Załącznik nr 2b do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

**Zadanie nr 2 - Oprogramowanie antywirusowe/EDR oraz centralna konsola zarządzająca WEB**

**Przedmiot zamówienia:**

1. Przedmiot zamówienia obejmuje dostarczenie i kompletne wdrożenie **oprogramowania antywirusowego/EDR - Endpoint Detection and Response** oraz konsolą zarządzającą WEB - wraz z niezbędnymi licencjami, świadczeniem usługi gwarancji dla wdrażanego systemu oraz przeszkoleniem personelu administrującego systemem.
2. Zamówienie nie zostało podzielone na części. Zamówienie dotyczy dostawy jednego zintegrowanego systemu wraz z wdrożeniem - jego zakres wymaga, aby wykonywane było ono kompleksowo przez jednego Wykonawcę z uwagi na możliwość wystąpienia niebezpieczeństwa wydłużenia terminu jego realizacji oraz przeciągania się procedur naprawczych w wypadku wystąpienia konieczności usunięcia awarii.

**Wymagania ogólne:**

1. Całość dostarczanego oprogramowania musi pochodzić z legalnego kanału dystrybucji, zapewniającego min. ważną gwarancję w Polsce, objęcie pomocą techniczną i serwisową oraz posiadanie ważnej licencji na oprogramowanie.
2. Całość dostarczanego rozwiązania, tzn. każde z dostarczonych komponentów, musi być nowe, wcześniej nieużywane / instalowane , rok produkcji nie starszy niż 2022.
3. Całość dostarczanego rozwiązania, tzn. każde z dostarczonych komponentów, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 36 miesięczną gwarancją jeśli w opisie parametrów nie wskazano inaczej.
4. Do każdego komponentu musi być dostarczony komplet standardowej dokumentacji dla użytkownika
5. Oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji.
6. Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:
7. Posiadane środowisko serwerowe,
8. Posiadaną konfigurację sieci,
9. Posiadaną konfiguracją baz danych i backupów,
10. Konfigurację stacji roboczych.

**Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z wdrożeniem oprogramowania:**

1. Wykonanie Planu Projektu dostarczanego rozwiązania, który będzie składał się co najmniej z następujących elementów:
   1. Planowana konfiguracja środowiska poszczególnych elementów w tym logiczną konfiguracją miejsc, zaprojektowanie kompleksowego systemu ochrony antywirusowej opartego na funkcjach wdrażanego oprogramowania z uwzględnieniem specyfiki całego projektu,
   2. Harmonogram prac - szczegółowy terminarz realizacji przedmiotu Umowy wraz z podziałem na Etapy przygotowany przez Wykonawcę w terminie 3dni roboczych od zawarcia umowy.

Plan Projektu musi zostać wykonany po wcześniejszej analizie środowiska wykonanej przez Wykonawcę oraz musi zostać zaakceptowany przez Zamawiającego.

1. Instalacja oraz kompletne uruchomienie i konfiguracja systemu antywirusowego/EDR (stacje końcowe oraz konsola zarządzająca web).
2. Testy rozwiązania.
3. Instruktaż dla administratorów prezentujący sposób zarządzania środowiskiem. Wykonawca po zainstalowaniu i skonfigurowaniu oprogramowania będzie miał obowiązek przeprowadzenia instruktażu dla administratorów Zamawiającego w zakresie konfiguracji i zarządzania
4. Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej i oprogramowania standardowego, która będzie składała się co najmniej z następujących elementów:
   1. Komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku,
   2. Dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim lub angielskim
5. Szczegóły dotyczące instalacji i uruchomienia poszczególnych komponentów zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
6. Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.

**Opis minimalnych wymagań na oprogramowanie antywirusowe /EDR oraz centralną konsolę zarządzająca**

Zamawiający wymaga, aby Wykonawca spełniał wymagania w zakresie:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE - podaje**  **Wykonawca**  **Nazwa oferowanych produktów**  **Wymogi dotyczące opisu oferowanych parametrów:**  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 |
| 1 | Program antywirusowy powinien mieć obsługę w języku polskim. | TAK |  |
| 2 | Oprogramowanie powinno obsługiwać systemy operacyjne:  **Windows ( workstation edition )**  Windows XP (SP3) x86  Windows 7 SP1 x86  Windows 7 SP1 x64  Windows 8 x86  Windows 8 x64  Windows 8.1 x86  Windows 8.1 x64  Windows 10 x86  Windows 10 x64  Windows 11 x64  **Windows (wersja serwerowa)**  Windows Server 2008 SP2  Windows Server 2008 R2  Windows Server 2012  Windows Server 2012 R2  Windows Server 2016  Windows Server 2019  **Android**  minimum od wersji 8.x wzwyż  **iOS**  minimum od wersji 8.x wzwyż  **macOS**  minimum od wersji 10.12.x wzwyż | TAK |  |
| 3 | Rozwiązanie powinno działać na komputerach wyposażonych w:  - 1,2 GHz procesor  - 512 MB dostępnej pamięci RAM  - 1 GB miejsca na dysku twardym dla wersji 32-bitowej i 64-bitowej | TAK |  |
| 4 | Instalacja oprogramowania musi być możliwa poprzez pobranie paczki instalacyjnej, poprzez sieć, za pomocą dystrybucji przez pocztę e-mail, poprzez Active Directory, grupy robocze. | TAK |  |
| 5 | Program antywirusowy oprócz automatycznej aktualizacji bazy danych wirusów  powinien posiadać możliwość zaktualizowania baz danych wirusów ręcznie, nawet jeśli komputer nie będzie miał dostępu do Internetu. | TAK |  |
| 6 | Program antywirusowy musi posiadać możliwość skanowania wybranych plików, folderów/katalogów (również plików skompresowanych), całych dysków (w tym sieciowych) czy partycji a także skanowania dowolnego zasobu podłączonego do stacji roboczej np.: dyski zewnętrzne, pamięci USB | TAK |  |
| 7 | Program antywirusowy musi posiadać moduł antywirusowy chroniący w czasie rzeczywistym. | TAK |  |
| 8 | Program antywirusowy musi posiadać moduł sprawdzający reputację plików w chmurze. | TAK |  |
| 9 | Program antywirusowy musi posiadać moduł automatycznej piaskownicy (auto sandbox), odizolowanego środowiska wirtualnego, w którym zasoby są emulowane dla obiektów w nim umieszczonych. Cały proces izolacji dzięki temu modułowi musi odbywać się lokalnie, na stacji roboczej. Całe środowisko wirtualne musi być odwzorowaniem 1:1 z systemem operacyjnym. Użytkownik powinien móc pracować w zwirtualizowanym środowisku, bez możliwości zapisu na stacji poza środowiskiem wirtualnym. | TAK |  |
| 10 | Program antywirusowy musi posiadać możliwość uruchomienia dowolnego pliku/programu w automatycznej piaskownicy (auto sandbox) również na żądanie użytkownika (manualnie) oraz musi chronić stacje poprzez uruchamianie nieznanych oraz niebezpiecznych załączników poczty w środowisku wirtualnym na stacji w lokalnej i automatycznej piaskownicy (auto-sandbox). | TAK |  |
| 11 | Program antywirusowy musi posiadać moduł HIPS (Host Intrusion Prevention System – ochrona antywłamaniowa). | TAK |  |
| 12 | Podczas pracy komputera program antywirusowy musi automatycznie skanować:  -pliki uruchamiane, otwierane,  -pliki kopiowane lub przenoszone,  -pliki tworzone,  -wszystkie pliki pobierane z Internetu, również po protokole HTTP/HTTPS. | TAK |  |
| 13 | W przypadku wykrycia wirusa program musi posiadać możliwość automatycznego  poddawania kwarantannie podejrzanych obiektów oraz opcję przywrócenia z kwarantanny usuniętych obiektów. | TAK |  |
| 14 | Program antywirusowy musi posiadać funkcję dodawania wyjątków do modułu antywirusowego, automatycznej piaskownicy (auto sandbox) czy modułu HIPS | TAK |  |
| 15 | Program antywirusowy powinien posiadać funkcję:  - definiowania filtrów URL umożliwiających blokowanie konkretnych stron internetowych  - tworzenia list zaufanych procesów  - tworzenia list zaufanych plików | TAK |  |
| 16 | Program antywirusowy musi posiadać dwukierunkowy konfigurowalny z konsoli web firewall z możliwością tworzenia polityk globalnych i z podziałem na aplikacje. | TAK |  |
| 17 | Program antywirusowy powinien umożliwiać konfigurację różnych polityk (ustawień globalnych dla stworzonych grup stacji końcowych) w celu szybkiej implementacji ustawień bezpieczeństwa dla wielu urządzeń jednocześnie. | TAK |  |
| 18 | Program antywirusowy musi posiadać dodatkowe narzędzie do skanowania systemu oraz narzędzie do analizowania bezpieczeństwa procesów | TAK |  |
| 19 | Oprogramowanie powinno mieć możliwość przeglądania obciążenia procesów oraz zawartości dysków na stacjach końcowych i serwerach z poziomu konsoli zarządzającej web | TAK |  |
| 20 | Program antywirusowy powinien umożliwiać zmianę ustawień priorytetu skanowania | TAK |  |
| 21 | Program antywirusowy powinien umożliwiać uruchomienie skanowania pamięci komputera po uruchomieniu | TAK |  |
| 22 | Program antywirusowy i konsola zarządzająca powinny umożliwiać tworzenie wyjątków ze skanowania folderów / plików | TAK |  |
| 23 | Program antywirusowy posiada zintegrowaną funkcję blokowania urządzeń  zewnętrznych / przenośnych przed odczytem, edycją i zapisem plików w tym samym czasie. | TAK |  |
| 24 | Program antywirusowy posiada zintegrowaną funkcję blokowania jedynie zapisu plików na urządzeniach zewnętrznych / przenośnych | TAK |  |
| 25 | Program antywirusowy powinien posiadać możliwość importu oraz eksportu ustawień. | TAK |  |
| 26 | Program antywirusowy powinien posiadać zintegrowaną funkcjonalność skanowania plików pod kątem danych wrażliwych (DLP). | TAK |  |
| 27 | Program antywirusowy musi posiadać zintegrowane środowisko, dzięki któremu możemy bezpiecznie działać w wirtualnym systemie nawet na zainfekowanej stacji. Środowisko to musi być odizolowanie od reszty systemu operacyjnego i mieć możliwość uruchomienia  takich sesji bez wprowadzonych wcześniejszych zmian przez użytkownika w tym  narzędziu (czyste środowisko). Ma również pozwalać na bezpieczniejsze wykonywanie  przelewów bankowych, bez obaw, że system operacyjny, na którym działa dany komputer nie został uprzednio zmodyfikowany i byłby w stanie zagrozić utracie np. danych logowania do kont bankowych. | TAK |  |
| 28 | Program antywirusowy bezpośrednio z poziomu interfejsu musi umożliwiać użytkownikowi wysłanie podejrzanego obiektu (np. pliku) do producenta oprogramowania antywirusowego w celu jego analizy. | TAK |  |
| 29 | Program antywirusowy powinien posiadać możliwość aktualizowania baz danych  antywirusowych ręcznie, nawet jeśli komputer nie będzie miał dostępu do Internetu. | TAK |  |
| 30 | Program antywirusowy powinien posiadać możliwość zablokowania dostępu do ustawień konfiguracyjnych przy pomocy hasła administratora na oraz hasła skonfigurowanego w konsoli zarządzającej. | TAK |  |
| 31 | Konsola zarządzająca web administratora powinna znajdować się w chmurze producenta znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu. Konsola nie powinna generować dodatkowych opłat/ kosztów | TAK |  |
| 32 | Konsola zarządzająca web musi posiadać możliwość wyboru języka polskiego, jako język całego interfejsu. | TAK |  |
| 33 | Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po  protokole HTTPS z certyfikatem. | TAK |  |
| 34 | Konsola web musi posiadać możliwość logowania użytkownika przy pomocy uwierzytelniania dwuskładnikowego (2FA). Logowanie się z użyciem metod uwierzytelniania dwuskładnikowego musi się odbywać na minimum dwa sposoby. | TAK |  |
| 35 | Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie oraz posiadać funkcję hierarchii i delegacji uprawnień administratorów zarówno dla grup jak i poszczególnych obiektów | TAK |  |
| 36 | Administrator z poziomu konsoli zarządzającej web musi mieć możliwość zarządzania kluczami licencyjnymi. | TAK |  |
| 37 | Administrator musi mieć możliwość przeniesienia z poziomu konsoli web aktywnej licencji na inną stację roboczą, urządzenia mobilne lub serwer bez utraty ważności licencji. | TAK |  |
| 38 | Konsola zarządzająca web musi posiadać możliwość zablokowania dostępu do ustawień programu na stacjach końcowych dla użytkowników nieposiadających uprawnień administracyjnych. | TAK |  |
| 39 | Konsola zarządzająca web musi posiadać funkcję, która uniemożliwia użytkownikowi komputera wyłączenie działania monitora antywirusowego i innych składników ochrony, jeżeli nie posiada on uprawnień administracyjnych. | TAK |  |
| 40 | Konsola zarządzająca web musi umożliwiać zarządzanie stacjami roboczymi oraz serwerami  i urządzeniami mobilnymi | TAK |  |
| 41 | Konsola zarządzająca web musi posiadać możliwość tworzenia grup i polityk dla stacji. | TAK |  |
| 42 | Konsola zarządzająca web powinna oferować predefiniowane domyślne ustawienia  rekomendowanych polityk (ustawień) dla stacji końcowych. | TAK |  |
| 43 | Konsola zarządzająca web musi posiadać funkcję planowania zadań, w tym planowania terminów automatycznego skanowania oraz umożliwiać zmianę ustawień priorytetu skanowania. | TAK |  |
| 44 | Rozwiązanie musi umożliwiać bezpośrednio  z konsoli zarządzającej web uruchamianie procedur (skryptów) serwisowych na stacjach klienckich  o minimalnych, następujących funkcjonalnościach:  -Czyszczenie plików tymczasowych  -Czyszczenie i sprawdzanie dysku  -Usuwanie błędów dysku  -Defragmentowanie dysku  -Czyszczenie kolejki drukarki  -Czyszczenie pamięci podręcznej DNS  -Czyszczenie kosza  -Sprawdzanie błędów na dysku twardym S.M.A.R.T. Check  -Włączenie szyfrowania dysku funkcją Bitlocker dla systemu Windows | TAK |  |
| 45 | Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich  zdalnie z konsoli na stacjach. | TAK |  |
| 46 | Konsola zarządzająca web musi posiadać narzędzie do wykonania instalacji oprogramowania na stacjach poprzez zakresy adresów sieciowych IP, grupy robocze lub Active Directory. | TAK |  |
| 47 | Konsola zarządzająca web musi zawierać zintegrowaną funkcjonalność menadżera  aktualizacji, który umożliwia zarządzanie pobieraniem i instalacją aktualizacji (updatów) systemu Windows, Java, Adobe i innego oprogramowania firm trzecich na stacjach końcowych | TAK |  |
| 48 | Producent powinien posiadać własne bezpieczne i sprawdzone repozytorium aplikacji do celów aktualizacji oprogramowania firm trzecich minimum 30 producentów. | TAK |  |
| 49 | Konsola zarządzająca web musi mieć możliwość zdefiniowana zalecanych aplikacji, które może pobrać użytkownik urządzeń mobilnych. | TAK |  |
| 50 | Konsola zarządzająca web umożliwia usuwanie aplikacji z urządzeń mobilnych. | TAK |  |
| 51 | Konsola zarządzająca web musi umożliwiać wyczyszczenie lub zablokowanie zdalne urządzenia mobilnego. | TAK |  |
| 52 | Konsola web posiada możliwość geolokalizacji z aktualną mapą urządzeń mobilnych wyposażonych w moduł GPS. | TAK |  |
| 53 | Konsola zarządzająca web musi posiadać możliwość śledzenia i analizy historii zagrożeń na wybranych komputerach. | TAK |  |
| 54 | Konsola zarządzająca web umożliwia wysyłanie automatycznych powiadomień o określonych zdarzeniach oraz raportów na wskazane adresy e-mail. | TAK |  |
| 55 | Konsola zarządzająca web musi posiadać moduł zapobiegania wyciekowi danych DLP  z możliwością włączenia skanowania plików  w wybranych lokalizacjach na komputerach pod kątem znajdujących się w nich danych wrażliwych przez zdefiniowane wzory z możliwością dodawania własnych reguł DLP oraz powinna  umożliwiać zapisywanie i sprawdzanie logów z tej czynności. | TAK |  |
| 56 | Konsola zarządzająca web musi posiadać możliwość uruchamiania komputerów zdalnie (WakeOnLAN), ponownego uruchomienia oraz wyłączania urządzeń z systemem Windows. | TAK |  |
| 57 | Konsola zarządzająca web musi posiadać zintegrowany moduł umożliwiający nawiązanie zabezpieczonego zdalnego połączenia z graficznym pulpitem zdalnym przez dedykowaną aplikację dla komputerów i serwerów znajdujących się w sieci LAN i poza nią, bez potrzeby tworzenia tuneli VPN każdej stacji komputera lub serwera. | TAK |  |
| 58 | Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do  użytkowania przez administratora w określonym przez niego czasie oraz możliwość poinformowania użytkowania przez administratora w celu odpytania go o zgodę na połączenie. | TAK |  |
| 59 | Konsola zarządzająca web musi posiadać funkcję tworzenia raportów o stacjach zarządzanych  w konsoli. | TAK |  |
| 60 | Konsola zarządzająca web musi posiadać funkcję gromadzenia logów wykonywanych czynności przez administratorów konsoli. | TAK |  |
| 61 | Konsola zarządzająca web musi posiadać moduł uruchamiania procedur (skrypty) zdefiniowanych przez producenta oraz przez użytkownika. | TAK |  |
| 62 | Konsola zarządzająca web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z stacji klienckiej. | TAK |  |
| 63 | Rozwiązanie musi posiadać dedykowaną aplikację lub stronę internetową do zgłoszeń serwisowych bez konieczności instalacji ochrony antywirusowej. System powinien mieć możliwość przyjmować zgłoszenia serwisowe bezpośrednio z aplikacji na stacji, pocztą email oraz poprzez dedykowaną stronę dla działu serwisu. | TAK |  |
| 64 | System musi umożliwiać przydzielanie zgłoszenia serwisowego dla konkretnego  administratora oraz powinien mieć zintegrowany system diagnozy stacji oraz możliwość podłączenia zdalnego. | TAK |  |
| 65 | Konsola zarządzająca web musi posiadać zintegrowany moduł z możliwością zaplanowania prac u użytkownika. | TAK |  |
| 66 | Konsola zarządzająca web zintegrowana  z wszystkimi modułami i funkcjami musi  umożliwić przeprowadzenia skanowania sieci firmowej (również za pomocą protokołu SNMP) w celu przeprowadzenia audytu urządzeń działających w tej sieci. | TAK |  |
| 68 | Ilość licencji - 150 szt. | TAK |  |
| 69 | Licencje wraz z gwarancją producenta na okres 60 miesięcy | TAK |  |
| 70 | Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu. | TAK |  |

......................dnia ...................... 2022 r. …………........................................

podpis osoby/osób uprawnionych

do reprezentacji Wykonawcy

lub pełnomocnika1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1 kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty