Załącznik nr 5 do Zapytania ofertowego - Deklaracja zgodności z wymaganiami Zamawiającego

Deklaracja zgodności z wymaganiami Zamawiającego stanowi treść oferty i tym samym nie podlega uzupełnieniu w toku postępowania.

L.p.	Wymagania – opis		spełnia [tak / nie] Kolumnę wypełnia Wykonawca
1	**Wymagania wspólne dla wszystkich elementów Systemu**		
1.1	System musi zapewniać wsparcie dla IPv4 oraz IPv6, zarówno w zakresie analizy ruchu, jak i systemu zarządzania.	wymagane	
1.2	Zamawiający posiada jeden 24 portowy przełącznik sieciowy Cisco Catalyst 4500X-24X. Zamawiający udostępni wykonawcy do 8 portów na wspomnianym przełączniku. Wykonawca na etapie instalacji Systemu, podłączy każde Urządzenie do przełącznika i skonfiguruje . Jeśli dostarczone Urządzenia będą wymagały większej ilości portów do obsługi ruchu, Wykonawca jest zobowiązany do dostarczenia w ramach wynagrodzenia z tytułu realizacji Umowy, odpowiedniego Urządzenia przełączającego.	wymagane	
1.3	Zarządzanie Systemem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW zabezpieczonej z wykorzystaniem protokołu TLS w wersji min 1.1 RFC 4346, 1.2 RFC 5246.	wymagane	
1.4	Wykonawca musi wykonać montaż Urządzeń w szafie rack 19” i dostarczyć na własny koszt wszystkie niezbędne elementy montażowe	wymagane	
1.5	System musi mieć wbudowane narzędzia diagnostyczne, co najmniej: ping i traceroute.	wymagane	
1.6	Urządzenia muszą być wyposażone w redundantne zasilacze AC.	wymagane	
1.7	Wykonawca jest zobowiązany do dostarczenia okablowania koniecznego do podłączenia Urządzeń i funkcjonowania Systemu w sieci Zamawiającego zgodnie z wymaganymi parametrami. Do serwerów muszą być dostarczone kable zasilające oraz kable sieciowe. Wykonawca musi dostarczyć po dwie wkładki SFP do dostarczanych serwerów i do przełącznika wskazanego w pkt 2, lub kable typu SFP DAC o długości 7mb (do połączenia switcha i dostarczonych serwerów, które zostaną zainstalowane w drugiej szafie stojącej obok). Kable sieciowe i wkładki muszą współpracować z przełącznikiem Cisco Catalyst 4500X-24X.	wymagane	
1.8	Wykonawca zapewni, że dostęp do wszystkich elementów Systemu zostanie zabezpieczony hasłem. Wszystkie dane logowania do Systemu zostaną przekazane Zamawiającemu przez Wykonawcę przy Odbiorze Systemu.	wymagane	

1.9	System musi zapewniać wysoką dostępność (HA) dla zapewnienia dostępności kluczowych usług Systemu (w szczególności, choć niewyłącznie, takich jak: rozwiązywanie nazw domenowych (DNS resolver), filtrowanie zapytań DNS na podstawie specjalizowanej bazy danych, zapewnienie dostępności konsoli zarządzającej dla administratorów)	wymagane	
1.10	System musi zostać dostarczony z zachowaniem redundancji eliminującej pojedyncze punkty awarii zarówno dla urządzeń realizujących wszystkie postawione w rozdziale IV. wymagania jak i dla modułu zarządzającego.	wymagane	
1.11	Wykonawca zobowiązany jest do zapewnienia dla Systemu Wsparcia technicznego producenta przez cały okres obowiązywania umowy.	wymagane	
2	**Moduł DNS**		
2.1	System DNS musi być dedykowaną platformą sprzętową lub być składową innego elementu Systemu.	wymagane	
2.2	System DNS musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System)	wymagane	
2.3	System DNS musi być zgodny z wymogami dokumentów RFC 1034, 1035, 2317, 2671, 2782, 3596 (RFC, tj. Request for Commnents http://www.ietf.org/rfc.html)	wymagane	
2.4	System DNS musi wspierać protokoły DNS w wersji IPv4 i IPv6	wymagane	
2.5	System DNS musi wspierać obsługę MultiMaster DNS	wymagane	
2.6	System DNS musi wpierać cache DNS	wymagane	
2.7	System DNS musi wspierać usługę walidacji DNSSEC	wymagane	
2.8	System DNS musi mieć pojemność bazy na minimum 800 000 rekordów	wymagane	
2.9	System DNS musi wspierać usługę DNS Anycast dla IPv4 i IPv6 (za pomocą protokołów BGP i OSPF oraz protokołu BFD)	wymagane	
2.10	System DNS musi posiadać funkcjonalność wykrywania i blokowania tunelowania w DNS (DNS tunneling) za pomocą silnika analitycznego bazującego na uczeniu maszynowym i pozwalającego na wykrycie nieznanych jeszcze wzorców tunelowania i wycieku danych przez protokół DNS.	wymagane	

2.11	System DNS musi posiadać funkcjonalność DNS firewalla, tzn. na podstawie następujących zdarzeń: - zapytanie DNS od konkretnego adresu IP - zapytanie DNS o konkretną domenę - odpowiedź DNS zawierająca konkretny adres IP - odpowiedź DNS z konkretną nazwą i adresem IP w rekordzie NS dla danej domeny (NSDNAME i NSIP) musi mieć możliwość podjęcia następujących działań: - blokowanie dostępu z odpowiedzią NXDOMAIN - blokowanie dostępu z odpowiedzią NODATA - przekierowanie na inny adres - zezwolenie na dostęp z logowaniem zdarzenia	wymagane	
2.12	System DNS musi posiadać ochronę przed atakami związanymi z protokołami DNS, BGP OSPF, NTP, w tym co najmniej: - Na protokoły BGP i OSPF wykorzystywane do DNS Anycast (m.in. blokowanie niespodziewanych pakietów BGP/OSPF, czy zbyt dużej liczby pakietów BGP/OSPF w danym okresie czasu) - Na protokół NTP wykorzystywany do synchronizacji czasu (m.in. blokowanie nieprawidłowych żądań NTP)	wymagane	
2.13	System DNS musi umożliwiać Zamawiającemu na przekierowanie użytkownika sieci na stronę z informacją o zablokowaniu zapytania DNS	wymagane	
2.14	System DNS musi umożliwiać Zamawiającemu na dostosowanie komunikatów o błędach i komunikatów informacyjnych wyświetlanych Użytkownikom, w szczególności wyświetlanie informacji powiązanych z sesją jak: - treść błędu, - źródłowy adres IP, - powód zablokowania danej sesji bazujący na kategorii zablokowanej domeny	wymagane	
2.15	System DNS musi posiadać funkcjonalność filtrowania odpowiedzi DNS na podstawie cyklicznie aktualizowanej przez producenta bazy reputacji domen infekujących malware/botnet/SURBL nowo obserwowanych domen w sieci Internet oraz wykrywania tunelowania w DNS (DNS tunneling) za pomocą silnika analitycznego (Machine Learning) pozwalającego na wykrycie nieznanych jeszcze wzorców tunelowania i wycieku danych za pomocą protokołu DNS.	wymagane	
2.16	System DNS musi umożliwiać Zamawiającemu na blokowanie lub przekierowywanie domen ze względu na kategorię serwowanej treści.	wymagane	

2.17	Baza kategoryzacji zawiera co najmniej 60 kategorii treści, uwzględniających co najmniej kategorie , które mogą być użyte przez Zamawiającego w dowolny sposób w celu stworzenia polityki filtrowania	wymagane	
2.18	System musi filtrować zapytania DNS, porównując poszczególne requesty ze specjalizowaną bazą danych (dostarczaną przez producenta Systemu), podzieloną na kategorie treści zawierającą informacje o domenach.	wymagane	
2.19	System DNS musi posiadać wsparcie dla bazy Internet Watch Foundation (IWF) lub równoważnej w zakresie filtrowania i raportowania.	wymagane	
2.20	System musi posiadać możliwość blokowania dostępu do treści przedstawiających seksualne wykorzystywanie dziecka (z ang. CSAM-child sexual abuse materials) poprzez aktywną implementację listy IWF “The child abuse image content URL list (CAIC)” lub równoważnej.	wymagane	
2.21	System DNS musi posiadać funkcjonalność blokowania zapytań DNS skorelowanych z domenami o niebezpiecznej treści: domeny wykorzystywane do propagacji złośliwego oprogramowania, domeny Phishing’owe, domeny wykorzystywane do zestawiania połączeń typu Command and Control z Botnetami	wymagane	
2.22	System DNS musi dać możliwość tworzenia listy domen dopuszczanych i listy domen zabronionych przez administratora systemu mających większy priorytet niż listy dostarczone wraz z Systemem.	wymagane	
2.23	System DNS musi umożliwić wprowadzenie polityki dostępu do treści zależnej od źródłowego adresu IP, przy czym zachodzące na siebie przestrzenie adresowe są traktowane jako oddzielne, tzn. przykładowo adres 10.1.1.20/32 może mieć inną politykę dostępu do treści niż 10.1.1.1/24	wymagane	
3	**Moduł zarządzania**		
3.1	Wykonawca musi dostarczyć jedną konsolę zarządzającą wszystkimi dostarczonymi elementami Systemu DNS.	wymagane	
3.2	System musi posiadać narzędzie graficzne do tworzenia przez Zamawiającego polityk filtrowania oraz mieć możliwość budowy / zmiany polityk filtrowania w oparciu o modyfikację plików płaskich lub REST API.	wymagane	
3.3	Konsola zarządzająca Systemem musi być dostarczona Zamawiającemu wraz z Systemem i dostęp do niej musi być realizowany przez Zamawiającego zarówno poprzez interfejs graficzny (lokalna lub centralna konsola), jak i *via command-line*.	wymagane	
3.4	System musi umożliwiać Zamawiającemu zarządzanie dostępem administratorów do konsoli zarządzającej w oparciu o przypisane role, w tym możliwość definiowania przez Zamawiającego własnych ról.	wymagane	

3.5	System musi zapewniać dostęp do interfesju graficznego konsoli zarządzającej z wykorzystaniem bezpiecznego połączenia szyfrowanego.	wymagane	
3.6	Konsola zarządzająca Systemem musi umożliwiać Zamawiającemu realizację wszystkich funkcjonalności związanych z zarządzaniem Systemem i realizację wszystkich uprawnień Zamawiającego	wymagane	
4	**Moduł raportowania**		
4.1	System musi posiadać co najmniej 10 predefiniowanych raportów i możliwość dodawania, co najmniej 10, własnych raportów przez Zamawiającego.	wymagane	
4.2	System musi umożliwiać Zamawiającemu archiwizowanie logów dostępowych (Access Log) po zdefiniowanym przez Zamawiającego okresie np. 30 dni.	wymagane	
4.3	System posiada raporty pokazujące ilość konkretnych zapytań, które zostały zablokowane wraz z ich kategorią – Malware, C&C, Phishing.	wymagane	
4.4	System zapewnia możliwość obrazowania ilości zapytań DNS w funkcji czasu w formie graficznej.	wymagane	
4.5	System musi umożliwiać Zamawiającemu anonimizację wybranych pól raportu – minimum IP użytkownika.	wymagane	
4.6	System musi posiadać narzędzie raportujące pozwalające na ręczne oraz zautomatyzowane generowanie raportów przedstawiających co najmniej:	wymagane	
4.6.a	TOP 10 – kategorii dozwolonych, przepuszczonych, zgodnie z polityką filtrowania,	wymagane	
4.6.b	TOP 10 – kategorii niedozwolonych, zablokowanych, zgodnie z polityką filtrowania,	wymagane	
4.6.c	TOP 10 – najpopularniejszych domen,	wymagane	
4.6.d	TOP 20 – zablokowanych domen,	wymagane	
4.6.e	TOP 20 – IP adresów ze szkodliwą aktywnością	wymagane	
4.7	System musi posiadać możliwość exportu raportów, co najmniej w formacie PDF.	wymagane	
5	**Inne***		
5.1	Wykonanie Wdrożenia Systemu zgodnie z Załącznikiem 3 Szczegółowy Opis Przedmiotu Zamówienia ustęp 5.	wymagane	
5.2	Wykonanie Re-lokacji Sytemu zgodnie z Załącznikiem 3 Szczegółowy Opis Przedmiotu Zamówienia ustęp 6.	wymagane	
5.3	Świadczenie Usługi Asysty Technicznej zgodnie z Załącznikiem 3 Szczegółowy Opis Przedmiotu Zamówienia ustęp 7.	wymagane	
5.4	Świadczenie Usługi Wparcia Serwisowego zgodnie z Załącznikiem 3 Szczegółowy Opis Przedmiotu Zamówienia ustęp 8.	wymagane	

5.5	Wykonanie Usługi Instruktażu zgodnie z Załącznikiem 3 Szczegółowy Opis Przedmiotu Zamówienia ustep 9.	wymagane	
5.6	Wykonanie deinstalacji Systemu zgodnie z Załącznikiem 3 Szczegółowy Opis Przedmiotu Zamówienia ustęp 10.	wymagane	
6	**Odniesienia**		
*	Zamawiający wymaga, aby Wykonawca spełnił wszystkie wymagania określone w danym punkcie oraz zrealizował pełen zakres usług. Zamawiający nie dopuszcza częściowej realizacji wymagań wskazanych w danym punkcie. Wymagania odnoszą się do rozdziału IV SOPZ		