Załącznik nr 1 do Zapytania

Opis przedmiotu zamówienia
Przedłużenie licencji oprogramowania antywirusowego ESET PROTECT Complete
lub dostawa innego równoważnego systemu antywirusowego dla Ministerstwa Zdrowia

I. Przedmiotem zamówienia jest:

1.1. Przedłużenie 1 800 licencji oprogramowania antywirusowego ESET PROTECT Complete ze wsparciem producenta na okres 12 miesięcy lub dostawa innego równoważnego systemu antywirusowego, ze wsparciem producenta na okres 12 miesięcy.

1.2. Zamawiający posiada licencje ESET PROTECT Complete, których ważność wygasa 2023-11-13.

1.3. Udzielone licencje na oprogramowanie antywirusowe musi umożliwiać co najmniej:

1. Ochronić stacje robocze i serwery w liczbie: **1000**
2. Ochronić urządzeń mobilnych w liczbie: **800**

1.4. W przypadku zaoferowania oprogramowania (systemu) równoważnego, Wykonawca musi, w terminie 4 dni roboczych od zawarcia umowy, wykonać następujące działania:

1. Dostarczenie wszystkich niezbędnych licencji (ze wsparciem producenta na min. 12 miesiące na oprogramowanie - również firm trzecich) wymaganych do wdrożenia i uruchomienia systemu.
2. Przeprowadzenie procesu deinstalacji obecnie używanego przez Zamawiającego oprogramowania antywirusowego ESET oraz zainstalowanie i skonfigurowanie oprogramowania równoważnego na wskazanych przez Zamawiającego urządzeniach:
   a) stacjach roboczych, laptopach (Microsoft Windows 10/11),
   b) serwerach (Microsoft Windows Server 2008R2/2012/2012 R2/2016/2019),
   c) urządzeniach mobilnych z systemem Android i Apple iOS.
3. Wykonanie pełnego wdrożenia oprogramowania równoważnego w produkcyjnym systemie pocztowym Zamawiającego na jednym klastrze serwera pocztowego Microsoft Exchange.
4. Wykonanie analizy przedwdrożeniowej środowiska Zamawiającego oraz dostarczenie projektu technicznego systemu równoważonego, obejmującego specyfikację techniczną określającą wymogi na infrastrukturę teleinformatyczną / środowisko wirtualne dla systemu, m.in:
   a) szczegółową specyfikację sprzętową serwerów/urządzeń sieciowych,
   b) ilość maszyn wirtualnych, procesorów wirtualnych, pamięci RAM, przestrzeni dyskowej,
   c) wymagane parametry łącza,
   d) wymagane parametry systemu operacyjnego,
   e) wymagania wirtualizacji (platforma VMware).

oraz szczegółowy opis zakresu prac, ich sekwencji oraz wskazania, kto ma je realizować

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

(Zamawiający, Wykonawca) niezbędnych do wdrożenia i konfiguracji systemu równoważnego.

5. Wykonanie dokumentacji powykonawczej systemu równoważnego zgodnie z wymogami Zamawiającego, zawierającej m. in. informacje o szczegółach wykonanych prac wdrożeniowych, instrukcje instalacji, konfiguracji i użytkowania wdrożonego oprogramowania równoważnego.
6. Przeprowadzenie warsztatów z instalacji, konfiguracji i zarządzania wdrożonym systemem równoważnym dla nie więcej niż 5 osób wskazanych przez Zamawiającego:
   a) warsztaty zostaną przeprowadzone w siedzibie Zamawiającego w dni robocze tj. od poniedziałku do piątku w godzinach od 8.00 do 16.00,
   b) warsztaty zostaną przeprowadzone na koszt Wykonawcy,
   c) warsztaty muszą obejmować wykład teoretyczny oraz ćwiczenia praktyczne,
   d) Wykonawca przygotuje materiały szkoleniowe w wersji papierowej lub wersji elektronicznej w ilości odpowiadającej liczbie szkolonych osób,
   e) Wykonawca przygotuje i wyda uczestnikom certyfikaty potwierdzające udział w szkoleniu, natomiast ich kopie przekaże Zamawiającemu.
7. Świadczenie wsparcia technicznego do oprogramowania równoważnego w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta oprogramowania przez okres obowiązywania Umowy.

1.5. W przypadku gdy Wykonawca zaoferuje wdrożenie oprogramowania równoważonego, Zamawiający rekomenduje aby Wykonawca dysponował zespołem, w którego skład wejdą konsultanci - co najmniej 3 osoby, z których każda:

- posiada minimum 4-letnie doświadczenie w zakresie wdrażania lub/i zarządzania zaoferowanym systemem antywirusowym oraz
- brała udział w przynajmniej 2 wdrożeniach zaoferowanego systemu antywirusowego w charakterze konsultanta oraz
- jako zespół posiadają wiedzę i doświadczenie w zakresie rozwiązań firmy Microsoft: Windows Server 2012/2012R2/ 2016/2019,
- co najmniej jedna z nich posiada doświadczenie w zakresie znajomości zagadnień sieciowych.

1.6. Zamawiający wymaga w ofercie wykazania (oświadczenie), że oferowane licencje oprogramowania równoważnego spełniają wymagania (w tym parametry) określone w pkt. II OPZ, w celu potwierdzenia równoważności funkcjonalności zaoferowanego rozwiązania z wymogami określonymi w OPZ.

II. Oprogramowanie równoważne musi spełniać poniższe wymagania:

II.1. Wymagania ogólne.

1. Pełne wsparcie dla systemu Windows 10/11.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja systemu dla stacjach roboczych Windows dostępna zarówno w języku polskim jak i angielskim.
4. Instalator musi umożliwiać wybór wersji językowej systemu, przed rozpoczęciem procesu instalacji.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

5. Pomoc w systemie (help) i dokumentacja do systemu dostępna w języku polskim.
6. Wsparcie techniczne do systemu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta systemu.

II.2. Wymagania w zakresie zarządzania zdalnego.

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2008R2, 2012, 2012 R2, 2016,2019 oraz systemach Linux.
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
4. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL.
5. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
6. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
7. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
8. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
9. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
10. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
11. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
12. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
13. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
14. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci z wyłączeniem urządzeń mobilnych.
15. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci - serwer pośredniczący (proxy) lub serwer centralny.
16. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
17. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.
18. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
19. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

20. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
21. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
22. Centralna administracja do zarządzania programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows musi być realizowana w modelu on-premise Zamawiającego.
23. Centralna administracja do zarządzania programami zabezpieczającymi na urządzeniach mobilnych z systemem Android / Apple iOS musi być realizowana w modelu chmury producenta.
24. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
25. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
26. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
27. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
28. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
29. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
30. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
31. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 - bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.
32. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play / Apple Store.
33. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
34. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
35. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
36. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
37. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

zintegrowanego z grupą z usługi Active Directory.

38. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
39. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
40. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
41. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
42. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
43. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
44. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
45. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
46. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
47. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
48. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
49. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
50. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich.
51. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
52. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
53. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.
54. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
55. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

operacyjnego, itp.

56. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
57. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
58. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
59. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś" dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
60. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
61. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
62. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
63. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
64. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
65. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.
66. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.
67. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
68. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.
69. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
70. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
71. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.
72. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
73. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

monitorującego.

74. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
75. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
76. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
77. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
78. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
79. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
80. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
81. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
82. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
83. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia.
84. Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań.

II.3. Wymagania w zakresie ochrony antywirusowej i antyspyware.

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak - nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania,

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).

9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Skanowanie plików spakowanych i skompresowanych.
13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
14. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „*" zastępującego dowolne znaki w ścieżce.
15. Administrator ma mieć możliwość dodania wykluczenia po tzw. HASH'u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
16. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
17. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu.
18. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
19. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie systemu.
20. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
21. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
22. Wbudowany konektor dla programów MS Outlook (funkcje systemu dostępne są bezpośrednio z menu programu pocztowego).
23. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook.
24. Skanowanie i oczyszczanie poczty przychodzącej P0P3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
25. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
26. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
27. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
28. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. System musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

29. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
30. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
31. System ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, P0P3S, IMAPS.
32. System ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
33. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
34. Administrator ma mieć możliwość zdefiniowania portów TCP, na których system będzie realizował proces skanowania ruchu szyfrowanego.
35. System musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
36. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
37. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
38. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
39. Wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej i/lub obu metod jednocześnie.
40. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z systemu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
41. Do wysłania próbki zagrożenia do laboratorium producenta system nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
42. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
43. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
44. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
45. Możliwość zabezpieczenia konfiguracji systemu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

hasła.

46. Możliwość zabezpieczenia systemu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji system musi pytać o hasło.
47. Hasło do zabezpieczenia konfiguracji systemu oraz deinstalacji musi być takie samo.
48. System ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji - poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
49. System ma mieć możliwość definiowania typu aktualizacji systemu operacyjnego o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykłe oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
50. Po instalacji systemu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
53. System ma umożliwiać 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 , urządzeń przenośnych oraz urządzeń dowolnego typu.
54. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
55. System musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.
56. System ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.
57. System ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od załogowanego użytkownika.
58. W momencie podłączenia zewnętrznego nośnika system musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
59. Użytkownik ma posiadać możliwość takiej konfiguracji systemu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
60. System musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
61. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

a) tryb automatyczny z regułami, gdzie system automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
b) tryb interaktywny, w którym to system pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie operacyjnym,
c) tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
d) tryb uczenia się, w którym system uczy się aktywności systemu operacyjnego i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu system musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
e) tryb inteligentny, w którym system będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

62. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
63. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
64. System musi posiadać zaawansowany skaner pamięci.
65. System musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
66. System musi być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
67. Funkcja generująca taki log musi oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla systemu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
68. System musi oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
69. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
70. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
71. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji systemu zgłosi posiadanie nieaktualnej bazy sygnatur.
72. System musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
73. System musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
74. System musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
75. System musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

76. W momencie wykrycia trybu pełno ekranowego system ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań oprogramowania.
77. Użytkownik ma mieć możliwość skonfigurowania systemu tak aby automatycznie włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
78. System ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
79. System musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
80. System musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji offline.
81. W trakcie instalacji system ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych.
82. W systemie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
83. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień systemu na stacji końcowej.
84. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym automatycznie zostają przywrócone dotychczasowe ustawienia.
85. Administrator ma możliwość wstrzymania polityk na 10 min, 30 min, 1 godzinę i 4 godziny
86. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
87. System musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki.
88. System musi posiadać funkcję ręcznej aktualizacji własnych komponentów oprogramowania.
89. Możliwość zmiany konfiguracji systemu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
90. System musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji.
91. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
92. System musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
93. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

94. System musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
95. System musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania wybranej ścieżki, w której znajdują się pliki i foldery, które mają zostać wyłączone ze skanowania.
96. System musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania obiektu co najmniej w oparciu o nazwę zagrożenia oraz jego lokalizację.
97. System musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania pliku, wskazując sumę kontrolną pliku (jego HASH).
98. System musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść"
99. System musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.
100. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
101. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
102. System ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
103. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.

II.4. Wymagania w zakresie ochrony poczty MS Exchange.

1. System musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019
2. System musi posiadać natywny 32 lub 64-bitowy skaner antywirusowy instalowany w zależności od systemu operacyjnego.
3. System musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. System musi umożliwiać Administratorowi na etapie instalacji wybór komponentów jakie mają być zainstalowane.
5. System musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
6. System ma zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
7. System musi mieć możliwość zdefiniowania ilości wątków skanujących w celu optymalizacji pracy serwera. Liczba wątków skanowania musi wynosić od 1 do 21.
8. W przypadku wykrycia oprogramowania złośliwego system musi umożliwić usunięcie wiadomości/załącznika, podmianę załącznika na czysty plik zawierający jedynie informację o infekcji.
9. Możliwość tworzenia różnych reguł blokowania wiadomości, w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.

10. System musi posiadać możliwość tworzenia białych i czarnych list domen/adresów IP, adresów e-mail.
11. System musi posiadać możliwość akceptacji białych list stworzonych na poziomie serwera MS Exchange.
12. System musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
13. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBLoraz mechanizm reputacji poczty.
14. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL z których będzie korzystać system.
15. System ma posiadać mechanizm greylisting (szara lista).
16. System musi posiadać możliwość tworzenia wyjątków dla mechanizmu szarej listy.
17. System ma posiadać możliwość stworzenia kwarantanny poczty per użytkownik.
18. Kwarantanna musi być dostępna dla użytkownika końcowego za pośrednictwem przeglądarki WWW.
19. Pliki zapisywane w katalogu kwarantanny powinny być szyfrowane.
20. Użytkownik końcowy musi posiadać możliwość zarządzania wiadomościami znajdującymi się w kwarantannie w tym co najmniej, mieć możliwość uwolnienia wiadomości z kwarantanny, jej usunięcia lub pozostawienia w kwarantannie.
21. Administrator musi mieć możliwość wglądu w globalną kwarantannę z poziomu interfejsu aplikacji oraz przeglądarki WWW.
22. System musi umożliwiać przesyłanie raportów dotyczących plików poddanych kwarantannie na wskazany adres e-mail.
23. System musi umożliwiać pominięcie reguł kwarantanny podczas zwolnienia wiadomości e-mail w środowisku klastrowym.

II.5. Pozostałe wymagania bezpieczeństwa.

1. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików serwera "na żądanie" lub według harmonogramu.
2. Wykrywanie niebezpiecznych aplikacji typu Adware, Spyware, Dialer itp.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wbudowana technologia ochrony przed atakami typu backscatter.
5. System musi umożliwiać zaawansowane skanowanie przy użyciu interfejsu AMSI.
6. Wbudowany skaner UEFI.
7. System musi umożliwiać skonfigurowanie wyjątków ochrony przed atakami sieciowymi (IDS).
8. System musi umożliwiać wykrywanie włamań wykorzystujących protokoły: SMB, RPC, RDP i informować użytkownika o wykryciu ataku.
9. System musi wyświetlać powiadomienia po wykryciu ataku.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

10. System musi zezwalać na połączenia przychodzące do udziałów administracyjnych po protokole SMB.
11. Wbudowany skaner skryptów JavaScript, wykonywanych przez przeglądarki internetowe.
12. System musi umożliwiać zdefiniowanie listy aplikacji, dla których jest przeprowadzane filtrowanie protokołu SSL/TLS.
13. System musi umożliwiać określenie białej listy domen, dla których analiza protokołu SSL/TLS nie będzie wykonywana.
14. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
15. Skanowanie plików spakowanych i skompresowanych.
16. Wbudowana technologia monitorowania zdarzeń bezpieczeństwa związanych z zagrożeniami typu malware, exploit, PUA, podłączenia do sieci Botnet.
17. Musi być możliwe uruchamianie modułu ochrony przed złośliwym oprogramowaniem w ramach usługi chronionej systemu Windows (dla systemów Windows Server 2012 R2 lub nowszych).
18. System musi w momencie instalacji na serwerze wykrywać usługi jakie są zainstalowane i tworzyć odpowiednie wyjątki dla nich.
19. System musi umożliwiać analizę zagrożeń przez porównanie skanowanych plików z białą i czarną listą obiektów w chmurze producenta.
20. System musi umożliwiać wybór jakie typy podejrzanych próbek będą przesyłane do producenta. W tym co najmniej: pliki wykonywalne, archiwa, skrypty, możliwy spam.
21. Musi istnieć możliwość pozostawienia lub usunięcia (natychmiast po wykonaniu analizy, po 30 dniach) plików wykonywalnych, archiwów, skryptów, możliwego spamu przesyłanych do producenta w celu przeprowadzenia analizy.
22. System musi umożliwiać zablokowanie przesyłania celem analizy dokumentów pakietu Microsoft Office oraz plików PDF z treścią aktywną.
23. System musi umożliwiać określenie plików i folderów, które nigdy nie będą przesyłane do producenta w celu analizy.
24. System musi być wyposażony w mechanizm chroniący serwer przed exploitami i atakami typu O-day.
25. System musi posiadać zaawansowany skaner pamięci umożliwiający wykrywanie zagrożeń próbujących działać na poziomie pamięci operacyjnej serwera.
26. Zainstalowany system ochrony musi być wyposażony w system HIPS.
27. System musi w natywny sposób wspierać środowiska klastrowe.
28. System musi umożliwiać wskazanie zewnętrznych lokalizacji w których przechowywane będą moduły i aktualizacje programu.
29. System musi wspierać WMI za pomocą których może przekazywać podstawowe informacje na temat swojej pracy do zewnętrznych systemów np. SIEM.
30. Wbudowana ochrona przed atakami typu phishing w wiadomościach e-mail.
31. System musi umożliwiać ochronę dostępu do urządzeń według zdefiniowanych reguł w określonych przedziałach czasu.
32. System musi tworzyć log ochrony protokołu SMTP.
33. Możliwość utworzenia kilku zadań skanowania (np.: co godzinę, po zalogowaniu, po

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (metody skanowania, obiekty skanowania, czynności).

34. System musi umożliwiać aktualizację modułów ochrony bez konieczności reinstalacji całego systemu.
35. System musi uruchamiać jeden skaner w pamięci, do którego odnoszą się wszystkie monitory skanujące i skanery na żądanie.
36. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach oraz procesów.
37. Administrator ma możliwość dodania wykluczenia ze skanowania po tzw. HASH'u, wskazującym bezpośrednio na określoną infekcję, a nie konkretny plik.
38. System musi być wyposażony w dwa niezależnie pracujące mechanizmy analizy heurystycznej (standardowa i zaawansowana heurystyka).
39. Administrator musi posiadać możliwość używania jednego poziomu analizy heurystycznej lub obu poziomów jednocześnie.
40. System musi umożliwiać automatyczne wysyłanie nowych zagrożeń (wykrytych przez heurystykę) do laboratorium producenta przez program antywirusowy - nie wymaga ingerencji użytkownika.
41. Wysyłanie nowych zagrożeń musi być możliwe za pomocą interfejsu systemu i nie może do tego celu wykorzystywać klienta pocztowego zainstalowanego w systemie operacyjnym.
42. System musi umożliwiać wysyłanie wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
43. W przypadku wykrycia wirusa, ostrzeżenie może zostać wysłane do administratora poprzez e-mail.
44. System musi posiadać wbudowany dziennik zdarzeń rejestrujący informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania.
45. Administrator musi mieć możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych systemu.
46. Możliwość zabezpieczenia hasłem musi obejmować wyłączenie systemu antywirusowego oraz jego odinstalowanie na urządzeniu końcowym.
47. System musi w sposób automatyczny i przyrostowy dokonywać aktualizacji silnika detekcji.
48. Aktualizacja musi być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD/DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
49. System musi posiadać możliwość automatycznego ściągania oraz udostępniania zbiorów aktualizacyjnych.
50. System musi wspierać aktualizacje za pośrednictwem serwera Proxy.
51. Administrator musi posiadać możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
52. System musi rejestrować wszystkie dane transmitowane za pośrednictwem funkcji ochrony sieci w formacie PCAP.
53. System musi umożliwiać zarejestrowanie dodatkowych informacji na temat systemu

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

operacyjnego, na przykład dotyczące uruchomionych procesów, aktywności procesora.

54. System musi rejestrować komunikację produktu z serwerami licencji producenta.
55. System musi automatycznie przesyłać powiadomienia o zdarzeniach pocztą e-mail na wskazany adres e-mailowy.
56. Musi istnieć możliwość zdefiniowania wykorzystywanego zestawu znaków. W tym co najmniej: Unicode (UTF-8).
57. Wsparcie dla RMM (Remote Monitoring and Management).
58. System musi posiadać możliwość zdalnej administracji za pomocą konsoli administracji zdalnej.
59. System musi posiadać wbudowany, dedykowany moduł command linę umożliwiający konfigurację oraz uruchamianie zadań zainstalowanej aplikacji.
60. System musi być wyposażony w narzędzie umożliwiające wygenerowanie raportu dotyczącego stanu komputera, w tym co najmniej zainstalowanych aplikacji, uruchomionych procesów, ważnych wpisów w rejestrze i uruchomionych usług.
61. Musi istnieć możliwość zdalnej administracji systemem za pomocą konsoli administracji zdalnej.
62. Do administracji zdalnej musi być wykorzystywany dedykowany agent.
63. Agent musi komunikować się z serwerem administracji zdalnej w bezpieczny sposób uniemożliwiający podsłuch komunikacji.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706