

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 23.12.2024 r.

1.1. W ramach realizacji przedmiotu zamówienia konieczne jest wykonanie następujących czynności, oraz doprowadzenie przez Wykonawcę do:

- 1.1.1. Dostawy licencji / subskrypcji na konto Zamawiającego dla posiadanego oprogramowania klasy „SIEM” wraz ze wsparciem producenta, liczoną od dnia uruchomienia, w infrastrukturze zamawiającego w modelu tradycyjnym (on-premise);
- 1.1.2. Dostępu do aktualizacji i poprawek oprogramowania opublikowanych przez producenta, dostępu do wsparcia technicznego producenta na poziomie Standard;
- 1.1.3. Konsultacje między Zamawiającym a Wykonawcą w celu opracowania analizy przedwdrożeniowej;
- 1.1.4. Wykonanie projektu technicznego rozbudowy w oparciu o istniejącą architekturę;
- 1.1.5. Prace właściwe związane z rozbudową jak również przygotowanie dokumentacji i instrukcji użytkownika wdrożonego systemu;
- 1.1.6. Przeprowadzenie przez Wykonawcę warsztatowego przekazania wiedzy z zakresu wdrożonego rozwiązania;
- 1.1.7. Zagwarantowanie i przeprowadzenie przez Wykonawcę autoryzowanego szkolenia w certyfikowanym ośrodku szkoleniowym;
- 1.1.8. Serwis oraz gwarancję wdrożonego rozwiązania w zakresie zdefiniowanym przez Zamawiającego, gwarancja na okres nie krótszy niż 12 miesięcy;

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 Enterprise” 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 przygotowania projektu technicznego, dokumentację wdrożenia w oparciu o rozbudowę aktualnie działającego systemu przy założeniu iż system będzie spełniał następujące wymagania zgodnie z opisem zamówienia.
- 1.6. Oferent przedstawi koszty przeprowadzenia szkolenia w autoryzowanym ośrodku oraz przekaże wiedzę w zakresie wdrażanego rozwiązania na infrastrukturze zamawiającego zgodnie z wymaganiami określonymi w niniejszym dokumencie.
- 1.7. 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.
- 1.8. 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	350	30.01.2025r.

2.2) Aktualne środowisko aplikacji SIEM Zamawiającego:

1.2.1. Zamawiający posiada uruchomione następujące maszyny wirtualne:

- 1.2.1.1. Splunk DMC (CM,DS.,LM);
- 1.2.1.2. Splunk Heavy Forwarder #1;
- 1.2.1.3. Splunk Heavy Forwarder #2;
- 1.2.1.4. Splunk Indexer #1;
- 1.2.1.5. Splunk Indexer #2;
- 1.2.1.6. Splunk Search Head #1;

1.2.2. Infrastruktura zamawiającego przeznaczona na realizację niniejszego postępowania .:

- 1.2.2.1. 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 dodatkowe co najmniej trzy wydzielone serwery każdy o parametrach CPU 32 core / vCPU 64core 2,9GHz oraz sumaryczną pamięć 128 GB RAM oraz dyski obsługujące min. 800 IOPS o pojemności 15TB na dane.

- 1.2.2.2. 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	500	12 miesięcy
Splunk Enterprise Security - Term License with Standard Success Plan - GB/day	500	12 miesięcy

3.2 Dostawa, licencji dla posiadanego przez Zamawiającego oprogramowania musi obowiązywać od dnia 23.12.2024 r. oraz zapewniać wsparcie producenta przez okres minimum 12 miesięcy kalendarzowych, liczonych od dnia uruchomienia licencji w infrastrukturze Zamawiającego.

4. Opis rozwiązania równoważnego systemu klasy SIEM.

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 January 2024r.”

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. Rozwiązanie powinno posiadać udokumentowane wdrożenia o podobnej skali.

4.5 W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego, Wykonawca dokona migracji danych z obecnie używanego rozwiązania SIEM „Splunk Enterprise” przy zachowaniu ciągłości działania systemu SIEM między aktualnym rozwiązaniem a rozwiązaniem równoważnym 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 geo-lokalizację zdarzeń na bazie adresów IP. Dane geo-lokalizacyjne 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 System musi wspierać pracę użytkowników o różnych rolach i w następujących obszarach:
 - 4.8.10.1 Analizy zdarzeń w obszarze bezpieczeństwa teleinformatycznego;
 - 4.8.10.2 Analizy pracy systemów informatycznych w zakresie wydajności i awarii systemów/urządzeń teleinformatycznych;
 - 4.8.10.3 Analizy pracy aplikacji własnych dedykowanych rozwiązań programowych;
 - 4.8.11 System musi posiadać predefiniowane widoki dedykowane dla specjalistów odpowiedzialnych za poszczególne domeny bezpieczeństwa:
 - 4.8.11.1 Wykrywanie i przeciwdziałanie złośliwemu oprogramowaniu;
 - 4.8.11.2 Wykrywanie i obsługa podatności;
 - 4.8.11.3 Analiza ruchu sieciowego;

- 4.8.11.4 Analiza oraz śledzenie wykorzystywanych portów i protokołów
- 4.8.12 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.
- 4.8.13 Rozwiązanie powinno pozwalać na analizę niestandardowych logów wygenerowanych przez aplikacje własne.
- 4.8.14 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 operacyjnego (Red Hat, Microsoft Windows), usługi serwerowej (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.
- 4.8.15 Zaoferowane rozwiązanie musi umożliwić zapewnić kontrolę dostępu na poziomie Role Based Access Control w granulacji na poziomie wartości poszczególnych, identyfikowanych danych.
- 4.8.16
- 4.8.17 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:
 - 4.8.17.1 Wysyłanie logów / danych ze źródłowego systemu na wskazany port TCP/UDP serwera, będącego częścią wdrażanego rozwiązania (np. syslog),
 - 4.8.17.2 Rozwiązanie musi wspierać zbieranie danych w formacie CEF oraz przyjmowanie logów z Syslog Relay,
 - 4.8.17.3 Wskazanie w interfejsie użytkownika wdrażanego rozwiązania Systemu na znajdujący się lokalnie plik / katalog,
 - 4.8.17.4 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,
- 4.8.18 Rozwiązanie musi umożliwiać następujące funkcje dotyczące pracy nad logami:
 - 4.8.18.1 Rozwiązanie musi umożliwiać parsowanie logów o długości co najmniej 10 000 znaków oraz zawierających więcej niż jedną linię,
 - 4.8.18.2 Rozwiązanie musi umożliwiać tworzenie bazy definicji formatów logów,
 - 4.8.18.3 Rozwiązanie musi wyszukiwać czas zdarzenia (timestamp) z analizowanego logu i wykorzystywać go do reguł korelacyjnych,
 - 4.8.18.4 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,
 - 4.8.18.5 Rozwiązanie musi umożliwiać tworzenie alertów/powiadomień po wykryciu zdarzenia wynikającego z korelacji danych, wykonanych przez regułę korelacyjną,

- 4.8.18.6 System musi umożliwiać tworzenie reguł korelacyjnych na bazie parsowanych logów/danych z różnych źródeł, oraz korelować dane w czasie rzeczywistym,
- 4.8.18.7 Reguły korelacji powinny być tworzone i zarządzane w interfejsie systemu, bez potrzeby użycia dodatkowych narzędzi firm trzecich,
- 4.8.18.8 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.),
- 4.8.18.9 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.
- 4.8.19 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 w wiadomości e-mail, w postaci PDF.
- 4.8.20 Rozwiązanie musi zapewnić rozliczność działań użytkowników, w szczególności rejestrowanie dostępu do przetwarzanych logów/danych.
- 4.8.21 Rozwiązanie musi umożliwiać odseparowanie środowiska pracy użytkowników o różnych rolach.
- 4.8.22 Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zawarte w zewnętrznych repozytoriach: Katalogi LDAP, Bazy danych, Dane geo-lokalizacyjne.
- 4.8.23 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, geo-lokalizacja, dane o zasobach).
- 4.8.24 Rozwiązanie musi wspierać geo-lokalizację zdarzeń na bazie adresów IP. Dane geo-lokalizacyjne dla zdarzeń mają służyć do prezentacji na mapie, jak również umożliwiać ich wykorzystanie w wyszukiwaniu wartości pól oraz w regułach korelacyjnych.
- 4.8.25 System musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI jak i języka zapytań charakterystycznego dla danego systemu SIEM.
- 4.8.26 Musi istnieć możliwość zastosowania reguł korelacyjnych dla danych historycznych w celu wykrycia podobnych zdarzeń w przeszłości.
- 4.8.27 System musi umożliwiać tworzenie reguł korelacyjnych o długim okresie działania. Okres ten nie może być ograniczany żadnymi innymi limitami, poza dostępnością danych w systemie.
- 4.8.28 Wynikiem działania reguły korelacyjnej powinno być utworzenie alarmu lub zwiększenie współczynnika ryzyka związanego z obiektem uczestniczącym w zdarzeniu (użytkownik, host, port itp.).

- 4.8.29 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.
- 4.8.30 Musi istnieć możliwość filtracji, alarmowania i korelowania w oparciu o dane geo-lokalizacyjne np. kraj lub miasto.
- 4.8.31 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.
- 4.8.32 System musi umożliwiać korzystanie z zewnętrznych wskaźników kompromitacji (ang. IOC) oraz zawiera implementację framework MITRE ATT&CK.
- 4.8.33 System musi zawierać mechanizmy zarządzania incydentami obejmujące co najmniej:
 - 4.8.33.1 Możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych;
 - 4.8.33.2 Możliwość przypisania incydentu do osoby;
 - 4.8.33.3 Możliwość zmiany statusu i priorytetu incydentu;
 - 4.8.33.4 Możliwość tworzenia komentarzy;
 - 4.8.33.5 Możliwość automatycznego i ręcznego modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy.
 - 4.8.33.6 Możliwość tworzenia wyjątków stałych i czasowych dla reguł i zdarzeń spełniających określone warunki.

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

5.1. Zakres rozbudowy systemu posiadanego „Splunk Enterprise”:

- 5.1.1. Dostawa i rozbudowa posiadanej przez Zamawiającego licencji na Oprogramowanie „Splunk Enterprise” oraz „Splunk Enterprise Security” zgodnie z pkt 3 do wersji umożliwiającej obsługę aktualnie działających źródeł w infrastrukturze Zamawiającego.
- 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 do rozwiązania Splunk Enterprise Security w tym:
 - 5.1.3.1. Budowę systemu detekcji zdarzeń bezpieczeństwa z wykorzystaniem reguł korelacyjnych;
 - 5.1.3.2. Normalizację istniejących źródeł do standardu CIM;
 - 5.1.3.3. Rozbudowę macierzy uprawnień RBAC (Role-Base Access Control);
- 5.1.4. Zapewnienie logowania nowych źródeł danych lub modyfikacja istniejących źródeł do których mogą należeć .: Centralnie Firewall, Active Directory, DNS, Urządzenia brzegowe z oddziałów terenowych na terenie kraju, ochrona Endpoint/EDR, 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 uruchomienie w infrastrukturze Zamawiającego dodatkowo min. 1 serwer służący do przeszukiwania zbiorów (SH) oraz 2 serwery odpowiedzialne za indeksowanie danych (IDX).
 - 5.1.6. Zapewnienie wsparcia technicznego i serwisu gwarancyjnego Wykonawcy na całość rozwiązania przez cały okres obowiązywania Umowy.
 - 5.1.7. Świadczenie usług dodatkowych prac oraz konsultacji w zakresie funkcjonowania Systemu mające na celu rozwój wdrożonego 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 zgodne z OPZ.
- 5.2.2. Wykonawca w maksymalnym terminie do 10 dni roboczych od zawarcia Umowy przeprowadzi analizę przedwdrożeniową w ramach rozbudowy środowiska wraz z Zamawiającym (Administratorzy DGLP, Administratorzy ZILP) konsultacje mające na celu opracowanie strategii wdrażania oraz omówienie infrastruktury Zamawiającego. Czas konsultacji w wymiarze nie dłuższym niż 24 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 25 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 5 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 10 dni roboczych od przeprowadzenia wdrożenia, o którym mowa w pkt 5.2.4 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 5.2.4 przeprowadzi warsztatowe przekazanie wiedzy zgodnie z wymaganiami Zamawiającego.

- 5.2.8. Wykonawca w maksymalnym terminie do 10 dni roboczych od zawarcia Umowy, zorganizuje autoryzowane szkolenie w certyfikowanym ośrodku szkoleniowym, o którym mowa w pkt 5.5 przy czym realizacja szkoleń nie może się odbyć później niż 3 miesiące kalendarzowe od dnia zawarcia Umowy.
- 5.2.9. Wykonawca będzie świadczył usługi wsparcia dla rozbudowanego środowiska w okresie równym okresowi obowiązywania licencji z zastrzeżeniem iż okres nie będzie mniejszy niż 12 miesięcy od dnia jej uruchomienia w środowisku Zamawiającego.
- 5.2.10. Do powyższych okresów realizacji zamówienia nie wlicza się terminów przewidzianych na czynności Zamawiającego takie jak procedury odbioru, oraz procedura udostępniania dostępu VPN.

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

- 5.3.1. Wykonawca wraz z dostawą licencji prześle 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 przez cały okres obowiązywania Umowy.
 - 5.3.2.2. Wykonawca w ramach wsparcia zapewni Zamawiającemu 160 roboczogodzin konsultacji w tym świadczenie prac mających na celu rozwój wdrożonego rozwiązania wychodzący ponad zakres rozbudowy w formie zdalnej, telefonicznej lub na wskazany przez Wykonawcę adres e-mail 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 z wdrożonego rozwiązania:

- 5.4.1. Wykonawca przeprowadzi warsztatowe przekazanie wiedzy powdrożeniowe obejmujące zakresem, konfigurację, zarządzanie, rozwiązywanie problemów dostarczonego i wdrożonego systemu oraz zmiany jakie zostały wprowadzone u Zamawiającego zgodnie z następującymi wymaganiami:

- 5.4.1.1. Liczba uczestników – do 8 osób;
- 5.4.1.2. Przekazanie wiedzy musi zawierać całość zagadnień obejmujących, zaawansowane administrowanie wdrożonym systemem wraz z rozbudową architektury, analizę gromadzonych danych oraz zapewnić wiedzę niezbędną w tym zakresie;
- 5.4.1.3. Warsztatowe przekazanie wiedzy zostanie przeprowadzone w lokalizacji Zamawiającego 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. Przekazanie wiedzy musi odbyć się w języku polskim;
- 5.4.1.5. Wykonawca zobowiązany będzie do przeprowadzenia warsztatów dot. przekazania wiedzy zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem.
- 5.4.1.6. Warsztatowe przekazanie wiedzy podlega ocenie warunkującej odbiór. Ocena zostanie dokonana na podstawie ankiety wypełnianej przez słuchaczy, obejmującej ocenę prowadzenia zajęć przez wykładowcę, zakresu przekazanej wiedzy. Kryteria oceny są następujące:
 - Najwyższa ocena 5, najniższa ocena 2;
 - Średnia ocen 3,0 i powyżej oznacza należyście przeprowadzone warsztaty z przekazania wiedzy;
 - Średnia ocen 2,9 i poniżej oznacza nienależyście przeprowadzone warsztaty z przekazania wiedzy;
- 5.4.1.7. Przekazanie wiedzy przeprowadzone nienależyście Wykonawca powtórzy na własny koszt, w terminie wyznaczonym przez Zamawiającego, jednak nie później niż w terminie 10 dni roboczych od dnia zakończenia warsztatów z przekazania wiedzy podlegających powtórzeniu.

5.5. Autoryzowane szkolenie w certyfikowanym ośrodku szkoleniowym:

- 5.5.1. Wykonawca zorganizuje i zagwarantuje szkolenie w autoryzowanym przez producenta rozwiązania ośrodku szkoleniowym obejmujące zakresem program szkolenia:
- 5.5.1.1. Splunk Enterprise System Administration (SESA);
 - 5.5.1.2. Splunk Enterprise Data Administration (SEDA);
 - 5.5.1.3. Using Splunk Enterprise Security (USES);
 - 5.5.1.4. Administering Splunk Enterprise Security (ASES);
- 5.5.2. Szkolenie zrealizowane zostanie zgodnie z następującymi wymogami:
- 5.5.2.1. Liczba uczestników – do 8 osób;
 - 5.5.2.2. Szkolenie zostanie przeprowadzone w certyfikowanym ośrodku szkoleniowym w formie lokalnej lub zdalnej;

- 5.5.2.3. Wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej¹
- 5.5.2.4. Prowadzenie szkolenia przez wykładowców musi odbyć się w języku polskim;
- 5.5.2.5. Wykonawca zobowiązany będzie do organizacji szkolenia zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym¹ i harmonogramem;
- 5.5.2.6. Sumaryczny czas na realizację programu szkoleń z zakresu pkt. 5.5.1 powinien wynosić min. 9 dni roboczych oraz nie powinien być krótszy niż 21 godzin lekcyjnych.
- 5.5.2.7. Szkolenie podlega ocenie warunkującej odbiór. Ocena zostanie dokonana na podstawie ankiety wypełnianej przez słuchaczy, obejmującej ocenę prowadzenia zajęć przez wykładowcę, ocenę materiałów szkoleniowych oraz zakresu przekazanej wiedzy. Kryteria oceny są następujące:
- Najwyższa ocena 5, najniższa ocena 2;
 - Średnia ocen 3,0 i powyżej oznacza należyście przeprowadzone szkolenie;
 - Średnia ocen 2,9 i poniżej oznacza nienależyście przeprowadzone szkolenie;
- 5.5.2.8. Szkolenie przeprowadzone nienależyście Wykonawca powtórzy na własny koszt, w terminie wyznaczonym przez Zamawiającego, jednak nie później niż w terminie 10 dni roboczych od dnia zakończenia szkolenia podlegających powtórzeniu.
- 5.5.3. 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 Wykonawca dokona migracji danych i ustawień w tym infrastruktury i źródeł z aktualnie działającego systemu klasy SIEM, przy zachowaniu ciągłości działania aktualnie działającego systemu, tak aby zachowana była ciągłość działania pracy oraz migracja nie wpływała na obniżenie bezpieczeństwa infrastruktury Zamawiającego.
- 6.1.3 Wykonawca dostosuje platformę do aktualnie używanych raportów oraz widoków.
- 6.1.4 Wykonawca dokona wdrożenia i zbuduje system w oparciu o detekcję zdarzeń z wykorzystaniem reguł korelacyjnych, normalizację źródeł do standardu CIM oraz rozbuduje macierz uprawnień RBAC (Role-Base Access Control);

¹ Zakres tematyczny szkolenia nie może być mniejszy niż oferowany przez autoryzowany program szkolenia producenta zaoferowanego rozwiązania

- 6.1.5 Wykonawca dokona migracji aktualnie działających źródeł oraz zapewni możliwość logowania nowych źródeł do których mogą należeć: Centralnie Firewall, Active Directory, DNS, Urządzenia brzegowe z oddziałów terenowych na terenie kraju, ochrona Endpoint, EMM, NSX, VMware, Serwery Pocztove, 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.
- 6.1.6 Architektura systemu musi być tak dostosowana aby zapewnić optymalną wydajność i skalowalność działających systemów w infrastrukturze Zamawiającego,
- 6.1.7 Zapewnienie wsparcia technicznego i serwisu gwarancyjnego Wykonawcy przez cały okres obowiązywania Umowy dla rozbudowanego rozwiązania.
- 6.1.8 Świadczenie usług dodatkowych prac oraz konsultacji w zakresie funkcjonowania Systemu mające na celu rozwój wdrożonego rozwiązania.

6.2 Prace właściwe związane z wdrożeniem rozwiązania równoważnego:

- 6.2.1 Wykonawca po podpisaniu Umowy w maksymalnym terminie do 5 dni roboczych dostarczy Zamawiającemu licencje na oprogramowanie zgodne z OPZ.
- 6.2.2 Wykonawca w maksymalnym terminie do 10 dni roboczych od zawarcia Umowy przeprowadzi analizę przedwdrożeniową w ramach rozbudowy środowiska wraz z Zamawiającym (Administratorzy DGLP, Administratorzy ZILP) konsultacje mające na celu opracowanie strategii wdrażania oraz omówienie infrastruktury Zamawiającego. Czas konsultacji w wymiarze nie dłuższym niż 24 godzin. roboczych.
- 6.2.3 Wykonawca w maksymalnym terminie 10 dni roboczych od przeprowadzenia analizy przedwdrożeniowej, o której mowa w pkt. 6.2.2. 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.
- 6.2.4 Wykonawca w maksymalnym terminie do 30 dni roboczych od dostarczenia projektu technicznego oraz scenariuszy testów akceptacyjnych , zainstaluje i skonfiguruje wszystkie komponenty zgodnie z opracowanym projektem technicznym w ramach migracji i rozbudowy środowiska z aktualnie działającego systemu do systemu równoważnego.
- 6.2.5 Wykonawca w maksymalnym terminie do 5 dni roboczych od przeprowadzenia rozbudowy środowiska, o którym mowa w pkt 6.2.4 przeprowadzi w obecności przedstawicieli Zamawiającego Testy akceptacyjne dla wdrożonego rozwiązania. Pozytywny wynik Testów akceptacyjnych będzie stanowił podstawę odbioru wdrożenia przez Zamawiającego.
- 6.2.6 Wykonawca w maksymalnym terminie do 10 dni roboczych od przeprowadzenia wdrożenia, o którym mowa w pkt 6.2.4 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.
- 6.2.7 Wykonawca w maksymalnym terminie do 14 dni roboczych od przeprowadzenia wdrożenia, o którym mowa w pkt 6.2.4 przeprowadzi warsztatowe przekazanie wiedzy zgodnie z wymaganiami Zamawiającego.
 - 6.2.8 Wykonawca w maksymalnym terminie do 10 dni roboczych od zawarcia Umowy, przedstawi zakres tematyczny i harmonogram autoryzowanego szkolenia² w certyfikowanym ośrodku szkoleniowym, o którym mowa w pkt 6.4 przy czym realizacja szkoleń nie może się odbyć później niż 3 miesiące kalendarzowe od dnia zawarcia Umowy.
 - 6.2.9 Wykonawca będzie świadczył usługi wsparcia dla wdrożonego środowiska w okresie równym okresowi obowiązywania licencji z zastrzeżeniem iż okres nie będzie mniejszy niż 12 miesięcy 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 dostępow VPN.
- 6.3 Warsztatowe przekazanie wiedzy wraz ze szkoleniem dla rozwiązania równoważnego:
- 6.3.1 Wykonawca przeprowadzi warsztatowe przekazanie wiedzy powdrożeniowe obejmujące zakresem, konfigurację, zarządzanie, rozwiązywanie problemów dostarczonego i wdrożonego systemu równoważnego oraz zmiany jakie zostały wprowadzone u Zamawiającego zgodnie z następującymi wymaganiami:
 - 6.3.1.1 Liczba uczestników – do 8 osób;
 - 6.3.1.2 Przekazanie wiedzy musi zawierać całość zagadnień obejmujących, zaawansowane administrowanie wdrożonym systemem wraz z rozbudową architektury, analizę gromadzonych danych oraz zapewnić wiedzę niezbędną w tym zakresie;
 - 6.3.1.3 Warsztatowe przekazanie wiedzy zostanie przeprowadzone w lokalizacji Zamawiającego 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 Przekazanie wiedzy musi odbyć się w języku polskim;
 - 6.3.1.5 Wykonawca zobowiązany będzie do przeprowadzenia przekazaniu wiedzy zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem.
 - 6.3.1.6 Warsztatowe przekazanie wiedzy podlega ocenie warunkującej odbiór. Ocena zostanie dokonana na podstawie ankiety wypełnianej przez słuchaczy, obejmującej ocenę prowadzenia zajęć przez wykładowcę, zakresu przekazanej wiedzy. Kryteria oceny są następujące:
 - Najwyższa ocena 5, najniższa ocena 2;
 - Średnia ocen 3,0 i powyżej oznacza należyście przeprowadzone warsztaty z przekazania wiedzy;

² Zakres tematyczny szkolenia nie może być mniejszy niż oferowany przez autoryzowany program szkolenia producenta zaoferowanego rozwiązania

– Średnia ocen 2,9 i poniżej oznacza nienależyte przeprowadzone warsztaty z przekazania wiedzy;

- 6.3.1.7 Przekazanie wiedzy przeprowadzone nienależyte Wykonawca powtórzy na własny koszt, w terminie wyznaczonym przez Zamawiającego, jednak nie później niż w terminie 10 dni roboczych od dnia zakończenia warsztatów z przekazania wiedzy podlegających powtórzeniu.

6.4 Autoryzowane szkolenie w certyfikowanym ośrodku szkoleniowym dla rozwiązania równoważnego:

- 6.4.1 Wykonawca zorganizuje i zagwarantuje szkolenie w autoryzowanym ośrodku szkoleniowym obejmujące zakresem program szkolenia równoważny z zakresem szkoleń zgodnym z pkt 5.5.1 dostosowanym do oferowanego rozwiązania równoważnego;
- 6.4.2 Szkolenie zrealizowane zostanie zgodnie z następującymi wymogami:
- 6.4.2.1 Liczba uczestników – do 8 osób;
 - 6.4.2.2 Szkolenie zostanie przeprowadzone w certyfikowanym ośrodku szkoleniowym w formie lokalnej lub zdalnej;
 - 6.4.2.3 Wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej³
 - 6.4.2.4 Prowadzenie szkolenia przez wykładowców musi odbyć się w języku polskim;
 - 6.4.2.5 Wykonawca zobowiązany będzie do organizacji szkolenia zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem³;
 - 6.4.2.6 Szkolenie podlega ocenie warunkującej odbiór. Ocena zostanie dokonana na podstawie ankiety wypełnianej przez słuchaczy, obejmującej ocenę prowadzenia zajęć przez wykładowcę, ocenę materiałów szkoleniowych oraz zakresu przekazanej wiedzy. Kryteria oceny są następujące:
 - Najwyższa ocena 5, najniższa ocena 2;
 - Średnia ocen 3,0 i powyżej oznacza należyte przeprowadzone szkolenie;
 - Średnia ocen 2,9 i poniżej oznacza nienależyte przeprowadzone szkolenie;
 - 6.4.2.7 Szkolenie przeprowadzone nienależyte Wykonawca powtórzy na własny koszt, w terminie wyznaczonym przez Zamawiającego, jednak nie później niż w terminie 10 dni roboczych od dnia zakończenia szkolenia podlegających powtórzeniu.
- 6.4.3 Wszyscy uczestnicy szkolenia otrzymają zaświadczenia w formie certyfikatu potwierdzające ukończenie szkolenia.

6.5 Prawo opcji dla rozwiązania posiadanego oraz rozwiązania równoważnego:

Nazwa licencji:	Ilość GB/dzień:	Okres obowiązywania:	Ilość paczek- w ciągu 12 miesięcy:
Splunk Enterprise - Term License with Standard	250	1 miesiąc	24

³ Zakres tematyczny szkolenia nie może być mniejszy niż oferowany przez autoryzowany program szkolenia producenta zaoferowanego rozwiązania

Success Plan - GB/day lub równoważna			
Splunk Enterprise Security - Term License with Standard Success Plan - GB/day lub równoważna	250	1 miesiąc	24

- 6.5.1 Wykonawca w ramach prawa opcji dostarczy i uruchomi licencje / subskrypcje w formie paczek na koncie Zamawiającego do wykorzystania w rozbiu miesięcznym przez cały okres obowiązywania Umowy na dodatkowe pakiety GB/day dla całego zaoferowanego środowiska przy zachowaniu funkcjonalności a jego uruchomienie jest zależne od zapotrzebowania zgłaszanego przez Zamawiającego.
- 6.5.2 Wykonawca w ramach opcji zapewni Zamawiającemu dodatkowo do 160 roboczogodzin konsultacji w tym świadczenie prac mających na celu rozwój wdrożonego rozwiązania wychodzący ponad zakres rozbudowy w formie zdalnej, telefonicznej lub na wskazany przez Wykonawcę adres e-mail do końca trwania Umowy.