…….
Nazwa i adres Wykonawcy

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego na zakup, dostawę, instalację oraz wdrożenie zintegrowanego systemu bezpieczeństwa teleinformatycznego dla Szpitala Wojewódzkiego im. Kardynała Stefana Wyszyńskiego w Łomży, znak sprawy: ZT-SZP-226/01/75/2022

OFERUJEMY:

L.p.	OPIS PARAMETRU		PARAMETR WYMAGANY	PARAMETR OFEROWANY
Urządzenie klasy UTM HA (2x UTM pracujące redundantnie w klastrze High Avalibity)				
1	Podać oferowane urządzenie klasy UTM w ilości 2szt., które zostanie użyte do stworzenia klastra HA (nazwa, model) wraz z niezbędnymi licencjami do uruchomienia systemu bezpieczeństwa teleinformatycznego		TAK, podać	
Wymagania Ogólne				
2	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i 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.		TAK	
3	Dostarczony system bezpieczeństwa musi być kompatybliny z posiadanymi przez Zamawiającego rozwiązaniami firmy Fortinet		TAK	
4	System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.		TAK	
5	W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych fizycznych 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	
6	System musi wspierać IPv4 oraz IPv6 w zakresie:		TAK	
7		Firewall.	TAK	
8		Ochrony w warstwie aplikacji.	TAK	
9		Protokołów routingu dynamicznego.	TAK	

10	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć oświadczenie lub 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, podać	
11	Rok produkcji - nie wcześniej niż 2021		TAK, podać	
12	Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż dostawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.		TAK, podać	
Redundancja, monitoring i wykrywanie awarii				
13	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	
14	System musi prowadzić monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.		TAK	
15	System musi prowadzić monitoring stanu realizowanych połączeń VPN.		TAK	
16	System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.		TAK	
Interfejsy, Dysk, Zasilanie				
17	System realizujący funkcję Firewall musi dysponować minimum:		TAK	
18		18 portami Gigabit Ethernet RJ-45.	TAK, podać	
19		16 gniazdami SFP 1 Gbps.	TAK, podać	
20	System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.		TAK, podać	
21	W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.		TAK, podać	
22	System musi być wyposażony w wbudowany układ zasilania AC.		TAK	
23	System musi umożliwiać doposażenie w dodatkowy (redundantny) wbudowany układ zasilania AC.		TAK	
Parametry wydajnościowe				
24	W zakresie Firewall'a obsługa nie mniej niż 4 milionów jednoczesnych połączeń oraz 450 tys. nowych połączeń na sekundę.		TAK	
25	Przepustowość Stateful Firewall: nie mniej niż 30 Gbps dla pakietów 512 B.		TAK, podać	
26	Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12 Gbps.		TAK, podać	
27	Wydajność szyfrowania IPSec VPN nie mniej niż 16 Gbps.		TAK, podać	
28	Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 7.5 Gbps.		TAK, podać	

29	Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 5 Gbps.		TAK, podać	
30	Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4.6 Gbps.		TAK, podać	
Funkcje Systemu Bezpieczeństwa				
31	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:		TAK	
32	Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.		TAK	
33	Kontrola Aplikacji.		TAK	
34	Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.		TAK	
35	Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.		TAK	
36	Ochrona przed atakami - Intrusion Prevention System.		TAK	
37	Kontrola stron WWW.		TAK	
38	Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.		TAK	
39	Zarządzanie pasmem (QoS, Traffic shaping).		TAK	
40	Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).		TAK	
41	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	
42	Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.		TAK	
43	Analiza ruchu szyfrowanego protokołem SSH.		TAK	
44	Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system		TAK	
Polityki, Firewall				
45	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.		TAK	
46	System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:		TAK	
47		Translację jeden do jeden oraz jeden do wielu.	TAK	
48		Dedykowany ALG (Application Level Gateway) dla protokołu SIP.	TAK	
49	W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.		TAK	
50	Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.		TAK	
51	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.		TAK	
52		Amazon Web Services (AWS).	TAK	
53		Microsoft Azure	TAK	
54		Google Cloud Platform (GCP).	TAK	
55		OpenStack.	TAK	
56		VMware NSX.	TAK	

Połączenia VPN				
57	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:		TAK	
58		Wsparcie dla IKE v1 oraz v2.	TAK	
59		Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).	TAK	
60		Obsługa protokołu Diffie-Hellman grup 19 i 20.	TAK	
61		Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.	TAK	
62		Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.	TAK	
63		Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.	TAK	
64		Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.	TAK	
65		Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.	TAK	
66		Mechanizm „Split tunneling" dla połączeń Client-to-Site.	TAK	
67	System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:		TAK	
68		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.	TAK	
69		Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.	TAK	
70		Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.	TAK	
Routing i obsługa łączy WAN				
71	W zakresie routingu rozwiązanie powinno zapewniać obsługę:		TAK	
72		Routingu statycznego.	TAK	
73		Policy Based Routingu.	TAK	
74		Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	TAK	
Funkcje SD-WAN				
75	System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.		TAK	
76	Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.		TAK	
Zarządzanie pasmem				
77	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.		TAK	
78	Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.		TAK	
79	System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.		TAK	
Ochrona przed malware				
80	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).		TAK	

81	System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.	TAK	
82	System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).	TAK	
83	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	
84	System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	TAK	
85	Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	TAK	
Ochrona przed atakami			
86	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.	TAK	
87	System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.	TAK	
88	Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	TAK	
89	Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.	TAK	
90	System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.	TAK	
91	System musi dysponować sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.	TAK	
92	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	
93	System powinien prowadzić wykrywanie i blokowanie komunikacji C&C do sieci botnet.	TAK	
Kontrola aplikacji			
94	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.	TAK	
95	Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	TAK	
96	Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.	TAK	
97	Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.	TAK	
98	Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	TAK	
Kontrola WWW			
99	Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.	TAK	

100	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	
101	Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.		TAK	
102	Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.		TAK	
103	Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.		TAK	
104	Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.		TAK	
105	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				
106	System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:		TAK	
107		Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.	TAK	
108		Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.	TAK	
109		Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.	TAK	
110	Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.		TAK	
111	Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.		TAK	
112	Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.		TAK	
Zarządzanie				
113	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	
114	Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.		TAK	
115	Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.		TAK	
116	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	
117	System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.		TAK	
118	Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.		TAK	

119	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				
120	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, komercyjnej platformy sprzętowej lub programowej.		TAK	
121	W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.		TAK	
122	Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.		TAK	
123	W przypadku kiedy usługa logowania, raportowania, korelacji zdarzeń realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.		TAK	
124	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	
125	Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.		TAK	
126	Musi istnieć możliwość logowania do serwera SYSLOG.		TAK	
Certyfikaty				
127	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:		TAK	
128		ICSA lub EAL4 dla funkcji Firewall.	TAK, podać	
Serwisy i licencje				
129	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:		TAK	
130		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, Sygnatury ochrony systemów przemysłowych SCADA na okres 12 miesięcy.	TAK	
Gwarancja oraz wsparcie				

131	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	
132	Wykonawca zapewni na czas wdrożenia przynajmniej jednego inżyniera posiadającego aktualny certyfikat ze znajomości oferowanego systemu/produktu wydany przez producenta zaoferowanego systemu/produktu		TAK, podać	
Oprogramowanie klasy SIEM				
133	Pełna nazwa oferowanego oprogramowania / systemu informatycznego klasy SIEM		TAK, podać	
134	Rozwiązanie SIEM musi zapewniać skalowalną architekturę spełniającą następujące wymagania:		TAK	
135		wszystkie elementy odpowiedzialne za zbieranie informacji, od tego miejsca określane jako Kolektory muszą być dostarczone w postaci maszyn wirtualnych	TAK	
136		producent wybranego rozwiązania musi udostępniać Kolektory w formie zarówno maszyn wirtualnych, jak i dedykowanych rozwiązań sprzętowych.	TAK, podać	
137		zadaniem kolektorów jest przesyłanie monitorowanych danych (np. zdarzeń) do warstwy je przechowującej i korelującej	TAK	
138		w wypadku awarii komunikacji pomiędzy warstwą przechowującą i korelującą a kolektorami muszą one mieć możliwość buforowania otrzymanych informacji	TAK	
139		system SIEM powinien mieć możliwość definiowania rozmiaru bufora dla zdarzeń otrzymywanych przez kolektor oraz monitorowania jego zajętości	TAK	
140		kolektory muszą mieć możliwość ograniczenia ilości zdarzeń przesyłanych do klastra SIEM	TAK	
141		kolektory muszą mieć możliwość kompresowania danych przesyłanych do warstwy przechowującej i korelującej	TAK	
142		kolektory muszą mieć możliwość ograniczania przepustowości, z którą zdarzenia są przesyłane do warstwy przechowującej i korelującej	TAK	
143		komunikacja pomiędzy warstwą przechowującą i korelującą musi odbywać się z wykorzystaniem szyfrowanego protokołu HTTPS. Musi odbywać się ona w kierunku od kolektorów do warstwy przechowującej i korelującej dla przesyłanych zdarzeń	TAK	
144		w wypadku awarii kolektora, kolektor zastępczy może być uruchomiony poprzez jego zarejestrowanie w warstwie przechowującej i korelującej. Konfiguracja (zarządzanie) kolektorów nie odbywa się indywidualnie, lecz są one centralnie zarządzane. Nie mogą one posiadać żadnych parametrów konfiguracyjnych poza adresami IP, nazwą kolektora oraz wymaganymi poświadczeniami, które byłyby wymagane w celu uruchomienia kolektora zastępczego	TAK	
145		wydajność kolektora nie może być mniejsza niż 5 000 EPS (zdarzeń na sekundę odbieranych w trybie ciągłym)	TAK	

146		kolektory muszą być w stanie przetwarzać informacje otrzymywane z wykorzystaniem protokołu NetFlow	TAK	
147		poszczególne kolektory muszą być w stanie automatycznie aktualizować nowe parsery wtedy, gdy zostaną one zaktualizowane w centralnym systemie zarządzającym rozwiązaniem SIEM	TAK	
148		kolektory mają mieć możliwość aktualizacji wersji swojego oprogramowania z warstwy zarządzającej	TAK	
149		rozwiązanie SIEM ma posiadać możliwość aktualizacji online dla parserów, reguł, raportów oraz typów wspieranych urządzeń. Aktualizacja ta musi być niezależna od oprogramowania systemowego (OS, funkcje wykonawcze, etc.) które ma posiadać swoje wersjonowanie. Zmiany dokonane w kolejnych wersjach powinny być ewidencjonowane w oficjalnej dokumentacji	TAK	
150		rozwiązanie ma posiadać możliwość zarządzania wieloma instancjami SIEM przy pomocy dedykowanej konsoli zarządzającej pochodzącej od tego samego producenta. Funkcjonalność ta może wymagać dodatkowej licencji	TAK	
151	Warstwa przechowywania i korelacji danych, od tego miejsca określana jako klaster SIEM, ma spełniać następujące wymagania:		TAK	
152		klaster SIEM musi być dostarczony w postaci maszyn wirtualnych	TAK	
153		producent wybranego rozwiązania musi udostępniać Klaster SIEM w formie zarówno maszyn wirtualnych, jak i dedykowanych rozwiązań sprzętowych.	TAK	
154		w przypadku przechowywania danych na dysku lokalnym lub udziale NFS ma być możliwe stworzenie architektury redundantnej w której podstawowa instalacja rozwiązania SIEM podczas regularnej pracy wykonuje wszystkie operacje produkcyjne, zaś instalacja backupowa synchronizuje wszystkie dane i w razie awarii jest w stanie przejąć funkcjonowanie środowiska SIEM	TAK	
155		rozwiązanie ma wspierać nie mniej niż poniżej wymienione środowiska wirtualizacyjne:	TAK	
156		a) VMware	TAK	
157		b) Hyper-V	TAK	
158		c) KVM	TAK	
159		d) AWS	TAK	
160		e) Azure	TAK	
161		klaster SIEM musi mieć możliwość skalowania się poprzez dodawanie kolejnych maszyn wirtualnych (Virtual Appliance - VA). Wspomniana skalowalność ma być realizowana również poprzez:	TAK	
162		a) przeprowadzaną w czasie rzeczywistym, w pamięci rozwiązania, dystrybuowaną pomiędzy elementy klastra korelację reguł	TAK	
163		b) dystrybuowanie pomiędzy elementami klastra SIEM raportowania oraz analizy danych. Sam mechanizm dystrybucji musi być całkowicie przeźroczysty z perspektywy użytkownika, tak aby nie musiał on decydować który z elementów ma być odpowiedzialny za wykonanie poszczególnych zadań	TAK	

164		klaster SIEM nie może posiadać ograniczeń licencyjnych związanych z ilością lub rozmiarem przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie (dotyczącym przechowywanych danych) może być rozmiar przestrzeni dyskowej	TAK	
165		klaster SIEM nie może posiadać ograniczeń licencyjnych związanych z rozmiarem gromadzonych danych w jednostce czasu. Przykładowo nie może być limitowana licencyjnie ilość bajtów danych w jednostce czasu (KB, GB, etc.)	TAK	
166		dane zbieranych zdarzeń (events) mogą być gromadzone na dyskach maszyn wirtualnych lub udziale NFS podczas działania w oparciu o pojedynczą maszynę wirtualną lub też z możliwością wykorzystania NFS w sytuacji pracy w trybie klastra SIEM (wiele maszyn wirtualnych - VA).	TAK	
167		klaster SIEM musi mieć możliwość obsłużenia (potencjalną możliwość docelowego wyskalowania do) nie mniej niż 500 tysięcy EPS	TAK	
168		klaster SIEM musi mieć możliwość składowania zbieranych danych zarówno w formie surowej (raw event log) jak i w formie sparsowanych danych (parsed event log)/danych znormalizowanych	TAK	
169		rozwiązanie SIEM nie może wymagać zastosowania dodatkowej przestrzeni dyskowej i/lub warstwy służącej do filtrowania lub wysyłania podzbiorów danych przesyłanych od kolektorów do warstwy korelującej w przypadku korzystania z dysków lokalnych lub udziału NFS	TAK	
170		zebrane dane muszą być przechowywane w sposób skompresowany	TAK	
171		system musi mieć możliwość anonimizacji zebranych danych w zakresie nie mniejszym niż: adresy IP, nazwy hostów, adresy email, nazwy użytkowników. Proces ten ma być możliwy w oparciu o role/profile użytkowników administracyjnych. Ujawnienie danych (deanonimizacja) ma się odbywać z wykorzystaniem użytkownika udzielającego lub zabraniającego jej wykonania. W przypadku zatwierdzenia wspomnianego żądania, dane są ujawniane na określony czas, po którym powtórnie ulegają anonimizacji	TAK	
172		klaster SIEM nie może wykorzystywać klasycznej relacyjnej bazy danych (w tym, choć nie tylko: MS SQL, Postgresql, MySQL, Oracle, itp.) celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami. Rozwiązanie musi wykorzystywać w tym celu nowoczesną bazę taką jak na przykład noSQL lub OLAP. Musi być możliwy wybór zastosowanej bazy danych do przechowywania zbieranych zdarzeń z pośród przynajmniej trzech różnych technologii z czego co najmniej jedna pochodzi od tego samego producenta	TAK	
173		w przypadku stosowania struktury OLAP możliwe powinno być obsłużenie warstwy zarządzania zapisem danych oraz ich przechowywania i wyszukiwania na jednej, dwóch lub trzech dedykowanych warstwach maszyn fizycznych bądź wirtualnych klastra SIEM. Dopuszczalne są następujące scenariusze:	TAK	

174		a) wszystkie warstwy działają w ramach jednej maszyny	TAK	
175		b) dedykowane maszyny do pracy jako warstwa zarządzania zapisem danych oraz dedykowane maszyny do zapisu i wyszukiwania danych	TAK	
176		c) dedykowane maszyny do pracy jako warstwa zarządzania zapisem danych, dedykowane maszyny do pracy jako warstwa zapisu danych oraz dedykowane maszyny do wyszukiwania danych	TAK	
177		Musi istnieć możliwość konfiguracji warstwy zarządzania jako klastra złożonego z większej liczby instancji, nie mniejszej niż 3, zabezpieczającego przed awarią tej funkcji.	TAK	
178		Musi istnieć możliwość zbudowania większej ilości replik danych, aby zapewnić niezawodność przechowywania.	TAK	
179		Musi istnieć możliwość zbudowania struktury rozproszonej, aby zapewnić większą wydajność zapisu i wyszukiwania.	TAK	
180		Klasyczne relacyjne bazy danych mogą być wykorzystywane jedynie do przechowywania szablonów, zdarzeń i innych ustrukturyzowanych informacji	TAK	
181		Maszyny wirtualne systemu SIEM mają działać w oparciu o system Linux który ma mieć możliwość aktualizacji. Aktualizacje zarówno rozwiązania SIEM jak i bazowego systemu operacyjnego muszą być dostarczane przez producenta rozwiązania w wygodnej formie pliku aktualizacyjnego	TAK	
182	System SIEM musi zapewniać wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI		TAK	
183	System SIEM musi być w stanie wykryć usługi Active Directory oraz LDAP oraz wyświetlać informacje o strukturze katalogowej drzewa w GUI		TAK	
184	Musi istnieć możliwość wykorzystania struktury katalogowej drzewa LDAP jako warunku podczas tworzenia raportów i w ramach pozostałych mechanizmów analitycznych		TAK	
185	Muszą być wspierane zewnętrzne metody uwierzytelniania użytkowników SIEM, nie mniej niż:		TAK	
186		a) Active Directory lub LDAP	TAK	
187		b) RADIUS	TAK	
188		c) SAML	TAK	
189	Musi istnieć integracja z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds - TI):		TAK	
190		wsparcie dla plików CSV musi być wykonywalne z wykorzystaniem interfejsu graficznego GUI	TAK	
191		definicje w ramach integracji muszą zawierać nie mniej niż:	TAK	
192		a) adresy IP	TAK	
193		b) domeny	TAK	
194		c) sumy kontrolne (hash)	TAK	
195		d) adresy URL	TAK	
196		wymagane jest, aby każda z zewnętrznych baz zagrożeń była w stanie wesprzeć do 200 tysięcy wpisów	TAK	

197		system SIEM musi być przygotowany na umożliwienie wykorzystania zestawu komercyjnych baz zagrożeń pochodzących od tego samego producenta. Producent musi mieć własny zespół analityczny, tworzący wspomniane bazy	TAK	
198		wraz z systemem SIEM musi być wspierany, już zintegrowany, zestaw baz zagrożeń niekomercyjnych (open source)	TAK	
199		system SIEM musi mieć możliwość korelacji informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym. Korelacja ta ma odbywać się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data)	TAK	
200		system SIEM musi mieć możliwość korelacji informacji z baz zagrożeń z danymi historycznymi	TAK	
201		system musi mieć możliwość odpytywania (ręcznego lub automatycznego) zewnętrznych źródeł reputacji takich jak np.VirusTotal, w tym również pochodzących od producenta samego systemu SIEM	TAK	
202		system musi mieć możliwość wizualizacji informacji w oparciu o kategorie MITRE ATT&CK w oparciu o wbudowane reguły, których ilość w tym kontekście ma wynosić nie mniej niż 900	TAK	
203	System SIEM musi mieć możliwość analizowania i odpytywania o zdarzenia w widoku analitycznym w trybie strumieniowym (streaming mode), w taki sposób, że raport docelowy dotyczący analizowanych zdarzeń wykonywany jest przed ich zapisaniem na dysk twardy		TAK	
204	Rozwiązanie SIEM musi dostarczać bez dodatkowych opłat następujące rodzaje raportów:		TAK	
205		a) PCI-DSS	TAK	
206		b) HIPAA	TAK	
207		c) SOX	TAK	
208		d) NERC	TAK	
209		e) FISMA	TAK	
210		f) ISO	TAK	
211		g) GLBA	TAK	
212		h) GPG13	TAK	
213		i) SANS Critical Controls	TAK	
214	System SIEM musi pozwalać na eksportowanie i importowanie pulpitów administracyjnych (dashboards), raportów oraz reguł w formacie XML		TAK	
215	System SIEM musi pozwalać na zbieranie konfiguracji urządzeń, identyfikowanie zmian w nich następujących wraz z możliwością porównywania poszczególnych wersji obok siebie w interfejsie GUI. zmian konfiguracji na NGFW przez operatora SIEM poprzez wyświetlenie konfiguracji tekstowej nowej i wybranej wcześniejszej wersji jednocześnie. Zmiany muszą być zaznaczone wyraźnie np. kolorem (dodano, usunięto, zmieniono).		TAK	
216	Pulpity administracyjne (dashboards) muszą mieć możliwość wspólnej prezentacji		TAK	
217	Dane w ramach pulpitów administracyjnych muszą pozwalać na następujące formy prezentacji:		TAK	
218		a) Bar	TAK	
219		b) Pie	TAK	
220		c) Line	TAK	
221		d) Table	TAK	

222		e) Combination (line and table view)	TAK	
223		f) Treemap	TAK	
224		g) Scatter graph	TAK	
225		h) Single values	TAK	
226		i) Gauges	TAK	
227		j) Geographical Map	TAK	
228		k) wartości graniczne (thresholds) w kolorach czerwonym, burszytnowym oraz zielonym mogą być definiowane w razie potrzeby na poszczególnych wykresac	TAK	
229	Rozwiązanie SIEM musi dostarczać zunifikowane narzędzia analityczne dzięki którym możliwe jest wykonywanie zapytań w oparciu o ten sam język zarówno dla logów/zdarzeń zbieranych z urządzeń jak i dla danych wydajnościowych		TAK	
230	Wymagane jest, aby kolektory systemu SIEM pozwalały na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne. Mechanizm ten nie może mieć żadnego wpływu na model licencjonowania		TAK	
231	Zarówno dane w stanie surowym jak i te sparsowane lub wzbogacone muszą być możliwe do przesłania do rozwiązania SIEM z kolektorów		TAK	
232	Przetwarzanie danych związanych z poszczególnymi zdarzeniami (events) wykonywane jest poprzez parsery systemowe		TAK	
233	Musi istnieć możliwość samodzielnej modyfikacji i poprawiania wszystkich parserów		TAK	
234	Tworzenie wlasnych parserów musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)		TAK	
235	Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) musi być w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI)		TAK	
236	Parsery mają być tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework) i jednocześnie zapewniać następujące właściwości:		TAK	
237		zdolność do definiowania wzorców które powtarzają się jako zmienne	TAK	
238		zdolność do definiowania funkcji pozwalających na identyfikację par wartości kluczowych	TAK	
239		zdolność do testowania poszczególnych funkcji	TAK	
240		zdolność do przekształcania danych w trakcie ich parsowania	TAK	
241	System SIEM musi pozwalać na przesłanie dowolnych zebranych zdarzeń z wykorzystaniem protokołu KAFKA		TAK	
242	Dla danych przechowywanych na dysku lokalnym lub udziale NFS system SIEM musi pozwalać na realizowane w oparciu o polityki archiwizowanie danych do innego udziału, takiego jak np. NFS		TAK	
243	Integralność danych zapisywanych na dysku lokalnym lub udziale NFS związanych ze zdarzeniami musi być weryfikowalna z wykorzystaniem GUI w oparciu o przeliczenie sum kontrolnych, które obliczane były w momencie zapisywania danych o zdarzeniach na dysk systemu SIEM		TAK	
244	System musi mieć możliwość uruchomienia w trybie zgodności z FIPS		TAK	
SIEM - zbieranie danych				
245	Rozwiązanie SIEM musi mieć możliwość zbierania danych z monitorowanych urządzeń, również innych niż logi, co ma być osiągalne poprzez nie mniej niż:		TAK	

246	A) aktywne wykrywanie urządzeń wewnątrz sieci bez wykorzystania dodatkowego oprogramowania typu agent oraz wsparcie dla takich metod pobierania zdarzeń jak:		TAK	
247		a) SNMP	TAK	
248		b) Syslog	TAK	
249		c) Windows Management Instrumentation (WMI) i Open Management Infrastructure (OMI)	TAK	
250		d) Microsoft RPC	TAK	
251		e) Cisco SDEE	TAK	
252		f) Checkpoint LEA	TAK	
253		g) JDBC	TAK	
254		h) VM SDK	TAK	
255		i) JMX	TAK	
256		j) Telnet	TAK	
257		k) SSH	TAK	
258		l) NetFlow	TAK	
259		m) HTTPS	TAK	
260		n) IMAP	TAK	
261		o) IMAP over SSL	TAK	
262		p) POP3	TAK	
263		r) Kafka API	TAK	
264		s) import z pliku CSV	TAK	
265		t) import z pliku PCAP	TAK	
266		u) REST API	TAK	
267	B) zdolność do monitorowania statusu oraz dostępności usług takich jak: DNS, FTP, TCP, UDP, ICMP, JDBC, LDAP, SMTP, IMAP, POP3, POP3S, SSH, HTTP, HTTPS		TAK	
268		wyniki powyższego monitoringu mają dawać możliwość obliczenia poziomu dostępności danej usługi (np. procentowego)	TAK	
269	C) wykryte urządzenie ma posiadać swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB) w ramach dostarczonego rozwiązania SIEM co jednocześnie ma umożliwiać prezentację następujących informacji (nie mniej niż):		TAK	
270		wersja oprogramowania/firmware/systemu operacyjnego	TAK	
271		numer seryjny urządzenia	TAK	
272		skonfigurowane interfejsy wraz z:	TAK	
273		a) nazwą interfejsu	TAK	
274		b) adresem IP oraz podsiecią	TAK	
275		c) statusem interfejsu (włączony, wyłączony)	TAK	
276		d) informacją o skonfigurowanym poziomie bezpieczeństwa	TAK	
277		e) prędkością interfejsu	TAK	
278		f) możliwością edycji nazwy oraz prędkości interfejsu	TAK	
279		procesach działających na urządzeniu lub systemie operacyjnym	TAK	
280		alarmach w przypadku zmiany statusu procesu np. jego uruchomienia lub zatrzymania	TAK	
281	D) możliwość automatycznego przypisania do grupy poszczególnych typów urządzeń znajdujących się w CMDB, np. grupa serwerów Windows, grupa rozwiązań firewall, etc.		TAK	

282	E) automatyczne wykrywanie aplikacji działających na poszczególnych urządzeniach. Wymagane jest aby baza urządzeń (CMDB) miała możliwość konfiguracji grup aplikacji celem automatycznego umieszczania w nich poszczególnych urządzeń, np. grupa aplikacyjna "IIS Servers" wyświetla wszystkie urządzenia z uruchomionymi usługami Microsoft IIS. Grupy typów urządzeń jak i grupy aplikacyjne muszą być dostępne do raportowania, analityki korelacyjnej oraz wyszukiwania informacji (zdarzeń, przepływów, wydajności, itp.)		TAK	
283	F) wymagane jest, aby rozwiązanie SIEM posiadało wbudowany szablon (template), który po przeprowadzeniu aktywnego wykrywania urządzeń będzie pozwalał na automatyczne określenie jakiego rodzaju dane będą z nich zbierane oraz jaki będzie interwał ich pobierania		TAK	
284	G) Monitorowanie metryk wydajnościowych ma dotyczyć nie mniej niż:		TAK	
285		a) utylizacji interfejsów sieciowych, występujących tam błędów, ilości wysłanych i odebranych danych (np. bajtów)	TAK	
286		b) obciążenia CPU	TAK	
287		c) wykorzystania pamięci	TAK	
288		d) wykorzystania przestrzeni dyskowej	TAK	
289		e) utylizacji poszczególnych procesów	TAK	
290	H) pobieranie informacji o zdarzeniach w oparciu o udostępniany przez monitorowane systemy mechanizm API		TAK	
SIEM - współpraca z aplikacjami typu agent				
291	Musi istnieć możliwość monitorowania urządzeń bez wykorzystania aplikacji typu agent oraz poprzez SSH, telnet, WMI, OMI, JMX oraz PowerShell		TAK, podać	
292	Rozwiązanie SIEM musi mieć możliwość zbierania zdarzeń (event) z systemów Windows oraz Linux w oparciu o aplikacje typu agent		TAK	
293	Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:		TAK	
294		centralne zarządzanie i możliwość aktualizacji z głównej konsoli systemu SIEM	TAK	
295		możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows	TAK	
296		możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application	TAK	
297		zdolność do monitorowania integralności plików	TAK	
298		zdolność do monitorowania rejestru systemowego	TAK	
299		zdolność do monitorowania urządzeń zewnętrznych (removable devices)	TAK	
300		zdolność do wykonywania poleceń PowerShell wraz z odsyłaniem wyniku ich działania w postaci logów	TAK	
301		zdolność do wykonywania poleceń WMI wraz z odsyłaniem wyniku ich działania w postaci logów	TAK	
302		agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS	TAK	
303		musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu	TAK	

304		agent Windows musi mieć możliwość buforowania zbieranych zdarzeń w wypadku utraty komunikacji z pozostałymi elementami klastra SIEM	TAK	
305		musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS	TAK	
306	Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Linux (Linux Agent), które posiadają nie mniej niż następujące możliwości:		TAK	
307		centralne zarządzanie i możliwość aktualizacji z głównej konsoli systemu SIEM	TAK	
308		możliwość zbierania logów z wykorzystaniem protokołu syslog	TAK	
309		możliwość zbierania logów z plików tekstowych	TAK	
310		zdolność do monitorowania integralności plików	TAK	
311		zdolność do monitorowania pliku w oparciu o jego sumę kontrolną	TAK	
312		musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu	TAK	
313	System SIEM musi mieć możliwość realizacji funkcjonalności UEBA (User EntityBehaviour Analysis) w oparciu o dedykowanego Agenta na systemy Windows oraz w oparciu o logi z systemu Windows. Metadane lub logi dotyczące funkcji UEBA nie mogą podlegać licencjonowaniu ze względu na EPS lub rozmiar		TAK	
SIEM - notyfikacje oraz zarządzanie incydentami				
314	System SIEM musi:			
315		posiadać narzędzia pozwalające na samodzielne tworzenie polityk informujących o incydentach	TAK	
316		pozwalać na nadawanie etykiet (tagów) poszczególnym incydentom oraz powinno pozwalać na wyszukiwanie w oparciu o nie	TAK	
317		posiadać możliwość uruchamiania skryptów w odpowiedzi na wybrane incydenty	TAK	
318		możliwość uruchamiania skryptów w odpowiedzi na wybrane incydenty musi być możliwa w oparciu o role z podziałem na użytkowników mających pełne prawa do uruchamiania skryptów i na użytkowników zgłaszających żądanie uruchomienia skryptu, które to żądanie musi być zatwierdzone przez użytkownika nadrzędnego	TAK	
319		posiadać możliwość integracji w oparciu o API z zewnętrznymi systemami do obsługi zgłoszeń (ticketingsystems) takimi jak ServiceNow, ConnectWise oraz Remedy	TAK	
320		mieć możliwość integracji z innymi systemami do obsługi zgłoszeń poprzez API (ticketing system)	TAK	
321		mieć wbudowany mechanizm obsługi zgłoszeń (ticketing system) niezależny od obsługi alarmów/incydentów	TAK	
SIEM - analityka				
322	System SIEM musi mieć możliwość:			
323	wyszukiwania zdarzeń (events) w czasie rzeczywistym bez konieczności indeksowania oraz używania wyrażeń logicznych takich jak AND, OR, NOT czy też cudzysłowów		TAK	

324	zagnieżdżania wyników wyszukiwań w oparciu o operatory IN oraz NOT IN		TAK	
325	wyszukiwania w oparciu o słowa kluczowe oraz w oparciu o sparsowane atrybuty zdarzeń względem analizowanych danych		TAK	
326	wyszukiwania historycznego z zastosowaniem kwerend zagnieżdżonych, ze wsparciem dla filtrowania typu Boolean, grupowaniem w oparciu o agregację danych, filtry czasowe, wyrażenia regularne, wyrażenia matematyczne.		TAK	
327	wyszukiwania w oparciu o zapytania wstępne uruchamiane zgodnie harmonogramem		TAK	
328	wyszukiwania w oparciu o niemniej niż następujące operatory: include =,!=, <,>, IS NULL, IS NOT NULL, contains, not contains, contains regex, not contains regex		TAK	
329	podejmowania w czasie rzeczywistym działań w oparciu o złożone wzorce zdarzeń		TAK	
330		w przypadku prostych zapytań musi na przykład być możliwe określenie wartości progowej (threshold) ilości zdarzeń X w określonym przedziale czasowym Y z Z wybranych wartości	TAK	
331		w przypadku zapytań przekrojowych wspierających filtry typu Boolean musi być możliwe:	TAK	
332		a) stworzenie wzorców zapytań za określony przedział czasu z wykorzystaniem operatorów takich jak: AND, OR, FOLLOWED BY, AND NOT, and NOT FOLLOWED_BY	TAK	
333		b) każdy z wzorców może być filtrowany i agregowany z wykorzystaniem operatorów takich jak: AVG, MAX, MIN, COUNT and COUNT DISTINCT	TAK	
334		c) ustalane wartości graniczne (thresholds) mogą być statyczne lub też mogą być otrzymywane jako rezultat analizy statystycznej	TAK	
335		1) analiza statystyczna i alarmowanie w oparciu o zdarzenia musi mieć możliwość działania w oparciu o:	TAK	
336		i. średnie kroczące (movingaverages)	TAK	
337		ii. odchylenia standardowe (standard deviations)	TAK	
338		2) w wypadku przekroczenia statystycznej wartości granicznej (statisticalthreshold) musi zostać wygenerowany alert w czasie zbliżonym do rzeczywistego	TAK	
339	wykorzystywania obiektów wykrytych i znajdujących się bazie urządzeń (CMDB), użytkowników i ich tożsamości oraz lokalizacji podczas wyszukiwania i tworzenia reguł		TAK	
340	tworzenia harmonogramu raportów i dostarczania ich pocztą elektroniczną		TAK	
341	możliwości eksportowania raportów do formatów CSV, PDF i RTF		TAK	
342	wyszukiwania zdarzeń poprzez pryzmat całej organizacji lub też w ujęciu fizycznego lub logicznego obszaru raportującego		TAK	
343	wykorzystania dynamicznych list pozwalających na obserwację źródeł generujących zdarzenia krytyczne, wraz z możliwością wykorzystania tychże list w dowolnej regule raportującej		TAK	
344	skalowania możliwości analitycznych poprzez dodawanie do systemu SIEM kolejnych maszyn wirtualnych bez konieczności wyłączania całego klastra SIEM		TAK	

345	automatycznego korelowania użytkownika z jego lokalizacją i adresem IP:		TAK	
346		musi istnieć możliwość tworzenia raportów i wyszukiwania użytkownika w połączeniu z jego adresem IP oraz lokalizacją. Lokalizacja może oznaczać port na przełączniku sieciowym, adres MAC lub połączenie VPN	TAK	
347		musi istnieć możliwość wzbogacania zdarzeń (events) przy których dane użytkownika pozbawione są informacji o adresie IP	TAK	
348		wykorzystanie funkcjonalności lokalizacji adresu IP (Geo IP) w oparciu o bazę pochodzącą od tego samego producenta	TAK	
349	możliwość wykrywania zdarzeń IPS falsepositive w oparciu o integrację z zewnętrznymi skanerami podatności		TAK	
SIEM - dodatkowe wymagania				
350	Oferowany system musi znajdować się w raportach Gartnera co najmniej od 2018 roku		TAK	
351	Dla systemu SIEM muszą być dostępne certyfikowane szkolenia w tym poprzez portal producenta		TAK	
352	Oprogramowanie musi być dostarczone w modelu licencji wieczystej		TAK	
353	System musi posiadać wsparcie producenta wraz z możliwością zakładania zgłoszeń serwisowych na portalu producenta, w tym dostępność do aktualnych wersji systemu na okres minimum 12 miesięcy.		TAK	
354	System musi pozwalać na obsługę/monitorowanie minimum 50 urządzeń		TAK, podać	
355	Wydajność systemu powinna pozwolić na obsługę nie mniej niż 1000 EPS (ilość zdarzeń na sekundę, obsugiwaną przez jedną licencję).		TAK, podać	
356	Model licencjonowania musi umożliwiać zwiększanie ilości urządzeń i EPS poprzez zakup dodatkowych rozszerzeń.		TAK	
357	Wraz z systemem SIEM musi być dostarczony, już zintegrowany, zestaw komercyjnych baz zagrożeń pochodzących od tego samego producenta. Producent musi mieć własny zespół analityczny, tworzący wspomniane bazy		TAK	
358	Wykonawca zapewni na czas wdrożenia przynajmniej jednego inżyniera posiadającego aktualny certyfikat ze znajomości oferowanego systemu/produktu wydany przez producenta zaoferowanego oprogramowania		TAK, podać	
Oprogramowanie klasy EDR				
359	Pełna nazwa oferowanego oprogramowania / systemu informatycznego klasy EDR		TAK, podać	
360	System ochrony i reagowania na zaawansowane zagrożenia dla urządzeń końcowych musi zapewniać kompleksową ochronę przed malware, zaawansowanymi atakami wykorzystującymi techniki opisane w modelu MITRE™ ATT&CK, ataki typu „fileless" – bez użycia plików, ataki z wykorzystaniem oprogramowania dostępnego w ramach systemu operacyjnego lub w znanych aplikacjach tzw. „LOLBAS". System musi potrafić zarówno wykrywać zagrożenia na poszczególnych etapach infekcji jak i mieć możliwość granularnego reagowania na wykryte incydenty zależnie od poziomu klasyfikacji danego zagrożenia.		TAK	
EDR - wsparcie dla systemów operacyjnych				
361	System musi wspierać ochronę następujących systemów operacyjnych (agentów działających na poniższych systemach operacyjnych):		TAK	
362		Systemy Windows 8.x/10/Server 2016/Server 2019/Server 2022	TAK	
363		Systemów „legacy" (Windows 7, Windows XP, Windows Server 2003)	TAK	
364		Systemy Apple MacOS	TAK	

365		Systemy Linux – minimum Redhat, Ubuntu, Oracle, SUSE	TAK	
EDR - zarządzanie instalacją i aktualizacją agentów				
366	Możliwość instalacji agenta poprzez SCCM, JAMF i RHEL Satellite		TAK	
367	Możliwość aktualizacji/zmiany wersji agenta z poziomu konsoli zarządzania bez udziału użytkownika hosta końcowego		TAK	
368	System musi dostarczać możliwość kreowania instalatorów zawierających parametry umożliwiające podłączenie się danego agenta do określonej grupy hostów oraz danej instancji systemu zarządzającego		TAK	
369	Podłączanie się do systemu zarządzającego musi wymagać podania hasła w postaci parametru – bez podania poprawnego hasła nie może być możliwości podłączenia się do systemu zarządzania		TAK	
EDR - wpływ agentów na zasoby urządzenia końcowego				
370	Poziom zużycia pamięci RAM dla procesów agenta musi wynosić średnio poniżej 200MB		TAK	
371	Poziom średni zużycia procesora (CPU) dla procesów agenta musi wynosić mniej niż 2%		TAK	
372	Instalator oprogramowania nie może zajmować więcej niż 100MB		TAK	
EDR - wykrywanie zagrożeń				
373	System musi umożliwiać wykrywanie podejrzanych aktywności dla działających, uruchamianych i zatrzymywanych procesów oraz w ramach interakcji pomiędzy procesami.		TAK	
374	System musi umożliwiać analizę i odzwierciedlanie informacji o parametrach z jakimi został wykonany dany proces (np. parametry z linii poleceń)		TAK	
375	System musi umożliwiać wykrywanie złośliwych zmian w rejestrach co najmniej w kontekście śledzonego wykonania danego procesu		TAK	
376	System musi umożliwiać wykrywanie żądań DNS wysyłanych z chronionej stacji		TAK	
377	System musi umożliwiać wykrywanie podejrzanej aktywności związanej z używaniem dynamicznie ładowanych bibliotek DLL		TAK	
378	System musi potrafić identyfikować podejrzane zachowanie użytkownika jak i samej stacji końcowej		TAK	
379	System musi posiadać zintegrowane informacje na temat zagrożeń bezpieczeństwa (tzw. Threat Intelligence) pozwalające na dokładniejszą analizę zagrożenia		TAK	
380	System musi umożliwiać agentowi działającemu na końcówce wykrywanie i reagowanie na zagrożenia w przypadku odłączenia od sieci (offline)		TAK	
381	System musi wykrywać zagrożenia korzystając z silnika NGAV (Next-Generation Antivirus)		TAK	
382	System musi umożliwiać dodawanie wykluczeń ze skanowania przez silnik NGAV (Next-Generation Antivirus)		TAK	
EDR - prewencja				
383	System musi umożliwiać wykrywać i kategoryzować urządzenia IoT w bezpośrednim sąsiedztwie sieciowym danego agenta		TAK	
384	System musi umożliwiać blokowanie uruchamiania złośliwych plików wykonywalnych i bibliotek DLL		TAK	
385	System musi umożliwiać zablokowanie połączeń sieciowych zewnętrznych jak i wewnętrznych wykonywanych przez złośliwe oprogramowanie		TAK	
386	System musi umożliwiać blokowanie manipulacji plikami przez złośliwe oprogramowanie: tworzenie, edycję, usuwanie		TAK	
387	System musi umożliwiać blokowanie wykonywania się złośliwych plików wykonywalnych i bibliotek DLL		TAK	

388	System musi umożliwiać zastosowywanie list zezwalających dla danych:		TAK	
389		Hash (funkcji skrótu) plików w formatach MD5, SHA1, SHA256	TAK	
390		Nazw plików	TAK	
391		Ścieżek plików - z możliwością używania * (wildcard) na początku, w środku oraz na końcu nazwy folderu	TAK	
392		Aplikacji z uwzględnieniem nazwy, wersji i producenta	TAK	
393		Dla konkretnego certyfikatu, którym podpisane są pliki	TAK	
394	System musi umożliwiać zastosowywanie list blokujących dla danych:		TAK	
395		Hash (funkcji skrótu) plików w formatach MD5, SHA1, SHA2	TAK	
396		Nazw plików	TAK	
397		Ścieżek plików - z możliwością używania * (wildcard) na początku, w środku oraz na końcu nazwy folderu	TAK	
398		Dla konkretnego certyfikatu, którym podpisane są pliki	TAK	
399	System musi umożliwiać blokowanie połączeń do znanych złośliwych stron internetowych, domen lub adresów IP. Lista ta musi być automatycznie akutalizowana przez producenta rozwiązania		TAK	
EDR - analiza historyczna zagrożeń				
400	Dane do analizy muszą pochodzić bezpośrednio z urządzeń końcowych		TAK	
401	Dane historyczne metadanych zebranych z urządzeń muszą być dostępne do analizy z okresu minimum 1 miesiąca		TAK, podać	
402	System musi umożliwiać wyszukiwanie oznak ataków w zebranych informacjach. Wyszukiwanie musi być możliwe w oparciu o wszystkie zebrane informacje ze stacji końcowej oraz zidentyfikowane taktyki i techniki MITRE		TAK	
403	Wyszukiwanie musi umożliwiać budowanie zaawansowanych zapytań z wykorzystaniem logicznych operatorów typu AND, OR, NOT, ISTNIEJE, znaków wildcard, zakresów liczb (np. adresów od 10.0.0.100 do 10.0.0.200)		TAK	
404	System musi w oparciu o zebrane dane samodzielnie (wykorzystując AI lub równoważne rozwiązanie) identyfikować zachowania wg nomenklatury MITRE. Zachowanie musi być również elementem w oparciu o który można wykonywać zapytania do zebranych informacji		TAK	
405	Musi istnieć możliwość zapisania utworzonych zapytań wraz z możliwością ich automatycznego uruchamiania wg określonego harmonogramu z częstotliwością minimalną 15 minut		TAK	
406	System musi umożliwiać tworzenie profili, które opisują jakie informacje z urządzenia końcowego będą zbierane		TAK	
407	Musi istnieć możliwość tworzenie różnych profili i przypisywać je do różnych grup komputerów		TAK	

408	Zbierane informacje muszą zawierać minimalnie informacje o inwentaryzacji plików, szczegółowe operacje na plikach (utworzenie, zapis, odczyt, zmiana nazwy, skasowanie, ustawienie czasu, bezpośredni dostęp do woluminu, bezpośredni zapis do woluminu), informacje o procesach (utworzenie, uruchomienie, zatrzymanie, utworzenie wątków, załadowanie sterownika, załadowanie biblioteki), informacje o połączeniach sieciowych (zapytania http, zapytań DNS, zaakceptowania połączenia, nasłuchiwania na połączenie, zamknięcia połączenia), zdarzeń systemowych, szczegółowe operacje na rejestrze systemu (utworzenie, skasowanie, zmiany nazwy klucza rejestru; wpisanie, odczytanie, skasowanie wartości rejestru)		TAK	
409	Z poziomu znalezionych informacji musi istnieć możliwość wykonywania akcji, np. dla znalezionego pliku, możliwość jego ściągnięcia przez operatora, usunięcia, dodania do czarnej listy		TAK	
EDR - zarządzanie fałszywymi alarmami (False Positives)				
410	System musi umożliwiać ręczne zarządzanie fałszywymi alarmami poprzez możliwość oznaczania źle sklasyfikowanej aktywności, celem poprawnego wykrywania w przyszłości		TAK	
411	System musi posiadać mechanizm automatycznej reklasyfikacji fałszywych alarmów (False Positives) i przeciwdziałać błędnemu ich wykrywaniu w przyszłości		TAK	
EDR - analiza zagrożeń				
412	System musi umożliwiać pobieranie fragmentów zrzutów pamięci z urządzeń końcowych		TAK	
413	System musi posiadać interfejs API pozwalający na śledzenie wykrytych incydentów oraz prowadzonych analiz zagrożeń z uwzględnieniem takich parametrów jak:		TAK	
414		Adres IP	TAK	
415		Nazwa hosta	TAK	
416		Użytkownik	TAK	
417		Data	TAK	
418		Ilość wystąpień danego zdarzenia	TAK	
419		Klasyfikacja aktywności	TAK	
EDR - reagowanie na incydenty bezpieczeństwa				
420	Incydenty bezpieczeństwa muszą być klasyfikowane (klasa zagrożenia) min. w następujące grupy:		TAK	
421		Złośliwe	TAK	
422		Podejrzane	TAK	
423		Niejednoznaczne – wymagające głębszej analizy	TAK	
424		Niechciane tzw. PUP – „Potential Unwanted Programs”	TAK	
425		Prawdopodobnie bezpieczne	TAK	
426	W ramach każdej klasy zagrożeń musi istnieć możliwość zastosowania lub nie poniższej reakcji lub działania ograniczającego wpływ incydentu na bezpieczeństwo:		TAK	
427		Możliwość zabicia/zatrzymania procesu	TAK	
428		Możliwość usunięcia pliku	TAK	
429		Możliwość przywrócenia stanu rejestru systemu do stanu z przed wykonania się danego zagrożenia	TAK	
430		Automatyczne wprowadzenie hosta w stan izolacji sieciowej – zgodnie z konfigurowalną polityką dostępu do sieci	TAK	

431	W wypadku klasyfikacji zagrożenia jako niejednoznaczne, system musi umożliwiać automatyczną detonację pliku w chmurze producenta – działanie tej funkcji może zostać wyłączona przez Zamawiającego		TAK	
432	Możliwość dynamicznej zmiany grupy agenta na inną, gdzie zostały przypisane polityki bezpieczeństwa o większych obostrzeniach		TAK	
433	Możliwość zbudowania (zaprogramowania) własnych akcji reagujących na daną klasyfikację zagrożenia		TAK	
434	Automatyczne blokowanie adresu IP z którym łączy się podejrzany proces na zewnętrznym urządzeniu firewall.		TAK	
435	W ramach reakcji na incydenty musi istnieć możliwość powiadamiania innych systemów za pomocą:		TAK	
436		a) Wysłania wiadomości pocztowej e-mail ze szczegółami zdarzenia	TAK	
437		b) Wysłania informacji za pomocą protokołu syslog	TAK	
438		c) Możliwości wysłania informacji do zewnętrznego systemu zawierającego w załączeniu dane w postaci XML lub JSON umożliwiające automatyczne założenie zgłoszenia	TAK	
439	Wszystkie powyższe akcje muszą być konfigurowalne per każda klasa zagrożenia		TAK	
440	Musi być możliwość zastosowania wszystkich akcji jednocześnie w ramach danej klasy zagrożenia (np. izolacja, wysłanie powiadomienia SYSLOG, usunięcie pliku i zablokowanie niebezpiecznego adresu IP na urządzeniu Firewall)		TAK	
441	Polityka reagowania na zagrożenia i incydenty bezpieczeństwa musi umożliwiać jej rozróżnienie dla poszczególnych grup agentów		TAK	
442	System musi posiadać funkcjonalność zdalnego dostępu do chronionego urządzenia końcowego (remote shell), z poziomu konsoli administratora systemu		TAK	
443	W ramach dostępu zdalnego (remote shell access) będą możliwe co najmniej następujące akcje:		TAK	
444		Listowanie plików w katalogach	TAK	
445		Listowanie konfiguracji adresacji IP na interfejsach	TAK	
446		Pobranie pliku z urządzenia końcowego	TAK	
447		Wgranie pliku na urządzenie końcowe	TAK	
448		Usunięcie pliku na urządzeniu końcowym	TAK	
449		Informacja o zalogowanych użytkownikach	TAK	
450		Zwracanie sumy kontrolnej (SHA1 oraz MD5) pliku na urządzeniu	TAK	
451		Lista zadań systemu operacyjnego (tasklist)	TAK	
452		Zrzucenie pamięci danego procesu	TAK	
453		Uruchomienie powłoki systemowej	TAK	
454		Pobranie wartości rejestru	TAK	
455		Listowanie i usuwanie aplikacji w systemie, które są uruchamiane przy starcie z klucza rejestru RUN	TAK	
EDR - zarządzanie podatnościami				
456	Wykrywanie i katalogowanie w czasie rzeczywistym wersji aplikacji komunikujących się za pomocą sieci		TAK	

457	Wykrywanie urządzeń IoT w sieci, gdzie znajdują się chronione hosty		TAK	
458	Wykrywanie w sieci innych hostów, które nie mają zainstalowanego agenta EDR		TAK	
459	System musi umożliwiać wykrywanie podatności w aplikacjach, które komunikują się za pomocą sieci z urządzeniami zewnętrznymi.		TAK	
460	Musi istnieć możliwość ograniczenia ryzyka dla konkretnej podatnej wersji aplikacji poprzez automatyczne ograniczenie możliwości komunikacji, na podstawie reguł bazujących na aktualizowanych informacjach CVE.		TAK	
EDR - wykrywanie zaawansowanych scenariuszy ataków				
461	System musi działać w oparciu o mechanizmy analizy zachowań procesów i wywołań funkcji systemowych, wsparte sztuczną inteligencją, w szczególności działającymi mechanizmami opartymi o modele matematyczne algorytmów uczenia maszynowego (Machine Learning)		TAK	
462	Uczenie maszynowe musi być wykorzystywane zarówno w analizie zachowań procesów jak i w analizie samych plików		TAK	
463	System musi wykrywać i umożliwiać reakcję w locie na znane zagrożenia bazując na ich zachowaniu oraz reputacji, w szczególności:		TAK	
464		Możliwość blokowania i reagowania w ramach sekwencji wykonania danego zagrożenia bazując na heurystyce zachowań (np. podczas próby szyfrowania plików przez zagrożenie typu ransomware)	TAK	
465		Możliwość korzystania z komercyjnych baz reputacji plików (np. Virus Total lub równoważna dostarczana przez producenta)	TAK	
466		Możliwość wykrywania zagrożeń typu RAT (Remote Access Trojan) na podstawie zachowań	TAK	
467		Wykrywanie zagrożeń musi umożliwiać konfiguracyjnie zarówno blokowanie uruchomienia danego pliku, jak i możliwość blokowania złośliwych akcji po uruchomieniu się danego zagrożenia	TAK	
468		System musi umożliwiać blokowanie złośliwych urządzeń USB należących do innych niż dozwolone przez politykę klas	TAK	
469		System musi umożliwiać logowanie dostępu urządzeń USB mających interakcję z systemem operacyjnym	TAK	
470		System minimalnie musi umożliwiać wykrywanie i blokowanie podejrzanej aktywności w interpreterach języków skryptowych takich jak:	TAK	
471		a) Powershell	TAK	
472		b) CScript	TAK	
473		c) Python	TAK	
474		d) Makra pakietu Microsoft Office	TAK	
EDR - architektura rozwiązania				
475	Centralne zarządzanie za pomocą przeglądarki internetowej poprze WebUI		TAK	
476	Dostęp do interfejsu API		TAK	

477	System zarządzania musi umożliwiać integrację z usługa katalogową Active Directory oraz rozwiązaniami Two Factor Authentication i rozwiązaniami typu SSO (Single Sign On)		TAK	
478	System zarządzania musi umożliwiać granularną kontrole opartą o predefiniowane role oraz wparcie dla modelu RBAC		TAK	
479	Agent systemu musi być zabezpieczony przed próbami deinstalacji z poziomu użytkownika oraz innych złośliwych procesów		TAK	
480	Rozwiązanie musi pozwalać na:		TAK	
481		Centralne zarządzanie	TAK	
482		Przechowywanie zdarzeń w centralnym systemie	TAK	
483		Funkcjonowanie oprogramowania w modelu chmurowym – Zamawiający nie musi instalować po swojej stronie żadnych komponentów (z wyjątkiem instalacji agentów na chronionych końcówkach)	TAK	
EDR - zgodność z normami				
484	Dostarczony system musi posiadać zgodność z GDPR, z możliwością usunięcia zapisanych informacji. Wyszukiwanie rekordów musi być możliwe poprzez nazwę użytkownika, nazwę urządzenia, adres IP, adres MAC		TAK	
485	Dostarczony system musi umożliwiać eksport szczegółowego audyty funkcjonowania sytemu, zawierającego przynajmniej informacje o tym kto, kiedy i jakie wprowadzał zmiany w politykach, podejmował akcje, generował raport GDPR, logował się do systemu		TAK	
EDR integracja rozwiązania z innymi komponentami				
486	System musi udostępniać API, za pomocą którego można wykonywać operacje zarządzania, konfiguracji polityki oraz wprowadzania końcówek w stan izolacji		TAK	
487	Wymagane jest dostarczenie dokumentacji do API		TAK	
488	System musi umożliwiać integrację z urządzeniami typu Firewall (co najmniej z producentami Check Point, Cisco, Fortinet, Palo Alto), co najmniej umożliwiając blokowanie adresów IP, z którymi komunikuje się złośliwe oprogramowanie		TAK, podać	
489	System musi umożliwiać integrację z rozwiązaniami typu Network Access Control (NAC), umożliwiając izolację podejrzanego komputera do osobnego VLAN		TAK	
490	System musi umożliwiać integrację z rozwiązaniem typu sandbox działającym lokalnie (on-premises) – system sandbox nie jest przedmiotem zapytania		TAK	
491	System musi umożliwiać budowanie dopasowanej pod rozwiązanie („custom”) integracji z zewnętrznymi systemami/urządzeniami bezpieczeństwa poprzez wywoływanie własnych/zmodyfikowanych samodzielnie skryptów		TAK	
492	System musi umożliwiać integrację z systemami typu SIEM. Zdarzenie musi zawierać przynajmniej informacje:		TAK	
493		Nazwa urządzenia	TAK	
494		Stan agenta na urządzeniu	TAK	
495		Adres MAC	TAK	
496		System operacyjny	TAK	

497		Źródłowe IP	TAK	
498		Nazwa procesu	TAK	
499		Ścieżka procesu	TAK	
500		Typ procesu	TAK	
501		Istotność	TAK	
502		Klasyfikacja	TAK	
503		Reguła wykrywająca zagrożenie	TAK	
504		Akcja	TAK	
505		Hash procesu	TAK	
506		Nazwa/rodzina/typ zagrożenia	TAK	
507		Techniki MITRE	TAK	
508		Cel ataku	TAK	
509		Zdarzenia audytowe systemu, wykonane akcje, zmiany w politykach, itp.	TAK	
510	System musi umożliwiać integrację z systemami typu help desk, dostarczając wszystkie informacje dostępne w incydencie, które mogą być wykorzystane w celu automatycznego utworzenia zgłoszenia		TAK	
EDR - licencje oraz serwisy				
511	W ramach zamówienia dostarczone zostaną licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów obejmujące co najmniej następujące funkcjonalności:		TAK	
512		Całość infrastruktury zainstalowana musi być w środowisku producenta, z możliwością instalacji niektórych komponentów rozwiązania (agregujący ruch z agentów do centralnego systemu zarządzania oraz umożliwiający wykonywanie akcji integracyjnych z lokalnego systemu) w infrastrukturze Zamawiającego (model chmurowo/hybrydowy)	TAK	
513		Dostęp do baz zagrożeń bezpieczeństwa – Threat Intelligence	TAK	
514		Aktualizacje baz zagrożeń CVSS	TAK	
515	Rozwiązanie musi być dostarczone w postaci *licencji/subskrypcji* pozwalającej na ochronę 700 urządzeń końcowych (bez względu na to, czy oprogramowanie zostanie zainstalowane na systemach typu PC, czy systemach serwerowych) na okres 12 miesięcy		TAK	
516	Wraz z *licencją/subskrypcją* musi zostać dostarczona usługa doradztwa technicznego, dostarczana przez producenta rozwiązania, wspomagająca proces implementacji oprogramowania w oparciu o najlepsze praktyki na okres minimum 12 miesięcy		TAK	
517	Wykonawca zapewni na czas wdrożenia przynajmniej jednego inżyniera posiadającego aktualny certyfikat ze znajomości oferowanego systemu/produktu wydany przez producenta zaoferowanego oprogramowania		TAK, podać	

UWAGA! Zamawiający infromuje, że parametry i warunki określone w kolumnie "PARAMETR WYMAGANY" - "TAK" są parametrami wymaganymi przez Zamawiającego. Zamawiajacy wymaga spełnienia każdego z parametrów/warunków wymaganych w złożonej ofercie. Brak informacji w kolumnie "PARAMETR OFEROWANY" o danym parametrze/warunku oznaczać będzie brak zaoferowania tego parametru/warunku przez Wykonawcę