Opis Przedmiotu Zamówienia

1. Opis ogólny zamówienia

Przedmiotem zamówienia jest dostawa licencji, rozbudowa posiadanego systemu SIEM opartego na architekturze „Splunk Enterprise" wraz z usługą serwisu i wsparcia technicznego. Zamawiający planuje rozbudowę centralnego, wspólnego dla wszystkich systemów węzła gromadzenia i korelacji zdarzeń w sieci PGL LP z okresem obowiązywania od dnia 29.12.2022r.

1.1. W ramach realizacji przedmiotu zamówienia konieczne jest wykonanie następujących czynności:

- 1.1.1. Dostawa licencji dla posiadanego przez Zamawiającego oprogramowania klasy „SIEM" wraz ze wsparciem producenta, liczonym od dnia uruchomienia licencji, w infrastrukturze zamawiającego;
- 1.1.2. Konsultacje między Zamawiającym a Wykonawcą w celu opracowania strategii wdrożenia oraz analizy przedwdrożeniowej;
- 1.1.3. Wykonanie projektu technicznego rozbudowy w oparciu o istniejącą architekturę;
- 1.1.4. Prace właściwe związanie z rozbudową jak również przygotowanie dokumentacji i instrukcji użytkownika wdrożonego systemu;
- 1.1.5. Przeprowadzenie przez Wykonawcę warsztatowego przekazania wiedzy;
- 1.1.6. Serwis oraz gwarancję wdrożonego rozwiązania w zakresie zdefiniowanym przez Zamawiającego;

1.2. Użyte w specyfikacji określenia wskazujące znaki towarowe, patenty lub pochodzenie przedmiotu zamówienia należy odczytywać wraz z wyrazami „lub równoważne". Wykonawca oferując przedmiot równoważny do opisywanego w specyfikacji jest zobowiązany zachować równoważność w zakresie parametrów użytkowych, funkcjonalnych i jakościowych, które muszą być na poziomie nie niższym od parametrów wskazanych przez Zakład Informatyki Lasów Państwowych w stosunku do wersji oprogramowania „Splunk Enterprise".

1.3. W ramach realizacji przedmiotu zamówienia Oferent przedstawi ofertę na rozbudowę systemu klasy SIEM „Splunk Enterpise" Zamawiającego lub równoważne rozwiązanie na warunkach opisanych w niniejszym dokumencie.

1.4. Oferowane oprogramowanie musi pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej, a gwarancja musi pochodzić od producenta i być świadczona przez sieć serwisową producenta, również na terenie Polski.

1.5. Oferent przedstawi w ofercie koszty min.: przygotowania projektu technicznego, dokumentacji wdrożenia w oparciu o rozbudowę aktualnie działającego systemu przy założeniu iż system będzie spełniał wymagania zgodnie z opisem zamówienia.

1.6. Wdrażany system musi zostać objęty serwisem oraz wsparciem technicznym producenta wdrażanego rozwiązania przez okres obowiązywania licencji od dnia jej uruchomienia oraz serwisem i wsparciem technicznym Wykonawcy przez okres obowiązywania Umowy zgodnie z warunkami Zamówienia.

1.7. Miejsce wdrożenia rozwiązania: Dyrekcja Generalna Lasów Państwowych, Warszawa 02-124 ul. Grójecka 127.

2. Opis środowiska Zamawiającego.

2.1. Aktualnie wykorzystywane licencje przez Zamawiającego:

W środowisku produkcyjnym Zamawiającego aktualnie wykorzystywana jest licencja wraz ze wsparciem producenta zgodnie z nw. tabelą:

Nazwa licencji:	Ilość GB/dzień:	Zakończenie kontraktu:
Splunk Enterprise - Term License with Standard Success Plan - GB/day	30	29.12.2022r.

2.2. Aktualne środowisko aplikacji SIEM Zamawiającego:

2.2.1. Zamawiający aktualnie w środowisku produkcyjnym przeznaczył dla aplikacji „Splunk Enterprise" zasoby maszyn wirtualnych opartych o środowisko VMware ESXi 7.0, w ilości 2 szt. każdy o parametrach CPU 32core (2proc x 16core 2,9GHz) oraz RAM 128GB.

2.2.2. Wdrożone rozwiązanie „Splunk Enterprise" działające u Zamawiającego aktualnie zbiera zdarzenia z rozwiązań takich jak: Active Directory, Syslog-ng oraz centralnych urządzeń Firewall.

2.3. Infrastruktura zamawiającego przeznaczona na realizację niniejszego postępowania:

2.3.1. Zamawiający w celu realizacji postawionego zadania, udostępni Wykonawcy własną infrastrukturę, komponenty systemu SIEM mogą być zainstalowane w infrastrukturze PGL LP (środowisko wirtualne VMware ESXi 7.0 lub nowsze) oraz zagwarantuje co najmniej trzy wydzielone serwery każdy o parametrach CPU 32core / vCPU 64core 2,9GHz oraz sumaryczną pamięć nie większą niż 352GB RAM oraz dyski SSD obsługujące min. 800 IOPS o pojemności 15TB na retencję danych Hot, Warm przez okres 7 dni, Cold 30 dni oraz Archived (Frozen) z wykluczeniem dysków SSD na okres 3 miesięcy.

2.3.2. W przypadku gdy oferowane rozwiązanie wymaga większej ilości zasobów sprzętowych niż określa Zamawiający, Wykonawca dostarczy odpowiednią platformę sprzętowo-programową w oparciu o środowisko wirtualnie VMware ESXi 7.0 lub nowsze wraz z odpowiednimi licencjami.

3. Opis zamawianych licencji dla rozwiązania posiadanego

3.1. W wyniku rozbudowy będącej przedmiotem postępowania, Zamawiający oczekuje iż będzie posiadał licencje oprogramowania oraz pakiety usług wsparcia producenta:

Nazwa licencji:	Ilość GB/dzień:	Okres obowiązywania:
Splunk Enterprise - Term License with Standard Success Plan - GB/day	250	24 miesiące

3.2. Dostawa, licencji dla posiadanego przez Zamawiającego oprogramowania musi obowiązywać od dnia 29.12.2022r. oraz zapewniać wsparcie producenta przez okres minimum 24 miesięcy kalendarzowych, liczonych od dnia uruchomienia licencji w infrastrukturze Zamawiającego.

4. Opis rozwiązania równoważnego systemu klasy SIEM.

4.1. Rozwiązanie musi pochodzić z oferty jednego producenta i być systemem komercyjnym, z zastrzeżeniem iż nie może to być rozwiązanie typu „open source".
4.2. Rozwiązanie klasy SIEM musi znajdować się w kwadracie „Leaders" raportu Gartnera „Magic Quadrant for Security Information and Event Management June 2022r."
4.3. System SIEM musi istnieć na rynku co najmniej 5 lat oraz posiadać wsparcie techniczne producenta w języku polskim.
4.4. Oferowane rozwiązanie musi umożliwić wykorzystanie w innych obszarach niż zarządzanie informacją bezpieczeństwa w oparciu o wspólne dane w szczególności w zakresie: monitorowania usług, wydajności aplikacji.
4.5. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego, Wykonawca dokona migracji danych z obecnie używanego rozwiązania SIEM „Splunk Enterprise" oraz dostosuje strukturę oprogramowania równoważnego do działającego systemu oraz zastosowanych w nim rozwiązań w infrastrukturze Zamawiającego.
4.6. W przypadku, gdy zaoferowany przez Wykonawcę produkt równoważny nie będzie właściwie działać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu produktu równoważnego.
4.7. Oprogramowanie równoważne nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowania.

4.8. Wymagania funkcjonalnie dla rozwiązania równoważnego systemu klasy SIEM:

4.8.1. Zaoferowane rozwiązanie musi umożliwiać Zamawiającemu skalowalność , rozbudowę architektury w przypadku wzrostu wymagań wydajnościowych i

pojemnościowych wynikających z przekazywania, gromadzenia oraz zwiększania poziomu szczegółowości logowanych zdarzeń (logów / danych).

4.8.2. Musi istnieć możliwość rozbudowy środowiska o dodatkowe węzły poprawiające wydajność systemu bez konieczności zakupu dodatkowych licencji lub modułów.

4.8.3. Zaoferowany System musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej w celu przechowywania danych archiwalnych.

4.8.4. Rozwiązanie musi posiadać możliwość planowanego przenoszenia danych na podstawie czasu lub okresu na pamięci masowe niższego poziomu.

4.8.5. Rozwiązanie nie może powodować utraty danych w przypadku przekroczenia limitu dziennego pobierania logów w odniesieniu do wykorzystywanej licencji w danym momencie.

4.8.6. System musi umożliwiać integrację danych gromadzonych z różnych źródeł, przetwarzane dane powinny być dostępne jako spójna informacja na poziomie analizy zdarzeń.

4.8.7. Zaoferowany system musi posiadać mechanizm uniemożliwiający usuwanie całości lub części logów, danych przez nieuprawnionych użytkowników. Dostęp do danych musi być dostępny tylko dla uprawnionych, uwierzytelnionych użytkowników.

4.8.8. Rozwiązanie musi wspierać geolokalizację zdarzeń na bazie adresów IP. Dane geolokalizacyjne dla zdarzeń mają służyć do prezentacji na mapie, jak również umożliwiać ich wykorzystanie w wyszukiwaniu wartości pól oraz w regułach korelacyjnych.

4.8.9. Tabele i wykresy prezentowane na bazie dostarczonych logów / danych muszą posiadać funkcję drążenia w dół, tzn. po zaznaczeniu danej pozycji w tabeli lub wykresie, interfejs powinien pokazywać odpowiadające im logi / dane.

4.8.10. Rozwiązanie powinno pozwalać na analizę standardowych logów infrastrukturalnych generowanych przez systemy operacyjne, firewalle, urządzenia sieciowe (przełączniki, routery, loadbalancery, itd.) systemy bezpieczeństwa IPS/IDS/ Application & URL Filtering / Anti-Bot, WAF itd.

4.8.11. Rozwiązanie powinno pozwalać na analizę niestandardowych logów wygenerowanych przez aplikacje własne.

4.8.12. System musi posiadać możliwość przesyłania, parsowania, korelowania i przechowywania logów i innych danych z co najmniej z następujących źródeł: Cisco ASA, F5 , A10, CISCO (przełączniki, routery, firewalle), systemu operacyjne (Red Hat, Microsoft Windows), usługi serwerowe (DNS, DHCP, WWW (Apache, IIS)), Oracle, SQL Server, Vmware vSphere, Logi Windows Events (Logi Application, Security, System I inne) , logi z ruchu sieciowego poprzez Netflow.

4.8.13. Zaoferowane rozwiązanie musi umożliwiać pobieranie logów / danych zapisanych w plikach (dziennikach systemowych / aplikacyjnych) jak również w postaci komunikatów przechwytywanych z portów TCP/UDP oraz z wykorzystaniem następujących mechanizmów:

4.8.13.1. Wysyłanie logów / danych ze źródłowego systemu na wskazany port TCP/UDP serwera, będącego częścią wdrażanego rozwiązania (np. syslog),

4.8.13.2. Rozwiązanie musi wspierać zbieranie danych w formacie CEF oraz przyjmowanie logów z Syslog Relay,

4.8.13.3. Wskazanie w interfejsie użytkownika wdrażanego rozwiązania Systemu na znajdujący się lokalnie plik / katalog,

4.8.13.4. Wykonywanie przez zaoferowane rozwiązania zapytań SQL w zewnętrznych bazach danych i pobieranie wyników zapytań. Alternatywnie musi istnieć możliwość komunikacji z bazami danych w standardzie JDBC lub ODBC,

4.8.14. Rozwiązanie musi umożliwiać następujące funkcje dotyczące pracy nad logami:

4.8.14.1. Rozwiązanie musi umożliwiać parsowanie logów o długości co najmniej 10 000 znaków oraz zawierających więcej niż jedną linię,

4.8.14.2. Rozwiązanie musi umożliwiać tworzenie bazy definicji formatów logów,

4.8.14.3. Rozwiązanie musi wyszukiwać czas zdarzenia (timestamp) z analizowanego logu i wykorzystywać go do reguł korelacyjnych,

4.8.14.4. Rozwiązanie musi umożliwiać wyszukiwanie zdarzeń w logach/danych o zadanych wartościach pól, w oparciu o wyrażenia regularne (REGEX) lub gotowych wzorców wyboru np: adres IP źródłowy/docelowy, port, protokół,

4.8.14.5. Rozwiązanie musi umożliwiać tworzenie alertów/powiadomień po wykryciu zdarzenia wynikającego z korelacji danych, wykonanych przez regułę korelacyjną,

4.8.14.6. System musi umożliwiać tworzenie reguł korelacyjnych na bazie parsowanych logów/danych z różnych źródeł, oraz korelować dane w czasie rzeczywistym,

4.8.14.7. Reguły korelacji powinny być tworzone i zarządzane w interfejsie systemu, bez potrzeby użycia dodatkowych narzędzi firm trzecich,

4.8.14.8. Rozwiązanie musi umożliwiać wykrywanie sytuacji niestandardowej niezgodnej z poprzednio zarejestrowanym wzorcem (np. w celu wykrycia ataku DOS, wykrycia wewnętrznego ruchu sieciowego który wcześniej nie występował, uruchomienia nowej niewystępującej wcześniej aplikacji, pojawienia się nowego użytkownika itp),

4.8.14.9. Zaoferowane rozwiązanie musi umożliwiać łatwe i samodzielne tworzenie reguł parsowania logów/danych, tworzenie widoków/raportów kolejnych/nowych dowolnych źródeł danych, przez pracowników Zamawiającego po przeprowadzonych szkoleniach oraz warsztatowe przekazanie wiedzy.

4.8.15. Rozwiązanie musi posiadać następujące funkcje dotyczące raportowania: W zaoferowanym Systemie musi istnieć możliwość tworzenia własnych raportów, zarówno w formie tekstowej jak i reprezentacji graficznej, a także automatycznego, cyklicznego wysyłania raportów wiadomością e-mail, w postaci PDF.

4.8.16. Rozwiązanie musi zapewnić rozliczność działań użytkowników, w szczególności rejestrowanie dostępu do przetwarzanych logów/danych.

4.8.17. Rozwiązanie musi umożliwiać odseparowanie środowiska pracy użytkowników o rożnych rolach.

4.8.18. Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zawarte w zewnętrznych repozytoriach: Katalogi LDAP, Bazy danych, Dane geolokalizacyjne.

4.8.19. System musi umożliwiać korelację zdarzeń pochodzących z różnych systemów źródłowych na podstawie dowolnych pól i zmiennych logu lub dowolnych innych danych wzbogacających log (dane o tożsamości, geolokalizacja, dane o zasobach).

4.8.20. Rozwiązanie musi wspierać geolokalizację zdarzeń na bazie adresów IP. Dane geolokalizacyjne dla zdarzeń mają służyć do prezentacji na mapie, jak również umożliwiać ich wykorzystanie w wyszukiwaniu wartości pól oraz w regułach korelacyjnych.

4.8.21. System musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI jak i języka zapytań charakterystycznego dla danego systemu SIEM.

4.8.22. Musi istnieć możliwość zastosowania reguł korelacyjnych dla danych historycznych w celu wykrycia podobnych zdarzeń w przeszłości.

4.8.23. System musi umożliwiać tworzenie reguł korelacyjnych o długim okresie działania. Okres ten nie może być ograniczany żadnymi innymi limitami, poza dostępnością danych w systemie.

4.8.24. Wynikiem działania reguły korelacyjnej powinno być utworzenie alarmu lub zwiększenie współczynnika ryzyka związanego z obiektem uczestniczącym w zdarzeniu (użytkownik, host, port itp.).

4.8.25. System musi posiadać możliwość automatycznego reagowania na zdarzenie oraz powiadamiania administratorów. Musi istnieć możliwość wysłania email oraz możliwość konfigurowania innych akcji w postaci skryptów, do których może być przekazywana dowolna liczba argumentów na podstawie treści alarmu.

4.8.26. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o dane geolokalizacyjne np. kraj lub miasto.

4.8.27. System musi umożliwiać prezentację zdarzeń związanych z użytkownikiem niezależnie od tego z jakiego konta korzystał. Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o te dane.

4.8.28. System musi umożliwiać korzystanie z zewnętrznych wskaźników kompromitacji (ang. IOC).

5. Opis usług dla rozbudowy rozwiązania posiadanego „Splunk Enterprise”

5.1. Zakres rozbudowy systemu posiadanego „Splunk Enterpirse”:

5.1.1. Dostawa i rozbudowa posiadanej przez Zamawiającego licencji na Oprogramowanie „Splunk Enterprise” zgodnie z pkt 3. do wersji umożliwiającej obsługę wskazanych przez zamawiającego źródeł oraz przyrost danych na poziomie zgodnym z dostarczoną licencją oraz retencję na poziomie wskazanym w pkt. 2.3.1.;

5.1.2. Wykonawca dostarczy niezbędne pakiety wsparcia producenta na całość rozwiązania ważne przez cały okres obowiązywania Licencji.

5.1.3. Rekonfiguracja aktualnie działającego środowiska w tym dostosowanie platformy do zbierania zdarzeń z nw. źródeł;

5.1.4. Zapewnienie logowania danych ze źródeł: Centralnie Firewall, Active Directory, DNS, Urządzenia brzegowe z oddziałów terenowych na terenie kraju, ochrona Endpoint, EMM, NSX, VMware, Serwery Pocztowe, Serwery Spam-u, urządzenia sieciowe Cisco, Cisco ISE, Ubiquity, syslog-ng, logi systemowe Windows Server, logi systemowe Linux, logi web serwisów (głównie Apache/Tomcat), Radius, Active Identity, Własne dedykowane rozwiązania systemowe.

5.1.5. Architektura systemu musi być tak dostosowana aby zapewnić optymalną wydajność i skalowalność uwzględniając min. 1 serwer służący do przeszukiwania zbiorów oraz 2 serwery odpowiedzialne za indeksowanie danych. Zamawiający szacuje iż 80% ruchu zdarzeń będzie generowanie z 5 systemów tj. Firewall Centralny, Active Directory, oraz urządzenia brzegowe klasy UTM oddziałów terenowych zamawiającego w ilości ~ 500 szt. scentralizowane do jednego repozytorium w węźle centralnym wraz z ochroną Endpoint.

5.1.6. Zapewnienie wsparcia technicznego i serwisu gwarancyjnego Wykonawcy przez cały okres obowiązywania Umowy dla rozbudowanego rozwiązania.

5.2. Prace właściwe związane z rozbudową systemu posiadanego „Splunk Enterprise”:

5.2.1. Wykonawca po podpisaniu Umowy w maksymalnym terminie do 5 dni roboczych dostarczy Zamawiającemu licencje na oprogramowanie.

5.2.2. Wykonawca w maksymalnym terminie do 5 dni roboczych od zawarcia Umowy przeprowadzi analizę przedwdrożeniową w ramach rozbudowy środowiska wraz z Zamawiającym (Administratorzy EI.C, Administratorzy Systemów Centralnych) konsultacje mające na celu opracowanie strategii wdrażania oraz omówienie infrastruktury Zamawiającego. Czas konsultacji w wymiarze nie dłuższym niż 8 godzin. roboczych.

5.2.3. Wykonawca w maksymalnym terminie 10 dni roboczych od przeprowadzenia analizy przedwdrożeniowej, o której mowa w pkt. 5.2.2. wykona projekt techniczny obejmujący zakresem zmiany jakie będą wymagane w celu osiągnięcia najbardziej optymalnej pod względem szybkości działania i niezawodności topologii rozwiązania oraz sposoby implementacji źródeł danych. Wykonawca również opracuje scenariusze testów akceptacyjnych, plan testów, który musi być zatwierdzony przez Zamawiającego.

5.2.4. Wykonawca w maksymalnym terminie do 15 dni roboczych od dostarczenia projektu technicznego oraz scenariuszy testów akceptacyjnych , zainstaluje i skonfiguruje wszystkie komponenty zgodnie z opracowanym projektem technicznym w ramach rozbudowy środowiska.

5.2.5. Wykonawca w maksymalnym terminie do 2 dni roboczych od przeprowadzenia rozbudowy środowiska, o którym mowa w pkt 5.2.4 przeprowadzi w obecności przedstawicieli Zamawiającego Testy akceptacyjne dla wdrożonego rozwiązania. Pozytywny wynik Testów akceptacyjnych będzie stanowił podstawę odbioru wdrożenia przez Zamawiającego.

5.2.6. Wykonawca w maksymalnym terminie do 7 dni roboczych od przeprowadzenia wdrożenia, o którym mowa w pkt 5.2.5 wykona szczegółową dokumentację powykonawczą zawierającą dokładny opis architektury, instalacji i konfiguracji systemu SIEM. Dokumentacja powykonawcza będzie zawierała szczegółowy opis zastosowanych rozwiązań. Dokumenty zostaną dostarczone Zamawiającemu w języku polskim, w wersji elektronicznej na wskazany adres zgodnie z treścią Umowy.

5.2.7. Wykonawca w maksymalnym terminie do 14 dni roboczych od przeprowadzenia wdrożenia, o którym mowa w pkt 5.2.5 przeprowadzi szkolenie oraz warsztatowe przekazanie wiedzy zgodnie z wymaganiami Zamawiającego.

5.2.8. Wykonawca będzie świadczył usługi wsparcia dla rozbudowanego środowiska w okresie równym okresowi obowiązywania licencji z zastrzeżeniem iż okres nie będzie mniejszy niż 24 miesiące od dnia jej uruchomienia w środowisku Zamawiającego.

5.2.9. Do powyższych okresów realizacji zamówienia nie wlicza się terminów przewidzianych na czynności Zamawiającego takie jak procedury odbioru, oraz procedura udostępniania dostępów VPN.

5.3. Warunki licencjonowania oraz system gwarancyjny systemu „Splunk Enterprise” lub równoważnego:

5.3.1. Wykonawca wraz z dostawą licencji przekaże warunki gwarancji i procedury awarii, dostępne kanały komunikacyjne z serwisem Producenta i Wykonawcy.

5.3.2. Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu:

5.3.2.1. Wsparcie wykonawcy oraz serwis wdrożonego systemu zgodnie z okresem obowiązywania Umowy.

5.3.2.2. Wykonawca w ramach wsparcia zapewni Zamawiającemu 24 godziny konsultacji w formie telefonicznej lub na wskazany przez Wykonawcę adres e-mail w skali miesiąca przez cały okres obowiązywania Umowy.

5.3.2.3. Przyjmowanie w ramach serwisu zgłoszeń Zamawiającego przez 24 godziny na dobę, 7 dni w tygodniu.

5.3.2.4. Czas naprawy nie może przekroczyć dwudziestu czterech godzin liczonych od chwili wysłania zgłoszenia w dni robocze, zgłoszenia wysłane w ostatni dzień tygodnia roboczego zrealizowane będą w najbliższy dzień roboczy do godz.: 15:00. Czas naprawy rozumiany jest jako czas usunięcia przez Wykonawcę zgłoszonego przez Zamawiającego problemu liczonego od chwili przekazania informacji Wykonawcy w formie elektronicznej lub telefonicznej na wskazane przez Wykonawcę źródła kontaktu.

5.3.2.5. Możliwość aktualizacji oprogramowania w tym poprawek bezpieczeństwa przez dostęp do zasobów producenta.

5.3.2.6. Bezpośredni i wolny od dodatkowych opłat dostęp do pomocy technicznej producenta przez telefon, e-mail, w języku Polskim oraz serwis WWW, w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją systemu w trybie całodobowym w każdy dzień tygodnia 24/7/365.

5.3.2.7. Możliwość pobrania bezpośrednio od producenta nowych wydań oprogramowania, w ramach ogólnie dostępnej oferty producenta.

5.3.3. W okresie obowiązywania gwarancji, Wykonawca będzie świadczył usługi wsparcia przez wykwalifikowanych pracowników, posiadających ugruntowaną wiedzę potwierdzoną certyfikatami w zakresie systemu będącego przedmiotem Umowy.

5.3.4. Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.

5.3.5. Jeżeli wykorzystanie którejkolwiek z wymienionych w OPZ funkcjonalności wymaga zastosowania dodatkowej licencji lub oprogramowania, to należy je dostarczyć.

5.4. Warsztatowe przekazanie wiedzy wraz ze szkoleniem dla rozbudowy systemu „Splunk Enterprise”:

5.4.1. Wykonawca przeprowadzi szkolenie powdrożeniowe obejmujące zakresem, konfigurację, zarządzanie, rozwiązywanie problemów dostarczonego i wdrożonego systemu u Zamawiającego zgodnie z następującymi wymaganiami:

5.4.1.1. Liczba uczestników – do 8 osób;

5.4.1.2. Program szkolenia musi zawierać całość zagadnień obejmujących, zaawansowane administrowanie wdrożonym systemem wraz z rozbudową architektury, analizę gromadzonych danych oraz zapewnić umiejętności i wiedzę niezbędną w tym zakresie;

5.4.1.3. Szkolenie zostanie przeprowadzone w lokalizacji Zamawiającego w miejscu wdrożenia rozwiązania lub w formie Zdalnej na środowisku produkcyjnym oraz na środowisku szkoleniowym przygotowanym przez Wykonawcę w celu omówienia elementów wrażliwych mogących doprowadzić do uszkodzenia środowiska produkcyjnego Zamawiającego;

5.4.1.4. Wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej w formacie PDF;

5.4.1.5. Prowadzenie szkolenia przez wykładowców musi odbyć się w języku polskim;

5.4.1.6. Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie.

5.4.1.7. Wykonawca zobowiązany będzie do przeprowadzenia szkolenia zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem.

5.4.2. Wszyscy uczestnicy szkolenia otrzymają zaświadczenia w formie certyfikatu potwierdzające ukończenie szkolenia.

6. Opis usług dla rozwiązania równoważnego systemu klasy SIEM.

6.1. Zakres prac związanych z wdrożeniem rozwiązania równoważnego:

6.1.1. Wykonawca dostarczy niezbędne licencje i pakiety wsparcia producenta równoważne na całość rozwiązania ważne przez cały okres obowiązywania Licencji.
6.1.2. Migracja danych i ustawień aktualnie działającego systemu klasy SIEM oraz dostosowanie platformy do zbierania zdarzeń z nw. źródeł;
6.1.3. Zapewnienie logowania danych ze źródeł: Centralnie Firewall, Active Directory, DNS, Urządzenia brzegowe z oddziałów terenowych na terenie kraju, ochrona Endpoint, EMM, NSX, VMware, Serwery Pocztowe, Serwery Spam-u, urządzenia sieciowe Cisco, Cisco ISE, Ubiquity, syslog-ng, logi systemowe Windows Server, logi systemowe Linux, logi web serwisów (głównie Apache/Tomcat), Radius, Active Identity, Własne dedykowane rozwiązania systemowe.
6.1.4. Architektura systemu musi być tak dostosowana aby zapewnić optymalną wydajność i skalowalność uwzględniając min. 1 serwer służący do przeszukiwania zbiorów oraz 2 serwery odpowiedzialne za indeksowanie danych. Zamawiający szacuje iż 80% ruchu zdarzeń będzie generowanie z 5 systemów tj. Firewall Centralny, Active Directory, oraz urządzenia brzegowe klasy UTM oddziałów terenowych zamawiającego w ilości ~ 500 szt. scentralizowane do jednego repozytorium w węźle centralnym wraz z ochroną Endpoint.
6.1.5. Zapewnienie wsparcia technicznego i serwisu gwarancyjnego Wykonawcy przez cały okres obowiązywania Umowy dla rozbudowanego rozwiązania.

6.2. Prace właściwe związane z wdrożeniem rozwiązania równoważnego:

6.2.1. Wykonawca niezwłocznie po podpisaniu Umowy w maksymalnym terminie do 5 dni roboczych dostarczy Zamawiającemu licencje na oprogramowanie równoważne.
6.2.2. Wykonawca w maksymalnym terminie do 14 dni roboczych od podpisania Umowy przeprowadzi szkolenie certyfikowane oraz warsztatowe przekazanie wiedzy zgodnie z wymaganiami Zamawiającego.
6.2.3. Wykonawca w maksymalnym terminie do 6 dni roboczych od zawarcia Umowy przeprowadzi analizę przedwdrożeniową w ramach wdrożenia rozwiązania równoważnego wraz z Zamawiającym (Administratorzy EI.C, Administratorzy Systemów Centralnych) konsultacje mające na celu opracowanie strategii wdrażania oraz omówienie infrastruktury Zamawiającego. Czas konsultacji w wymiarze nie dłuższym niż 8 godzin. roboczych.
6.2.4. Wykonawca w maksymalnym terminie 11 dni roboczych od przeprowadzenia analizy przedwdrożeniowej, o której mowa w pkt. 6.2.3 wykona projekt techniczny obejmujący zakresem zmiany jakie będą wymagane w celu osiągnięcia najbardziej optymalnej pod względem szybkości działania i niezawodności topologii rozwiązania oraz sposoby implementacji źródeł danych oraz migracji danych z posiadanego przez Zamawiającego oprogramowania klasy SIEM. Wykonawca również opracuje scenariusze testów akceptacyjnych, plan testów, który musi być zatwierdzony przez Zamawiającego.
6.2.5. Wykonawca w maksymalnym terminie do 16 dni roboczych od dostarczenia projektu technicznego oraz scenariuszy testów akceptacyjnych , zainstaluje i skonfiguruje wszystkie komponenty zgodnie z opracowanym projektem

technicznym w ramach wdrożenia środowiska wraz z migracją danych z systemu obecnie używanego przez Zamawiającego.

6.2.6. Wykonawca w maksymalnym terminie do 2 dni roboczych od przeprowadzenia rozbudowy środowiska, o której mowa w pkt 6.2.5 przeprowadzi w obecności przedstawicieli Zamawiającego Testy akceptacyjne dla wdrożonego środowiska. Pozytywny wynik Testów akceptacyjnych będzie stanowił podstawę do odbioru wdrożonego rozwiązania przez Zamawiającego.

6.2.7. Wykonawca w maksymalnym terminie do 7 dni roboczych przeprowadzenia wdrożenia, o którym mowa w pkt 6.2.5 opracuje szczegółową dokumentację powykonawczą zawierającą dokładny opis architektury, instalacji i konfiguracji systemu SIEM. Dokumentacja powykonawcza będzie zawierała szczegółowy opis zastosowanych rozwiązań. Dokumenty zostaną dostarczone Zamawiającemu w języku polskim, w wersji elektronicznej na wskazany adres zgodnie z treścią Umowy.

6.2.8. Wykonawca w maksymalnym terminie do 14 dni roboczych od przeprowadzenia wdrożenia, o którym mowa w pkt 6.2.5 przeprowadzi szkolenie powdrożeniowe oraz warsztatowe przekazanie wiedzy zgodnie z wymaganiami Zamawiającego.

6.2.9. Wykonawca będzie świadczył usługi wsparcia dla wdrożonego rozwiązania równoważnego w okresie równym okresowi obowiązywania licencji z zastrzeżeniem iż okres nie będzie mniejszy niż 24 miesiące od dnia jej uruchomienia w środowisku Zamawiającego.

6.2.10. Do powyższych okresów realizacji zamówienia nie wlicza się terminów przewidzianych na czynności Zamawiającego takie jak procedury odbioru, oraz procedura udostępniania dostępów VPN.

6.3. Warsztatowe przekazanie wiedzy wraz ze szkoleniem dla rozwiązania równoważnego:

6.3.1. Wykonawca przeprowadzi szkolenie obejmujące zakresem, konfigurację, zarządzanie, rozwiązywanie problemów dostarczonego i wdrożonego systemu u Zamawiającego oraz Szkolenie Certyfikowane przez autoryzowany ośrodek szkoleniowy na terenie RP dla oferowanego rozwiązania równoważnego zgodnie z następującymi wymaganiami:

6.3.1.1. Liczba uczestników szkolenia powdrożeniowego oraz szkolenia certyfikowanego – do 8 osób;

6.3.1.2. Program szkolenia musi zawierać całość zagadnień obejmujących, podstawową administrację, zaawansowane administrowanie wdrożonym systemem wraz z rozbudową architektury, analizę gromadzonych danych oraz zapewnić umiejętności i wiedzę niezbędną w tym zakresie;

6.3.1.3. Szkolenie powdrożeniowe zostanie przeprowadzone w lokalizacji Zamawiającego w miejscu wdrożenia rozwiązania lub w formie Zdalnej na środowisku produkcyjnym oraz na środowisku szkoleniowym przygotowanym przez Wykonawcę w celu omówienia elementów wrażliwych mogących doprowadzić do uszkodzenia środowiska produkcyjnego Zamawiającego;

6.3.1.4. Szkolenie certyfikowane dla produktów producenta rozwiązania równoważnego zostanie przeprowadzone przez autoryzowany ośrodek szkoleniowy w formule Zdalnej lub w autoryzowanym ośrodku szkoleniowym na terenie Polski obejmujący zakresem pkt. 6.3.1.2;

6.3.1.5. Wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej w formacie PDF;

6.3.1.6. Prowadzenie szkolenia przez wykładowców musi odbyć się w języku polskim;

6.3.1.7. Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie.

6.3.1.8. Wykonawca zobowiązany będzie do przeprowadzenia szkolenia zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem.

6.3.2. Wszyscy uczestnicy szkolenia otrzymają zaświadczenia w formie certyfikatu potwierdzające ukończenie szkolenia.