



Krajowe Centrum
Monitorowania
Lotnictwa Medycznego

Opis Przedmiotu Zamówienia

Zakup licencji oprogramowania do
skanowania podatności

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

fax. (22) 22-99-933

e-mail: centrala@lpr.com.pl

3-391
4355
irm.pl



Spis treści

Spis treści.....	2
1. Słownik skrótów i pojęć.....	3
2. Cel zamówienia.....	4
3. Przedmiot zamówienia	4
4. Wymagania ogólne.....	4
5. Wymagania dla Oprogramowania.....	5
6. Świadczenie Wsparcia Technicznego	8
7. Zasady odbioru przedmiotu zamówienia	10



1. Słownik skrótów i pojęć

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć.

Tabela 1. Lista skrótów oraz pojęć

Skrót / Pojęcie	Definicja
Aktualizacje	Wszelkie uaktualnienia, modyfikacje, poprawki, patche, wydania uzupełniające, nowe wersje, podwyższenia wersji (upgrade), obniżenia wersji (downgrade) oraz inne zmiany lub dostosowania Oprogramowania dostarczane lub udostępniane w ramach Wsparcia Technicznego, w tym wskazane w OPZ lub Umowie, mające na celu zapewnienie prawidłowego, zgodnego z przeznaczeniem, bezpiecznego i niezakłóconego korzystania z Oprogramowania.
Awaria	Oznacza częściowy lub całkowity brak prawidłowego działania Oprogramowania w środowisku produkcyjnym, skutkujący niedostępnością Oprogramowania albo istotnym ograniczeniem możliwości korzystania z jego funkcjonalności, w tym w szczególności brakiem możliwości uruchomienia, wyłączenia, obsługi lub zarządzania Oprogramowaniem.
Dokumentacja	Oznacza dokumenty potwierdzające uprawnienie Zamawiającego do korzystania z Oprogramowania, w tym licencje na Oprogramowanie, a także dokumenty potwierdzające objęcie Oprogramowania Wsparciem Technicznym Producenta lub autoryzowanego serwisu Producenta
Oprogramowanie	Oznacza powszechnie dostępne i eksploatowane na dzień złożenia oferty Oprogramowanie będące przedmiotem zamówienia, spełniające wymagania określone w OPZ i Umowie.
SWD PRM	System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego - system teleinformatyczny umożliwiający przyjmowanie zgłoszeń alarmowych z centrów powiadamiania ratunkowego, o których mowa w art. 3 ust. 2 ustawy z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (Dz.U. z 2023r., poz.748), oraz powiadomień o zdarzeniach, dysponowanie zespołów ratownictwa medycznego, rejestrowanie zdarzeń medycznych, prezentację położenia geograficznego miejsca zdarzenia, pozycjonowanie zespołów ratownictwa medycznego oraz wsparcie realizacji zadań przez zespoły ratownictwa medycznego, wojewódzkiego koordynatora ratownictwa medycznego i krajowego koordynatora ratownictwa medycznego.
Producent	Oznacza producenta Oprogramowania oferowanego przez Wykonawcę.
Umowa	Oznacza umowę zawartą pomiędzy Zamawiającym a Wykonawcą w celu realizacji przedmiotu zamówienia.



Skrót / Pojęcie	Definicja
Wsparcie Techniczne	Oznacza usługę świadczoną przez Producenta lub podmiot przez niego autoryzowany, polegającą na zapewnieniu poprawności, ciągłości i bezpieczeństwa działania Oprogramowania, w tym na udostępnianiu Aktualizacji oraz usuwaniu Awarii Oprogramowania zgodnie z warunkami określonymi w OPZ i Umowie.
Wykonawca	Oznacza podmiot ubiegający się o udzielenie zamówienia, a po zawarciu Umowy - podmiot zobowiązany do realizacji zamówienia zgodnie z OPZ i Umową.
Zamawiający	Lotnicze Pogotowie Ratunkowe.

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

2. Cel zamówienia

Celem zamówienia jest zakup dwóch licencji na Oprogramowanie do skanowania podatności wraz z Wsparciem Technicznym.

3. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa dwóch licencji na Oprogramowanie do skanowania podatności na okres 24 miesięcy wraz ze Wsparciem Technicznym dla wyżej wskazanego Oprogramowania na czas obowiązywania licencji.

4. Wymagania ogólne

- Wykonawca zobowiązany jest do przekazania Zamawiającemu aktualnego zestawienia w zakresie Oprogramowania zawierającego m.in. oznaczenie producenta, pełna nazwa produktu, metryka licencyjna, wersja i edycja Oprogramowania, rodzaj licencji, okres obowiązywania licencji, w sposób umożliwiający Zamawiającemu jednoznaczną identyfikację i weryfikację zaoferowanego Oprogramowania.
- Wykonawca do zaoferowanej licencji na Oprogramowanie zobowiązany jest dostarczyć Zamawiającemu nośnik z wersją instalacyjną Oprogramowania (dla Oprogramowania w wersji pudełkowej), lub dane dostępne do pobrania Oprogramowania oraz kanału subskrypcji, licencję (umowę licencyjną w wersji elektronicznej) oraz wszystkie wymagane klucze licencyjne i aktywacyjne w formie elektronicznej na adres email wskazany w Umowie. Warunki udzielenia licencji określa Umowa.
- Zamawiający wymaga, aby dostarczane Oprogramowanie było sprawdzone w praktyce rynkowej, co oznacza, że Oprogramowanie realizujące wszystkie wymagane funkcje musi być dostępne na rynku przez co najmniej 6 miesięcy przed terminem złożenia oferty.
- Przedmiot zamówienia pochodzić będzie z legalnego kanału dystrybucji na terenie Unii Europejskiej dla danego Producenta.
- Wykonawca oświadcza, że posiada prawo swobodnego dysponowania przedmiotem zamówienia oraz, że dostarczone Oprogramowanie nie będzie dotknięte żadną wadą fizyczną, ani wadą prawną,



a w szczególności nie jest i nie będzie obciążone prawami i roszczeniami osób lub podmiotów trzecich.

6. Wykonawca zapewnia, że dostarczone Oprogramowanie będzie spełniać wymagania wynikające z obowiązujących przepisów prawa oraz będzie zgodne z obowiązującymi normami.

5. Wymagania dla Oprogramowania

Tabela 2 przedstawia minimalne wymagania określone przez Zamawiającego, które musi spełniać oferowane przez Wykonawcę Oprogramowanie.

Tabela 2. Minimalne wymagania dla Oprogramowania

Kod wymagania	Opis wymagania
S.01	Dostarczone Oprogramowanie musi pozwalać na skanowanie sieci Zamawiającego pod kątem podatności i nieprawidłowych konfiguracji z uwzględnieniem zarówno urządzeń fizycznych, jak i serwerów wirtualnych, takich jak: • serwery wirtualne z systemami operacyjnymi Windows oraz Linux (Ubuntu, Debian, Oracle Linux, Rocky Linux, CentOS); • urządzenia sieciowe Cisco, Palo Alto, Fortinet; • Load Balancer-y (F5, Haproxy); • serwery DNS (PowerDNS, BIND); • serwery fizyczne pod kontrolą VMware ESXi, Hyper-V, Proxmox, Harvester; • bazy danych (MariaDB, PostgreSQL, Oracle Database, Redis); • serwery web (Apache, Tomcat, Nginx).
S.02	Oprogramowanie musi umożliwiać instalację w środowisku wirtualnym VMware vSphere 7 lub nowszym poprzez instalację na wspieranym przez producenta systemie operacyjnym Linux lub Windows Server, uruchomionym jako maszyna wirtualna x86-64. Dopuszcza się również dostarczenie gotowego obrazu maszyny wirtualnej, jeżeli producent taki obraz udostępnia.
S.03	Licencja musi uprawniać Zamawiającego do wykonywania nielimitowanej liczby skanów oraz skanowania nielimitowanej liczby adresów IP/hostów w ramach własnej infrastruktury Zamawiającego, bez rozliczania per pojedynczy adres IP.
S.04	Oprogramowanie musi zawierać predefiniowane szablony, polityki lub pluginy umożliwiające wykrywanie podatności związanych co najmniej z: WannaCry, Zerologon, ProxyLogon, Log4Shell oraz SolarWinds/Solorigate, w zakresie podatności publikowanych w bazach CVE/NVD oraz bazie producenta.
S.05	Oprogramowanie musi dostarczać gotowe polityki umożliwiające weryfikację zgodności z dobrymi praktykami wykorzystując CIS Benchmarks w następujących zakresach: • CIS Ubuntu Linux Benchmark, • CIS Microsoft Windows Server, • CIS Kubernetes Benchmark, • CIS VMware ESXi Benchmark.
S.06	Oprogramowanie musi umożliwiać definiowanie własnych polityk skanowania podatności.



S.07	Oprogramowanie musi udostępniać możliwość wykrywania błędów i podatności w konfiguracji IaC w zakresie technologii: • Terraform, • Docker, • Helm, • Kubernetes.
S.08	Oprogramowanie musi umożliwiać skanowanie zgodności konfiguracji z politykami oraz skanowanie pod kątem podatności następujących rozwiązań: • Bazy danych (szczególnie Oracle Database, MongoDB oraz PostgreSQL), • Palo Alto firewall, • VMware vCenter, • F5 / Haproxy Load Balancer.
S.09	Oprogramowanie musi wspierać możliwość przeprowadzania audytów konfiguracji urządzeń sieciowych (przynajmniej urządzeń Cisco) w trybie offline poprzez skanowanie plików konfiguracyjnych.
S.10	Oprogramowanie musi posiadać możliwość aktywnego skanowania sieci w celu wykrycia nowych urządzeń oraz usług wraz z ich wersjami (host discovery).
S.11	Oprogramowanie musi wspierać skanowanie podatności bez uwierzytelniania oraz z uwierzytelnieniem, wspierając następujące metody: • w przypadku protokołu SSH: autentykacja kluczem OpenSSH, hasłem, certyfikatem lub z wykorzystaniem protokołu Kerberos, • w przypadku systemu Windows: Kerberos, LM Hash, NTLM Hash, • w przypadku bazy danych Oracle: autentykacja hasłem z możliwością wskazania roli (NORMAL, SYSOPER, SYSDBA).
S.12	Oprogramowanie musi posiadać możliwość autentykacji do następujących rozwiązań: • F5 Load Balancer, • Palo Alto firewall, • VMware vCenter.
S.13	Oprogramowanie musi wspierać skanowanie z wykorzystaniem autentykacji przy poniższych protokołach: • FTP, • POP3, • IMAP, • SNMP v2c.
S.14	W przypadku skanowania systemów operacyjnych Linux/Unix oraz urządzeń Cisco, Oprogramowanie musi umożliwiać podniesienie uprawnień (w zależności od systemu/urządzenia: su, sudo, enable).
S.15	Oprogramowanie musi zawierać funkcjonalność tworzenia harmonogramów skanowania podatności.
S.16	Oprogramowanie musi pozwalać na porównywanie wyników dwóch skanów podatności pod kątem wystąpienia nowych podatności i błędów.
	Oprogramowanie musi umożliwiać filtrowanie wyników skanu korzystając z następujących parametrów:



S.17	• CVE, CVSS, • nazwa/adres hosta, • dostępność exploit-u, • łatwość wykorzystania podatności, • dostępność patch-a.
S.18	Oprogramowanie musi prezentować wynik skanowania wraz z rekomendacją od jakich Aktualizacji zacząć, aby wyeliminować największe ryzyko.
S.19	Oprogramowanie musi prezentować dynamicznie obliczaną ocenę pilności wykrytej podatności, opartą przynajmniej o dostępność exploit-u, CVSSv3, ilość zagrożonych urządzeń i datę wykrycia podatności.
S.20	Oprogramowanie musi mieć możliwość przechowywania historii wykonanych skanów.
S.21	Oprogramowanie musi umożliwiać eksportowanie wyników skanowania przynajmniej do formatów HTML, CSV oraz PDF.
S.22	Oprogramowanie powinno wspierać generowanie następujących raportów: • top podatności, • wykryte systemy operacyjne, • niewspierane oprogramowanie, • podatności ze znanymi exploit-ami.
S.23	Oprogramowanie musi wspierać personalizację generowanych raportów poprzez możliwość dodania nazwy oraz własnego logotypu.
S.24	Oprogramowanie musi umożliwiać włączenie rozszerzonego logowania diagnostycznego skanów, w tym zapisu informacji o komunikacji skanera z celem, a jeżeli produkt wspiera przechwytywanie pakietów, również eksport takiego ruchu do analizy.
S.25	Oprogramowanie musi wspierać możliwość pracy (na infrastrukturze Zamawiającego) w trybie air-gapped i umożliwiać ręczną aktywację oraz Aktualizację bez dostępu do sieci Internet.
S.26	Aktualizacja reguł wykrywania podatności musi być wykonywana automatycznie w przypadku dostępu systemu do Internetu.
S.27	Interfejs Oprogramowania musi przedstawiać informacje takie jak użycie procesora, pamięci RAM, ilość skanowanych systemów, ilość sesji TCP, wolumen przesyłanego ruchu sieciowego.
S.28	Oprogramowanie musi umożliwiać wymuszenie polityki haseł dla administratorów logujących się do systemu.
S.29	Oprogramowanie musi udostępniać w pełni funkcjonalny interfejs graficzny dostępny w języku polskim lub angielskim.
S.30	Interfejs graficzny rozwiązania musi być dostępny poprzez stronę WWW kompatybilną co najmniej z przeglądarkami: • Google Chrome, • Mozilla Firefox, • Microsoft Edge.
S.31	Oprogramowanie musi udostępniać API lub CLI umożliwiające automatyzację eksportu wyników skanów w formacie maszynowym, np. CSV, JSON, XML lub równoważnym.
S.32	Dokumentacja Oprogramowania musi być napisana w języku polskim lub języku



	angielskim.
S.33	Dokumentacja musi być dostarczona wraz z Oprogramowaniem lub udostępniona na stronie WWW Producenta Oprogramowania.
S.34	Dokumentacja musi opisywać obszary związane z instalacją, konfiguracją oraz administracją Oprogramowania, a także zawierać przewodnik użytkownika.
S.35	Zamawiający wymaga dostarczenia dwóch licencji na Oprogramowanie do skanowania podatności. Okres obowiązywania licencji na Oprogramowanie, nie może być krótszy niż 24 miesiące.

6. Świadczenie Wsparcia Technicznego

W Tabeli 3 został przedstawiony szczegółowy opis wymagań dotyczących świadczenia Wsparcia Technicznego dla Oprogramowania. Celem tych wymagań jest zapewnienie Zamawiającemu pełnej dostępności, niezawodności oraz ciągłości działania Oprogramowania poprzez określenie obowiązków Wykonawcy m.in. w zakresie Wsparcia Technicznego, Aktualizacji oraz Awarii.

Wymagania obejmują zarówno okres obowiązywania licencji, sposób realizacji zgłoszeń serwisowych, dostęp do Aktualizacji Oprogramowania, procedury kontaktowe, jak i szczegółowe zobowiązania Wykonawcy do dostarczenia Dokumentacji oraz zapewnienia Wsparcia Technicznego zgodnie ze standardami Producenta. Ich celem jest zagwarantowanie, aby proces serwisu Wsparcia Technicznego był przejrzysty, efektywny oraz realizowany w sposób minimalizujący przestoje w użytkowaniu Oprogramowania.

Tabela 3. Świadczenie Wsparcia Technicznego

Kod wymagania	Opis wymagań
SWT.1	Na dostarczone Oprogramowanie Wykonawca zapewni Wsparcie Techniczne liczone od daty podpisania protokołu odbioru, na okres 24 miesiące.
SWT.2	Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu: 1) prawo do pobierania nowych wersji i Aktualizacji przez okres minimum 24 miesiące od podpisania protokołu odbioru, 2) możliwość Aktualizacji Oprogramowania poprzez dostęp do zasobów Producenta rozwiązania, 3) dostęp do pomocy technicznej Producenta, 4) nieograniczona ilość zgłoszeń serwisowych, 5) dostęp do materiałów Producenta takich jak: Dokumentacja techniczna, internetowa baza wiedzy, 6) dostęp do poprawek i uaktualnień Oprogramowania oraz nowych wersji, 7) dostęp do portalu WWW Producenta Oprogramowania umożliwiającego zarządzanie posiadanymi licencjami, podniesienie lub obniżenie (jeśli Producent oficjalnie wspiera poprzednie wersje) wersji Oprogramowania,



	8) dostęp do rejestru licencji (dostępnego przez portal WWW Producenta Oprogramowania).
SWT.3	Wykonawca wraz z dostawą przekaże procedury zgłaszania Awarii, dostępne kanały komunikacyjne z serwisem Producenta. Do zamówienia muszą zostać dostarczone procedury zgłaszania Awarii w formie elektronicznej edytowalnej.
SWT.4	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 – _____.
SWT.5	Przyjęcie do realizacji zgłoszenia powinno zostać niezwłocznie potwierdzone przez Wykonawcę, zwrotnie na adres e-mail zgłaszającego.
SWT.6	Za moment zgłoszenia przyjmuje się datę i godzinę zarejestrowania przez system elektroniczny Wykonawcy, w szczególności odebrania przesyłki e-mail przez system pocztowy lub zarejestrowanie zdarzenia przez Zamawiającego w udostępnionym przez Wykonawcę 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 SWT.5 .
SWT.7	Do dostarczonego Oprogramowania Wykonawca zobowiązuje się dostarczyć informacje pozwalające na jednoznaczną identyfikację Oprogramowania.
SWT.8	Zamawiający uprawniony jest do opóźnienia terminu rozpoczęcia usuwania Awarii Oprogramowania przez Wykonawcę, w takim przypadku gwarantowany czas naprawy ulegnie odpowiedniemu wydłużeniu i będzie liczony względem wskazanego przez Zamawiającego terminu.
SWT.9	W przypadku zdiagnozowania błędów w używanej przez Zamawiającego wersji Oprogramowania, Wykonawca zapewni Zamawiającemu dostęp do najnowszych wersji Oprogramowania, pozwalających na usunięcie tych błędów. W przypadku wykrycia błędu, dla którego brak jest w danym momencie odpowiedniej Aktualizacji, Wykonawca dokona eskalacji zgłoszenia do Producenta.
SWT.10	Z tytułu świadczenia Wsparcia Technicznego Zamawiający nie ponosi dodatkowych kosztów.
SWT.11	Wykonawca zapewni usunięcie Awarii w terminie nie dłuższym niż 72 godziny od momentu zgłoszenia.



7. Zasady odbioru przedmiotu zamówienia

1. Wykonawca zobowiązany jest dostarczyć Oprogramowanie wraz z Dokumentacją potwierdzającą Wsparcie Techniczne.
2. Termin oraz sposób odbioru przedmiotu Umowy, określony został w Projektowanych Postanowieniach Umowy.