Opis przedmiotu zamówienia

Dotyczący przedłużenia licencji oprogramowania antywirusowego **ESET Endpoint Antivirus + File Security** lub dostawa innego równoważnego systemu antywirusowego

I. Przedmiotem zamówienia jest:

I.1. Przedmiotem zamówienia jest dostawa oprogramowania antywirusowego lub odnowienie posiadanej przez Zamawiającego licencji ESET Endpoint Antivirus + File Security na system zabezpieczający przed złośliwym oprogramowaniem wraz ze wsparciem technicznym świadczonym przez Wykonawcę, na okres 24 miesięcy od dnia 2021-02-28 dla minimum 2450 stanowisk. Pula licencji podzielona na 4 odrębne pule (z unikalnymi kluczami licencji) - 2075+200+150+25 licencji.
I.2. Wykonawca zapewni Zamawiającemu wsparcie techniczne na oprogramowanie antywirusowe przez okres obowiązywania Umowy.
I.3. W przypadku zaoferowania oprogramowania (systemu) równoważnego, Wykonawca zobowiązany jest, w terminie 5 dni kalendarzowych od dnia podpisania umowy, wykonać następujące działania:

1. Dostarczenie wszystkich niezbędnych licencji (ze wsparciem producenta na min. 24 miesięcy licząc od dnia wdrożenia) na oprogramowanie (również firm trzecich, np. systemy operacyjne, bazy danych) wymaganych do wdrożenia i uruchomienia systemu.
2. Przeprowadzenie wdrożenia i uruchomienia centralnej konsoli zarządzającej w siedzibie Zamawiającego.
3. Przeprowadzenie procesu zdalnej, nieinwazyjnej deinstalacji obecnie używanego przez Zamawiającego oprogramowania antywirusowego ESET na 2200 stanowiskach (w tym blisko 500 notebookach będących w posiadaniu pracowników Zamawiającego, którzy aktualnie świadczą pracę zdalną z uwagi na wprowadzony stan epidemii) oraz zainstalowanie oprogramowania równoważnego na wskazanych przez Zamawiającego urządzeniach, tj. stacjach roboczych, notebookach i serwerach.
4. Prace związane z wdrożeniem i uruchomieniem systemu oraz z deinstalacją obecnie używanego przez Zamawiającego oprogramowania ESET mają się odbyć w siedzibie Zamawiającego w dniach roboczych (Pon-Pt w godz. 7.30-15.30) - dotyczy wdrożenia i uruchomienia centralnej konsoli zarządzającej oraz reinstalacji nowego rozwiązania antywirusowego na stacjach roboczych w siedzibie Zamawiającego. Oprogramowanie na notebookach będących w posiadaniu pracowników Zamawiającego musi zostać zainstalowane w sposób zdalny.
5. Przeprowadzenie szkolenia z instalacji, konfiguracji i zarządzania wdrożonym systemem równoważnym dla nie więcej niż 5 osób wskazanych przez Zamawiającego

I.4. Świadczenie wsparcia technicznego do oprogramowania równoważnego w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta oprogramowania przez okres obowiązywania Umowy.
I.5. Zamawiający wymaga złożenia w ofercie szczegółowego opisu rozwiązania równoważnego wraz z podaniem funkcjonalności proponowanego rozwiązania (pełna dokumentacja w języku polskim), w celu potwierdzenia równoważności funkcjonalności zaoferowanego rozwiązania.

II. Oprogramowanie równoważne musi spełniać poniższe wymagania:

II.1. Wymagania ogólne.
1. Pełne wsparcie dla systemu Windows 7/8/8.1/10, Linux i MAC OS.
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.
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 2012, 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. 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.
5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
6. Narzędzie administracyjne musi wspierać połączenia poprzez serwery proxy występujące w sieci Zamawiającego.
7. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
8. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
9. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
10. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
11. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
12. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
13. Serwer administracyjny musi oferować możliwość instalacji servera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
14. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
15. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
16. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
17. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
18. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
19. Centralna konfiguracja i zarządzanie ochroną antywirusową i antyspyware'ową.
20. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
21. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
22. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
23. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
28. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
29. 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.
30. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
31. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej.
32. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
33. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
34. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
35. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
36. 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.
37. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
38. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich.
39. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
40. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
41. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.

42. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych
i dynamicznych komputerów.
43. 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 operacyjnego, itp.
44. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
45. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
46. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
47. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
48. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta.
49. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
50. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
51. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości e-mail lub komunikatu SNMP.
52. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
53. Serwer administracyjny musi oferować możliwość obserwacji poziomu wykorzystania licencji.
54. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
55. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPV4 iIPv6 lub wyszukania konkretnej nazwy zagrożenia.
56. 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, 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. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
16. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
17. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany

takim fakcie odpowiednim powiadomieniem i informacją w interfejsie systemu.
18 . Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
19. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli.
20. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook.
21. Skanowanie i oczyszczanie poczty przychodzące] POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
22. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
23. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
24. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
25. System ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
26. System ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
27. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
28. Administrator ma mieć możliwość zdefiniowania portów TCP, na których system będzie realizował proces skanowania ruchu szyfrowanego.
29. System musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
30. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
31. 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.
32. 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.
33. Do wysłania próbki zagrożenia do laboratorium producenta system nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
34. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
35. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
36. Możliwość zabezpieczenia konfiguracji systemu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
37. 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.
39. 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.
40. 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.
41. 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.
42. 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.
43. W momencie podłączenia zewnętrznego nośnika system musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
44. Użytkownik ma posiadać możliwość takiej konfiguracji systemu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika

45. System musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS) lub dowolny inny system wyrywania i zapobiegania włamaniom IDS, IPS (Intrusion Detection System, Intrusion Prevention System).
46. System musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
47. 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.
48. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
49. System musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
50. System musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
51. System musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
52. 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.
53. 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.
54. System musi posiadać możliwość aktywacji poprzez podanie klucza licencyjnego oraz możliwość aktywacji offline.
55. W systemie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
56. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień systemu na stacji końcowej.
57. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym automatycznie zostają przywrócone dotychczasowe ustawienia.
58. System musi posiadać funkcję ręcznej aktualizacji własnych komponentów oprogramowania.
59. System musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
60. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
61. System musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
62. 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.
63. 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.
64. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.

II.4. 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. System musi posiadać możliwość zdalnej administracji za pomocą konsoli administracji zdalnej.
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.
10. Wbudowany skaner skryptów JavaScript, wykonywanych przez przeglądarki internetowe.
11. System musi umożliwiać zdefiniowanie listy aplikacji, dla których jest przeprowadzane filtrowanie protokołu SSL/TLS.
12. System musi umożliwiać określenie białej listy domen, dla których analiza protokołu SSL/TLS nie będzie wykonywana.
13. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
14. Skanowanie plików spakowanych i skompresowanych.

15. Wbudowana technologia monitorowania zdarzeń bezpieczeństwa związanych z zagrożeniami typu malware, exploit, PUA, podłączenia do sieci Botnet.
16. System musi umożliwiać wybór jakie typy podejrzanych próbek będą przesyłane do producenta. W tym co najmniej: pliki wykonywalne, archiwa, skrypty, możliwy spam.
17. System musi umożliwiać zablokowanie przesyłania celem analizy dokumentów pakietu Microsoft Office oraz plików PDF z treścią aktywną.
18. System musi umożliwiać określenie plików i folderów, które nigdy nie będą przesyłane do producenta w celu analizy.
19. System musi być wyposażony w mechanizm chroniący serwer przed exploitami i atakami typu 0-day.
20. System musi posiadać zaawansowany skaner pamięci umożliwiający wykrywanie zagrożeń próbujących działać na poziomie pamięci operacyjnej serwera.
21. Zainstalowany system ochrony musi być wyposażony w system HIPS.
22. System musi w natywny sposób wspierać środowiska klastrowe.
23. System musi wspierać WMI za pomocą których może przekazywać podstawowe informacje na temat swojej pracy do zewnętrznych systemów np. SIEM.
24. Wbudowana ochrona przed atakami typu phishing w wiadomościach e-mail.
25. System musi tworzyć log ochrony protokołu SMTP.
26. System musi umożliwiać aktualizację modułów ochrony bez konieczności reinstalacji całego systemu.
27. System musi uruchamiać jeden skaner w pamięci, do którego odnoszą się wszystkie monitory skanujące i skanery na żądanie.
28. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach oraz procesów.
29. Wysyłanie nowych zagrożeń musi być możliwe za pomocą interfejsu systemu i nie może do tego celu wykorzystywać klienta pocztowego zainstalowanego w systemie operacyjnym.
30. System musi umożliwiać wysyłanie wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
31. W przypadku wykrycia wirusa, ostrzeżenie może zostać wysłane do administratora poprzez e-mail.
32. System musi w sposób automatyczny i przyrostowy dokonywać aktualizacji silnika detekcji.
33. 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).
34. System musi posiadać możliwość automatycznego ściągania oraz udostępniania zbiorów aktualizacyjnych.
35. System musi wspierać aktualizacje za pośrednictwem serwerów proxy obecnych w sieci Zamawiającego.
36. System musi rejestrować wszystkie dane transmitowane za pośrednictwem funkcji ochrony sieci w formacie PCAP.
37. System musi umożliwiać zarejestrowanie dodatkowych informacji na temat systemu operacyjnego, na przykład dotyczące uruchomionych procesów, aktywności procesora.
38. System musi rejestrować komunikację produktu z serwerami licencji producenta.
39. System musi automatycznie przesyłać powiadomienia o zdarzeniach pocztą e-mail na wskazany adres e-mailowy.
40. Musi istnieć możliwość zdefiniowania wykorzystywanego zestawu znaków. W tym co najmniej: Unicode (UTF-8).
41. Wsparcie dla RMM (Remote Monitoring and Management).
42. 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.
43. Do administracji zdalnej musi być wykorzystywany dedykowany agent.
44. Agent musi komunikować się z serwerem administracji zdalnej w bezpieczny sposób uniemożliwiający podsłuch komunikacji.