Załącznik nr 1

Dane Zamawiającego:
Samodzielny Publiczny
Zakład Opieki Zdrowotnej
w Mońkach
Al. Niepodległości 9
19-100 Mońki

ZAPYTANIE CENOWE

DANE WYKONAWCY

1. Pełna nazwa (oznaczenie, firma) ……..……..……..…….……
2. Adres siedziby (ulica, kod pocztowy, miejscowość) …….....……..……
3. REGON …….…… NIP ……..……..……KRS/CEiDG.....……
4. Telefony (z numerem kierunkowym) ……..……..……..…….…….
5. Faks (z numerem kierunkowym) ……..……..……
6. E-mail ……..……..…….
7. Adres skrzynki ePUAP.....

Odpowiadając na zapytanie ofertowe na dostarczenie, zamontowanie, wdrożenie i wsparcie w zakresie Systemu bezpieczeństwa UTM oraz system logowania i raportowania dla potrzeb Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Mońkach niniejszym oferuję:

SYSTEM BEZPIECZEŃSTWA – UTM – 1 szt. Dostarczenie, montaż, konfiguracja, podłączenie do obecnej infrastruktury

Lp.	Opis minimalnych wymaganych parametrów technicznych	Wartość wymagana	Wartość oferowana
Wymagania ogólne			
1.	Rok produkcji - 2021/2022	TAK, podać	
2.	Sprzęt fabrycznie nowy, niepowystawowy	TAK	
3.	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i	TAK	

	bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.		
4.	W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.	TAK	
5.	System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.	TAK	
<u>SYSTEM BEZPIECZEŃSTWA – UTM</u>:			**Model, nazwa /nr katalogowy …….** **Producent ……..…….** **Kraj pochodzenia ……..……** **Rok produkcji ……**
Redundancja, monitoring i wykrywanie awarii:			
6.	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.	TAK	

7.	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	TAK	
8.	Monitoring stanu realizowanych połączeń VPN.	TAK	
9.	System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.	TAK	
Interfejsy, Dysk, Zasilanie:			
10.	System realizujący funkcję Firewall musi dysponować minimum: • 18 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 4 gniazdami SFP+ 10 Gbps.	TAK	
11.	System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.	TAK	
12.	W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.	TAK	
13.	System musi być wyposażony w zasilanie AC.	TAK	
Parametry wydajnościowe:			
14	W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 280 tys. nowych połączeń na sekundę.	TAK	
15.	Przepustowość Stateful Firewall: nie mniej niż 27 Gbps dla pakietów 512 B.	TAK	
16.	Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps.	TAK	
17.	Wydajność szyfrowania IPSec VPN nie mniej niż 13 Gbps.	TAK	
18.	Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix -	TAK	

	minimum 5 Gbps.		
19.	Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.	TAK	
20.	Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.	TAK	
Funkcje Systemu Bezpieczeństwa: W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:			
21.	Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.	TAK	
22.	Kontrola Aplikacji.	TAK	
23.	Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.	TAK	
24.	Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.	TAK	
25.	Ochrona przed atakami - Intrusion Prevention System.	TAK	
26.	Kontrola stron WWW.	TAK	
27.	Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.	TAK	
28.	Zarządzanie pasmem (QoS, Traffic shaping).	TAK	
29.	Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).	TAK	
30.	Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.	TAK	
31.	Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.	TAK	
32.	Analiza ruchu szyfrowanego protokołem SSH.	TAK	
33.	Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z	TAK	

	możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system		
Polityki, Firewall			
34.	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.	TAK	
	System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP.	TAK	
	W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.	TAK	
	Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.	TAK	
	Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.	TAK	
Połączenia VPN			
	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).	TAK	

	• Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site.		
	System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Routing i obsługa łączy WAN 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	TAK	
Funkcje SD-WAN			

	System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.	TAK	
	Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.	TAK	
Zarządzanie pasmem			
	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.	TAK	
	Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.	TAK	
	System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	TAK	
Ochrona przed malware			
	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).	TAK	
	System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.	TAK	
	System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).	TAK	
	System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.	TAK	
	System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	TAK	
	Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	TAK	
Ochrona przed atakami:			
	Ochrona IPS powinna opierać się co najmniej na	TAK	

	analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.		
	System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.	TAK	
	Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora	TAK	
	Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.	TAK	
	System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS	TAK	
	Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.	TAK	
	Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	TAK	
Kontrola aplikacji			
	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.	TAK	
	Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	TAK	
	Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.	TAK	
	Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.	TAK	
	Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	TAK	

Kontrola WWW			
	Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.	TAK	
	W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.	TAK	
	Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.	TAK	
	Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.	TAK	
	Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.	TAK	
	Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.	TAK	
	W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.	TAK	
Uwierzytelnianie użytkowników w ramach sesji			
	System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.	TAK	
	Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.	TAK	
	Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	TAK	

	Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	TAK	
Zarządzanie			
	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.	TAK	
	Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	TAK	
	Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.	TAK	
	System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.	TAK	
	System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.	TAK	
	Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.	TAK	
	Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	TAK	
Logowanie			
	Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej,	TAK	

	komercyjnej platformy sprzętowej lub programowej.		
	W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.	TAK	
	Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.	TAK	
	Musi istnieć możliwość logowania do serwera SYSLOG.	TAK	
Certyfikaty			
	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.	TAK	
Serwisy i licencje			
	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.	TAK	
Gwarancja oraz wsparcie			
	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	TAK	

Opisy do wymagań ogólnych			
	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.	TAK	
	Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.	TAK	
	Szkolenie użytkownika z działania urządzenia i jej obsługi	TAK	

Cena PLN

1) netto: ……..…….……..… zł

słownie: ……...……...…….…… złotych

2) stawka podatku VAT: ……...% tj. …...……..…...……zł

słownie: ……...……...…….złotych

3) brutto: ……...……..…...……..... zł

słownie: ……...……...……..……..…….. złotych

....

(Miejscowość, data) *Podpis osoby (osób) uprawnionej(ych) do składania oświadczeń woli w imieniu Wykonawcy*

SYSTEM LOGOWANIA I RAPORTOWANIA– 1 szt. Konfiguracja, podłączenie do obecnej infrastruktury

Lp.	Opis minimalnych wymaganych parametrów technicznych	Wartość wymagana	Wartość oferowana
Wymagania ogólne			
SYSTEM LOGOWANIA I RAPORTOWANIA:			**Nazwa /nr katalogowy …….** **Producent ……..…….** **Kraj pochodzenia ……..……**
1.	W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud	TAK	

	(GCP).		
Interfejsy, Dysk:			
2.	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.	TAK	
Parametry wydajnościowe:			
3.	System musi być w stanie przyjmować minimum 5 GB logów na dzień.	TAK	
4.	Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów. W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:	TAK	
Logowanie			
5.	Podgląd logowanych zdarzeń w czasie rzeczywistym.	TAK	
6.	Możliwość przeglądania logów historycznych z funkcją filtrowania.	TAK	
7.	System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. Listę najczęściej wykrywanych ataków. b. Listę najbardziej aktywnych użytkowników. c. Listę najczęściej wykorzystywanych aplikacji. d. Listę najczęściej odwiedzanych stron www. e. Listę krajów , do których nawiązywane są połączenia. f. Listę najczęściej wykorzystywanych polityk Firewall. g. Informacje o realizowanych połączeniach IPSec.	TAK	
8.	Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.	TAK	
9.	Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem	TAK	

	centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.		
10.	System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.	TAK	
Raportowanie			
11.	Generowanie raportów co najmniej w formatach: PDF, CSV.	TAK	
12.	Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.	TAK	
13.	Funkcję definiowania własnych raportów.	TAK	
14	Możliwość spolszczenia raportów.	TAK	
15.	Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.	TAK	
Korelacja logów			
16.	Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.	TAK	
17.	Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.	TAK	
18.	Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.	TAK	
19.	Funkcję analizy logów archiwalnych względem	TAK	

	aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.		
Zarządzanie			
20.	1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. • Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.	TAK	
21.	System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.	TAK	
Serwisy i licencje			
22.	Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.	TAK	
Opisy do wymagań ogólnych			
23.	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system	TAK	

	zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.		
24.	Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.	TAK	

Cena PLN

1) netto: ……..…….……..… zł

słownie: ……...……...…….…… złotych

2) stawka podatku VAT: ……...% tj. …...……...……zł

słownie: ……...……...…….złotych

3) brutto: ……...…….…...……..... zł

słownie: ……...……...…….……..…….. złotych

....

(Miejscowość, data) *Podpis osoby (osób) uprawnionej(ych) do składania oświadczeń woli w imieniu Wykonawcy*

1. Oświadczamy, że zrealizujemy przedmiot zamówienia **w terminie …….. (wymagany 4 miesiące)** od dnia podpisania umowy.
2. Sprzęt będzie spełniał wymagania przedmiotowych norm zharmonizowanych i będą posiadać wymagane prawem deklaracje zgodności producentów i certyfikaty CE wystawione przez jednostkę notyfikującą.
3. Oświadczamy, że oferowany przez nas termin gwarancji wynosi:

   ……..…….. miesięcy(wymagane min. 12 miesiące)
4. Oświadczam/y, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO** wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu. [W przypadku gdy

wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (przez jego wykreślenie)].

....

(Miejscowość, data) Podpis osoby (osób) uprawnionej(ych)

5. do składania oświadczeń woli w imieniu Wykonawcy

6. **WSZELKĄ KORESPONDENCJĘ** w sprawie niniejszego postępowania należy kierować do:

Imię i nazwisko	
Adres	
Telefon	
e-mail	

Oferty cenowe należy złożyć w formie pisemnej w Sekretariacie SP ZOZ w Mońkach lub przy użyciu środków komunikacji elektronicznej na adres e-mail: sekretariat@szpital-monki.h2.pl; informatyk@szpital-monki.h2.pl w terminie **do 31.05.2022 roku, do godz. 12:00**

Kontakt:
Andrzej Haffke, tel.: 668 877 555
Samodzielny Publiczny Zakład Opieki Zdrowotnej w Mońkach
ul. Al. Niepodległości 9
19-100 Mońki