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

Zakup systemu analizy przepływów na potrzeby infrastruktury informatycznej SWD PRM

Spis treści

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

I. Słowniki i skróty

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

Skrót/pojęcie	Definicja
Awaria	Oznacza utrudnienie działania oprogramowania analizy flow lub implementacji subskrypcji licencji w środowisku produkcyjnym w zakresie podstawowych funkcjonalności.
Dni Robocze	Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8:00 do 15:35.
Oprogramowanie Standardowe	Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące w użytkowaniu lub zamówieniu Zamawiającego.
Oprogramowanie	Oprogramowanie do analizy przepływów będące przedmiotem niniejszego postępowania.
Subskrypcja licencji/Licencje	Subskrypcja na licencje urządzeń PA-3220 będące w posiadaniu Zamawiającego.
SWD PRM	System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego wraz z zainstalowanym oprogramowaniem standardowym, aplikacyjnym oraz infrastrukturą sprzętową.
Umowa	Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia.
Usługa Serwisu	Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania Oprogramowania oraz jego poszczególnych komponentów.
Użytkownik	Zamawiający oraz jego pracownicy.
Wykonawca	Podmiot realizujący zamówienie.
Zamawiający	Lotnicze Pogotowie Ratunkowe.

II. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. Zadanie nr 1 – zakup Oprogramowania systemu analizy bezpieczeństwa przepływów (Security Flow):

   - system przewidziany jest do wykrywania ataków, zagrożeń i anomalii z wykorzystaniem danych statystycznych pobieranych z urządzeń sieciowych. System działa w oparciu o heurystykę, a nie sygnaturowe wykrywanie nadużyć;
   - system posiada możliwość pobrania i analizy informacji sieciowych raportowanych z wykorzystaniem protokołu NetFlow (RFC 3954);
   - rozwiązanie zostanie objęte gwarancją i wsparciem technicznym na Oprogramowanie przez okres 3 lat od dnia podpisania protokołu odbioru przedmiotu zamówienia. Wszelkie zapisy zawierające parametry techniczne należy odczytywać jako parametry minimalne.

2. Zadanie nr 2 – zakup subskrypcji licencji Wildfire dla posiadanych przez Zamawiającego urządzeń NGFW PA-3220.

III. Wymagania Ogólne

Zadanie 1 – Wymagania dotyczące systemu analizy bezpieczeństwa przepływów (NetFlow)

Tabela 1 Specyfikacja pojedynczego kompletu

Lp.	Numer produktu	Opis	Ilość
1	**L-ST-SMC-VE-K9**	Cisco Secure Network Analytics Mgmt Console Virtual Edition	1
2	**L-ST-FC-VE-K9**	Cisco Secure Network Analytics Flow Collector Virt Edition	1
3	**L-ST-DS-VE-K9**	Cisco Secure Network Analytics Data Store Virtual Appliance	1
4	**ST-SEC-SUB**	Cisco Stealthwatch Enterprise XaaS Subscription	1
4.1	ST-FR-LIC	Cisco Secure Network Analytics Flow Rate License	1100
5	**L-ST-FS-VE-K9**	Cisco Secure Network Analytics Flow Sensor, Virtual Edition	1
6	**L-LC-TI-FC1K=**	Cisco Secure Network Analytics Threat Intelligence -FC1K Lic	1

Zamawiający dopuszcza rozwiązanie równoważne, pod warunkiem spełnienia przez nie następujących minimalnych wymagań:

Tabela 2 Wymagania na rozwiązanie równoważne

Kod wymagania	Opis wymagań
	Architektura Rozwiązania
WN.01	Rozwiązanie stanowi kompleksowe rozwiązanie pozwalające na pozyskanie i analizę zdarzeń oraz incydentów zachodzących w sieci. W szczególności system posiada: a. Centralną konsolę zarządzania, której zadaniem jest: i. Monitorowanie i zarządzanie wszystkimi elementami systemu, ii. Wyświetlanie administratorowi zdarzeń w sposób przejrzysty w celu szybkiej interpretacji i oceny zdarzenia, iii. Posiadającą wiele narzędzi ułatwiających administratorowi codzienną pracę z systemem. b. Kolektor Netflow zbierający informację o przepływach danych oraz logi z następujących urządzeń sieciowych: i. Przełączniki, ii. Routery, iii. Firewall'e, iv. Serwery Proxy, v. Generatory Netflow. c. Sensor Netflow – narzędzie do generowania informacji o przepływach danych z segmentów, z których wysyłanie statystyk natywnie (netflow, ipfix) z infrastruktury sieciowej nie jest możliwe. Sensor generuje statystyki analizując kopię ruchu wysyłanej z: i. Przełączników sieciowych LAN ii. Środowiska zwirtualizowanego – w tym środowiska VMware
WN.02	Rozwiązanie powinno umożliwiać zbieranie przepływów nie mniej niż 1100 Flow na sekundę.
WN.03	Rozwiązanie jako dane źródłowe wykorzystuje niepróbkowany (non-sampled) NetFlow.
WN.04	Rozwiązanie zapewnia pracę w modelu redundantnym – w szczególności ma możliwość redundancji kolektorów Netflow oraz redundancję centralnej konsoli zarządzania.
Wykrywanie ataków i anomalii	
WN.05	Rozwiązanie zapewnia behawioralne metody wykrywania ataków/anomalii.
WN.06	Rozwiązanie umożliwia profilowanie ruchu poszczególnych hostów i grup hostów celem wykrywania anomalii/ataków wynikających z: a. przekroczenia wartości bazowych (zarówno zdefiniowanych przez administratora, jak i wynikających z procesu „uczenia się" systemu charakterystyk ruchowych) dla typowego wzorca ruchu danej stacji, b. zmiany charakterystyki ruchu dla stacji, c. naruszenia założonej polityki bezpieczeństwa.
WN.07	Rozwiązanie umożliwia wykrywanie ataków typu zero-day.
WN.08	Rozwiązanie umożliwia wskazanie zarażonych hostów wewnątrz organizacji.

Kod wymagania	Opis wymagań
WN.09	Rozwiązanie umożliwia wskazanie ataków, które zostały dopuszczone przez ominięcie systemów AV.
WN.10	Rozwiązanie umożliwia wykrywanie ataków polimorficznych, mutujących jak też zaszyfrowanych w oparciu o zmiany zachowania w sieci atakowanego hosta.
WN.11	Rozwiązanie posiada wbudowane mechanizmy i algorytmy korelowania zdarzeń celem wyświetlenia administratorowi zagregowanych zdarzeń o największym potencjalnym zagrożeniu.
WN.12	Rozwiązanie umożliwia wykrywanie ataków i anomalii ze wskazaniem celu ataku jak też hostów atakujących co najmniej: a. DoS oraz DDoS, b. Skanowanie sieci oraz hostów, c. Połączenia Command and Control, d. Eksfiltracja danych, e. Próby skompromitowania hostów poprzez propagację wirusów i łamanie haseł metodą „brute force”, f. Naruszenie polityki nałożonej przez administratora (np. ruch z sieci użytkowników do obszaru chronionego), g. Anomalie polegające na ściąganiu przez jednego hosta z jednego lub wielu źródeł danych o wielkości przekraczającej normalny poziom.
WN.13	Rozwiązanie posiada możliwość różnicowania zachowań hostów w zależności od dnia tygodnia dla: a. Statystki ruchowej hosta, b. Całościowego ruchu generowanego przez hosta, c. Wolumenu ruchu pakietów z flagą SYN, d. Maksymalnego poziomu ruchu pakietów z flagą SYN.
WN.14	Rozwiązanie uwzględnia zmiany wynikające z typowych działań i rozwoju organizacji i posiada zdolność „uczenia się” – przykładowo pozwala uwzględniać zmiany charakterystyki ruchu serwera, który w przeciągu roku zwiększył wolumen ruchu kilkakrotnie i odpowiednio do niego dostosowywać odpowiednie wartości progowe.
WN.15	Rozwiązanie umożliwia konfigurację „soft-firewalla” w sieci celem raportowania o niepożądanych przepływach ruchu pomiędzy wskazanymi obszarami sieci. Istnieje możliwość zdefiniowania następujących parametrów: a. Adres IP hosta źródłowego, docelowego oraz całych grup, do których hosty należą, b. Protokół i port hosta źródłowego i docelowego oraz całych grup, do których hosty należą, c. Nazwy użytkowników, między którymi odbywa się połączenie (w przypadku integracji z systemem tożsamości), d. Ilość bajtów i pakietów, e. Określenie czasu, w którym zaszło połączenie (np. między 8:00 a 16:00), f. Czas trwania połączenia w godzinach, minutach, sekundach.
WN.16	Rozwiązanie posiada możliwość raportowania w przypadku naruszenia polityki zdefiniowanej przez administratora. Raport dla administratora zawiera m.in. informację o rodzaju komunikacji, która

Kod wymagania	Opis wymagań
	naruszyła politykę, ile razy polityka została naruszona oraz który użytkownik dokonał tego naruszenia wraz z podaniem jego adresu IP.
WN.17	Rozwiązanie posiada mechanizmy wykrywania sytuacji wycieku danych ze wskazanych serwerów (np. serwerów plików) przez atakującego z wewnątrz, jak i z zewnątrz organizacji.
WN.18	Rozwiązanie posiada narzędzie do graficznego przedstawiania propagacji malware między hostami.
WN.19	Rozwiązanie posiada możliwość analizy przepływów pod kątem wykrywania niechcianego ruchu P2P takiego jak KaZaa, Gnutella, eDonkey.
WN.20	Dla łatwego definiowania dopuszczalnych zachować między hostami system posiada trzy poziomy polityk: a. Domyślna uniwersalna polityka dla hostów wewnętrznych oraz zewnętrznych, b. Polityki specyficzne dla danej grupy hostów o podobnych właściwościach (np. serwery NTP, DNS, DHCP, skanery sieci, stacje użytkowników), c. Polityki dla pojedynczych hostów.
WN.21	Rozwiązanie pozwala na modyfikowanie polityk, które opierają się na zbudowanym wzorcu zachowania „baseline” (np. wolumen ruchu, przyrost nowych połączeń) w zakresie: a. Ustawienia progu minimalnego, przed którym alarm nie będzie generowany, b. Ustawienia progu maksymalnego, po którym alarm będzie zawsze generowany, c. Ustawienie czułości (tolerancji) na odstępstwa od zbudowanego wzorca.
WN.22	Rozwiązanie zezwala na wyłączenie alarmów dla poszczególnych hostów lub grup hostów.
WN.23	Kolektor NetFlow zachowuje przepływy i zdarzenia, które są aktywne w momencie jego wyłączenia lub restartu.
WN.24	Rozwiązanie posiada możliwość pobierania informacji z bazy producenta o znanych serwerach, Command and Control, TOR oraz adresach Bogon. W informacjach tych zawarte są znane poniższe dane wykorzystywane do ataków: a. Adresy IP, b. Numery portów, c. Protokoły, d. Nazwy hostów, e. URL’e.
Narzędzia monitorowania sieci	
WN.25	Kolektory Netflow działają w oparciu o analizę Netflow i nie wykorzystują modelu FPC (Full Packet Capture) do działania i analizy.
WN.26	Rozwiązanie zapewnia możliwość przechowywania exportów Netflow i informacji o flow przez co najmniej 30 dni ze wszystkimi szczegółami dotyczącymi flow.
WN.27	Rozwiązanie przechowuje wszystkie dane w bazie danych z możliwością odwoływania się do nich przez system w czasie rzeczywistym a nie tylko na żądanie użytkownika.
WN.28	Rozwiązanie posiada możliwość wykrywania źle skonfigurowanych lub niepoprawnie funkcjonujących urządzeń sieciowych i hostów w tym routerów, serwerów i stacji roboczych.

Kod wymagania	Opis wymagań
WN.29	Rozwiązanie posiada możliwość monitoringu interfejsów sieciowych monitorowanych urządzeń w tym interfejsów agregowanych.
WN.30	Rozwiązanie zapewnia możliwość monitoringu wykorzystania interfejsu z dokładnością do usługi sieciowej.
WN.31	Rozwiązanie posiada możliwość wskazania „TopX" hostów i usług dla wskazanej usługi sieciowej.
WN.32	Rozwiązanie posiada możliwość definiowania aplikacji i ich automatycznej identyfikacji z dokładnością do poziomu Skype, Teredo, AIM, WebEx, Dropbox, Facebook.
WN.33	Rozwiązanie posiada możliwość definiowania raportów z wykorzystaniem informacji o własnych definicjach aplikacji przygotowanych przez administratora.
WN.34	Rozwiązanie posiada możliwość raportowania nieaktywności/aktywności poszczególnych hostów.
WN.35	Rozwiązanie posiada możliwość definiowania raportów zorientowanych na wolumeny ruchu.
WN.36	Rozwiązanie posiada wbudowane narzędzia zaawansowanej deduplikacji informacji o przepływach (flow), zapewnia unikalność flow'ów i nie powiela informacji o pojedynczym flow w raportach. Pojedynczy przepływ danych jest identyfikowany raz i pokazywany w raportach jako jeden strumień danych bez względu na ścieżkę danych. System uwzględnia również, że na ścieżce mogą pojawić się firewalle sieciowe oraz systemy proxy.
WN.37	Rozwiązanie umożliwia wskazanie hostów, na których uruchomiona jest określona usługa lub klient.
WN.38	Rozwiązanie posiada możliwość wskazania „wykorzystania" określonych portów TCP/UDP oraz wolumenu ruchu ICMP.
WN.39	Rozwiązanie zapewnia mechanizmy „trendingu" dla sieci i ruchu, w szczególności dla całkowitego wolumenu ruchu, oddzielnie ruchu wyjściowego i wejściowego, ilości nowych/starych/nieaktywnych hostów oraz przepływów.
WN.40	Rozwiązanie umożliwia raportowanie z wykorzystaniem Differentiated Services jako atrybutu.
WN.41	Rozwiązanie umożliwia raportowanie z wykorzystaniem ASN jako atrybutu.
WN.42	Rozwiązanie umożliwia monitorowanie sieci korzystających z IPv6 oraz sieci ze środowiskiem mieszanym IPv4/IPv6.
WN.43	Rozwiązanie posiada możliwość wykrywania rekonesansu w sieci, w tym wykonywanie skanowania po portach.
WN.44	Rozwiązanie posiada możliwość alarmowania w przypadku skanowania sieci i kierowania ruchu do nieaktywnych hostów.
WN.45	Rozwiązanie posiada możliwość raportowania nadużycia zasobów organizacji np. a. Ponadnormatywne korzystanie z Internetu b. Korzystanie z portali społecznościowych c. Dostęp do systemów „wrażliwych"

Kod wymagania	Opis wymagań
	d. Wykorzystanie protokołów lub aplikacji, które nie zostały dopuszczone do użytku w sieci
WN.46	Rozwiązanie posiada możliwość raportowania o pojawieniu się w sieci nowej niedopuszczonej przez administratora aplikacji.
WN.47	Rozwiązanie posiada możliwość raportowania informacji o hostach próbujących ominąć (bypass) serwery proxy.
WN.48	Rozwiązanie jest wyposażony w moduł, który automatycznie klasyfikuje serwery do konkretnych grup funkcjonalnych – w tym: a. Serwery WEB, b. Serwery DNS, c. Serwery DHCP, d. Serwery NTP, e. Serwery pocztowe, f. Kontrolery domeny.
WN.49	Rozwiązanie ma możliwość zdefiniowania krajów, z którymi komunikacja jest niepożądana. Dla szybkiej analizy system obrazuje wszystko na mapie świata, wyróżniając te kraje odpowiednim kolorem oraz pokazując jak dużo danych było transmitowanych.
WN.50	Rozwiązanie posiada narzędzie audytu pod kątem wykorzystywanych protokołów i algorytmów szyfrowania. Umożliwia odczyt tych danych na dwa sposoby: a. Obrazowo na wykresach, które pokazują porównanie wolumenu ruchu przesyłanego przez sieć za pomocą tych protokołów, b. Szczegółowo w tabeli z pokazaniem wszystkich atrybutów danego przepływu.
WN.51	Rozwiązanie posiada moduł tworzenia map graficznych z następującymi możliwościami: a. Budowanie topologii poprzez import dowolnego obrazu (np. mapy Polski) i dowolnego rozmieszczenia na nim grup hostów, b. Definiowania graficznie przepływów między grupami hostów oraz następujących wartości na tych przepływach w celu szybkiej analizy potencjalnych problemów sieciowych: i. Wolumen ruchu wyrażony w bitach lub bajtach na sekundę, ii. Ilość pakietów na sekundę (PPS), iii. Czas transmisji pakietów w obie strony (Round Trip Time - RTT), iv. Czas odpowiedzi serwerów (SRT).
WN.52	Rozwiązanie dostarcza szczegółowych informacji o aplikacjach takich jak: a. RTT – round trip time b. SRT – Server response time c. Retransmisje w sieci d. Szczegóły flag protokołu TCP e. URLe dla ruchu WEB
WN.53	Rozwiązanie umożliwia dekapsulację VXLAN.
WN.54	Rozwiązanie umożliwia generowanie telemetrii służącej monitorowaniu ruchu szyfrowanego HTTPS w następującym zakresie:

Kod wymagania	Opis wymagań
	a. Analiza inicjalnego pakietu połączenia (IDP – Initial Data Packet) w celu monitorowania wykorzystywanych protokołów i algorytmów w ruchu HTTPS b. Dane zawierające informację na temat pakietów i czasów ich transmisji, które służą do zbudowania wzorca sesji znanego malware.
WN.55	Rozwiązanie umożliwia przetwarzanie nagłówka X-Forwarder-For (XFF) w celu identyfikacji rzeczywistego adresu IP klienta połączonego do serwera WEB przez system proxy lub load balancer.
WN.56	Rozwiązanie umożliwia monitorowanie maszyn wirtualnych (w tym pracujących w środowisku VMware), ruchu odbywającego się w ramach środowiska wirtualnego, jak i wychodzącego ze środowiska wirtualnego.
Zarządzanie	
WN.57	Rozwiązanie zarządzający dostępny poprzez bezpieczny kanał komunikacji z wykorzystaniem połączeń szyfrowanych SSL.
WN.58	Możliwość ograniczenia dostępu do stacji zarządzającej do pojedynczych hostów lub też do grupy hostów.
WN.59	Możliwość uwierzytelnienia administratorów z wykorzystaniem zewnętrznych serwerów RADIUS, TACACS+, LDAP.
WN.60	Możliwość uwierzytelnienia SSO (Single Sign On) przez protokół SAML.
WN.61	Rozwiązanie umożliwia różnicowanie dostępu dla administratorów – w szczególności pozwala na: a. Ograniczenie grup hostów, które może monitorować dany administrator, b. Ograniczenie czynności, które może wykonać dany administrator, c. Ograniczenie dostępu w trybie tylko do odczytu (read-only access), d. Ograniczenie informacji, do których ma dostęp dany administrator np.: i. Administrator1 ma dostęp do statystyk urządzeń sieciowych, charakterystyk ruchu i innych danych dotyczących monitoringu sieciowego ii. Administrator2 ma dostęp do informacji o naruszeniu polityk, outbreak i innych danych dotyczących bezpieczeństwa
WN.62	Rozwiązanie umożliwia włączenie cyklicznego generowania raportów we wskazanym przez administratora reżimie czasowym i wysyłanie poprzez email do zdefiniowanych odbiorców.
WN.63	Rozwiązanie umożliwia tworzenie raportów z wykorzystaniem geolokacji – w szczególności raportów per kraj.
WN.64	Rozwiązanie posiada ponad 100 gotowych i zdefiniowanych przez producenta widoków (dashboardów) składających się z pojedynczych elementów (widżetów), z czego każdy element jest oddzielnym raportem w postaci tabelarycznej lub graficznej (wykresy kołowe, dane prezentowane na osi czasu).
WN.65	Rozwiązanie umożliwia tworzenie własnych dashboardów, w których użytkownik ma możliwość zdefiniowania dowolnej ilości widżetów z danymi pożądanymi przez siebie. Użytkownik może ograniczyć dostęp do tych raportów tylko dla siebie lub też udostępnić je dla innych użytkowników systemu.

Kod wymagania	Opis wymagań
WN.66	Dashboardy i widżety gotowe oraz te definiowane przez użytkownika dają następujące możliwości: a. Prezentacja wyników i danych na bieżąco z możliwością zastosowania zaawansowanego filtrowania oraz definicji ram czasowych, b. Możliwość zapisu całego dashboard'u do pliku PDF wraz z widżetami graficznymi, c. Możliwość eksportu danych z pojedynczych widżetów do pliku CSV w przypadku widżetów tabelarycznych oraz do plików JPEG i PNG w przypadku widżetów graficznych, d. Możliwość definiowania harmonogramu dla eksportu danych do plików CSV oraz PDF postępowania z tymi plikami w następujący sposób: i. Wysłanie tych plików jako załączniki do wiadomości email do wskazanych odbiorców w formie nieskompresowanej lub zarchiwizowanej ZIP ii. Zarchiwizowanie tych plików lokalnie w systemie zarządzania w postaci archiwum ZIP oraz zdefiniowanie czasu przechowywania tych archiwów w celu zarządzania przestrzenią dyskową systemu.
WN.67	Rozwiązanie umożliwia automatyczne usunięcie źródła Netflow (exportera), który nie transmitował ruchu do kolektora przez np. 30 dni.
WN.68	Rozwiązanie zarządzania ma możliwość konfiguracji podstawowych ustawień sieciowych wszystkich elementów całego systemu (generatory Netflow, kolektory, forwardery) bez konieczności logowania się na każdy element z osobna w zakresie: a. Ustawień SNMP, b. Ustawień NTP, c. Ustawień Proxy, d. Ustawień serwerów DNS, e. Włączenia lub wyłączenia dostępu do CLI poprzez SSH.
WN.69	Konsola zarządzająca umożliwia podział na domeny i pracę wielu użytkowników odpowiedzialnych za różne obszary sieci (np. MPLS VPN), do której przypisane są inne kolektory NetFlow i przypisanie granularne uprawnień administratorom tych obszarów.
WN.70	Konsola ma możliwość robienia kopii zapasowych konfiguracji oraz przechowywania jej w postaci zaszyfrowanej.
Współpraca i integracja z systemami zewnętrznymi	
WN.71	Wszystkie logi, wykresy oraz raporty są eksportowalne do zewnętrznych odbiorców – odpowiednio w formacie CSV, JPEG i PDF.
WN.72	Rozwiązanie zapewnia raportowanie o zdarzeniach i incydentach przez syslog, SNMP i email.
WN.73	Rozwiązanie zapewnia możliwość integracji z zewnętrznymi systemami klasy SIEM.
WN.74	Rozwiązanie zapewnia możliwość współpracy i integracji z systemem Cisco ISE (Identity Services Engine) w zakresie: a. RADIUS proxy, b. Pobierania informacji o tożsamości użytkowników uwierzytelnionych przez ISE, c. Pobierania informacji o profilu hosta po profilowaniu dokonanym przez ISE, d. Pobierania informacji o kontekście użytkownika przechowywanym przez ISE,

Kod wymagania	Opis wymagań
	e. Wysyłanie informacji o adresie IP w celu zablokowania danego IP poprzez ISE.
WN.75	Rozwiązanie posiada możliwość integracji z Active Directory w celu otrzymania szczegółowych informacji na temat użytkownika jak adres email, nr telefonu, grupa AD, do której użytkownik przynależy.
WN.76	Rozwiązanie umożliwia zdefiniowanie listy zewnętrznych serwisów internetowych, na których można sprawdzić informację o analizowanym adresie IP (np. DShield.org, Talos). Lista ta jest dostępna w menu podręcznym przy adresach IP w interfejsie graficznym konsoli zarządzania i pozwala na wywołanie serwisu z zapytaniem o ten adres jednym kliknięciem myszy.
WN.77	Rozwiązanie jest wyposażony w otwarty interfejs REST API z ogólnie dostępną dokumentacją i pozwala na przeprowadzenie wszystkich codziennych operacji administratora, przynajmniej w zakresie: a. Zarządzanie użytkownikami systemu oraz definiowanie ich ról, b. Włączanie i wyłączanie alarmów, c. Edycja polityk wbudowanych, d. Definicja i edycja własnych alarmów, e. Tworzenie sprecyzowanych zapytań o przepływy i odczytywanie tych danych, f. Pobieranie raportów dotyczących ruchu i incydentów bezpieczeństwa ze sprecyzowanymi parametrami.

Zadanie 2 – zakup subskrypcji licencji „Wildfire" do posiadanych przez Zamawiającego urządzeń NGFW PA-3220

Przedmiotem zadania 2 jest zakup subskrypcji licencji Wildfire dla 4 urządzeń będących w posiadaniu Zamawiającego PA-3220 firmy Palo Alto Networks o numerach seryjnych podanych poniżej, na okres 12 miesięcy:

- 016201027237
- 016201027240
- 016201027236
- 016201027278

Urządzenia pracują w parach redundantnych w dwóch lokalizacjach Centrów Danych. Zamawiający wymaga dostarczenia subskrypcji licencji na okres 12 miesięcy od dnia 10.12.2022 roku.

Model PA-3220
Serial # 016201027278

Model PA-3220
Serial # 016201027236

Rysunek 1. Numery seryjne urządzeń dla których wymagane jest dostarczenie licencji

IV. Wymagania dodatkowe

Wykonawca zapewni 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 Oprogramowania lub licencji będących przedmiotem zamówienia

V. Świadczenie usługi serwisowej

Kod wymagania	Opis funkcjonalności
WUS.01	Na dostarczone rozwiązanie (Zadanie nr 1) do analizy przepływów wykonawca zapewni usługę serwisu liczoną od daty podpisania protokołu odbioru na okres 36 miesięcy opartego na świadczeniach serwisowych producenta, natomiast dla subskrypcji (Zadanie nr 2) licencji na okres 12 miesięcy.
WUS.02	Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu: • prawo do pobierania nowych wersji i aktualizacji przez okres minimum 36 miesięcy od podpisania protokołu odbioru produktu dla zadania 1 oraz 12 miesięcy dla zadania 2; • możliwość aktualizacji oprogramowania poprzez dostęp do zasobów producenta rozwiązania; • dostęp do pomocy technicznej producenta; • nieograniczoną ilość zgłoszeń serwisowych; • dostęp do materiałów producenta takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe producentów • dostęp do poprawek i uaktualnień oprogramowania objętego usługą wsparcia oraz nowych wersji; • dostęp do portalu www producenta oprogramowania umożliwiającego zarządzanie posiadanymi licencjami, podniesienie lub obniżenie (jeśli producent oficjalnie wspiera poprzednie wersje) wersji oprogramowania; • dostęp do rejestru licencji (dostępnego przez portal www producenta

	oprogramowania/urządzeń).
WUS.03	Wykonawca wraz z dostawą Oprogramowania przekaże warunki gwarancyjne i serwisowe, w tym procedury zgłaszania awarii, dostępne kanały komunikacyjne z serwisem producenta. Do zamówienia muszą zostać dostarczone procedury zgłaszania awarii w formie elektronicznej edytowalnej.
WUS.04	Przyjęcie do realizacji zgłoszenia powinno zostać niezwłocznie potwierdzone przez Wykonawcę, zwrotnie na adres e-mail zgłaszającego.
WUS.05	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
WUS.06	Gwarancja obejmuje między innymi: 1) niespełnienie deklarowanych przez producenta parametrów i/lub funkcji użytkowych Oprogramowania; 2) usuwanie wykrytych usterek i Awarii w działaniu oprogramowania.
WUS.07	Zamawiający uprawniony jest do opóźnienia terminu rozpoczęcia usuwania awarii przez Wykonawcę, w takim przypadku gwarantowany czas naprawy ulegnie odpowiedniemu wydłużeniu i będzie liczony względem wskazanego przez Zamawiającego terminu.
WUS.08	W przypadku zdiagnozowania błędów w używanej przez Zamawiającego wersji oprogramowania, Wykonawca zapewni Zamawiającemu dostęp do najnowszych wersji oprogramowania posiadających wsparcie producenta, pozwalających na usuniecie tych błędów. W przypadku wykrycia błędu, dla którego brak jest w danym momencie odpowiedniej aktualizacji, Wykonawca 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.09	Z tytułu świadczenia przez producenta lub autoryzowany serwis producenta usługi serwisu gwarancyjnego Zamawiający nie ponosi dodatkowych kosztów.
WUS.10	Dla oprogramowania obowiązują prawa gwarancyjne producenta.
WUS.11	Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.

I.Zasady Ogólne

1) Przedmiot Umowy (zadanie nr 1 i 2) należy dostarczyć zgodnie z zasadami wskazanymi w Umowie nie później niż do dnia 22.12.2022 r.
2) Odbiór zostanie przeprowadzony w biurze Zamawiającego przy ul. Maszewskiej 20 w Warszawie, w obecności przedstawicieli Wykonawcy i Zamawiającego w godz. 8:00 – 15:35 lub elektronicznie
3) Odbiór zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego i Wykonawcy protokołu odbioru ilościowo – jakościowego, którego wzór stanowi załącznik nr 3 do Umowy.
4) Przedmiot Umowy podlegać będzie odbiorowi ilościowo – jakościowemu.

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 Umowy.
2) Wykonawca będzie odpowiedzialny za dostarczenie i zaprezentowanie dostarczonego przedmiotu Umowy.
3) Podstawą dokonania odbioru ilościowo – jakościowego jest przeprowadzenie z pozytywnym skutkiem sprawdzeń kompletności oraz poprawności działania Oprogramowania dostarczonego w ramach Umowy wraz z wymaganymi licencjami – weryfikacja polega na sprawdzeniu obecności licencji w portalu producenta przypisanych do konta Zamawiającego.
4) Pozytywny wynik odbioru ilościowo – jakościowego zostanie potwierdzony podpisaniem protokołu odbioru ilościowo – jakościowego.