

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

Zamawiający zaleca zapisanie dokumentu w formacie PDF.

Formularz asortymentowo – cenowy

Przedmiotem zamówienia jest podniesienie poziomu bezpieczeństwa teleinformatycznego w Szpitalu Ogólnym w Wysokim Mazowieckiem poprzez dostawę licencji na oprogramowanie klasy Endpoint Detection and Response w architekturze serwera.

Lp.	Przedmiot zamówienia	j.m.	Ilość	Cena netto za jednostkę miary w PLN	Stawka VAT (%)	Wartość brutto ogółem w PLN
1.	Dostawa licencji na oprogramowanie klasy Endpoint Detection and Response w architekturze serwera	komplet	1			

Oferowane oprogramowanie (podać typ i nazwę producenta):

Typ

Nazwa producenta

Zestawienie wymaganych parametrów technicznych

Przedmiot zamówienia obejmuje dostawę licencji na oprogramowanie klasy Endpoint Detection and Response w architekturze serwera wraz z usługą wsparcia przy wdrożeniu zgodnie z poniżej określonymi wymaganiami.

Lp.	Wymagane parametry techniczne (wartości minimalne wymagane)	Oferowane parametry
Wymagania ogólne		
1.	Zamawiający wymaga dostarczenia 250 licencji oprogramowania antywirusowego wraz z modułem EDR na okres 60 miesięcy o parametrach określonych w OPZ.	
2.	Zamawiający wymaga pomocy zdalnej przy wdrożeniu proponowanego rozwiązania przez certyfikowanego inżyniera tego rozwiązania.	
3.	Zamawiający wymaga aby oferent wraz z oprogramowaniem dostarczył cztery vouchery na szkolenia zdalne zorganizowane przez autoryzowany przez producenta ośrodek szkoleniowy. Szkolenie minimum trzy dniowe z obsługi konsoli centralnego zarządzania oraz modułu EDR.	
4.	Rozwiązanie musi posiadać wsparcie polskojęzyczne na okres minimum 60 miesięcy, obejmujące w szczególności: 1) Dostęp do poprawek i uaktualnień Oprogramowania 2) Dostęp do polskojęzycznego wsparcia drogą telefoniczną, mailową, bądź przez dedykowany portal. Wsparcie również obejmuje prawo do aktualizacji	
5.	Rozwiązanie musi wspierać systemy operacyjne Windows 7/8/8.1/10/11, przy czym najnowsza wersja systemu musi wspierać przynajmniej systemy Windows 10 oraz Windows 11.	
6.	Rozwiązanie musi zapewniać wsparcie dla 32- i 64-bitowej wersji systemu Windows.	
7.	Wersja systemu na stacjach roboczych Windows dostępna w języku polskim.	
8.	Wsparcie techniczne do systemu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta systemu.	
Wymagania w zakresie zarządzania zdalnego		
9.	1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server (od 2012) oraz na systemach Linux. 2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. 3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. 4. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. 5. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 6. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. 7. Rozwiązanie musi zapewniać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby	

	<p>certykatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.</p> <p>8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.</p> <p>9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).</p> <p>10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.</p> <p>11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.</p> <p>12. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.</p> <p>13. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.</p> <p>14. 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.</p> <p>15. Rozwiązanie musi zapewniać korzystanie z minimum 80 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.</p> <p>16. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.</p> <p>17. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.</p>	
Wymagania w zakresie ochrony stacji roboczych		
10.	<p>1. Rozwiązanie musi wspierać systemy operacyjne Windows 7/8/8.1/10/11.</p> <p>2. Rozwiązanie musi wspierać architekturę ARM64.</p> <p>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.</p> <p>5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.</p> <p>6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.</p> <p>7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.</p> <p>8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.</p> <p>9. 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.</p> <p>10. 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).</p> <p>11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.</p> <p>12. 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.</p> <p>13. 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.</p> <p>14. 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.</p> <p>15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:</p> <ul style="list-style-type: none"> • 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. <p>16. 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</p>	

	<p>systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.</p> <p>17. 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.</p> <p>18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).</p> <p>20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>21. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego MS Outlook.</p> <p>22. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:</p> <ul style="list-style-type: none"> • 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. <p>23. Rozwiązanie musi być wyposażone w moduł bezpiecznej przeglądarki.</p> <p>24. Przeglądarka musi automatycznie szfrować wszelkie dane wprowadzane przez Użytkownika.</p> <p>25. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.</p> <p>26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.</p> <p>27. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.</p> <p>28. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.</p> <p>29. 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.</p>	
Wymagania w zakresie ochrony serwerów		
11.	<p>1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux.</p> <p>2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.</p> <p>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.</p> <p>5. 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.</p> <p>6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.</p> <p>8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p>Dodatkowe wymagania dla ochrony serwerów Windows:</p> <p>9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.</p> <p>10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).</p> <p>11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.</p> <p>12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>13. 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.</p> <p>14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.</p> <p>15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.</p> <p>16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.</p> <p>17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.</p> <p>Dodatkowe wymagania dla ochrony serwerów Linux:</p> <p>18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.</p> <p>19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.</p> <p>20. 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 zawieszonoego mikro-serwisu.</p>	
Wymagania w zakresie ochrony urządzeń mobilnych opartych o system Android		

12.	<ol style="list-style-type: none"> 1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: <ol style="list-style-type: none"> a) nazwę aplikacji, b) nazwę pakietu, c) kategorię sklepu Google Play, d) uprawnienia aplikacji, e) pochodzenie aplikacji z nieznanego źródła. 	
Szyfrowanie		
13.	<ol style="list-style-type: none"> 1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. 	
Endpoint Detection and Response		
14.	<ol style="list-style-type: none"> 1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta. 2. Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta. 3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica”. 6. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia. 7. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Rozwiązanie musi umożliwić administratorowi weryfikację 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. 9. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz ich zablokowania. 10. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli. 	

Kolumna „Oferowane parametry” musi być w całości wypełniona. Wykonawca zobowiązany jest do podania oferowanych parametrów w następujących jednostkach:

TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę

NIE – wykonawca nie spełnia konkretnego parametru

Wartości określone w kolumnie „Wymagane parametry techniczne (wartości minimalne wymagane)” należy traktować jako niezbędne minimum, którego niespełnienie będzie skutkowało odrzuceniem oferty.