**Załącznik nr 5**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zadanie nr 3 - Działania zwiększające poziom cyberbezpieczeństwa szpitala**

**Zamawiający dopuszcza rozwiązania równoważne, spełniające wymagania funkcjonalne i wydajnościowe OPZ.**

**3a) Narzędzie do centralnej analiza logów, widoczności zagrożeń i wsparcia reagowania na incydenty bezpieczeństwa w sieci**

**System służący do centralnego zbierania i analizy logów, poprawiający widoczność zagrożeń oraz umożliwiający generowaniu alertów/powiadomień, a także cyklicznych raportów o stanie bezpieczeństwa; z gwarancją i wsparciem producenta oraz wdrożeniem, dokumentacją i szkoleniem personelu szpitala**

**Analiza logów, ich korelacja i generowanie alertów oraz cyklicznych raportów pozwala na znaczne zwiększenie widoczności zagrożeń i odpowiednie reagowanie na incydenty**

Producent (marka) …………………………………..…………………..……(Należy podać)

Model ……………………………………………………..………………… (Należy podać)

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis parametru** | **Parametr wymagany** | **Parametr oferowany** |
|  | **Interfejsy, Dysk, Zasilanie:** |  |  |
|  | System musi dysponować co najmniej:  4 portami Gigabit Ethernet RJ-45.  Rozwiązanie musi dysponować powierzchnią dyskową min. 8 TB.  Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 1 lub wyższy poziom zapewniający redundancję danych.  System musi być wyposażony w zasilanie AC. | Tak, podać |  |
|  | **Parametry wydajnościowe:** |  |  |
|  | System musi być w stanie przyjmować minimum 100 GB logów na dzień.  System musi być w stanie przeanalizować minimum 2000 logów na sekundę.  Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 180 systemów. | Tak, podać |  |
|  | **W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:** |  |  |
|  | **Logowanie**   1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. 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.   1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514, TCP/514 oraz TCP/6514 (Syslog over TLS).   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**  W zakresie raportowania system musi zapewniać:   1. Generowanie raportów co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. | Tak |  |
|  | **Korelacja logów**  W zakresie korelacji zdarzeń system musi zapewniać:   1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. 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.  1. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie. | Tak |  |
|  | **Zarządzanie**  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.  a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.  System musi umożliwiać definiowanie 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**  Gwarancja: System musi być objęty serwisem gwarancyjnym producenta lub autoryzowanego partnera serwisowego przez **okres 60 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.  Z uwagi na konieczność ochrony danych – serwis gwarancyjny powinien zapewnić brak konieczności zwrotu wadliwego urządzenia do producenta w przypadku uszkodzenia urządzenia.  System musi zapewnić możliwość weryfikacji zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia) na okres 60 miesięcy | Tak |  |
|  | **Rozszerzone wsparcie serwisowe**  Rozwiązanie odpowiedzialne za centralny system logowania, raportowania i korelacji System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego partnera serwisowego przez okres **60 miesięcy.**  Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważny system zarządzania jakością w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji winien być nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.  Oferent winien przedłożyć dokumenty:  • Oświadczanie Producenta lub Autoryzowanego Partnera świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).  • Certyfikat ISO 9001 lub równoważny system zarządzania jakością podmiotu serwisującego. | Tak |  |
|  | **Rozwiązanie zapewniające dostarczanie informacji:**  System zapewniający prawidłowe zbieranie informacji o ruchu powinien zostać dostarczony w postaci klastra urządzeń pracujących w trybie Active-passive. Każde z urządzeń powinno spełniać następujące wymagania: | Tak |  |
|  | **Interfejsy, Dysk, Zasilanie:**   1. System - dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  * 10 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 4 gniazdami SFP+ 10 Gbps.  1. System - posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 2. System - pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System jest wyposażony w zasilanie AC. 4. Wyposażenie dodatkowe: 8 sztuk modułów – transceiverów 10GE SFP+, (SR 10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C) | Tak, podać |  |
|  | **Parametry wydajnościowe:**   1. Obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę. 2. Przepustowość -: nie mniej niż 38 Gbps dla pakietów 512 B. 3. Przepustowość -z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. 4. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 5 Gbps. 5. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps.   Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps. | Tak |  |
|  | **Funkcje Systemu Bezpieczeństwa:**  W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). | Tak |  |
|  | **Polityki**   1. Polityka – ochrony -l uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje 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.  1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 3. Polityka -ochrony umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach - jest aktywna. 5. Element systemu -integruje 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. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. | Tak |  |
|  | **Ochrona przed malware**   1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. | Tak |  |
|  | **Ochrona przed atakami**   1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookiesdla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. | Tak |  |
|  | **Kontrola aplikacji**   1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). | Tak |  |
|  | **Kontrola WWW**   1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |  |  |
|  | **Uwierzytelnianie użytkowników w ramach sesji**   1. System umożliwia 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.  1. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP | Tak |  |
|  | **Zarządzanie**   1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. | Tak |  |
|  | **Logowanie**   1. Elementy systemu bezpieczeństwa realizują logowanie do dostarczanego systemu zbierania i analizy logów. 2. W ramach logowania element systemu - zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. | Tak |  |
|  | **Testy wydajnościowe oraz funkcjonalne**  Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.) | Tak |  |
|  | **Serwisy i licencje**  Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:       Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen; Weryfikacja zgodności konfiguracji z dobrymi praktykami producenta (audyt konfiguracji i polityk urządzenia) na okres 60 miesięcy. | Tak |  |
|  | **Gwarancja oraz wsparcie**  System jest objęty serwisem gwarancyjnym producenta lub autoryzowanego partnera serwisowego przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent lub autoryzowany partner serwisowy zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię. | Tak |  |
|  | 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 | Podać, czy jest taki wymóg |  |
|  | Na wezwanie Zamawiającego Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. | Tak |  |
|  | Uruchomienie wszystkich licencji, Serwisów oraz gwarancji (60 miesięcy) liczy się od daty dostawy rozwiązania do Zamawiającego. | Tak |  |
|  | **Wdrożenie rozwiązania:** | Tak |  |
|  | Dostawa sprzętu zgodnie z niniejszymi wymaganiami.  Wykonawca jest zobowiązany do przygotowania dokumentu projektu technicznego przed rozpoczęciem prac instalacyjnych. Dokument projektu technicznego powinien zawierać analizę obecnego stanu infrastruktury sieciowej Szpitala, określenie wolumenu i przyrostu logów sieciowych, typu incydentów.  Dokument powinien zawierać zarówno opis planowanej instalacji i głównych parametrów konfiguracji dostarczonego sprzętu jak i oprogramowania. Projekt musi również zawierać listę prac i zadań niezbędnych do wykonania po stronie Zamawiającego.  Przygotowanie logiczne systemu, konfiguracja ADOM, konfiguracja polityk retencji logów  Zintegrowanie dostarczanego rozwiązania z infrastrukturą Zamawiającego:  - integracja z System zapewniającym zaawansowaną ochronę przed zagrożeniami typu zero-day, ransomware i złośliwym oprogramowaniem  - integracja z firewallem,  - integracja ze switchami, accesspointami i pozostałymi urządzeniami i rozwiązaniami sieciowymi, a także konfiguracja syslog.  - Walidacja otrzymywanych logów, konfiguracja parsowania logów  - Dostosowanie dashboardów, alertowania oraz powiadamiania  - Testy oraz korekty dla scenariuszy blokady ruchu, incydentów bezpieczeństwa oraz anomalii systemowych urządzeń  - Konfiguracja raportów dotyczących bezpieczeństwa, ruchu sieciowego, aplikacji, anomalii  - Wykonanie prac instalacyjno-wdrożeniowych zgodnie z wcześniej zaakceptowanym przez Zamawiającego harmonogramem.  - Wykonanie powykonawczej dokumentacji technicznej uwzgledniającej stan infrastruktury Zamawiającego w obszarze wykonywanych prac.  - Wsparcie powdrożeniowe przez okres min. 2 miesięcy w zakresie monitoringu stabilności, ew. błędów, anomalii, korekty konfiguracyjne w razie potrzeby w trybie 24/7/365 (minimalnie 20 godzin miesięcznie)  - Udostępnienie systemu ticketowego oraz Service Desk do obsługi zgłoszeń w zakresie wsparcia powdrożeniowego w trybie 24/7/365  - Szkolenia – Wykonawca zapewni szkolenia dotyczące wdrażanego rozwiązania. Zamawiający dopuszcza możliwość przeprowadzenia szkoleń w trybie zdalnym. Szkolenie musi trwać nie mniej niż 8 godzin dydaktycznych (np. 2 dni × 4h).  - W ramach wdrożenia Zamawiający wymaga, aby dodano całą dostarczoną infrastrukturę do systemu monitoringu zamawiającego (Zabbix) i sparametryzowanie czujek i powiadomień.  Należy uwzględnić, iż Zamawiający może wymagać wykonania prac wdrożeniowo-konfiguracyjnych w dni powszednie poza standardowymi godzinami pracy (czyli w godzinach 16:00 – 6:00); i /lub w weekendy i/lub dni ustawowo wolne od pracy po uprzednim ustaleniu konkretnych przedziałów czasowych z personelem IT Zamawiającego. | Tak |  |
|  | Gwarancja, serwis oraz wsparcie producenta/licencji jak również rozszerzone wsparcie techniczne biegną od dnia dostarczenia rozwiązań/licencji do siedziby Zamawiającego. Terminy odbioru protokolarnego nie mają wpływu na rozpoczęcie okresu wsparcia, aby uniknąć przerwy w świadczeniu usług. | Tak |  |

**3b) System zapewniający zaawansowaną ochronę przed zagrożeniami typu zero-day, ransomware i złośliwym oprogramowaniem**

**System analizy podejrzanych plików pod kątem zagrożeń "zero day"; pozwalający na uruchomienie pliku w wyizolowanym środowisku testowym, z gwarancją i wsparciem producenta oraz wdrożeniem, dokumentacją i szkoleniem personelu szpitala**

Producent (marka) …………………………………..…………………..……(Należy podać)

Model ……………………………………………………..………………… (Należy podać)

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis parametru** | **Parametr wymagany** | **Parametr oferowany** |
|  | System może składać się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji. Poszczególne elementy wchodzące w skład systemu mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych | Tak |  |
|  | **System operacyjny** |  |  |
|  | Dla zapewnienia wysokiej sprawności i skuteczności działania elementy systemu muszą pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. | Tak |  |
|  | **Parametry wydajnościowe** |  |  |
|  | System musi umożliwiać równoległą analizę próbek z wykorzystaniem co najmniej 14 instancji środowisk testowych VM oraz zapewniać wydajność pozwalającą na analizę co najmniej 450 plików na godzinę w warunkach referencyjnych producenta, potwierdzoną publiczną dokumentacją lub oświadczeniem producenta. | Tak, podać |  |
|  | System musi umożliwiać jednoczesną analizę próbek w środowiskach Windows 10 oraz Windows 11. W ramach dostawy należy zapewnić licencjonowanie umożliwiające uruchomienie co najmniej 10 instancji/obrazów Windows wykorzystywanych do analizy (zgodnie z modelem licencjonowania producenta). System musi umożliwiać analizę dokumentów pakietu Microsoft Office w środowiskach Windows, w tym co najmniej w 5 niezależnych profilach/obrazach testowych (np. różne wersje Office/ustawienia) lub równoważnym mechanizmie zapewniającym zróżnicowanie środowisk analizy. | Tak, podać |  |
|  | **Funkcje podstawowe i uzupełniające** |  |  |
|  | System musi umożliwiać „pełny sanboxing”, tzn. wykonanie w maszynie wirtualnej dla następujących rodzajów próbek znajdujących się w wiadomościach pocztowych: adres URL, dokumenty Microsoft Office, pliki wykonywalne (w tym języki skryptowe JavaScript, Visual Basic, PowerShell, bat), pliki PDF (Adobe Acrobat), pliki SWF (Adobe Flash). | Tak |  |
|  | System musi umożliwiać wgrywanie co najmniej 12 własnych obrazów systemów operacyjnych. | Tak, podać |  |
|  | Funkcjonalność Sandbox dla instancji Windows: sprawdzanie procesów i rejestru, połączenia z Botnet C&C oraz złośliwymi URL, dostęp do pakietów przeprocesowanych przez VM, logów działania badanego oprogramowania oraz zrzutów ekranu w badanej VM. | Tak |  |
|  | Procesowanie plików o rozmiarze co najmniej 8 MB. | Tak |  |
|  | Sanboxing dla plików zarchiwizowanych (.tar, .gz,.tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj), wykonywalnych (.exe, .dll), PDF, Windows Office Document, Javascript, AdobeFlash oraz JavaArchive (JAR). | Tak |  |
|  | Sandboxing plików multimedialnych: .avi, .mpeg, .mp3, .mp4. | Tak |  |
|  | Skanowanie stron www z linkami URL. | Tak |  |
|  | Czarne i białe listy dla sum kontrolnych plików. | Tak |  |
|  | Szczegółowe raportowanie charakterystyki badanego pliku oraz zachowania: modyfikacji plików w systemie, zachowania uruchomionych procesów, zmian w rejestrze, zachowania sieci, snapshotu VM. Administrator powinien mieć możliwość definiowania cyklicznych raportów. | Tak |  |
|  | Dostęp do analizowanych plików w celu dodatkowego badania: przykładowe pliki, logi z analizy (tracer), zapis pakietów pcap. | Tak |  |
|  | System musi umożliwiać generowanie alertów podczas wykrywania zagrożeń i raportowanie ich za pomocą: Syslog, SNMP, SMTP. | Tak |  |
|  | System musi umożliwiać zarządzanie min. przez panel WebUI za pomocą przeglądarki internetowej. | Tak |  |
|  | System musi umożliwiać elastyczną rozbudowę o dodatkowe maszyny zarówno w środowisku lokalnym (on-prem) jak i chmurowym (cloud). | Tak |  |
|  | Rozwiązanie musi wspierać rozbudowy do klastra HA. | Tak |  |
|  | **Wymagania licencyjne** |  |  |
|  | Bazy sygnatur wykorzystywanych przez funkcje skanujące powinny być systematycznie aktualizowane.  System powinien zapewnić wbudowane wykrywanie i blokowanie phishingu w czasie rzeczywistym (real-time anti-phishing – RTAP) | Tak |  |
|  | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji skanujących oraz analitycznych, a także funkcjonalności RTAP na okres 60 miesięcy. | Tak |  |
|  | **Gwarancja oraz wsparcie** |  |  |
|  | System musi być objęty serwisem gwarancyjnym producenta lub autoryzowanego partnera serwisowego przez okres 60 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.  Z uwagi na konieczność ochrony danych – serwis gwarancyjny powinien zapewnić brak konieczności zwrotu wadliwego urządzenia do producenta. | Tak |  |
|  | **Rozszerzone wsparcie serwisowe**  System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 4 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego partnera serwisowego przez okres **60 miesięcy**.  Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważny system zarządzania jakością w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji winien być nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.  Oferent winien przedłożyć dokumenty:  • Oświadczanie Producenta lub Autoryzowanego Partnera świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).  • Certyfikat ISO 9001 lub równoważny system zarządzania jakością podmiotu serwisującego. | Tak |  |
|  | **Integracje z innymi systemami** |  |  |
|  | System powinien umożliwiać lokalne logowanie i raportowanie oraz współpracować z systemem centralnego logowania i raportowania. | Tak |  |
|  | Powinna istnieć możliwość implementacji systemu w trybie nasłuchu oraz współpracy z systemami zabezpieczeń NGFW (Next Generation Firewall), SWG (Security Web Gateway), SEG (Secure Email Gateway) oraz w oparciu o interfejsy programistyczne API. | Tak |  |
|  | **Wdrożenie rozwiązania- dostarczone usługi:** |  |  |
|  | Dostawa sprzętu zgodnie z niniejszymi wymaganiami. | Tak |  |
|  | Wykonawca jest zobowiązany do przygotowania dokumentu projektu technicznego przed rozpoczęciem prac instalacyjnych. Dokument projektu technicznego powinien zawierać zarówno opis planowanej instalacji i głównych parametrów konfiguracji dostarczonego sprzętu jak i oprogramowania. Projekt musi również zawierać listę prac i zadań niezbędnych do wykonania po stronie Zamawiającego. | Tak |  |
|  | Wykonanie prac instalacyjno-wdrożeniowych zgodnie z wcześniej zaakceptowanym przez Zamawiającego harmonogramem. | Tak |  |
|  | Zintegrowanie dostarczanego rozwiązania z infrastrukturą Zamawiającego:  - Integracja z Istniejącym systemem ochrony poczty Zamawiającego, a także z systemem poczty elektronicznej  - Rekonfiguracja systemów wysyłających podejrzane pliki do analizy w Sandbox’ie (NGFW, SEG) | Tak |  |
|  | Wykonanie powykonawczej dokumentacji technicznej uwzgledniającej stan infrastruktury Zamawiającego w obszarze wykonywanych prac. | Tak |  |
|  | Szkolenia – Wykonawca zapewni szkolenia dotyczące wdrażanego rozwiązania. Zamawiający dopuszcza możliwość przeprowadzenia szkoleń w trybie zdalnym. Szkolenie musi trwać nie mniej niż 8 godzin dydaktycznych (np. 2 dni × 4h). | Tak |  |
|  | W ramach wdrożenia Zamawiający wymaga, aby dodano całą dostarczoną infrastrukturę do systemu monitoringu zamawiającego (Zabbix) i sparametryzowanie czujek i powiadomień. | Tak |  |
|  | Należy uwzględnić, iż Zamawiający może wymagać wykonania prac wdrożeniowo-konfiguracyjnych w dni powszednie poza standardowymi godzinami pracy (czyli w godzinach 16:00 – 6:00); i /lub w weekendy i/lub dni ustawowo wolne od pracy po uprzednim ustaleniu konkretnych przedziałów czasowych z personelem IT Zamawiającego. | Tak |  |
|  | Gwarancja, serwis oraz wsparcie producenta/licencji biegną od dnia dostarczenia rozwiązań/licencji do siedziby Zamawiającego. Terminy odbioru protokolarnego nie mają wpływu na rozpoczęcie okresu wsparcia, aby uniknąć przerwy w świadczeniu usług. | Tak |  |

**3c) Obowiązkowy drugi składnik uwierzytelniający (2FA) dla pracowników korzystających z poczty dostępnej z sieci publicznej**

**System 2FA dla systemu pocztowego dla użytkowników poczty z gwarancją i wsparciem producenta oraz wdrożeniem, dokumentacją i szkoleniem personelu szpitala**

**(Rekonfiguracja poczty elektronicznej wraz z dostarczeniem i wdrożeniem rozwiązania umożliwiającego dwuskładnikowe uwierzytelnianie dla użytkowników korzystających z poczty elektronicznej spoza szpitalnej infrastruktury sieciowej (LAN)**

Producent (marka) …………………………………..…………………..……(Należy podać)

Model ……………………………………………………..………………… (Należy podać)

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis parametru** | **Parametr wymagany** | **Parametr oferowany** |
|  | Zabezpieczenie logowania do poczty przy użyciu mechanizmu MFA dla:   * Klienta www * Urządzeń mobilnych * Aplikacji desktop   Dotyczy: do 250 użytkowników | Tak |  |
|  | Możliwość instalacji aplikacji MFA na urządzeniach mobilnych:   * Android * IOS   Dotyczy: do 250 użytkowników | Tak |  |
|  | System musi wspierać co najmniej dwie niezależne metody MFA, w tym co najmniej jedną metodę opartą o aplikację mobilną (TOTP/push) oraz jedną metodę opartą o standard FIDO2 lub równoważny.  Dopuszczalne metody mogą obejmować:   * SMS, * połączenie głosowe, * dedykowana aplikacja, * Windows Hello, * FIDO2, * Certyfikat X.509 | Tak |  |
|  | Zabezpieczenie dostępu do Panelu zarządzania dla administratorów przy pomocy MFA. | Tak |  |
|  | Rejestrowanie logów dotyczących logowania i uwierzytelniania. | Tak |  |
|  | Generowanie alertów bezpieczeństwa związanych z procesem MFA. | Tak |  |
|  | Możliwość integracji z rozwiązaniami bezpieczeństwa, takimi jak XDR czy SIEM. | Tak |  |
|  | Możliwość integracji z Rozwiązaniem do centralnej analizy logów, widoczności zagrożeń i wsparcia reagowania na incydenty bezpieczeństwa w sieci (oferowanym w części 1a). | Tak |  |
|  | Możliwość przypisania kilku metod MFA dla jednego użytkownika. | Tak |  |
|  | Rozwiązanie musi spełniać obowiązujące wymogi bezpieczeństwa i ochrony danych osobowych (RODO) oraz być zgodne z uznanymi standardami bezpieczeństwa informacji (np. ISO 27001, SOC 2 lub równoważne). | Tak |  |
|  | Wykonawca zapewni Zamawiającemu subskrypcję licencji o wymaganej funkcjonalności na okres 36 miesięcy od dnia uruchomienia licencji podczas wdrożenia, z zachowaniem ciągłości ważności licencji. Dopuszcza się realizację zamówienia w modelu subskrypcji odnawianej cyklicznie (np. rocznie), pod warunkiem zapewnienia nieprzerwanego dostępu do usług przez cały okres 36 miesięcy dla wymaganej ilości 2FA (maksymalnie do 250 użytkowników).  Potwierdzenie | Tak podać |  |
|  | Wdrożenie, instalacja:   * wdrożenie MFA dla kont użytkowników * konfiguracja metody MFA dla grup użytkowników   Dotyczy: do 250 użytkowników | Tak |  |
|  | Dopuszcza się rekonfigurację obecnego środowiska pocztowego, wdrożenie rozwiązania typu reverse proxy/IdP lub migrację do środowiska wspierającego MFA, pod warunkiem zachowania funkcjonalności systemu poczty oraz integracji z istniejącą infrastrukturą. Dotyczy: do 250 użytkowników | Tak |  |
|  | Rozwiązanie musi umożliwiać integrację z posiadanym systemem ochrony poczty (FortiMail 200F) poprzez standardowe mechanizmy uwierzytelniania (np. LDAP, SAML, RADIUS, API) bez wymogu stosowania rozwiązania tego samego producenta. Dotyczy: do 250 użytkowników | Tak |  |
|  | Możliwość wykorzystania wdrożonego rozwiązania MFA do połączeń VPN (jedno MFA dla poczty i opcjonalnie wykorzystane także do zdalnego dostępu VPN). | Tak |  |
|  | Zaproponowane rozwiązanie nie może powodować konfliktów, powinno współistnieć bez zakłóceń z posiadanym, przedłużanym oraz rozbudowywanym przez Zamawiającego Oprogramowaniem Antywirusowym/EDR Bitdefender (oferowanym w części 1d). | Tak |  |

**3d) Rozbudowa o rozwiązania klasy EDR wraz z wydłużeniem wsparcia**

**Rozszerzenie posiadanej licencji oprogramowania Antywirusowego (Elite) do wersji Enterprise (Ultra), która zawiera pełne funkcje EDR (Endpoint Detection & Response). W ramach systemu umożliwiona zostanie wielowarstwowa ochrona, w tym: antywirus, firewall, kontrola treści, anti-exploit (także zero-day), kontrola aplikacji i urządzeń oraz automatyczne zarządzanie podatnościami (risk management). Rozwiązanie umożliwi wczesne wykrywanie zagrożeń przy użyciu AI i analizy zachowań z gwarancją i wsparciem producenta oraz wdrożeniem, dokumentacją i szkoleniem personelu szpitala**

Producent (marka) …………………………………..…………………..……(Należy podać)

Nazwa (nazwy produktów) …………………………………..………………… (Należy podać)

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis parametru** | **Parametr wymagany** | **Parametr oferowany** |
|  | Rozszerzenie posiadanych licencji Bitdefender do wariantu obejmującego funkcje EDR, Network Sensor oraz zarządzanie podatnościami (zgodnie z aktualnym modelem licencjonowania producenta). | Tak |  |
|  | **Wydłużenie wsparcia do 31 maja 2031 r.** | Tak, Podać |  |
|  | Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. | Tak |  |
|  | Interfejs oraz pomoc techniczna świadczona w języku polskim. | Tak |  |
|  | Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi. | Tak |  |
|  | Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. | Tak |  |
|  | Wbudowana technologia do ochrony przed rootkitami. | Tak |  |
|  | Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. | Tak |  |
|  | Możliwość ustawienia zadania skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. | Tak |  |
|  | Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich. | Tak |  |
|  | Możliwość dodawania wykluczeń na podstawie:  a) Plik  b) Folder  c) Rozszerzenie  d) Proces  e) Hash pliku  f) Hash certyfikatu  g) Nazwa zagrożenia  h) Wiersz poleceń  i) IP/maska | Tak, podać |  |
|  | Skanowanie poczty opartej o protokoły IMAP, MAPI, POP3 i SMTP w czasie rzeczywistym. | Tak |  |
|  | Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie w przeglądarce. | Tak |  |
|  | Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta. | Tak |  |
|  | Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS. | Tak |  |
|  | Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. | Tak |  |
|  | Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. | Tak |  |
|  | Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. | Tak |  |
|  | Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows i macOS. | Tak |  |
|  | Oprogramowanie klienckie powinno działać jako jeden zintegrowany agent/klient na punkcie końcowym (bez konieczności instalowania wielu niezależnych agentów dla poszczególnych modułów). | Tak |  |
|  | System musi umożliwiać kontrolę dostępu do urządzeń na podstawie interfejsów, do których zostały one podłączone | Tak |  |
|  | Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej na podstawie ich wykrycia lub wpisanych ręcznie ID urządzenia lub ID produktu. | Tak |  |
|  | Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. | Tak |  |
|  | Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:   1. Możliwość wymuszenia funkcji DEP systemu Windows. 2. Możliwość wymuszenia relokacji modułów (ASLR) dla Windows. | Tak |  |
|  | Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:  -Pierwszy dostęp.  -Dostęp do poświadczeń.  -Wykrycie.  -Crimeware.  -Ruch boczny. | Tak |  |
|  | Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików w momencie szyfrowania, a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Oprogramowanie musi dać możliwość odzyskania plików na żądanie lub automatycznie, o następujących rozszerzeniach:  3fr, ai, arw, bay, cdr, cer, cr2, crt, crw, dcr, der, dll, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, exe, indd, jpe, jpeg, jpg, mdf, mef, mrw, nef, nrw, odb, odc, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pdf, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, png, r3d, raf, rtf, rw2, rwl, sr2, srf, srw, wb2, wpd, wps, x3f, xlk, xls, xlsb, xlsm, xlsx, msg, py, ini, xml, msi, cab, tsf, dgn, log, gif, csv, avi, mov, mp4 | Tak |  |
|  | System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym z Windows. | Tak |  |
|  | Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows. | Tak |  |
|  | Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows. | Tak |  |
|  | System musi umożliwiać skanowanie oprogramowania układowego UEFI. | Tak |  |
|  | Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows i macOS do SIEM lub z systemem Windows i Linux do serwera Syslog (JSON). | Tak |  |
|  | Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników naruszeń bezpieczeństwa (IOC). | Tak |  |
|  | Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. | Tak |  |
|  | Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło. | Tak |  |
|  | Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju. | Tak |  |
|  | Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików. | Tak |  |
|  | Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows po doinstalowaniu odpowiedniego modułu. Zmiana ustawień zabezpieczona jest hasłem. | Tak |  |
|  | Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej. | Tak |  |
|  | Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238. | Tak |  |
|  | Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz na określenie godziny, o której te maszyny będą usuwane. | Tak |  |
|  | Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS. | Tak |  |
|  | System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej. |  |  |
|  | Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie. | Tak |  |
|  | Ochrona proaktywna oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie. Ochrona ta musi wykrywać zagrożenia takie jak:   1. Ukierunkowane ataki. 2. Podejrzane pliki i ruch w sieci. 3. Exploity. 4. Ransomware. 5. Grayware. | Tak |  |
|  | System zarządzania ryzykiem– Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100, gdzie liczba mniejsza stanowi mniejsze ryzyko, a liczba większa większe ryzyko. System ponadto musi posiadać:   1. Funkcję, która pozwala wyszukiwać podatności ustawień punktów końcowych oraz naprawiać je lub ignorować z podziałem na typ wykrytej konfiguracji:   -Przeglądarka  -Sieć  -System operacyjny  -Luki  System ponadto musi określać nasilenie zagrożenia wynikłego z wykrytej podatności w oparciu o punkty procentowe oraz posiadać funkcję cofnięcia wprowadzonych zmian w ustawieniach systemów.   1. System zarządzania ryzykiem powinien określać luki w wykrytym zainstalowanym oprogramowaniu podając przy tym numer CVE tych luk. 2. System pozwala na śledzenie i wykrywanie ryzykownych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem o liczbie użytkowników, których takie działanie dotyczy oraz jaka jest jego szkodliwość. 3. System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania. 4. System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich szkodliwość wyrażona w procentach. 5. System zarządzania ryzykiem powinien wspierać ocenę konfiguracji i podatności w oparciu o uznane standardy i dobre praktyki (np. CIS, ISO 27001 lub równoważne) oraz umożliwiać mapowanie wyników do wymagań regulacyjnych istotnych dla Zamawiającego (w tym RODO oraz NIS2). | Tak |  |
|  | Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni. | Tak |  |
|  | Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem. | Tak |  |
|  | Możliwość utworzenia konsoli typu Partner, która pozwala na zarządzanie wieloma firmami z poziomu jednej scentralizowanej konsoli zarządzającej, konsola partnerska musi umożliwiać:   1. Pobieranie przez partnera plików z kwarantanny podległych firm. 2. Zarządzanie systemem ochrony firm podrzędnych przez Partnera z jednej konsoli lub tworzenie bezpośrednich dostępów użytkowników dla tych firm. 3. Odseparowanie przez administratora konsoli podrzędnej od konsoli partnera nadrzędnego. | Tak |  |
|  | System umożliwia tymczasowe wyłączenie wszystkich lub wybranych modułów ochrony na określony czas, który wynosi 15 minut, 30 minut, 1 godzina, 2 godziny, 4 godziny. Po ponownym uruchomieniu ochrony możliwość przeprowadzenia pełnego skanowania. | Tak |  |
|  | **Komponenty EDR**  Główne elementy:   1. Sensor EDR, który gromadzi i przetwarza dane dotyczące punktu końcowego i zachowania aplikacji w celu ich raportowania. 2. Analityka Bezpieczeństwa, komponent służący do interpretacji metadanych gromadzonych przez sensor EDR. 3. Możliwość instalacji dodatkowego, dedykowanego agenta z sensorem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną równolegle ochronę świadczoną przez innego producenta oprogramowania antywirusowego. | Tak, podać |  |
|  | **Wykrywanie podejrzanej aktywności**  Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.  Bazowanie na systemach opartych o techniki MITRE ATT&CK i własnej inteligencji.  Zgłaszanie naruszeń jako incydent w module EDR. | tak |  |
|  | **Badanie incydentów i wizualizacja**  Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym czasie.  Produkt integruje się z bazą wiedzy MITRE ATT&CK i odpowiednio oznacza zdarzenia bezpieczeństwa.  Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi danymi lub działaniami z następującymi informacjami:   1. Karta podsumowująca zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia. 2. Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej. 3. System gromadzi informacje o działaniach podejmowanych przez produkt w związku ze zdarzeniem bezpieczeństwa. | tak |  |
|  | **Incydenty**  Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i chronologicznej linii zdarzeń oraz daje możliwość:   1. Filtrowania zdarzeń. 2. Zakończenia procesów. 3. Dodania procesów do czarnej listy. 4. Dodania procesów do białej listy. 5. Izolacji hosta. 6. Przesłania pliku do Sandbox. 7. Sprawdzenia informacji o pliku w Google. 8. Sprawdzenia informacji o pliku w VirusTotal.   Możliwość szybkiego podglądu incydentów za pomocą spersonalizowanych widoków list lub widoku domyślnego.   1. Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie. 2. System umożliwia blokowanie na podstawie utworzonych reguł czarnej listy przy pomocy kategorii: 3. a) Hash MD5 lub SHA256.   b) Pełna ścieżka do aplikacji.  c) Reguła połączenia.   1. Możliwość importu reguł czarnej listy dla hash, ścieżek do aplikacji oraz reguł połączeń z pliku CSV. 2. System musi oferować szeroki zakres filtrowania dodanych reguł blokowania minimum po nazwie pliku, hash pliku, typu hash, ścieżce, protokole porcie/zakresie portów, daty dodania. 3. Możliwość wygenerowania i wyeksportowania listy incydentów do pliku .csv. | tak |  |
|  | **Zarządzanie aktualizacjami systemów operacyjnych i kompatybilnego oprogramowania**  Wspierane systemy operacyjne Windows:   * Windows 11 * Windows 10 * Windows Server 2025 * Windows Server 2022 * Windows Server 2019 * Windows Server 2016   Wspierane systemy operacyjne Linux (64-bit):   * CentOS 7 – GA+ (7.2003) * Red Hat Enterprise Linux RHEL 7 – GA+ (7.1-7.9) * Red Hat Enterprise Linux REL 8 – GA+ (8.4) * SUSE Linux Enterprise SLES 12 – SP5 * SUSE Linux Enterprise SLES 15 – GA+ (SP5) * SUSE Linux Enterprise SLED 15 – GA+ (SP5)   Wspierane systemy operacyjne macOS:   * macOS Tahoe (26.x) * macOS Sequoia (15.x) * macOS Sonoma (14.x) * macOS Ventura (13.x) * macOS Monterey (12.x) * macOS Big Sur (11.x)   Wymagany Pełny Dostęp do Dysku. | Tak, Podać |  |
|  | Możliwość działania w trybie automatycznym:   * 1. Możliwość wykrycia i wylistowania brakujących kompatybilnych łatek.   2. Możliwość zaplanowania oddzielnej automatycznej instalacji w oparciu o kategorię poprawek (bezpieczeństwo / niezwiązane z zabezpieczeniami).   3. Możliwość opóźnienia ponownego uruchomienia, jeśli instalacja łatki tego wymaga. | Tak |  |
|  | Rozwiązanie musi zezwalać na tryb manualny – wykrywanie i instalacja łatek na żądanie. | Tak |  |
|  | Rozwiązanie musi oferować możliwość podejrzenia wszystkich kompatybilnych brakujących łatek ze wspieranych punktów końcowych. Informacje te zostaną zebrane w zakładce inwentarza aktualizacji.   * 1. Rozwiązanie umożliwia sprawdzenie, które punkty końcowe posiadają zainstalowane lub brakujące aktualizacje.   2. Rozwiązanie przesyła informacje zwrotne w przypadku niepowodzenia instalacji łatki.   3. Rozwiązanie daje użytkownikowi możliwość szybkiej instalacji brakujących łatek na urządzeniu.   4. Użytkownik powinien mieć możliwość dodania do czarnej listy jednej lub wielu łatek. | Tak |  |
|  | Rozwiązanie raportuje brakujące łatki z perspektywy punktu końcowego (zainstalowane/ brakujące na każdym punkcie końcowym). | Tak |  |
|  | Rozwiązanie zapewnia możliwość pobierania aktualizacji poprzez serwer pośredniczący lub bezpośrednio przez Internet. | Tak |  |
|  | Funkcja skanowania dostępnych aktualizacji dla nowo zainstalowanych kompatybilnych aplikacji na punkcie końcowym. | Tak |  |
|  | System musi umożliwiać wyświetlenie listy numerów CVE dla podatności naprawianych przez daną aktualizację. | Tak |  |
|  | **Sensor analizujący ruch sieciowy pod postacią maszyny wirtualnej**  System musi obsługiwać czujnik sieciowy który gromadzi i wstępnie przetwarza zdarzenia związane z siecią w celu wzbogacenia kontekstu incydentów. | Tak |  |
|  | System musi umożliwiać obsługę protokołów IPv4 oraz IPv6 niezależnie od tego czy urządzenie jest obsługiwane przez agenta systemu antywirusowego czy też nie. | Tak |  |
|  | System musi umożliwiać analizę ruchu urządzeń IoT jeśli wykorzystują one do komunikacji protokoły IPv4 oraz IPv6. | Tak |  |
|  | System musi przechwytywać kopię ruchu przez port SPAN. | Tak |  |
|  | **System zdalnego zarządzania szyfrowaniem punktów końcowych z systemami Windows oraz macOS**  Szyfrowanie dysków korzysta z natywnej funkcji BitLocker na systemach Windows.  Szyfrowanie dysków korzysta z natywnej funkcji FileVault na systemach macOS.  **Systemy Operacyjne Komputerów**   * Windows 11 Pro * Windows 11 Pro for Workstations * Windows 11 Enterprise * Windows 11 Education * Windows 10 Education * Windows 10 Enterprise * Windows 10 Pro * Windows 10 IoT Core * Windows 10 IoT Core Commercial   **Systemy operacyjne serwera**  Wymagana instalacja funkcji Bitlocker.   * Windows Server 2022 * Windows Server 2019 * Windows Server 2016   **Systemy Operacyjne Mac OS X**   * macOS Sequoia (15.x) * macOS Sonoma (14.x) * macOS Ventura (13.x) * macOS Monterey (12.x) * macOS Big Sur (11.x) | Tak |  |
|  | Możliwość szyfrowania i deszyfrowania punktów końcowych poprzez politykę bezpieczeństwa zastosowaną na komputerach. | Tak |  |
|  | Możliwość podglądu klucza odzyskiwania do funkcji Bitlocker i FileVault z konsoli administracyjnej po wpisaniu hasła. | Tak |  |
|  | Użytkownik musi ustawić PIN do funkcji Szyfrowania zgodnie z wymaganiami. | Tak |  |
|  | Moduł Szyfrowania zapewnia zgodność z wymogami RODO odnośnie do szyfrowania danych. | Tak |  |
|  | Rozwiązanie nie wymaga dodatkowego klienta, czy serwera zarządzającego do obsługi modułu szyfrowania. | Tak |  |
|  | Administrator ma możliwość ustawienia, czy system szyfrujący ma pytać o hasło w momencie uruchomienia systemu operacyjnego, jeśli aktywny jest moduł TPM | Tak |  |
|  | System automatycznie zaimportuje klucz odzyskiwania do konsoli po instalacji oprogramowania z modułem szyfrowania. | Tak |  |
|  | Możliwość dodania wyjątków od szyfrowania dla dysków innych niż systemowe. | Tak |  |
|  | Liczba licencji jest zależna od ilości systemów operacyjnych, nie od ilości dysków na punkcie końcowym. | Tak |  |
|  | **Wspierane systemy operacyjne**  **System Operacyjny Windows:**  **Systemy Operacyjne Komputerów**   * Windows 11 October 2024 Update (24H2) * Windows 11 October 2023 Update (23h2) * Windows 10 November 2022 Update (22H2) * Windows 11 September 2022 Update (22H2) * Windows 11 (initial release) * Windows 10 November 2021 Update (21H2) * Windows 10 May 2021 Update (21H1) * Windows 10 October 2020 Update (20H2) * Windows 10 May 2020 Update (20H1) * Windows 10 May 2019 Update (19H1) * Windows 10 October 2018 Update (Redstone 5) * Windows 10 April 2018 Update (Redstone 4) * Windows 10 Fall Creators Update (Redstone 3) * Windows 10 Creators Update (Redstone 2) * Windows 10 Anniversary Update (Redstone 1) * Windows 10 November Update (Threshold 2) * Windows 10 (initial release)   Windows Tablet oraz systemy wbudowane  Windows 10 IoT Enterprise  Windows ARM64 desktop  Windows 11 October 2024 Update (24H2)  Windows 10 November 2022 Update (22H2)  Windows 11 September 2022 Update (22h2)  Windows 10 November 2021 Update (21H2)  Systemy operacyjne serwera  Windows Server 2025 64x  Windows Server 2022 Core  Windows Server 2022  Windows Server 2019 Core  Windows Server 2019  Windows Server 2016  Windows Server 2016 Core  Systemy Operacyjne Linux i wersja kernel  Oparte o RPM  RHEL 7.x - 3.10.0 (build 957) 64-bit  RHEL 8.x - 4.18.0 64-bit  RHEL 9.x - 5.14.0 64-bit  Oracle Linux 7.x (UEK) - 4.18.0 64-bit  Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit  Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit  Oracle Linux 8.x (RHCK) – 4.18.0 64-bit  Oracle Linux 9.x (UEK) – 5.15.0 64-bit  Oracle Linux 9.x (RHCK) – 5.14.0 64-bit  CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit  CentOS 8 Stream - 4.18.0 64-bit  CentOS 9 Stream - 5.14.0 64-bit  Fedora 37 – 42 – wsparcie do wygaśnięcia. 64-bit  AlmaLinux 8.x - 4.18.0 64-bit  AlmaLinux 9.x - 5.14.0 64-bit  Rocky Linux 8.x - 4.18.0 64-bit  Rocky Linux 9.x - 5.14.0 64-bit  CloudLinux 7.x - 3.10 (build 957) 64-bit  CloudLinux 8.x - 4.18.0 64-bit  Miracle Linux 8.x - 4.18.0 64-bit  Kylinv10 RHEL - 4.19.90 64-bit  Microsoft Azure Linux 3 – 6.6.64.x.azl3 64-bit  Oparte o Debian  Debian 9 - 4.9.0 32-bit/64-bit  Debian 10 - 4.19 32-bit/64-bit  Debian 11 - 5.10 32-bit/64-bit  Debian 12 – 6.1.0 64-bit  Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64 bit  Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit  Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit  Ubuntu 22.04.x - 5.15 / 5.19 64-bit  Ubuntu 23.04.x – 6.2.0 64-bit  Ubuntu 24.04.x – 6.8.0 64- bit  PopOS 22.04.x – 6.2.6 64-bit  Pardus 21 – 5.10.0 64-bit  Mint 20.x – 5.4.0 64-bit  Mint 21.x – 5.15.0 64-bit  Mint 22.x – 6.8.0.x 64-bit  Zorin OS – 6.5.x 64-bit  Linux Mint Debian Edition 6 – 6.1.x 64-bit  Oparte o SUSE  SLES 12 SP4 - 4.12.14-x 64-bit  SLES 12 SP5 - 4.12.14-x 64-bit  SLES 15 SP1 - 4.12.14-x 64-bit  SLES 15 SP2 - 5.3.18-x 64-bit  SLES 15 SP3 - 5.3.18-x 64-bit  SLES 15 SP4 – 5.14.21 64-bit  SLES 15 SP5 – 5.14.21 64-bit  SLES 15 SP6 – 6.4.x 64-bit  SLED 15 SP4 – 5.14.21 64-bit  openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit  Cloud based Linux  AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit  Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit  Amazon Linux 2023 – 6.1.x 64-bit  Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit  Azure Mariner 2 - 5.15 64-bit  Linux dla ARM  Oparte o RPM  RHEL 8.x – 4.18.0-x  RHEL 9.x – 5.14  AlmaLinux 9.x – 5.14  Rocky Linux 9.x – 5.14  Oparte o Debian  Debian 11 – 5.10 / 6.1  Debian 12 – 6.1.0.x  Ubuntu 20.04.x – 5.15  Ubuntu 22.04.x – 5.15 / 5.19  Ubuntu 24.04.x – 6.8.0.x  Oparte o SUSE  SLES 15 SP4 – 5.14.21-x  openSUSE Leap 15.4-15.5 – 5.14.21-x  Oparte o chmurę  Amazon Linux v2 – 5.10  Amazon Linux 2023 - 6.1  Systemy Operacyjne Mac OS X  macOS Tahoe (26.x)  macOS Sequoia (15.x)  macOS Sonoma (14.x)  macOS Ventura (13.x)  macOS Monterey (12.x)  macOS Big Sur (11.x)  Obsługiwane Środowiska Microsoft Exchange  Security for Exchange wspiera następujące wersje i role Microsoft Exchange:   * Exchange Server 2019 z rolą Edge Transport lub Mailbox * Exchange Server 2016 z rolą Edge Transport lub Mailbox * Exchange Server 2013 z rolą Edge Transport lub Mailbox * Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox   Security for Exchange jest kompatybilny z Microsoft Exchange Database Availability  Groups (DAG).  Ochrona środowisk wirtualnych (SVE)   1. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej. 2. Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie: 3. OVA 4. XVA 5. VHD 6. VHDX 7. VMDK   Środowiska wspierane:   * VMware vSphere and vCenter Server: * version 6.5 * version 6.7, including update 1, update 2a and update 3 * version 7.0, including update 1, update 2, update 2b, update 2c and update 2d * version 8.0, including update 1, update 2 * VMware ESXi 8.0, including update 1, update 2 * VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x * VMware Workstation 11.x, 10.x, 9.x, 8.0.6 * VMware Player 7.x, 6.x, 5.x * Citrix Xen Hypervisor: 8.4. * Citrix Xen Hypervisor: 7.1 (with the XS71ECU2060 hotfix), 8.2. * Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906 * Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR * Citrix VDI-in-a-Box 5.x * Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor), 2022, 2025 * Proxmox Virtual Environment 8.4, 9.0 * Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor) * Oracle VM 3.0 * Oracle VM VirtualBox 5.2, 5.1 |  |  |

**Zadanie nr 1 - Integracja i rozbudowa systemów informatycznych szpitala**

**1e) Dostawa zestawów komputerowych (sprzęt komputerowy z urządzeniami peryferyjnymi - monitor, klawiatura, myszka) – 30 sztuk**

**Zestaw komputerowy składający się z biznesowego komputera, monitora, myszkę klawiaturę wraz z konfiguracją migracją danych wdrożeniem i gwarancją**

**Komputer, klawiatura i mysz**

Producent (marka) …………………………………..…………………..……(Należy podać)

Model ……………………………………………………..………………… (Należy podać)

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Opis parametru** | **Parametr wymagany** | **Parametr oferowany** |
|  | Typ obudowy | Small Form Factor (SFF) |  |
|  | Procesor | Procesor klasy x86 o wydajności nie niższej niż Intel Core i5-14500, na podstawie testu CPU Mark według wyników opublikowanych na stronie www.cpubenchmark.net, aktualnym na dzień publikacji ogłoszenia o zamówieniu.  Wykonawca zobowiązany jest wskazać dokładny model oferowanego procesora. |  |
|  | Pamięć RAM | Minimum 16 GB DDR5 (1x16 GB), 4800 MT/s, 2 sloty UDIMM, możliwość rozbudowy do min. 64 GB |  |
|  | Dysk | Minimum 512 GB SSD PCIe NVMe 2280 TLC 4X4 SSD |  |
|  | Napęd optyczny | Nagrywarka DVD typu SuperMulti Slim |  |
|  | Grafika | Zintegrowana z procesorem, obsługująca rozdzielczość UHD |  |
|  | System operacyjny | Wymagania ogólne:  1. Licencja na Microsoft Windows 11 Professional PL (klucz licencyjny zapisany przez producenta komputera w BIOSie/UEFI, umożliwiający automatyczną aktywację systemu) – zainstalowany (preinstalowany przez producenta komputera) Microsoft Windows 11 Professional PL 64 bit lub równoważny.  2. Licencja musi być przeznaczona na rynek Polski, posiadać wszystkie atrybuty legalności przewidziane przez producenta dla danego typu i wersji licencji oraz maksymalną ilość dostępnych aktywacji przewidzianą przez producenta.  3. Wykonawca dostarcza licencję wraz z oryginalnymi atrybutami legalności.  Równoważność – Microsoft  1. Zamawiający w oparciu o art. 99 ust. 5 ustawy Prawo zamówień publicznych wskazał znak towarowy firmy Microsoft jako wzorzec funkcjonalno-jakościowy przedmiotu zamówienia.  2. Oznacza to, że Zamawiający dopuszcza złożenie oferty zawierającej sprzęt z systemem operacyjnym o parametrach funkcjonalnych i wydajnościowych nie gorszych od parametrów wzorca, pod warunkiem, że zaoferowany system:  1) Będzie w pełni i poprawnie funkcjonował z posiadaną infrastrukturą informatyczną Zamawiającego (sprzęt i oprogramowanie), w szczególności z:  a) sieciowymi systemami operacyjnymi MS Windows Server;  b) oprogramowaniem aplikacyjnym: MS Office, ESET Antywirus, Adobe Reader, Szafir, Certum, Kamsoft );  c) urządzeniami drukującymi, kopiującymi i skanującymi firm HP, OKI, Brother (oficjalnie dostępne sterowniki producentów dla oferowanego systemu).  2) Zachowa pełną funkcjonalność wymaganą przez Zamawiającego dla pracy w środowisku biurowym i medycznym.  3. Wykazanie równoważności leży po stronie Wykonawcy i powinno zostać udokumentowane i złożone wraz z ofertą.  4. W przypadku zaoferowania przez Wykonawcę innego systemu operacyjnego niż MS Windows, Zamawiający zastrzega prawo do przesłania dokumentów poświadczających równoważność do producenta danego systemu/oprogramowania celem ich weryfikacji. |  |
|  | Zabezpieczenia | Minimum TPM 2.0, BIOS protection |  |
|  | Porty | Minimum: Przód: 1x USB-C 10 Gb/s, 3x USB-A 10 Gb/s, combo audio;  Tył: 4x USB, LAN, HDMI, DisplayPort, Audio |  |
|  | Interfejs sieciowy | Minimum: 1 x 10/100/1000 Mbit/s  Wi-Fi 802.11a/b/g/n/ax  Bluetooth |  |
|  | Gniazda | Minimum: 1x PCIe 3.0 x1, 1x PCIe 4.0 x16, 1x M.2 2230, 1x M.2 2280 |  |
|  | Zasilacz | Sprawność min. 92%, aktywna PFC |  |
|  | Klawiatura i mysz | Klawiatura przewodowa, czarna, standardowa, w układzie QWERTY (US lub PL); Mysz przewodowa optyczna |  |
|  | Gwarancja | 1. Minimum 36 miesięcy świadczonej na miejscu (on-site). 2. Serwis realizowany przez producenta i/lub autoryzowanego partnera serwisowego producenta. Firma serwisująca musi posiadać autoryzację producenta dostarczanych komputerów na świadczenie usług serwisowych. 3. W przypadku niewywiązywania się autoryzowanego serwisu z obowiązków gwarancyjnych, producent przejmie realizację świadczeń gwarancyjnych bez dodatkowych kosztów dla Zamawiającego. 4. Wykonawca zobowiązany jest do załączenia do oferty oświadczenia producenta oferowanych komputerów, że w przypadku niewywiązywania się autoryzowanego serwisu z obowiązków gwarancyjnych, producent przejmie realizację świadczeń gwarancyjnych bez dodatkowych kosztów dla Zamawiającego.  W przypadku wymiany sprzętu dysk SSD pozostaje u Zamawiającego, a Wykonawca zapewnia nowy nośnik na własny koszt. |  |
|  | Konfiguracja | Komputery zostaną przygotowane przez Wykonawcę na podstawie zdefiniowanego obrazu systemu, z uwzględnieniem aplikacji medycznych przekazanych przez Szpital. |  |
|  | Wymagane certyfikaty | 1. Producent sprzętu:  1) PN/EN-9001 (ISO 9001) – system zarządzania jakością  2) PN/EN-14001 (ISO 14001) – system zarządzania środowiskowego  3) PN/EN-50001 (ISO 50001) – system zarządzania energią  lub równoważny w zakresie co najmniej produkcji, projektowania, rozwoju urządzeń, systemów lub rozwiązań informatycznych.  2. Komputer:  1) Certyfikat TCO, zgodny z informacjami na stronie https://tcocertified.com/product-finder  2) Certyfikat EPEAT dla krajów Unii Europejskiej, zgodnie z danymi na stronie https://epeat.net/search-computers-and-displays  3) Deklaracja zgodności CE  4) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS UE |  |

**Monitor**

Producent (marka) …………………………………..…………………..……(Należy podać)

Model ……………………………………………………..………………… (Należy podać)

|  |  |  |  |
| --- | --- | --- | --- |
| L.p. | Opis parametru | Parametr wymagany | Parametr oferowany |
| 1 | Typ wyświetlacza | LCD z podświetleniem LED |  |
| 2 | Proporcje obrazu | 16:9 |  |
| 3 | Przekątna ekranu | 21.5 cala |  |
| 5 | Typ matrycy | IPS |  |
| 6 | Powierzchnia matrycy | Powłoka antyrefleksyjna |  |
| 7 | Ekran dotykowy | Nie |  |
| 8 | Technologia podświetlania | Podświetlenie krawędzi; WLED |  |
| 12 | Rozdzielczość | 1920 x 1080 (FHD) |  |
| 14 | Jasność | min. 250 nitów |  |
| 15 | Kontrast statyczny | min. 1 000:1 |  |
| 17 | Częstotliwość odświeżania | min. 100 Hz |  |
| 22 | Kąt widzenia poziomy | min. 178 ° |  |
| 23 | Kąt widzenia pionowy | min. 178 ° |  |
| 24 | Wyświetlane kolory | min. 16,7 mln |  |
| 25 | Gniazda we/wy | Minimum: 1 x VGA  1 x HDMI  1 x DisplayPort |  |
| 26 | Wbudowane głośniki | TAK |  |
| 28 | Regulacja: wysokości/odchylenia | Tak (min. 100 mm)/ Tak (pochylenie od  min. -5° do +23°) |  |
| 29 | Zakrzywienie | Płaski |  |
| 31 | Klasa energetyczna | D |  |
| 35 | Mocowanie VESA | 100 × 100 mm |  |
| 36 | Odłączana podstawa | Tak |  |
| 37 | Waga z podstawą | max.4 kg (z podstawą) |  |
| 38 | Gwarancja | 1. Minimum 36 miesięcy świadczonej na miejscu (on-site).  2. Serwis realizowany przez producenta i/lub autoryzowanego partnera serwisowego producenta. Firma serwisująca musi posiadać autoryzację producenta dostarczanych monitorów na świadczenie usług serwisowych.,  3. W przypadku niewywiązywania się autoryzowanego serwisu z obowiązków gwarancyjnych, producent przejmie realizację świadczeń gwarancyjnych bez dodatkowych kosztów dla Zamawiającego.  4. Wykonawca zobowiązany jest do załączenia do oferty oświadczenia producenta oferowanych monitorów, że w przypadku niewywiązywania się autoryzowanego serwisu z obowiązków gwarancyjnych, producent przejmie realizację świadczeń gwarancyjnych bez dodatkowych kosztów dla Zamawiającego. |  |
| 39 | Wymagane certyfikaty | 1. Producent sprzętu:  1) PN/EN-9001 (ISO 9001) – system zarządzania jakością  2) PN/EN-14001 (ISO 14001) – system zarządzania środowiskowego  3) PN/EN-50001 (ISO 50001) – system zarządzania energią  lub równoważny w zakresie co najmniej produkcji, projektowania, rozwoju urządzeń, systemów lub rozwiązań informatycznych.  2. Monitor:  1) Certyfikat TCO, zgodny z informacjami na stronie https://tcocertified.com/product-finder  2) Certyfikat EPEAT dla krajów Unii Europejskiej, zgodnie z danymi na stronie https://epeat.net/search-computers-and-displays  3) Deklaracja zgodności CE  4) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS UE |  |
| 40 | Akcesoria w zestawie | Przewód HDMI  Kabel zasilający AC |  |

**Wdrożenie i instalacja zestawu komputerowego**

|  |  |  |  |
| --- | --- | --- | --- |
| L.p. | Opis parametru | Parametr wymagany | Parametr oferowany |
| 1 | **Usługa wdrożenia Zestawów /stacji roboczej (wymiana sprzętu)** | 1. Wstępna konfiguracja  • Uruchomienie nowej stacji, nadanie nazwy zgodnej z konwencją  • Aktualizacja systemu, konfiguracja IP i zabezpieczeń  2. Dołączenie do domeny  • Ustawienie DNS, dołączenie do Active Directory  • Automatyczne zastosowanie polityk GPO  3. Instalacja oprogramowania  •Ręczna instalacja wymaganych aplikacji z uwzględnieniem przeznaczenia stacji roboczej  4.Instalacja oprogramowania chroniącego końcówkę – Bitdefender oraz podpięcie pod konsolę zarządczą  5.Instalacja urządzeń peryferyjnych  •Konfiguracja drukarek, skanerów, monitorów i urządzeń specjalnych  •Test poprawnego działania  6. Testy i przekazanie  • Weryfikacja działania systemu, aplikacji i dostępu do zasobów  •Wstępne przekazanie stacji użytkownikowi  7. Migracja danych użytkownika (jeśli wymagane)  • Kopiowanie danych lokalnych ze starej stacji (pulpit, dokumenty, pliki robocze)  • Zachowanie ustawień aplikacji, o ile to możliwe  •Potwierdzenie poprawności przenie-sionych danych przez użytkownika |  |