ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa zamówienia

Dostawa systemu do monitorowania i analizowania przepływów sieciowych wraz z gwarancją i usługami wsparcia w okresie 36 miesięcy.

I.1 Kody CPV

48000000-8 Pakiety oprogramowania i systemy informatyczne.
32420000-3 Urządzenia sieciowe.
35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa.
72250000-2 Usługi w zakresie konserwacji i wsparcia systemów.

II. Przedmiot zamówienia

(1) Przedmiotem zamówienia są:

a) dostawa Systemu (dalej: Analizatora Flow) do monitorowania i analizowania przepływów sieciowych (ang. flow) spełniającego wymagania opisane w pkt III.1.
b) usługi wsparcia producenta (tzw. maintenance) dla Analizatora Flow, opisane w pkt. III.2.
c) usługi świadczenia gwarancji opisane w pkt. III.3.

(2) Zamawiający dokonał opisu przedmiotu zamówienia z wykorzystaniem następujących definicji:

Analizator Flow	oznacza Rozwiązanie Sprzętowe lub Rozwiązanie wirtualne, opisane w pkt III.1 niniejszego dokumentu.
Dzień Roboczy	oznacza dzień od poniedziałku do piątku nie będący dniem ustawowo wolnym od pracy na terenie Rzeczypospolitej Polskiej.
Gwarant	Oznacza podmiot, który udzielił gwarancji, spełniającej co najmniej wymogi wskazane w pkt III.3 OPZ dla Rozwiązania sprzętowego.
Wsparcie producenta	oznacza oferowane przez producenta danego rozwiązania aktualizacje, definicje, sygnatury i inne usprawnienia funkcjonalności, udostępniane dla Analizatora Flow przez zdefiniowany okres czasu zgodnie z pkt III.2 OPZ .
SSL/TLS	ang. Secure Socket Layer / Transport Layer Security oznacza protokół szyfrowania komunikacji sieciowej. (ze wsparciem co najmniej w wersji TLS 1.2 lub TLS 1.3)
Rozwiązanie sprzętowe	(ang. Hardware Appliance) oznacza produkt, który realizuje wymogi wskazane w pkt III.1 OPZ z wykorzystaniem urządzeń fizycznych i Oprogramowania, objętych jedną gwarancją i wsparciem producenta dla Oprogramowania przez producenta całego rozwiązania.
Rozwiązanie wirtualne	(*ang. Software Appliance*) oznacza Oprogramowanie, które realizuje wymogi wskazane w pkt III.1 OPZ bez wykorzystania dedykowanej warstwy urządzeń fizycznych objęte wsparciem

	producenta.

(3) Przedmiot zamówienia został opisany przez wskazanie znaków towarowych, szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę z uwagi na fakt, że Zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób, a wskazaniu temu towarzyszą wyrazy "lub równoważny".

(4) W opisie przedmiotu zamówienia, Zamawiający w zakresie każdego wskazania wymienionego w powyższym pkt (3) wskazał kryteria stosowane w celu oceny równoważności. W przypadku zaoferowania rozwiązania równoważnego, na Wykonawcy spoczywa obowiązek wykazania jego równoważności, w sposób umożliwiający Zamawiającemu weryfikację spełniania przez rozwiązanie równoważne wszystkich kryteriów równoważności.

(5) Przedmiot zamówienia został opisany przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, a Zamawiający dopuszcza rozwiązania równoważne opisywanym i takim odniesieniom towarzyszą wyrazy "lub równoważne".

(6) W przypadku gdy opis przedmiotu zamówienia odnosi się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp., Zamawiający nie odrzuci oferty tylko dlatego, że oferowane dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 Pzp., że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.

(7) W przypadku gdy opis przedmiotu zamówienia odnosi się do wymagań dotyczących wydajności lub funkcjonalności, o których mowa w art. 101 ust. 1 pkt 1 Pzp., zamawiający nie odrzuci oferty zgodnej z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszącymi normy europejskie, z europejską oceną techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, oceny techniczne, specyfikacje i systemy referencji technicznych dotyczą wymagań dotyczących wydajności lub funkcjonalności określonych przez zamawiającego, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107, że dostawa lub usługa, spełniają wymagania dotyczące wydajności lub funkcjonalności określone przez zamawiającego.

(8) W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przypadkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.

(9) Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po

stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.

(10) Wykonawca zobowiązany jest posiadać status partnera producenta Analizatora Flow z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga, aby Wykonawca posiadał nie niższy niż drugi w kolejności poziom partnerstwa licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta. Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa jest w zdaniu poprzedzającym.

III. Specyfikacja wymagań

III.1 Wymagania dot. Analizatora Flow:

Lp.	Opis wymagania	Parametry minimalne
1.	Rodzaj platformy systemu i parametry ilościowe	1.1. Komponenty Analizatora Flow mogą być dostarczone w postaci Wirtualnej lub sprzętowej wraz z zachowaniem wysokiej dostępności (dotyczy zarówno wirtualnych komponentów jak i fizycznych). 1.2. dwa redundantne zasilacze – w przypadku Rozwiązania sprzętowego. 1.3. Interfejsy sieciowe do analizy danych: min. 2 typu SFP+ i 2 typu 10/100/1000BASE-T – w przypadku Rozwiązania sprzętowego. 1.4. Interfejs sieciowy do zarządzania Analizatorem Flow i HW – w przypadku Rozwiązania sprzętowego. 1.5. Wykonawca dostarczy wkładki kompatybilne z w/w interfejsami czyli min. 4 sztuk 1000Base-T oraz 4 sztuk 1000Base-SX (LC) oraz 4 sztuk 10GBase-SR (LC), objętymi tą samą gwarancją tj. Analizator Flow – w przypadku Rozwiązania sprzętowego. 1.6. Analizator Flow musi przetwarzać co najmniej 10 000 przepływów na sekundę (FPS: ang. Flow Per Second). 1.7. Analizator Flow musi analizować ruch z co najmniej 2000 adresów IP. 1.8. Każdy z komponentów Analizatora Flow musi być zarządzany z konsoli zarządzającej sprzętowej lub wirtualnej (umożliwiająca instalację na platformie VMware). 1.9. Dostarczony Analizator Flow w formie Hardware Appliance musi posiadać co najmniej 3TB pojemności dyskowej z odpowiednio dostosowanych (rekomendowanych przez producenta) parametrach wydajnościowych: IOPS lub Data transfer rate[1].

[1] Stanowi kryterium oceny ofert

2.	Jednorodność i aktualność wsparcia	Analizator Flow nie może znajdować się na liście (typu „end-of-life" oraz „end-of-support"), wskazującej, że wsparcie serwisowe producenta, dla takiego urządzenia zostanie zakończone przed rokiem 2025.
3.	Ogólne	3.1. Analizator Flow musi pozwalać na analizę zdarzeń zachodzących w sieci, w szczególności system musi obejmować zakres: 3.1.1. Wszystkie zarejestrowane połączenia i zdarzenia bezpieczeństwa muszą być możliwe do wyświetlenia i analizy. 3.1.2. Analizator Flow musi obsłużyć (dot. analizy) kopie ruchu sieciowego dostarczoną za pomocą SPAN i urządzeń TAP. 3.1.3. Analizator Flow powinien działać w oparciu o analizę Flow: NetFlow, sFlow, IPFIX i na podstawie danych z telemetrii (np. z urządzeń sieciowych typu Cisco Nexus) [2]. 3.2. Analizator Flow musi umożliwiać monitorowanie sieci korzystających z IPv6 oraz sieci ze środowiskiem mieszanym IPv4/IPv6. 3.3. Musi zapewniać możliwość wysyłania zdarzeń bezpieczeństwa (w tym: audytowe, zarejestrowane zdarzenia, anomalie) w postaci logów do zewnętrznego systemu klasy SIEM. 3.4. Musi mieć wewnętrzne mechanizmy do monitorowania wydajności i dostępności poszczególnych jego komponentów za pomocą GUI/CLI lub API. 3.5. Analizator Flow przechowujący dane dot. przepływów sieciowych musi dostarczać mechanizm szyfrowania danych, FIPS 140-2 lub 140-3 lub równoważny*.

*Zamawiający wskazuje następujące kryteria stosowane w celu oceny równoważności dla normy FIPS 140-2 lub 140-3 i uzna za normę równoważną opisywanej, normę która:

1. Definiuje szczegółowe wymagania bezpieczeństwa na moduły szyfrujące,
2. Została wydane przez NIST (ang. National Institute of Standards and Technology) lub została wydana przez podmiot prawa publicznego, powołany przez co najmniej jedno z Państw Członkowskich Unii Europejskiej lub NATO, do definiowania standardów bezpieczeństwa przetwarzania informacji,
3. Opisuje warunki zmian certyfikowanego rozwiązania, które wymagają powtórnej certyfikacji,
4. Została wskazana w obowiązującym na dzień składania ofert przepisie prawa powszechnie obowiązującego, na terenie Państwa Członkowskiego Unii Europejskiej lub

[2] Stanowi kryterium oceny ofert

NATO, jako norma wymagana dla rozwiązań służących do realizowania zadań związanych z informatyzacją działalności państwa.

4.	Wykrywanie ataków/anomalii oraz narzędzia monitorowania sieci	4.1. Musi umożliwiać profilowanie ruchu poszczególnych hostów i grup hostów w celu wykrywania anomalii/ataków wynikających z: 4.1.1. przekroczenia wartości bazowych (zarówno zdefiniowanych przez administratora jak i wynikających z „uczenia się" systemu charakterystyk ruchowych) dla typowego wzorca ruchu dla stacji, 4.1.2. zmiany charakterystyki ruchu dla stacji, 4.1.3. naruszenia założonej polityki bezpieczeństwa. 4.2. Powinien umożliwiać wskazanie „zarażonych lub podejrzanych pod względem bezpieczeństwa" hostów lub systemów[3]. 4.3. Musi posiadać możliwość wykrywania rekonesansu w sieci, w tym wykonywanie skanowania portów. 4.4. Musi umożliwiać wykrywania ataków DoS lub DDoS wraz ze wskazaniem celu ataku jak też hostów atakujących. 4.5. Musi umożliwiać monitorowanie niepożądanych przepływach ruchu pomiędzy wskazanymi obszarami sieci i adresami IP. 4.6. Musi mieć możliwość identyfikowania ruchu sieciowego powiązanego z kategoriami typu: TOR, CnC, Botnet. W tym celu bazy IP (reputacyjne) dla w/w kategorii muszą być dostarczane i aktualizowane przez producenta Analizatora Flow (na czas wsparcia wskazanym w n/w pkt. III.2 (dot. Zasady świadczenia usług wsparcia technicznego). 4.7. Musi posiadać mechanizmy monitorowania połączeń do określonych serwerów, obszarów sieciowych lub IP oraz alertowania gdy w komunikacji pojawi się więcej niż określony wolumen ruchu z jednego adresu IP. 4.8. Musi posiadać wbudowaną analitykę pozwalającą na wykrywanie potencjalnych wycieków danych na podstawie wolumenu ruchu, a także informacji dotyczących czasu połączenia do sieci zewnętrznych. 4.9. Musi posiadać możliwość raportowania nieaktywności oraz aktywności poszczególnych hostów. 4.10. Musi posiadać możliwość informowania (co najmniej w GUI) o pojawieniu się nowych hostów (lub adresów IP)

[3] Stanowi kryterium oceny ofert

		w określonych podsieciach.
5.	Analiza i przechowywanie informacji o przepływie sieciowym (ang. Flow)	5.1. Musi zapewniać możliwość przechowywania informacji o przepływach (ang. flow). Jedynym możliwym ograniczeniem na ilość danych może wynikać jedynie z przestrzeni dyskowej przeznaczonej na dane w Analizatorze Flow . 5.2. Musi posiadać narzędzia graficznego przedstawiania przepływów (ang. flow) w sieci. 5.3. Powinien umożliwiać identyfikowanie Malware w zaszyfrowanym ruchu sieciowym bez potrzeby deszyfrowania ruchu[4]. 5.4. Musi umożliwiać identyfikowanie zagrożeń (bezpieczeństwa) w zaszyfrowanym ruchu sieciowym bez potrzeby deszyfrowania ruchu. 5.5. Musi dostarczać funkcjonalność geolokalizacji oraz możliwość jej wykorzystania podczas budowania polityk lub reguł bezpieczeństwa.
6	Zarządzanie	6.1. Musi umożliwiać zarządzanie politykami lub regułami bezpieczeństwa za pomocą interfejsu graficznego. W przypadku użycia technologii Java wymagane jest dostarczenie odpowiednich licencji aby móc legalnie użytkować tą technologię. 6.2. Musi wspierać połączenia do GUI bezpiecznym kanałem szyfrowanym z wykorzystaniem SSL/TLS. 6.3. Musi posiadać możliwość uwierzytelnienia z wykorzystaniem kont lokalnych i za pomocą LDAP-a lub AD. 6.4. Musi umożliwiać różnicowanie praw dostępu dla administratorów, w szczególności musi pozwalać na: 6.4.1. ograniczenie grup hostów, które może monitorować dany administrator. 6.4.2. ograniczenie czynności, które może wykonać dany administrator. 6.4.3. ograniczenie dostępu tylko do odczytu - read-only. 6.5. Musi umożliwiać predefiniowanie raportów, które będą generowane cyklicznie we wskazanych przez administratora odstępach czasu. 6.6. Musi pozwalać na zdefiniowanie min. 30 administratorów o różnych uprawnieniach, mogących pracować równolegle i lokalnie analizować dane zarejestrowane przez ten system.

[4] Stanowi kryterium oceny ofert

7	Współpraca i integracja z systemami zewnętrznymi	7.1. Raporty muszą mieć możliwość eksportu do plików co najmniej w formacie PDF lub XLSX lub HTML. 7.2. Musi być możliwe raportowanie o zdarzeniach bezpieczeństwa co najmniej za pomocą GUI. 7.3. Musi istnieć możliwość wysyłania zdarzeń bezpieczeństwa, audytowych oraz dot. „zdrowia" systemu do zewnętrznego systemu klasy SIEM.

III.2 Zasady świadczenia usług wsparcia producenta

(1) Wykonawca zobowiązany jest zapewnić wsparcie Producenta Analizatora Flow (dalej określanego jako „**Producent**") lub autoryzowanego podmiotu współpracującego z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta lub poziomie niższym, o nie więcej niż jeden stopień, działającego w imieniu tego Producenta (dalej określanego jako „**Partner**"), dla dostarczonych subskrypcji, przez okres 36 miesięcy, od dnia odbioru przedmiotu zamówienia opisanego w pkt III.1.

(2) Zapewnienie usługi wsparcia, obejmuje nieograniczony dostęp do wszystkich udostępnionych przez Producenta aktualizacji, poprawek, komunikatów, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy, instrumentów zgłaszania błędów.

(3) Dostęp do uaktualnień sygnatur/reguł i poprawek i aktualizacji licencji/oprogramowania będzie realizowany przez konto udostępnione przez producenta wraz z niezbędnymi danymi logowania, umożliwiające samodzielne (bezpośrednio u producenta) pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiające zakładanie zgłoszeń serwisowych w trybie 24/7/365.

(4) Zgłoszone serwisowe będą usuwane w terminie do końca następnego Dnia Roboczego (ang. NBD) następującego po dniu, w którym awaria została zgłoszona.

III.3 Zasady świadczenia usług gwarancji

(1) Wykonawca zobowiązany jest zapewnić Zamawiającemu gwarancję dla dostarczonego Rozwiązania sprzętowego, udzieloną przez Producenta tych urządzeń (dalej określanego jako „**Producent**") lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta lub poziomie niższym, ale nie więcej niż jeden stopień, działający w imieniu tego Producenta , obejmującą okres 36 miesięcy, od dnia odbioru sprzętu opisanego w pkt III.1.

(2) Wykonawca, zobowiązany będzie zapewnić wykonywanie zobowiązań z tytułu Gwarancji, zgodnie z następującymi zasadami:

   (a) Zamawiający będzie uprawniony do dokonywania zgłoszeń awarii w trybie 24/7/365, za pośrednictwem telefonu lub dedykowanej aplikacji lub adresu poczty elektronicznej, wskazanych przez Wykonawcę;

   (b) Serwis gwarancyjny realizowany będzie w miejscu wskazanym przez Zamawiającego na terenie m.st. Warszawy.

   (c) Zgłoszone awarie będą usuwane w terminie do końca następnego Dnia Roboczego następującego po dniu, w którym awaria została zgłoszona.

(3) W przypadku w którym usunięcie awarii będzie wymagać odinstalowania urządzenia, które uległo awarii:

(a) Naprawa będzie mogła być wykonana wyłącznie w lokalizacji instalacji urządzenia, bez wydawania go poza tą lokalizację;

(b) Wydanie urządzenia poza miejsce jego instalacji, w celu dokonania naprawy, będzie mogło nastąpić dopiero, po trwałym usunięciu danych ze wszystkich nośników danych na tym urządzeniu np. dyski Flash, karty SD, dyski twarde lub ich zdemontowaniu przez Gwaranta i zdeponowaniu ich u Zamawiającego;

(4) W przypadku nie przywrócenia pełnej funkcjonalności urządzenia w terminie określonym w pkt III.3 powyżej Wykonawca zobowiązuje się zapewnić urządzenie zastępcze na własny koszt, o parametrach nie gorszych niż naprawiane urządzenie oraz zapewniających nie gorszy poziom bezpieczeństwa. W przypadku zwrotu urządzenia zastępczego, Gwarant zapewni trwałe usunięcie danych ze wszystkich nośników danych na tym urządzeniu np. dyski Flash, karty SD, dyski twarde lub ich zdemontowaniu przez Gwaranta i zdeponowaniu ich u Zamawiającego. W takim przypadku termin usunięcia awarii przez Gwaranta wynosi 30 dni kalendarzowych od chwili zgłoszenia awarii.

(5) Gwarant jest zobowiązany do wymiany urządzenia na nowe na własny koszt, o parametrach nie gorszych niż naprawiane urządzenie w przypadku w którym usunięcie awarii o której mowa w pkt. 4 powyżej jest niemożliwe. W takim przypadku Gwarant zapewni wsparcie techniczne w stosunku do nowego urządzenia.

(6) Wykonywania zobowiązań gwarancyjnych, wymagające fizycznego dostępu do lokalizacji instalacji urządzenia, wymagać będzie spełnienia przez osoby wykonujące te czynności w imieniu gwaranta następujących wymogów:

(a) Przedłożenia (na żądanie Zamawiającego) aktualnego zaświadczenia o niekaralności lub

(b) Poświadczenia bezpieczeństwa dostępów do informacji niejawnych o klauzuli „Poufne”.