Krajowe Centrum
Monitorowania
Ratownictwa Medycznego

Lotnicze Pogotowie Ratunkowe

ul. Księżycowa 5
01-934 Warszawa
tel. (22) 22-99-931/932
fax. (22) 22-99-933

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl

Załącznik nr 2 do SWZ

Opis Przedmiotu Zamówienia

Rozbudowa Infrastruktury POK-ZOK Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego na potrzeby systemu typu SIEM

Spis treści

Spis treści

1. Słowniki i skróty

Dla potrzeb niniejszego opracowania przyjmuje się następujące definicje skrótów i pojęć:

Skrót/pojęcie	Definicja
Awaria	Oznacza Awaria Krytyczna i/lub Awaria Niekrytyczna i/lub Awaria Zwykła.
Awaria Krytyczna	Oznacza brak działania środowiska powstałego w wyniku realizacji przedmiotowego postępowania, praca nie może być kontynuowana, operacja krytyczna dla procesu biznesowego jest niemożliwa. Awarie Krytyczne mają jedną lub więcej z poniższych cech: 1) dane biznesowe zostały uszkodzone; 2) funkcjonalność sprzętu i oprogramowania udokumentowana w projekcie technicznym nie działa; 3) System w zakresie funkcjonowania sprzętu i oprogramowania zdefiniowanego w projekcie technicznym przerywa działania i nie daje się uruchomić pomimo prób, stosując procedury przygotowane przez Wykonawcę, tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji; 4) wszelkie błędy związane z bezpieczeństwem przechowywania i przetwarzania danych, które mogą wpłynąć na: a) uwierzytelnianie, b) niezaprzeczalność, c) poufność, d) integralność, e) dostępność, f) rozliczalność; wszelkie awarie związane z bezpieczeństwem dostępu do Systemu (w tym nieautoryzowanym dostępem do danych).
Awaria Niekrytyczna	Utrudnia działanie Systemu w środowisku produkcyjnym w zakresie funkcjonalności krytycznej i uniemożliwia działanie Systemu w zakresie pozostałych funkcjonalności. W tym kontekście „utrudnia” oznacza istnienie sposobu jego obejścia, stosując przygotowane przez

	Wykonawcę procedury tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji (co może mieć wpływ na wygodę w użytkowaniu Systemu lub wymagać procedur ręcznych). „Uniemożliwia" oznacza brak możliwości jego obejścia.
Awaria Zwykła	Wszelki awaria niebędąca Awarią Krytyczną lub Awarią Niekrytyczną.
CPD	Centrum Przetwarzania Danych.
Dni Robocze	Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 08.00 do 15:35.
Dokumentacja	Wytworzone przez Wykonawcę w ramach realizacji Umowy i podlegające zatwierdzeniu przez Zamawiającego materiały w formie papierowej, jak również informacje zapisane na innych nośnikach, w tym nośnikach elektronicznych, w szczególności aktualizacja projektu infrastruktury fizycznej systemu, wykaz ilościowo-cenowy, dokumenty robocze wytworzone przez Wykonawcę w ramach realizacji Umowy. Za Dokumentację uznaje się także aktualizację projektu technicznego i dokumentacji powykonawczej Zamawiającego zawierającą w szczególności dokumentację prądową szaf serwerowych.
HA	High Availability - System wysokiej niezawodności (SWN), system wysokiej dostępności − systemy informatyczne charakteryzujące się odpowiednio dostosowywaną niezawodnością, dostępnością, wydajnością do specyficznych, zwykle krytycznych, zastosowań danego systemu.
Lokalizacja/ Lokalizacje	Oznacza wskazane przez Zamawiającego lokalizacje na terenie RP określone w przedmiocie niniejszego zamówienia. Zamówienie będzie realizowane w dwóch Ośrodkach Przetwarzania Danych w Warszawie oraz w Radomiu. Bliższe dane adresowe zostaną przekazane po podpisaniu Umowy.
NBAD	Network Behavior Anomalny Detection.
Oprogramowanie	Oprogramowanie Standardowe.
Oprogramowanie Standardowe	Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące przedmiotem dostaw w ramach realizacji niniejszego przedmiotu zamówienia, którego producentem jest Wykonawca lub podmiot trzeci.
POK	Podstawowy Ośrodek Krajowy.
SWD PRM	System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego.

SIEM	Security Information and Event Management.
System	System pozwalający łączyć logi dotyczące zdarzeń, zagrożeń i ryzyka który oferuje reagowanie na incydenty, zarządzanie logami i zaawansowane mechanizmy raportowania. Umożliwia konsolidowanie, korelowanie, ocenę i priorytetyzację zdarzeń dotyczących bezpieczeństwa posiadający ochronę antymalware.
ZOK	Zapasowy Ośrodek Krajowy.
Umowa	Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia.
Urządzenia	Sprzęt teleinformatyczny wraz z niezbędnym wyposażeniem i odnoszącą się do niego dokumentacją techniczną producenta, w tym również okablowanie strukturalne, będące przedmiotem niniejszego zamówienia.
Usługa Serwisu Gwarancyjnego	Usługa świadczona w ramach gwarancji udzielonej przez producenta lub autoryzowany serwis producenta, polegająca na zapewnieniu poprawności i ciągłości prawidłowego działania Urządzeń oraz ich poszczególnych komponentów, w szczególności usuwanie Awarii i błędów.
Wykonawca/Dostawca	Podmiot realizujący zamówienie.
Zamawiający	Lotnicze Pogotowie Ratunkowe.

Pozostałe pojęcia użyte w dokumencie należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem.

2. Przedmiot zamówienia

Przedmiotem zamówienia jest zakup Urządzeń i Oprogramowania Standardowego oraz niezbędnych licencji na potrzeby budowy Systemu typu SIEM pozwalającego na monitorowanie w czasie rzeczywistym i reagowanie na incydenty związane z bezpieczeństwem informatycznym SWD PRM. W związku z koniecznością budowy Systemu klasy SIEM, Zamawiający zamierza nabyć 3 serwery oraz oprogramowanie klasy SIEM, które zamierza na nich zainstalować. Licencje dostarczone wraz z oprogramowaniem muszą pozwolić na uruchomienie całości środowiska.

W ramach niniejszego postępowania Zamawiający zamierza zakupić 3 serwery wraz z systemem operacyjnym oraz oprogramowanie klasy SIEM wraz z licencją pozwalającą na uruchomienie 6 maszyn wirtualnych - po dwa na każdy serwer fizyczny. Wykonawca musi dostarczyć i zainstalować po jednym komplecie urządzeń we wskazanych przez Zamawiającego szafach RACK w ośrodkach POK i ZOK oraz w dodatkowej lokalizacji znajdującej się na terenie Miasta Stołecznego Warszawy.

Zamawiający zamierza uruchomić System na 6 maszynach wirtualnych w zarządzaniu wirtualizatora KVM na 3 fizycznych serwerach, które zamierza nabyć w ramach niniejszego postępowania w specyfikacji zgodnej z Tabelą nr 1.

2.1 Serwery – w ilości 3 sztuk

Wykonawca dostarczy Urządzenia w ukompletowaniu pojedynczego zestawu zgodnie z wymaganiami wskazanymi w Tabeli nr 1.

Ponadto Wykonawca wykona także usługę polegającą na montażu ww. Urządzeń we wskazanych przez Zamawiającego szafach typu RACK w lokalizacjach POK i ZOK oraz w lokalizacji znajdującej się na terenie Miasta Stołecznego Warszawy. W przypadku takiej konieczności, Wykonawca jest zobowiązany do modyfikacji instalacji prądowej, zabezpieczeń prądowych rozbudowywanych szaf RACK Zamawiającego oraz aktualizacji projektu technicznego i dokumentacji powykonawczej będących w posiadaniu Zamawiającego wraz z przekazaniem autorskich praw majątkowych Zamawiającemu do aktualizacji dokumentacji na zasadach określonych umową, w celu akceptacji modyfikacji przez administratora CPD.

Tabela nr 1 (ukompletowanie pojedynczego serwera)

Kod wymagania	Opis wymagania
S1.01	Procesor musi posiadać częstotliwość taktowania co najmniej 2,35 GHz.
S1.02	Procesor musi posiadać co najmniej 32 rdzeni i 64 wątki.
S1.03	Pamięć cache L3 procesora nie może być mniejsza niż 128 MB.
S1.04	Serwer musi posiadać co najmniej 512 GB pamięci RAM DDR4.
S1.05	Taktowanie pamięci RAM nie może być mniejsze niż 3200 MHz.
S1.06	Serwer musi posiadać co najmniej 160 TB pojemności netto.
S1.07	Prędkość obrotowa dysków co najmniej 7200 obr/min lub dyski SSD.
S1.08	Dyski muszą dać się wymienić w trakcie pracy serwera (hot-plug).
S1.09	Serwer musi posiadać kontroler RAID pozwalający na tworzenia co najmniej RAID 5 i 10.
S1.10	Serwer musi posiadać interfejs SAS pozwalający na łączenie się z zewnętrznymi dyskami o prędkości co najmniej 10 Gb/s.
S1.11	Serwer musi posiadać co najmniej dwa interfejsy SFP+ o szybkości co najmniej 10 Gb/s każdy.
S1.12	Serwer musi zostać dostarczony z dwoma wkładkami SPF+ o prędkości co najmniej 10 Gb/s każda kompatybilnymi z interfejsem serwera.
S1.13	Serwer musi posiadać kartę Ethernet z co najmniej dwoma portami RJ-45 o szybkości co najmniej 1 Gb/s.
S1.14	Serwer musi posiadać redundantne zasilanie 230V AC.
S1.15	Serwer musi posiadać interfejs do zdalnego zarządzania wraz z licencją na co najmniej 3 lata.
S1.16	Serwer musi posiadać wsparcie producenta na co najmniej 3 lata.
S1.17	Dostarczone urządzenie musi stanowić całość pochodzącą od jednego producenta (oprogramowanie oraz sprzęt) i być serwisowane przez autoryzowany serwis producenta ze wparciem na 3 lata z czasem reakcji następnego dnia roboczego (NBD). W przypadku awarii dysku, uszkodzony nośnik zostaje u Zamawiającego, a w jego miejsce zostanie dostarczony nowy wolny od wad.

2.2 Oprogramowanie i licencje

W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencjami. Wykonawca musi dostarczyć licencje dla całości środowiska zgodnie z Tabelą 2. Zamawiający przewiduje monitorować co najmniej 5000 Urządzeń. System musi pozwalać na gromadzenie co najmniej 230 GB logów dziennie oraz posiadać wydajność co najmniej 7000 EPS.

Wymagania dostarczonego Systemu opisuje Tabela nr 2.

Tabela nr 2

Kod wymagania	Opis wymagania
S2.01	System musi posiadać dostępny gotowy moduł do integracji z systemem zarządzania tożsamością, który musi uzupełniać zdarzenia o informacje o użytkowniku.
S2.02	System musi monitorować przypadki naruszenia bezpieczeństwa oraz posiadać mechanizmy śledzenia statusu rozwiązywania problemów.
S2.03	System audytu musi mieć możliwość zbierania i analizowania w czasie rzeczywistym informacji i logów z systemu zarządzania tożsamością.
S2.04	System audytu winien być wyposażony w możliwość zbierania i analizowania w czasie rzeczywistym informacji i logów bezpośrednio z systemów i aplikacji objętych rozwiązaniem do zarządzania tożsamością.
S2.05	System musi mieć możliwość zbierania, analizowania i korelowania w czasie rzeczywistym informacji i logów z urządzeń IDS, IDP i Firewall jak również systemów współpracujących z sieciową usługą syslog.
S2.06	System musi zapewniać wysoką dostępność (konfiguracja klastra HA) w zakresie kolekcji logów i bazy danych. Awaria pojedynczego elementu nie może wpływać na możliwość pobierania i rejestrowania logów. Musi istnieć możliwość dodania kolejnych węzłów klastra w trakcie używania Systemu dla spełnienia większych wymagań dotyczących wydajności lub dostępności.
S2.07	System audytu winien zapewniać mechanizm pozwalający na archiwizowanie danych i logów pochodzących zarówno z samego systemu zarządzania tożsamością jak i z systemów i serwerów objętych zarządzaniem tożsamością oraz umożliwiać ich przechowywanie w bazie danych dla potrzeb audytu.
S2.08	System winien posiadać możliwość sporządzania dowolnych raportów z zebranych informacji o zdarzeniach zachodzących w systemach z których informacje są zbierane.
S2.09	System winien zapewniać możliwość monitorowania zdarzeń w systemach do niego połączonych w czasie rzeczywistym i wysyłania powiadomienia za pomocą

	protokołu SMTP oraz webhook-ów w przypadku wystąpienia określonego zdefiniowanego wcześniej zdarzenia.
S2.10	System audytu i monitorowania zdarzeń powinien pracować w czasie rzeczywistym i działać (kolekcjonować dane i korelować zdarzenia) nawet w przypadku krótkiej awarii lub czasowego wyłączenia bazy danych zbierającej te informacje.
S2.11	System powinien zapewnić jak najmniejszą ingerencję w monitorowane systemy. Oznacza to możliwość zbierania logów bez konieczności instalacji dedykowanych agentów na źródłach danych urządzeń produkcyjnych, natomiast wykorzystania zaimplementowanych już w systemach mechanizmów bezagentowych.
S2.12	System musi jednocześnie umożliwiać zbieranie danych z monitorowanych systemów z wykorzystaniem agentów w przypadku, gdy dostęp bezagentowy nie zapewnia odpowiedniego poziomu bezpieczeństwa przesyłanych danych lub, gdy istnieją inne przesłanki do wykorzystania agentów.
S2.13	System musi dostarczać gotowe oprogramowanie agentów do zbierania danych i monitorowania systemów dla platform MS Windows oraz Unix i Linux.
S2.14	System musi zapewniać szyfrowanie danych w komunikacji pomiędzy agentem a serwerem Systemu kolekcjonującym dane.
S2.15	System musi zapewniać buforowanie danych po stronie agenta w przypadku utraty lub niemożności przesłania danych między agentem a serwerem.
S2.16	System powinien posiadać możliwość dostępu do funkcji pozwalających na przetwarzanie i raportowanie wyników zbierania zdarzeń, wraz z ich analizą i korelacjami, poprzez konsolę webową. Dostęp do tej konsoli musi odbywać się za pomocą protokołu HTTPS.
S2.17	System musi posiadać konsolę, która na bazie zdefiniowanego filtru pozwala na śledzenie w czasie rzeczywistym wybranych zdarzeń.
S2.18	System musi zapewnić możliwości implementacji w środowisku rozproszonym.
S2.19	System musi mieć możliwości zarządzania powiadomieniami o incydentach w postaci e-mail.
S2.20	System powinien posiadać funkcję zarządzania użytkownikami i uprawnieniami w systemie w oparciu o role. Zapewnić możliwość definiowania różnych uprawnień do systemu w zależności od wykonywanych czynności oraz ograniczać dostęp do przechowywanych w systemie danych w oparciu o filtry.
S2.21	System w ramach dostarczonej licencji na Oprogramowanie musi zapewniać możliwość instalacji co najmniej 6 maszyn wirtualnych zarządzanych przez wirtualizator KVM.

S2.22	System musi posiadać możliwość elastycznego jego rozbudowy o dodatkowe moduły zwiększające jego wydajność w przypadku niewydolności lub zbyt dużej ilości napływających zdarzeń.
S2.23	System musi udostępniać możliwość tworzenia własnych reguł pasujących do analizy spływających do Systemu informacji w oparciu o wyrażenia regularne przy pomocy wbudowanego narzędzia.
S2.24	System musi udostępniać narzędzia do analizy przepływów sieciowych NetFlow w wersji v5 oraz v9.
S2.25	Produkt musi mieć możliwość przesyłania wybranych danych pomiędzy niezależnymi instancjami Systemów funkcjonującymi w środowisku rozproszonym.
S2.26	System musi mieć możliwość centralnego wyszukiwania i analizy całości danych zgromadzonych przez wszystkie zainstalowane instancje serwerów.
S2.27	System musi umożliwiać podłączenie do źródeł zewnętrznych zawierających informacje o niepożądanych adresach IP, sieciach lub złośliwych domenach. Dane z tych źródeł muszą być dostępne do budowy reguł korelacyjnych.
S2.28	System musi umożliwiać podłączenie oraz analizę danych dla źródeł korzystających z: 1) plików; 2) usługi syslog; 3) baz danych (w tym Oracle); 4) CheckPoint (LEA); 5) Cisco SDEE; 6) Windows Event (WMI); 7) NetIQ Audit; 8) SNMP; 9) ActiveMQ.
S2.29	System musi wspierać mechanizm filtrowania danych spływających ze źródeł danych. System musi umożliwiać zdefiniowanie filtra oddzielnie dla każdego ze źródeł.
S2.30	System musi mieć możliwość przechowywania zgromadzonych danych w postaci znormalizowanej dla wszystkich źródeł danych.
S2.31	System musi umożliwiać opisywanie (tagowanie) źródeł danych na potrzeby prezentacji, filtrowania oraz analizy spływających danych.
S2.32	System musi umożliwiać wyszukiwanie i przeglądanie danych bieżących oraz archiwalnych w lokalnym zbiorze danych gromadzonych przez System.
S2.33	System musi posiadać mechanizm wyszukiwania rozproszonego w sytuacji, gdy w środowisku zainstalowane są dwie lub więcej instancji Systemu, a wynik wyszukiwania musi zawierać dane ze wskazanych przez operatora systemów.

S2.34	System musi zawierać mechanizm detekcji – automatycznie informowanie o zidentyfikowanych w zbiorze danych zgromadzonych wskutek agregacji i korelacji zdarzeniach, mogących świadczyć o występowaniu zdarzeń bezpieczeństwa. Alarmowanie to powinno być realizowane poprzez wyświetlanie odpowiednich informacji na konsoli użytkownika systemu i/lub poprzez wysyłanie powiadomień, np. za pośrednictwem poczty elektronicznej.
S2.35	System musi posiadać możliwość korelacji zdarzeń na podstawie zdefiniowanych reguł, możliwość zaimplementowania gotowych oraz tworzonych ad-hoc wzorców korelacji dla incydentów bezpieczeństwa. Rozwiązanie musi zapewniać możliwość korelowania zbieranych zdarzeń w oparciu o reguły powiązane z poszczególnymi zdarzeniami.
S2.36	System powinien umożliwiać opisywanie korelacji w oparciu o alternatywne narzędzia dostarczone przez producenta. Niezależnie od sposobu tworzenia reguł korelacyjnych system musi mieć możliwość zdefiniowania zbioru akcji, które zostaną wykonane przez system w wyniku zadziałania reguły korelacyjnej.
S2.37	System musi być skalowalny w obszarze detekcji zdarzeń co oznacza możliwość uruchomienia więcej niż jednego modułu odpowiedzialnego za obsługę reguł korelacyjnych.
S2.38	System musi posiadać wbudowane narzędzie do obsługi incydentów bezpieczeństwa oraz definiowania procesów do obsługi różnych typów incydentów.
S2.39	Narzędzie do definiowania i obsługi procesów obsługi incydentów (workflow) musi zapewniać: 1) interakcję z operatorami Systemu; 2) wykorzystywanie w procesie obsługi zgromadzonych danych oraz reguł korelacyjnych; 3) przypisywanie im akcji do wykonania w ramach zdefiniowanych procesów obsługi incydentów; 4) możliwość definiowania wielu kroków w procesie obsługi incydentu; 5) możliwość automatycznego wykonania czynności przez system SIEM lub przekazania procesu do dalszego kroku (eskalacji) w przypadku przekroczenia przez operatora zdefiniowanego w procesie czasu do obsługi kroku procesu; 6) możliwość wysłania e-maila z zdefiniowaną treścią i załączonymi automatycznie danymi pochodzącymi z systemy SIEM; 7) możliwość automatycznego wykonywania zdefiniowanych skryptów przez moduł obsługujący procesy; 8) możliwość wykorzystania elementów warunkowych przy definiowaniu procesów oraz działań; 9) możliwość obsługi sytuacji pojawienia się błędów w automatycznym procesie wykonywania czynności i skierowania procesu na ścieżkę manualnej realizacji czynności przez operatora.

S2.40	System musi zapewnić możliwość ręcznego oraz automatycznego generowania incydentów wraz z opcją przypisania wybranego procesu do obsług danego typu incydentu.
S2.41	System musi posiadać funkcję automatycznego tworzenia incydentów z poziomu modułu odpowiedzialnego za detekcję i korelację zdarzeń. Automatycznie tworzony incydent musi posiadać opcję przypisania procesu.
S2.42	System musi posiadać mechanizmy śledzenia statusu rozwiązywania problemów.
S2.43	System musi zawierać mechanizm retencji danych – musi umożliwiać przechowywanie danych za okres minimum 180 dni (dane przechowywane w Systemie będą dostępne dla funkcji analitycznych i detekcji). Zapewnienie przechowywania logów i danych historycznych umożliwi korelację zdarzeń z różnych źródeł w różnych okresach, a także zapewni dostęp do zdarzeń historycznych.
S2.44	Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.
S2.45	System musi zawierać moduł, który w czasie rzeczywistym prezentować będzie dane odbiegające od statystycznego wzorca zachowania obserwowanego przez system monitorowania bezpieczeństwa teleinformatycznego źródła danych lub danego typu zdarzeń w całym monitorowanym środowisku.
S2.46	Moduł detekcji musi prezentować dane w formie wykresu oraz zapewnić operatorom dostęp do danych źródłowych, które odbiegają od wzorca statystycznego.
S2.47	System musi być skalowalny tak by zapewnić wymaganą wydajność Systemu na etapie gromadzenia, analizy oraz korelacji zdarzeń.
S2.48	System musi mieć Możliwość tworzenia raportów w oparciu o dane pochodzące z podłączonych źródeł danych (np. logów generowanych przez systemy i aplikacje, przepływów sieciowych, kontroli dostępu, itp.). Możliwość generowania raportów z podziałem na odpowiednio zdefiniowane okresy czasu oraz umożliwienie ich wyeksportowania do elektronicznego formatu pliku (przynajmniej CSV oraz PDF).
S2.49	System musi posiadać możliwość wprowadzania zmian w raportach domyślnie zainstalowanych w systemie (dostosowanie wzorca graficznego).
S2.50	W Systemie muszą być dostępne raporty dotyczące wewnętrznego stanu Systemu oraz raporty związane z incydentami bezpieczeństwa.
S2.51	System musi umożliwiać programowanie manualnych lub automatycznych akcji, które będą stanowić rozszerzenie standardowych możliwości systemu. Akcje te mają być dostępne z poziomu konsoli lub mogą być wykorzystane w regułach służących do korelacji zdarzeń.

S2.52	Programowalne akcje muszą mieć możliwość współpracy z zewnętrznymi źródłami danych LDAP oraz usługami dostępnymi przez SOAP.
S2.53	Producent musi dostarczyć narzędzia do tworzenia własnych raportów dla Systemu.
S2.54	System musi wspierać na platformie Microsoft Windows następujące przeglądarki internetowe: 1) Google Chrome w ostatniej stabilnej wersji; 2) Mozilla Firefox w ostatniej stabilnej wersji.
S2.55	System musi posiadać możliwość agregacji logów zbieranych z wielu źródeł danych, włączając w to urządzenia sieciowe, systemy operacyjne serwerów, oprogramowanie bezpieczeństwa (antywirusowe, firewall, IPS/IDS), aplikacje i bazy danych, polegająca na zgromadzeniu zbieranych do bazy danych Systemu oraz przetworzeniu ich do postaci użytecznej dla Systemu, mająca na celu zapewnienie, iż w procesie monitorowania nie zostaną pominięte zdarzenia bezpieczeństwa.
S2.56	System musi wspierać protokół SNMP w wersji v2c oraz v3.
S2.57	System oraz licencje muszą pozwalać na gromadzenie co najmniej 230 GB logów dziennie.
S2.58	System musi zapewniać wydajność niezbędna do parsowania logów/danych, których wielkość dochodzi do 230 GB dziennie oraz dla których częstość zdarzeń na sekundę (EPS) może dochodzić do 7000 EPS nie może wtedy dochodzić do utraty (dropowania) logów/danych. Zdarzenia muszą być przechowywane w systemie przez co najmniej 180 dni.
S2.59	System musi posiadać możliwość rozbudowy o kolejne EPS poprzez rozszerzenie licencji na Oprogramownie.
S2.60	Musi umożliwiać integrację z zewnętrznymi repozytoriami danych, co najmniej NAS.
S2.61	System musi utrzymywać centralne repozytorium logów pobieranych z innych urządzeń i systemów oraz realizować funkcje Security Information and Event Management (SIEM) i Network Behavior Anomalny Detection (NBAD).
S2.62	System na podstawie statystyk i opisu ruchu (NetFlow, sflow itp.) pobieranych bezpośrednio z urządzeń sieciowych (routerów, przełączników) musi dokonywać analizy stanu i efektywności pracy sieci, w tym wykrywania sytuacji nieprawidłowych (anomalii).
S2.63	System musi dokonywać wykrywania anomalii w systemie informatycznym za pomocą analizy behawioralnej z wykorzystaniem uczenia maszynowego. W tym celu muszą być na bieżąco budowane profile normalnego stanu i zachowania sieci oraz identyfikowane odchylenia (m. in. zmiany stanu, nagłe zwiększenia lub zmniejszenia natężenia ruchu i przekroczenie wartości progowych).

S2.64	System musi zapewniać głęboką analizę pakietów (deep packet inspection) dostarczając takich informacji jak: rodzaj aplikacji, porty komunikacji, adresy IP, zawartość nagłówków pakietów, kierunki transmisji, właściwości ilościowe transmisji.
S2.65	System musi obsługiwać SSO (Single sign-on) minimum przy użyciu OpenID Connect oraz Kerberos.
S2.66	System musi posiadać możliwość logowania przy użyciu LDAP bądź Active Directory.
S2.67	System musi wspierać personalizację notyfikacji na stacjach końcowych w przypadku wykrycia zagrożenia przez moduł anty-malware.
S2.68	System musi wykrywać i blokować oprogramowanie typu ransomware używając technologii uczenia maszynowego i analizy behawioralnej.
S2.69	Na dzień otwarcia ofert System musi być dostępny w postaci kontenerów Dockerowych.
S2.70	System musi posiadać ochronę antymalware na stacjach końcowych zarówno dla systemów Windows jak i Linux.
S2.71	Oprogramowanie powinno być dostępne w pakietach zgodnych z RedHat/Suse (rpm) oraz Debian/Ubuntu (deb).
S2.72	W przypadku wykrycia malware/ransomware System musi umożliwiać zdalną izolację hosta.
S2.73	System musi posiadać możliwość tworzenia oraz usuwania kluczy API z poziomu panelu zarządzania.
S2.74	System powinien mieć możliwość automatycznej migracji danych archiwalnych do storage obiektowego zgodnego z S3. Tak zarchiwizowane dane muszą być przeszukiwalne.

3. Wymagania ogólne

Kod wymagania	Opis wymagania
W1.01	Urządzenia muszą być dostarczone jako fabrycznie nowe, nie używane w innych projektach, oraz nie starsze niż 6 miesięcy od daty produkcji.
W1.02	Wszystkie Urządzenia muszą pochodzić z oficjalnego kanału dystrybucji na Polskę lub Unię Europejską dla danego producenta.
W1.03	Urządzenia, Oprogramowanie i licencje, jak i ich elementy składowe, nie mogą znajdować się na aktualnej, na czas składania ofert, liście elementów producenta przewidzianych do wycofania z produkcji (end of life), sprzedaży lub serwisowania.
W1.04	Urządzenia objęte będą co najmniej 36 miesięcznym serwisem świadczonym przez autoryzowany serwis producenta siedem dni w tygodniu.
W1.05	Wszelkie koszty dostawy przedmiotu zamówienia pokryje Wykonawca (załadunek, wyładunek, transport i ubezpieczenie na czas transportu do miejsca wyznaczonego przez Zamawiającego).
W1.06	Zamawiający wymaga, by dostarczone Oprogramowanie wraz z modułami było Oprogramowaniem w wersji wspieranej przez producenta na dzień składania ofert – lub wersją sugerowaną przez producenta rozwiązania.
W1.07	Jeżeli wyraźnie nie wskazano należy uznać, że wszystkie Urządzenia muszą być dostarczone wraz z niezbędnym do instalacji okablowaniem w tym do sieci prądowej spełniające wymogi administratora CPD, sieci LAN Zamawiającego oraz do Fabric Interconnects Zamawiającego.
W1.08	Zamawiający wymaga by w ramach usługi instalacyjnej serwerów Wykonawca użył wolnego miejsca w szafach wskazanych przez Zamawiającego.
W1.09	W przypadku takiej konieczności Wykonawca musi zmodyfikować instalację prądową zabezpieczenia prądowe rozbudowywanych w ramach projektu szaf RACK Zamawiającego oraz zaktualizować projekt techniczny oraz dokumentację powykonawczą Zamawiającego w tym zakresie w celu akceptacji modyfikacji przez administratora CPD. Wykonawca zobowiązany będzie do przekazania autorskich praw majątkowych do dokonanej aktualizacji projektu technicznego i dokumentacji powykonawczej na zasadach określonych w Umowie.

4. Warunki licencji

Kod wymagania	Opis wymagania
WR1.01	Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej: klucze lub licencje dostępne do pobrania na stronie www producenta Oprogramowania.
WR1.02	W przypadku licencji dostępnych w formie elektronicznej na stronie producenta, Wykonawca przekaże dane autoryzacyjne lub Zamawiający poda konto do portalu producenta, jakie posiada, a do którego licencje mają być dołączone.
WR1.03	Wykonawca dostarczy Oprogramowanie na informatycznych nośnikach danych lub w innej postaci umożliwiającej prawidłową instalację tego Oprogramowania oraz certyfikaty autentyczności, klucze instalacyjne oraz inne dokumenty i zabezpieczenia najpóźniej w dacie odbioru tego Oprogramowania
WR1.04	Informatyczne nośniki danych, kopie, certyfikaty autentyczności, klucze instalacyjne oraz inne dokumenty i zabezpieczenia, o których mowa w poprzednim ustępie, powinny być zgodne z wymaganiami określonymi przez producenta Oprogramowania. Zamawiający jest uprawniony do weryfikacji, czy certyfikaty autentyczności, klucze instalacyjne oraz inne dokumenty i zabezpieczenia są wystarczające i zgodne z wymogami określonymi przez producenta. W tym celu Zamawiający może zwracać się do osób trzecich, w tym producenta Oprogramowania.
WR1.05	Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru, minimum 36 miesięczne wsparcie techniczne producenta Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).
WR1.06	Oprogramowanie musi posiadać wsparcie techniczne zapewniające aktualizacje Oprogramowania do najnowszej wersji oraz wsparcie telefoniczne, email lub stronę www producenta w przypadku problemów z Oprogramowaniem.
WR1.07	Wykonawca zagwarantuje, że jeżeli w ramach opłat należnych producentowi Oprogramowania mieści się opłata za jakiekolwiek dodatkowe świadczenia, w szczególności dostarczanie aktualizacji lub poprawek błędów lub inne usługi serwisowe, nieprzedłużenie korzystania z tych świadczeń przez Zamawiającego nie może powodować ustania licencji na korzystanie z Oprogramowania lub uprawniać do wypowiedzenia umowy licencyjnej.
WR1.08	Usługa wsparcia producenta (*maitanance*) będzie obejmowała aktualizacje oferowanego Oprogramowania do najnowszych wersji udostępnionych przez producenta Oprogramowania przez okres co najmniej 36 miesięcy. W ramach tej usługi Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta oraz mieć dostęp do bazy wiedzy i aktualizacji zakupionego Oprogramowania.

WR1.09	Wykonawca jest odpowiedzialny, względem Zamawiającego, za wszelkie wady prawne, a w szczególności za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej, w tym praw wynikających z ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. z 2021 r., poz. 1036).
WR1.10	W ofercie Wykonawca powinien przedstawić: 1) nazwy licencji wraz liczbą licencjonowanych jednostek; 2) koszty licencji wraz z usługą wsparcia technicznego producenta przez taki sam okres jak aktualnie posiadane licencje; 3) oświadczenie o spełnianiu każdego wymagania wraz ze wskazaniem miejsca w dokumentacji Oprogramowania.
WR1.11	Dostarczone licencje powinny dotyczyć Oprogramowania Standardowego, powszechnie dostępnego na rynku przez publiczny system sprzedaży dostępnych dla klientów z siedzibą na terenie Polski.
WR1.12	Dla Oprogramowania muszą być dostępne na terenie Polski autoryzowane szkolenia.
WR1.13	Oprogramowanie stanowiące przedmiot zamówienia powinno być opisane na publicznie i powszechnie dostępnych stronach WWW producenta.
WR1.14	Wykonawca musi zapewnić Zamawiającemu możliwość odnowienia, po wygaśnięciu zawartej umowy serwisowej, usługi wsparcia producenta bez konieczności uiszczania dodatkowych opłat wznowieniowych, z wyjątkiem sytuacji, kiedy producent w okresie trwania usługi zakończy świadczenie usług wsparcia technicznego dla licencji będących przedmiotem zamówienia.

5. Usługa instalacji

Urządzenia będące przedmiotem zamówienia mają zostać uruchomione w jednakowej konfiguracji sprzętowej w każdym z dwóch ośrodków POK i ZOK oraz w dodatkowej lokalizacji znajdującej się na terenie Miasta Stołecznego Warszawy, tj.:

1) POK - Urządzenia wskazane w pkt 2.1 OPZ – 1 sztuka;
2) ZOK – Urządzenia wskazane w pkt 2.1 OPZ – 1 sztuka;
3) lokalizacja znajdująca się na terenie Miasta Stołecznego Warszawy- Urządzenia wskazane w pkt 2.1 OPZ – 1 sztuka.

Urządzenia muszą zostać zainstalowane i uruchomione tj. zamontowane i podłączone do prądu we wskazanych przez zamawiającego szafach RACK oraz mają zostać uruchomione prądowo i zweryfikowane pod względem poprawności działania i parametrów podczas pracy na poziomie BIOSu.

Wymagania dotyczące usługi instalacji Urządzeń:

Kod wymagania	Opis wymagania
WDRU.1	Usługi instalacyjne muszą obejmować w szczególności: 1) dostarczenie Urządzeń do wskazanych przez Zamawiającego Lokalizacji; 2) rozpakowanie Urządzeń oraz utylizacja/magazynowanie opakowań; 3) montaż Urządzeń we wskazanych przez Zamawiającego szafach RACK; 4) w przypadku powstałej konieczności modyfikacja instalacji elektrycznej oraz zabezpieczeń prądowych rozbudowywanych w ramach projektu szaf RACK Zamawiającego; 5) aktualizacja projektu technicznego i dokumentacji powykonawczej Zamawiającego zakresie instalacji zasilającej szaf teleinformatycznych w celu akceptacji modyfikacji przez administratora CPD; 6) podłączenie Urządzeń do zapewnianych przez Zamawiającego obwodów zasilających; 7) uruchomienie Urządzeń.
WDRU.2	Zamawiający wymaga by Wykonawca w ramach instalacji w Ośrodkach Przetwarzania Danych (POK, ZOK) uzgodnił warunki uruchomienia infrastruktury z podmiotami zarządzającymi tymi ośrodkami.

WDRU.3	Zamawiający wymaga, aby osoby ze strony Wykonawcy realizujące przedmiot zamówienia, w przypadku konieczności dostępu do infrastruktury systemów Ośrodków Krajowych (POK, ZOK) udostępnianej przez Zamawiającego, posiadały aktualne zaświadczenie o niekaralności, a w przypadku braku tego zaświadczenia – poświadczenie bezpieczeństwa osobowego o minimalnej klauzuli "poufne". Zamawiający informuje, iż w ramach realizacji przedmiotu zamówienia nie przewiduje sytuacji powodującej konieczność dostępu przez Wykonawcę do informacji niejawnych.

6. Świadczenie serwisu gwarancyjnego i gwarancji

Kod wymagania	Opis funkcjonalności
WUS.01	Na dostarczone Urządzenia/Oprogramowanie Wykonawca zapewni serwis gwarancyjny producenta lub autoryzowanego serwisu producenta liczony od daty podpisania protokołu odbioru przedmiotu zamówienia na okres minimum 36 miesięcy opartego na świadczeniach serwisowych producenta.
WUS.02	Usługa wsparcia technicznego producenta lub autoryzowanego serwisu producenta musi być realizowana w trybie 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku, naprawa lub wymiana uszkodzonego Urządzenia w ciągu 8 godzin od momentu zgłoszenia – w sytuacji wystąpienia Awarii Krytycznej Urządzenia.
WUS.03	Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu: 1) prawo do pobierania nowych wersji i aktualizacji przez okres minimum 36 miesięcy od podpisania protokołu odbioru produktu; 2) możliwość wymiany Urządzenia na nowe w przypadku zdiagnozowania niedającej się naprawić Awarii Urządzenia; 3) dostarczenie sprawnego Urządzenia lub jego elementu podlegającego wymianie do miejsca zainstalowania Urządzenia uszkodzonego w uzgodnieniu z Zamawiającym; 4) możliwość aktualizacji Oprogramowania poprzez dostęp do zasobów producenta rozwiązania; 5) dostęp do pomocy technicznej producenta;

	6) nieograniczona ilość zgłoszeń serwisowych; 7) dostęp do materiałów producenta takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe producenta Oprogramowania/Urządzeń; 8) dostęp do poprawek i uaktualnień Oprogramowania objętego usługą wsparcia producenta oraz nowych wersji; 9) dostęp do portalu www producenta Oprogramowania umożliwiającego zarządzanie posiadanymi licencjami, podniesienie lub obniżenie (jeśli producent oficjalnie wspiera poprzednie wersje) wersji Oprogramowania; 10) dostęp do rejestru licencji (dostępnego przez portal www producenta Oprogramowania/Urządzeń).
WUS.04	Wykonawca wraz z dostawą Urządzeń przekaże warunki gwarancyjne i serwisowe producenta Urządzeń, w tym procedury zgłaszania awarii, dostępne kanały komunikacyjne z serwisem producenta. Do zamówienia muszą zostać dostarczone procedury zgłaszania awarii w formie elektronicznej edytowalnej.
WUS.05	Do kontaktów/zgłoszeń Wykonawca udostępnia: 1) numer telefonu – _____ (infolinia bezpłatna), _____ (dla telefonów komórkowych i z zagranicy); 2) e-mail - _____. Do kontaktów/zgłoszeń Zamawiający udostępnia: 1) numer telefonu – _____; 2) e-mail - _____.
WUS.06	Przyjęcie do realizacji zgłoszenia powinno zostać niezwłocznie potwierdzone zwrotnie na adres e-mail zgłaszającego.
WUS.07	Za moment zgłoszenia przyjmuje się datę i godzinę zarejestrowania przez system elektroniczny wskazany przez producenta lub autoryzowany serwis, w szczególności odebrania przesyłki e-mail przez system pocztowy lub zarejestrowanie zdarzenia przez Zamawiającego w udostępnionym przez producenta systemie zgłoszeniowym. W przypadku zgłoszenia telefonicznego moment zgłoszenia zostanie ustalony z Zamawiającym w trakcie tego zgłoszenia i potwierdzony w e-mailu, o którym mowa w wymaganiu WUS.05.
WUS.08	Przez usunięcie Awarii należy rozumieć przywrócenie pierwotnej funkcjonalności sprzętu i systemu operacyjnego sprzed wystąpienia Awarii albo zaproponowanie

	procedury obejścia zaistniałych Awarii bez rozwiązania problemu, pod warunkiem, że na przedstawioną przez Wykonawcę propozycję Zamawiający wyrazi zgodę.
WUS.09	Usunięcie Awarii Krytycznej nastąpi w terminie nie dłuższym niż 8 godzin od momentu zgłoszenia.
WUS.10	Usunięcie Awarii Niekrytycznej nastąpi w terminie nie dłuższym niż 24 godziny od momentu zgłoszenia.
WUS.11	Usunięcie Awarii Zwykłej nastąpi w terminie nie dłuższym niż 72 godziny od momentu zgłoszenia.
WUS.12	Po wymianie Urządzenia lub modułu będącego wyposażeniem tego Urządzenia lub Oprogramowania zostanie on objęty serwisem na takich samych zasadach jak wymienione Urządzenie lub moduł będący wyposażeniem tego Urządzenia lub Oprogramowania.
WUS.13	Najpóźniej w terminie 1 Dnia Roboczego, po usunięciu Awarii zostanie przedstawiony raport z Awarii (prezentujący, co najmniej czasy przyjęcia zgłoszenia o Awarii oraz rozwiązania incydentu serwisowego, a także przyczyny, sposoby rozwiązania i działania zapobiegające występowaniu Awarii w przyszłości).
WUS.14	Do każdego dostarczonego Urządzenia i Oprogramowania Wykonawca zobowiązuje się dostarczyć kartę gwarancyjną producenta, zawierającą numer seryjny, termin i warunki ważności gwarancji. Jeśli dla danego dostarczonego Urządzenia lub Oprogramowania producent nie przewiduje wystawiania własnych kart gwarancyjnych, kartę taką wystawi Wykonawca. W celu ułatwienia Zamawiającemu zarządzania kartami gwarancyjnymi dopuszcza się wystawianie zbiorczych kart gwarancyjnych Wykonawcy, jednakże każdorazowo z podaniem nr seryjnych lub innych danych umożliwiających jednoznaczną identyfikację Urządzenia lub Oprogramowania, którego dotyczy gwarancja Wykonawcy. W wypadku, jeżeli postanowienia gwarancji producenta są mniej korzystne od warunków zapisanych w Umowie, stosuje się zapisy Umowy.
WUS.15	W przypadku, gdy wadliwe Urządzenie uniemożliwia wykorzystanie funkcjonalności lub uniemożliwia pracę jakiegokolwiek jego podsystemu Wykonawca zapewni możliwość na czas naprawy dostarczenia, skonfigurowania i uruchomienia Urządzenia zastępczego o takich samych lub zbliżonych parametrach technicznych i funkcjonalnych, w sposób, który pozwoli na przywrócenie utraconych funkcjonalności Systemu lub podsystemu.

WUS.16	Usługi serwisowe, będą świadczone w miejscu użytkowania Urządzeń, z możliwością naprawy w serwisie producenta lub autoryzowanego serwisu, jeśli naprawa u użytkownika okaże się niemożliwa. Jeżeli naprawa odbywać się będzie poza miejscem użytkowania Urządzeń, przed zabraniem Urządzenia właściwy serwis zobowiązany będzie do wymontowania i pozostawienia u Zamawiającego dysków i wymiennych pamięci flash. Serwis pokryje koszty transportu oraz koszty ewentualnego ubezpieczenia przedmiotu zamówienia do miejsca naprawy oraz jego zwrotu do Lokalizacji. W przypadku Urządzeń, dla których jest wymagany uzasadniony dłuższy czas na naprawę lub wymianę Zamawiający dopuszcza możliwość dostarczenia Urządzenia zastępczego na czas naprawy o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia Awarii. Po usunięciu Awarii, dyski wymienne i/lub pamięci flash z Urządzenia zastępczego pozostają u Zamawiającego.
WUS.17	Uszkodzone elementy Urządzeń będą wymienione przez serwis na nowe, wolne od wad i o parametrach nie gorszych od uszkodzonych.
WUS.18	Wykonawca jest zobowiązany do zagwarantowania dokonania naprawy/wymiany Urządzenia w Lokalizacji przez producenta lub autoryzowany serwis. Jednakże, o ile Zamawiający wyrazi uprzednią zgodę, dopuszcza się realizację świadczenia gwarancyjnego w ten sposób, że na podstawie informacji diagnostycznych przekazanych przez Zamawiającego podczas zgłoszenia Awarii, właściwy serwis prześle na swój koszt zamiennik uszkodzonego Urządzenia, natomiast fizycznej wymiany uszkodzonego Urządzenia dokona odpowiednio przeszkolony przez Wykonawcę pracownik Zamawiającego, czyniąc to na ryzyko Wykonawcy. Jednakże taki tryb realizacji naprawy nie zwalnia z obowiązku zapewnienia przywrócenia pierwotnego stanu pracy Systemu.
WUS.19	Gwarancja obejmuje między innymi: 1) wady materiałowe i konstrukcyjne, a także nie spełnienie deklarowanych przez producenta parametrów i/lub funkcji użytkowych Urządzeń i Oprogramowania; 2) naprawę wykrytych uszkodzeń, w tym wymianę uszkodzonych modułów na nowe; 3) usuwanie wykrytych usterek i Awarii w działaniu Urządzeń lub Oprogramowania.

WUS.20	W okresie gwarancji, w przypadku awarii dysku twardego lub innego nośnika danych, będzie on wymieniony przez gwaranta na nowy bez konieczności zwrotu uszkodzonego dysku twardego lub innego nośnika danych przez Zamawiającego i dokonywania ekspertyzy dysku poza siedzibą Zamawiającego.
WUS.21	Dwukrotne uszkodzenie tego samego Urządzenia lub modułu będącego wyposażeniem tego Urządzenia w okresie gwarancji, obliguje producenta lub autoryzowany serwis do jego wymiany na fabrycznie nowy, wolny od wad, spełniający co najmniej te same parametry i zgodny funkcjonalnie z naprawianym Urządzeniem, w terminie 14 dni od chwili ostatniego zgłoszenia o uszkodzeniu. Okres gwarancji na wymienione Urządzenie będzie biegł od nowa tj. od daty protokołu stwierdzającego tę wymianę, przez okres standardowo udzielany przez producenta, lecz nie krócej niż do dnia gwarancji udzielanej przez producenta na Uzupełnienia.
WUS.22	Wszystkie części zamienne muszą pochodzić z oficjalnego kanału dystrybucji na terenie Unii Europejskiej.
WUS.23	Wszystkie naprawy Urządzeń oraz aktualizacje muszą być wykonywane przez autoryzowany serwis producenta Urządzeń.
WUS.24	Zamawiający uprawniony jest do opóźnienia terminu rozpoczęcia usuwania Awarii w takim przypadku gwarantowany czas naprawy ulegnie odpowiedniemu wydłużeniu i będzie liczony względem wskazanego przez Zamawiającego terminu.
WUS.25	W przypadku zdiagnozowania błędów w używanej przez Zamawiającego wersji Oprogramowania, Wykonawca zapewni Zamawiającemu dostęp do najnowszych wersji Oprogramowania Urządzeń posiadających wsparcie producenta, pozwalających na usuniecie tych błędów. W przypadku wykrycia błędu, dla którego brak jest w danym momencie odpowiedniej aktualizacji, właściwy serwis dokona eskalacji zgłoszenia do producenta. Wykonawca zapewnia i zobowiązuje się, że zgodnie z niniejszą specyfikacją korzystanie przez Zamawiającego z Oprogramowania w ramach wsparcia technicznego nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
WUS.26	Z tytułu świadczenia przez producenta lub jego autoryzowany serwis usługi serwisu gwarancyjnego Zamawiający nie ponosi dodatkowych kosztów.
WUS.27	Zamawiający wymaga elastyczności w rozbudowie, aby była możliwość bez konieczności uzyskania zgody Wykonawcy czy producenta, rozbudowy posiadanych Urządzeń o kolejne moduły rozszerzeń. Rozbudowa nie może powodować utraty praw gwarancyjnych do istniejącej i rozszerzonej konfiguracji danego Urządzenia.

WUS.28	Dla Oprogramowania obowiązują prawa gwarancyjne producenta.
WUS.29	Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.

7. Zasady odbioru przedmiotu Umowy

I. Zasady Ogólne

1. Zamawiający wymaga, aby Wykonawca zrealizował przedmiot zamówienia w terminie maksymalnie 30 dni od dnia podpisania Umowy.
2. Odbiór zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego i Wykonawcy protokołu odbioru ilościowo – jakościowego.

II. Odbiór ilościowo – jakościowy

1. Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowo – jakościowego jest sprawdzenie kompletności dostarczonego przedmiotu Umowy i potwierdzenie zgodności z ilością określoną w Umowie oraz sprawdzenie wszystkich wymagań funkcjonalnych i potwierdzenie zgodności ze szczegółowym opisem przedmiotu zamówienia.
2. Wykonawca będzie odpowiedzialny za dostarczenie i instalację dostarczonego przedmiotu zamówienia.
3. Podstawą dokonania odbioru ilościowo – jakościowego jest przeprowadzenie z pozytywnym skutkiem sprawdzeń kompletności oraz poprawności działania Urządzeń i Oprogramowania dostarczonego w ramach przedmiotu zamówienia wraz z wymaganymi licencjami
4. Pozytywny wynik odbioru ilościowo – jakościowego zostanie potwierdzony podpisaniem przez Strony protokołu odbioru ilościowo – jakościowego.

Lotnicze Pogotowie Ratunkowe
ul. Księżycowa 5
01-934 Warszawa
tel. (22) 22-99-931/932
fax. (22) 22-99-933

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl