

Załącznik nr 2 – formularz ofertowy techniczny

Dotyczy: postępowania**: Przyspieszenie procesów cyfryzacji w Specjalistycznym Szpitalu Wojewódzkim w Ciechanowie**

Numer pozycji/części: 1

**ZESTAWIENIE PARAMETRÓW GRANICZNYCH (ODCINAJĄCYCH)**

Przedmiot przetargu: **Pakiet I Rozbudowa systemu AV/XDR**

|  |  |  |  |
| --- | --- | --- | --- |
| **Podać producenta oraz nazwę zaoferowanego systemu** | | | |
| **L.p.** | **Element konfiguracji** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
| **1** | **Rozbudowa posiadanej licencji systemu AV/XDR** | Rozbudowa licencji posiadanego systemu antywirusowego **ESET( lub równoważny)\*** o dodatkowe licencje dla 700 stacji roboczych i serwerów wraz z licencjami XDR. Wymaga się zapewnienia 36 miesięcznego wsparcia technicznego na dotychczas posiadane licencje oraz 36 miesięcznej gwarancji oraz 36 miesięcznego wsparcia technicznego na dostarczane licencje.  \*równoważny, tj spełniający wszystkie wymagania określone poniżej. |  |
| **2** | **Administracja zdalna w chmurze** | * Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. * Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. * Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. * Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. * Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. * Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. * Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. * Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. * Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. * Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. * Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. * Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. | 1. System oferuje liczbę szablonów raportów w liczbie………………………………………………………………….   (w opz rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta) |
| **3** | **Ochrona stacji roboczych** | * Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). * Rozwiązanie musi wspierać architekturę ARM64. * Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. * Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. * Rozwiązanie musi posiadać funkcjonalność przywrócenie plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware. * Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. * Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. * Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. * Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. * Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. * Rozwiązanie musi integrować się z Intel Threat Detection Technology. * Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). * Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. * Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. * Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. * Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. * Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, * tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, * tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, * tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, * tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. * Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. * Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. * Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. * Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). * Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. * Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. * Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, * tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, * tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, * tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. * Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. * Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. * Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. * Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. * Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. * Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. * W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. | 1. Oferowane rozwiązanie posiada możliwość filtrowania adresów URL w oparciu o:…………………….. kategorii i podkategorii.   (w opz wymagane min. 140 kategorii i podkategorii.)   1. Oferowane rozwiązanie umożliwia kontrolę nośników danych\*:    * ***tylko wg producenta***    * ***wg producenta + modelu***    * ***wg producenta + modelu + wersji firmware***   \*należy zaznaczyć tylko oferowane rozwiązanie |
| **4** | **Ochrona stacji roboczych – Linux** | * Rozwiązanie musi wspierać systemy operacyjne Ubuntu Desktop, Red Hat Enterprise Linux oraz Linux Mint. * Rozwiązanie musi posiadać wsparcie dla dystrybucji 64-bitowych. * Pomoc (help) musi być dostępna co najmniej w języku polskim oraz angielskim. * Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. * Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. * Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. * Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. * Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". * Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. * Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. |  |
| **5** | **Ochrona serwera** | * Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. * Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. * Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. * Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. * Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. * Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. * Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. * Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. * Dodatkowe wymagania dla ochrony serwerów Windows: * Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. * Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). * Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. * Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. * Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. * Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. * Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.* * Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. * Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. * Dodatkowe wymagania dla ochrony serwerów Linux: * Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. * Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. * Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. * Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. |  |
| **6** | **Szyfrowanie** | * System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11. * System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). * Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. * Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. * Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO). |  |
| **7** | **Ochrona urządzeń mobilnych opartych o system Android** | * Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. * Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. * Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). * Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. * Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia, * przywrócenie urządzenie do ustawień fabrycznych, * zablokowania urządzenia, * uruchomienie sygnału dźwiękowego, * lokalizację GPS. * Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. * Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: * nazwę aplikacji, * nazwę pakietu, * kategorię sklepu Google Play, * uprawnienia aplikacji, * pochodzenie aplikacji z nieznanego źródła. |  |
| **8** | **Sandbox w chmurze** | * Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. * Rozwiązanie musi wykorzystywać do działania chmurę producenta. * Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do * chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, * dokumenty oraz inne pliki typu .jar, .reg, .msi. * Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. * Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru * przesyłanych próbek. * Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub * folderów z przesyłania. * Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. * Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. * Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. * Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. * Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. * Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: Czysty, * Podejrzany, * Bardzo podejrzany, * Szkodliwy. * W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. * W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. * Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. |  |
| **9** | **Moduł XDR** | * Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. * Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. * Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. * Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. * Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. * Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. * Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. * Serwer musi posiadać minimum 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. * Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. * Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. * Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. * Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. * W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. * W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. * Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, * urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. * Konsola administracyjna musi mieć możliwość tagowania obiektów. * Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell. | Oferujemy system posiadający:   1. Liczba wbudowanych reguł korelacyjnych:…………………………… 2. Budowa reguł korelacyjnych z wykorzystaniem AI/ML:…………….. 3. Integracje z systemami zewnętrznymi (ponad wymagane w OPZ SIEM/SOAR )\*:……………………………………………….   \*należy wymienić te systemy |

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Wymaganie ogólne** | **Wymagane parametry techniczne minimalne** | **Wymagany opis spełnienia warunku** |
|  | **Gwarancja i wsparcie techniczne** | Zamawiający wymaga zapewnienia min. 36 miesięcznej gwarancji oraz min. 36 miesięcznego nieodpłatnego wsparcia technicznego na wszystkie elementy składające się na przedmiot zamówienia.  Przez „okres gwarancji i wsparcia technicznego” Zamawiający rozumie okres, w którym Wykonawca zapewnia:  1) gwarancję jakości – obejmującą usuwanie wad sprzętu i oprogramowania w ramach gwarancji producenta lub równoważnej,  2) wsparcie techniczne – obejmujące nadzór autorski, aktualizacje, poprawki, łatki bezpieczeństwa, prawo do bezpłatnego korzystania z nowych wersji oprogramowania, zobowiązanie do ich usuwania zgłoszonych usterek i błędów oraz uzyskiwania pomocy i konsultacji dotyczących dostarczonego systemu..  Wsparcie techniczne musi być zapewnione:  – bezpośrednio przez producenta oferowanego systemu/sprzętu, lub  – przez wykonawcę, pod warunkiem posiadania autoryzacji producenta do świadczenia takiego wsparcia i zapewnienia równoważnego poziomu obsługi (SLA, aktualizacje, dostęp do baz wiedzy, poprawki).  Gwarancja sprzętowa i licencyjna musi być realizowana przez producenta (np. rejestracja urządzeń/licencji w systemie producenta).  Okres gwarancji oraz wsparcia technicznego na wszystkie elementy składające się na przedmiot zamówienia liczony jest od dnia podpisania końcowego protokołu odbioru, bez zastrzeżeń ze strony zamawiającego. |  |

|  |  |
| --- | --- |
| **L.p.** | **Kryteriu oceny ofert (K4):** |
|  | **Możliwość tworzenia dashboardów niestandardowych przez administratora ☐ NIE – brak funkcjonalności (0 pkt)\* ☐ TAK – system umożliwia tworzenie dashboardów niestandardowych (2 pkt)\***   * **należy usunąć niewłaściwe** |

|  |
| --- |
| kwalifikowany podpis elektroniczny |