceptacji jej przez Zamawiającego;
9) przygotowanie i realizacja scenariuszy użycia systemu bezpieczeństwa zgodnie z wymaganiami:

   Scenariusz użycia systemu zawiera co najmniej zadania:
   a) skonfigurowanie kilku źródeł zdarzeń,
   b) opisanie procesu normalizacji,
   c) stworzenie reguł korelacyjnych w systemie SIEM mających na celu analizowanie w referencji do listy i/lub pól wyliczeniowych i/lub analizy statystycznej, lub w inny sposób mający ujawnić incydent bezpieczeństwa,
   d) stworzenie scenariusza reakcji w zakresie czynności wykonywanych przez pierwszą linię wsparcia,
   e) opisanie szczegółowej ścieżki eskalacji.

   Zamawiający wymaga przygotowania i wdrożenia minimum 20 scenariuszy użycia systemu dla zidentyfikowanych przez Zamawiającego ryzyk – każdorazowo scenariusz użycia systemu musi zostać zaakceptowany przez Zamawiającego. Przykładowe scenariusze użycia systemu:
   a) logowanie użytkownika ze zmianą geolokalizacji,
   b) wykrywanie utworzenia użytkownika (lokalnego i domenowego),
   c) wykrywanie złośliwego oprogramowania na chronionym obiekcie,

d) komunikacja z wewnątrz infrastruktury Zamawiającego do adresu/domeny o podejrzanej reputacji,
e) udane logowanie na konto użytkownika/uprzywilejowane poprzedzone kilkukrotnym nieudanym logowaniem;

10) przygotowanie scenariuszy reakcji.

Scenariusz reakcji składa się z podzadań realizujących funkcje:

a) wzbogacenie wiedzy o artefaktach tj. adresy IP, domeny, hash'e plików, nazwy plików, rozpoznawalność wskaźników kompromitacji przez narzędzia klasy CTI/OSINT, w celu wyciągania adekwatnych wniosków i podejmowania trafnych decyzji,
b) analizy zidentyfikowanego zdarzenia, w tym szczególności potwierdzenia, że zagrożenie w przypadku uruchomienia w środowisku Zamawiającego może stać się incydentem lub jest incydentem, jak również rozpoczęcia pobierania lub zabezpieczenia dodatkowych danych z zaatakowanego źródła ataku zasobu na potrzeby realizacji pierwszej linii wsparcia,
c) reakcji rozumianej jako ograniczenie możliwości wystąpienia zdarzenia niepożądanego, uruchomienia procesu eskalacyjnego lub innych czynności stosowanych do zagrożenia w zakresie uzgodnionym z Zamawiającym,
d) informowania i raportowania obejmującego dokumentowanie wykonanych czynności oraz rezultatów przeprowadzonej analizy lub zasadności czynności reakcji [to zrobi technik serwisu];

11) przeprowadzenie testów akceptacyjnych potwierdzających poprawne wdrożenie systemu i jego konfigurację, w tym w szczególności:

a) przygotowanie i uzyskanie aprobaty Zamawiającego dla scenariuszy testów systemu,
b) weryfikację wdrożonych scenariuszy użycia oraz implementacji nowych przypadków zgłoszonych przez Zamawiającego,
c) weryfikację możliwości wdrożenia przypadków użycia w środowisku Zamawiającego,
d) potwierdzenie działania wszystkich wdrożonych reguł, dla wszystkich zaimplementowanych scenariuszy w ustalonym przedziale czasowym.

Wykonawca realizuje testy akceptacyjne w środowisku produkcyjnym, zgodnie ze scenariuszami testowymi opracowanymi przez siebie i zaakceptowanymi przez Zamawiającego na etapie odbioru dokumentacji powdrożeniowej. Wykonawca jest zobowiązany niezwłocznie po przeprowadzeniu testów akceptacyjnych przekazać ich wyniki Zamawiającemu w formie dokumentu elektronicznego w formacie .docx lub .pdf.

3. Wszelkie okna serwisowe będą wymagały akceptacji Zamawiającego. Wykonawca poinformuje Zamawiającego o potrzebie okna serwisowego nie później niż w terminie 7 dni roboczych przed planowanym terminem okna serwisowego.

4. W przypadku pojawienia się nowych skuteczniejszych technik identyfikacji zagrożeń, Wykonawca ma obowiązek w ramach wsparcia zaktualizować w porozumieniu z Zamawiającym istniejące scenariusze użycia systemu bezpieczeństwa, zrealizowane na etapie wdrożenia systemu SIEM (nie dotyczy zgłoszeń z priorytetem „none").
5. Zapewnić podłączenie wskazanych przez Zamawiającego źródeł zdarzeń.
6. Zapewnić uruchomienie i konfigurację parserów dla niestandardowych źródeł danych, w przypadku wymagania integracji ich przez Zamawiającego
7. Zapewnić uruchomienie i konfigurację reguł korelacyjnych, ustawień i obszarów bezpieczeństwa infrastruktury i sieci, mechanizmów oceny ryzyka, powiadamiania oraz obsługi incydentów.
8. Zapewnić dostrojenie i skalibrowanie reguł korelacji.
9. W ciągu 15 dni roboczych od wdrożenia dostarczyć dokumentację powdrożeniową oraz dokumentację systemu SIEM (techniczną oraz dla użytkownika) – dokumentacja w formie edytowalnej (co najmniej .docx, .xlsx, .pdf), w tym w szczególności:
    1) projekt wdrożenia rozwiązania w infrastrukturze Zamawiającego,
    2) dokumentacja powdrożeniowa systemu,
    3) dokumentacja techniczna i użytkownika,
    4) wyniki testów akceptacyjnych

    Ww. dokumenty zostaną sporządzone w języku polskim lub dostarczone wraz z tłumaczeniem na język polski.
10. Udzielić gwarancji na okres trwania subskrypcji dostarczonego systemu, która liczona będzie od dnia podpisania ostatecznego protokołu odbioru przedmiotu zamówienia. W ramach gwarancji (bez dodatkowego wynagrodzenia) Wykonawca zobowiązany jest naprawić system w przypadku powstałych awarii.
11. Wykonawca zapewni elektroniczny dostęp do informacji na temat posiadanego oprogramowania oraz co najmniej do poprawek, aktualizacji. W ramach wynagrodzenia za dostawę systemu SIEM w okresie trwania subskrypcji Wykonawca jest zobowiązany świadczyć usługi wsparcia technicznego, które będą realizowane poprzez zlecenia lub zgłoszenia w trakcie trwania subskrypcji:
    1) zgłoszenia będą dokonywane przez Zamawiającego w trybie NBD (następny dzień roboczy),
    2) zgłoszenia będą obsługiwane w ramach zdefiniowanych parametrów SLA i kategorii zgłoszenia:
        a) high - zgłoszenie krytyczne, przez co rozumie się brak działania systemu/niepoprawne działanie systemu/brak możliwości zalogowania się – usunięcie awarii usługi/systemu lub zaproponowanie obejścia nastąpi do 6h od momentu przekazania zgłoszenia do Wykonawcy przez Zamawiającego, z zastrzeżeniem, że w przypadku zaproponowania obejścia Wykonawca przywróci prawidłowe działanie usługi/systemu w terminie do 24h od momentu zgłoszenia awarii przez Zamawiającego;
        b) medium - przez co rozumie się zgłoszenie inne niż high polegające na zmianie konfiguracji/sprawdzeniu poprawności działania funkcjonalności systemu w razie

wątpliwości co do prawidłowości ich działania lub ich naprawy w przypadku awarii - zmiana/przywrócenie konfiguracji, wyjaśnienie wątpliwości/usunięcie awarii funkcjonalności lub zaproponowanie obejścia nastąpi do 8h od momentu przekazania zgłoszenia do Wykonawcy przez Zamawiającego, z zastrzeżeniem, że w przypadku zaproponowania obejścia Wykonawca przywróci prawidłowe działanie funkcjonalności/systemu w terminie do 48h od momentu zgłoszenia awarii przez Zamawiającego;

c) low - przez co rozumie się pozostałe nieprawidłowości działania systemu niewyszczególnione jako high i medium - usunięcie nieprawidłowości lub zaproponowanie obejścia nastąpi do 2 dni roboczych od momentu przekazania zgłoszenia do Wykonawcy;
d) none – usługi wsparcia (do 200 roboczogodzin) niewyszczególnione jako high, medium, low zgłoszenia dotyczące m.in. udzielenia przez Wykonawcę informacji, konsultacji, a także dokonania zmiany w konfiguracji usług/systemu, wdrożenia nowych scenariuszy reakcji lub dodania nowych reguł korelacji dodanych do już istniejących.

3) Zamawiający poinformuje Wykonawcę o zgłoszeniu none określając zakres zgłoszenia. Udzielenie odpowiedzi na zgłoszenie nastąpi do 2 dni roboczych od momentu przesłania zgłoszenia do Wykonawcy przez Zamawiającego. W przesłanej odpowiedzi Wykonawca określi termin i liczbę roboczogodzin niezbędną do realizacji zgłoszenia, z zastrzeżeniem, że termin realizacji zgłoszenia nie przekroczy 5 dni roboczych od momentu akceptacji liczby roboczogodzin przez Zamawiającego. Brak zakwestionowania przez Zamawiającego liczby roboczogodzin w terminie 2 dni roboczych od otrzymania ww. odpowiedzi od Wykonawcy, uznaje się za akceptację warunków realizacji zgłoszenia przez Zamawiającego. Zamawiający jest uprawniony zakwestionować wskazaną liczbę roboczogodzin przez Wykonawcę, w szczególności gdy informacje pozyskane przez Zamawiającego z rynku wskażą, że liczba roboczogodzin niezbędnych do zamknięcia zgłoszenia znacząco odbiega (co najmniej o 40%) od wskazanej liczby roboczogodzin przez Wykonawcę. Wówczas Strony przystąpią do negocjacji w celu ustalenia ostatecznej liczby roboczogodzin. Po ustaleniu przez Strony ostatecznej liczby roboczogodzin – akceptacja przez Zamawiającego, Wykonawca przystąpi do realizacji zgłoszenia. Realizacja zgłoszenia w terminie dłuższym niż ww. (5 dni) może nastąpić wyłącznie za zgodą Zamawiającego. Zgłoszenie zostanie zrealizowane w sposób wskazany przez Zamawiającego – w sposób zdalny lub w siedzibie Zamawiającego. w przypadku braku rozwiązania zgłoszenia z innej przyczyny niż awaria systemu SIEM, Wykonawca wskaże element, który powoduje nieprawidłowość działania systemu,
4) usługi wsparcia technicznego będą składane za pośrednictwem poczty elektronicznej/systemu wskazanego przez Wykonawcę,
5) **Prawo opcji:** w ramach prawa opcji Zamawiający jest uprawniony do zlecenia dodatkowo 200 roboczogodzin konsultacji. Zamawiający poinformuje Wykonawcę o

zamiarze skorzystania z opcji określając zakres potrzeby Zamawiającego. Proces ustalenia liczby roboczogodzin uruchamianych w ramach prawa opcji jest ustalany w sposób tożsamy jak dla zamówienia podstawowego (realizacja zgłoszenia none), z zastrzeżeniem, że uruchomienie opcji następuje w momencie zaakceptowania przez Zamawiającego liczby roboczogodzin. Zamawiający jest uprawniony wielokrotnie korzystać z prawa opcji do momentu wyczerpania limitu 200 roboczogodzin.
W przypadku nie wykorzystania przez Zamawiającego opcji w całości lub w części Wykonawcy nie przysługuje jakiekolwiek roszczenie za jej niewykorzystanie, w tym za utracone korzyści.

12. W ramach wsparcia technicznego (nie dotyczy zgłoszenia ‘none’) Wykonawca zapewni przeglądy kwartalne w trakcie których zostanie zweryfikowana poprawność pracy dostarczonego oprogramowania, przeprowadzona aktualizacja oraz sporządzona dokumentacja z przeglądu.
13. Wykonawca zapewni w ramach umowy 3-dniowe warsztaty przeprowadzone przez Wykonawcę dla 6 osób (min. 3 x 8h) w zakresie użytkowania i administrowania wdrożonym systemem. Warsztaty odbędą się w siedzibie Zamawiającego – ul. Józefa Lewartowskiego 6, 00-190 Warszawa. Wykonawca przygotuje materiały szkoleniowe dla wszystkich uczestników szkoleń. Warsztaty będą podzielone na część teoretyczno-opisową wszystkich funkcjonalności systemu jak i zadania praktyczne. Termin szkolenia zostanie uzgodniony przez Strony w trybie roboczym. Szczegółowy harmonogram warsztatu (podział na dni) wraz zakresem przedmiotowym zostanie przedstawiony Zamawiającemu w terminie do 3 dni roboczych od podpisania ostatecznego protokołu odbioru przedmiotu zamówienia.

Procedura odbioru przedmiotu zamówienia będzie obejmowała, w szczególności:

1) Instalację i konfigurację systemu – w tym scenariusze użycia i reakcji, reguły korelacji;
2) Dostawę i aktywację licencji na oprogramowanie;
3) Testy akceptacyjne systemu;
4) Dostarczenie dokumentacji – projektu wdrożenia, dokumentacji technicznej i użytkownika, dokumentacji powdrożeniowej;
5) Warsztaty z obsługi systemu.

Odbiór każdego z ww. etapów będzie potwierdzona protokołem odbioru. Wynagrodzenie za wykonanie przedmiotu umowy będzie ryczałtowe i płatne jednorazowo, po zakończeniu wszystkich odbiorów.

Przedmiot zamówienia jest określony we Wspólnym Słowniku Zamówień jako:

48000000-8 Pakiety oprogramowania i systemy informatyczne;
72000000-5 Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia;
72260000-5 Usługi w zakresie oprogramowania
72263000-6 Usługi wdrażania oprogramowania

72611000-6 Usługi w zakresie wsparcia technicznego
80510000-2 Usługi szkolenia specjalistycznego