Załącznik nr 1 do ogłoszenia: Opis potrzeb Zamawiającego

1. Cel:

Zamawiający planuje rozbudowę, przedłużenie i rozszerzenie do 4700 licencji oprogramowania antywirusowego ESET PROTECT Advanced ON-PREM lub dostawę innego równoważnego oprogramowania antywirusowego ze wsparciem producenta na okres 36 miesięcy od dnia 1.07.2023 r.

Celem konsultacji jest uzyskanie przez Zamawiającego informacji o wariantach i kosztach rozbudowy, przedłużenia i rozszerzenia do 4700 licencji oprogramowania antywirusowego ESET PROTECT Advanced ON-PREM lub dostawy innego równoważnego oprogramowania antywirusowego ze wsparciem producenta na okres 36 miesięcy od dnia 1.07.2023 r.

Środowisko Zamawiającego:

Zamawiający obecnie posiada 4500 licencji oprogramowania ESET PROTECT Entry ON-PREM ważnych do dnia 31.06.2023.

Powyższe oprogramowanie przeznaczone będzie dla komputerów i urządzeń mobilnych pracowników Państwowej Inspekcji Pracy, na których zainstalowany jest Windows 10 Pro 64-bit lub Android/IOS, dlatego zaoferowane oprogramowanie musi być w pełni kompatybilne z wymienionymi systemami.

2. Oczekiwane parametry techniczne:

ESET PROTECT Advanced ON-PREM – licencja ważna 36 miesięcy od dnia 1.07.2023 wraz ze wsparciem producenta albo inne równoważne oprogramowanie antywirusowe spełniające następujące kryteria równoważności:

Oprogramowanie równoważne do oprogramowania, o którym mowa powyżej, musi spełniać następujące wymagania minimalne (oprogramowanie równoważne musi spełniać niżej wymienione minimalne wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):

I. Wymagania ogólne:

1. Pełne wsparcie dla systemu Windows 7/8/8.1/10, Android/IOS.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.

3. Wersja systemu dla stacji 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. Administracja zdalna:

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux.
2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
4. Konsola administracyjna musi umożliwiać podgląd szczegółów dotyczących bazy danych, takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
7. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
8. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
9. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.
10. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
11. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
12. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
13. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
14. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym.
15. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.

16. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
17. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
18. Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image".
19. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.
20. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.
21. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
22. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
23. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.
24. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.
25. Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń, takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.
26. Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.
27. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.
28. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.
29. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
30. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
31. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
32. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.
33. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.

34. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
35. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
36. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.
37. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
38. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
39. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.
40. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
41. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.
42. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
43. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
44. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
45. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
46. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.

47. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
48. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
49. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
50. 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.
51. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
52. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
53. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
54. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
55. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
56. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
57. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
58. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
59. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
60. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.

61. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
62. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
63. Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
64. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
65. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
66. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
67. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
68. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
69. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
70. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może
71. zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV.
72. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
73. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
74. Powiadomienia mailowe mają być wysyłane w formacie HTML.
75. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
76. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
77. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
78. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
79. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.

80. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
81. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
82. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
83. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
84. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
85. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
86. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
87. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
88. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
89. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
90. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
91. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.
92. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
93. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).
94. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.
95. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).

96. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

III. 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. 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 minut 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.

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 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:
    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.
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 minut, 30 minut, 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.
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.
97. System musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania obiektu, co najmniej w oparciu o nazwę zagrożenia oraz jego lokalizację.
98. System musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania pliku, wskazując sumę kontrolną pliku (jego HASH).
99. System musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść".
100. 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.
101. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
102. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
103. System ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
104. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.

IV. Sandbox w chmurze:

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    a. Czysty,
    b. Podejrzany,
    c. Bardzo podejrzany,
    d. Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

V. Szyfrowanie:

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
5. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.
6. Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane.
7. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.
9. Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej.
10. Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego.
11. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:
    a) ilość znaków,
    b) czy hasło ma zawierać wielkie litery,
    c) czy hasło ma zawierać małe litery,
    d) czy hasło ma zawierać cyfry,
    e) czy hasło ma zawierać znaki specjalne,
    f) okres ważności,
    g) ilość nieudanych logowań,
    h) możliwość zmiany hasła.
12. Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom.
13. Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.

VI. 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.
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.
14. System musi umożliwiać określenie białej listy domen, dla których analiza protokołu SSL/TLS nie będzie wykonywana.
15. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
16. Skanowanie plików spakowanych i skompresowanych.
17. Wbudowana technologia monitorowania zdarzeń bezpieczeństwa związanych z zagrożeniami typu malware, exploit, PUA, podłączenia do sieci Botnet.
18. Musi być możliwe uruchamianie modułu ochrony przed złośliwym oprogramowaniem w ramach usługi chronionej systemu Windows (dla systemów Windows Server 2012 R2 lub nowszych).
19. System musi w momencie instalacji na serwerze wykrywać usługi jakie są zainstalowane i tworzyć odpowiednie wyjątki dla nich.
20. System musi umożliwiać analizę zagrożeń przez porównanie skanowanych plików z białą i czarną listą obiektów w chmurze producenta.
21. System musi umożliwiać wybór jakie typy podejrzanych próbek będą przesyłane do producenta. W tym co najmniej: pliki wykonywalne, archiwa, skrypty, możliwy spam.

22. 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.
23. System musi umożliwiać zablokowanie przesyłania celem analizy dokumentów pakietu Microsoft Office oraz plików PDF z treścią aktywną.
24. System musi umożliwiać określenie plików i folderów, które nigdy nie będą przesyłane do producenta w celu analizy.
25. System musi być wyposażony w mechanizm chroniący serwer przed exploitami i atakami typu O-day.
26. System musi posiadać zaawansowany skaner pamięci umożliwiający wykrywanie zagrożeń próbujących działać na poziomie pamięci operacyjnej serwera.
27. Zainstalowany system ochrony musi być wyposażony w system HIPS.
28. System musi w natywny sposób wspierać środowiska klastrowe.
29. System musi umożliwiać wskazanie zewnętrznych lokalizacji w których przechowywane będą moduły i aktualizacje programu.
30. System musi wspierać WMI za pomocą których może przekazywać podstawowe informacje na temat swojej pracy do zewnętrznych systemów np. SIEM.
31. Wbudowana ochrona przed atakami typu phishing w wiadomościach e-mail.
32. System musi umożliwiać ochronę dostępu do urządzeń według zdefiniowanych reguł w określonych przedziałach czasu.
33. System musi tworzyć log ochrony protokołu SMTP.
34. Możliwość utworzenia kilku zadań skanowania (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (metody skanowania, obiekty skanowania, czynności).
35. System musi umożliwiać aktualizację modułów ochrony bez konieczności reinstalacji całego systemu.
36. System musi uruchamiać jeden skaner w pamięci, do którego odnoszą się wszystkie monitory skanujące i skanery na żądanie.
37. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach oraz procesów.
38. Administrator ma możliwość dodania wykluczenia ze skanowania po tzw. HASH'u, wskazującym bezpośrednio na określoną infekcję, a nie konkretny plik.
39. System musi być wyposażony w dwa niezależnie pracujące mechanizmy analizy heurystycznej (standardowa i zaawansowana heurystyka).

40. Administrator musi posiadać możliwość używania jednego poziomu analizy heurystycznej lub obu poziomów jednocześnie.
41. System musi umożliwiać automatyczne wysyłanie nowych zagrożeń (wykrytych przez heurystykę) do laboratorium producenta przez program antywirusowy - nie wymaga ingerencji użytkownika.
42. Wysyłanie nowych zagrożeń musi być możliwe za pomocą interfejsu systemu i nie może do tego celu wykorzystywać klienta pocztowego zainstalowanego w systemie operacyjnym.
43. System musi umożliwiać wysyłanie wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
44. W przypadku wykrycia wirusa, ostrzeżenie może zostać wysłane do administratora poprzez e-mail.
45. System musi posiadać wbudowany dziennik zdarzeń rejestrujący informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania.
46. Administrator musi mieć możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych systemu.
47. Możliwość zabezpieczenia hasłem musi obejmować wyłączenie systemu antywirusowego oraz jego odinstalowanie na urządzeniu końcowym.
48. System musi w sposób automatyczny i przyrostowy dokonywać aktualizacji silnika detekcji.
49. 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).
50. System musi posiadać możliwość automatycznego ściągania oraz udostępniania zbiorów aktualizacyjnych.
51. System musi wspierać aktualizacje za pośrednictwem serwera Proxy.
52. Administrator musi posiadać możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
53. System musi rejestrować wszystkie dane transmitowane za pośrednictwem funkcji ochrony sieci w formacie PCAP.
54. System musi umożliwiać zarejestrowanie dodatkowych informacji na temat systemu operacyjnego, na przykład dotyczące uruchomionych procesów, aktywności procesora.
55. System musi rejestrować komunikację produktu z serwerami licencji producenta.
56. System musi automatycznie przesyłać powiadomienia o zdarzeniach pocztą e-mail na wskazany adres e-mailowy.

57. Musi istnieć możliwość zdefiniowania wykorzystywanego zestawu znaków. W tym co najmniej: Unicode (UTF-8).
58. Wsparcie dla RMM (Remote Monitoring and Management).
59. System musi posiadać możliwość zdalnej administracji za pomocą konsoli administracji zdalnej.
60. System musi posiadać wbudowany, dedykowany moduł command linę umożliwiający konfigurację oraz uruchamianie zadań zainstalowanej aplikacji.
61. 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.
62. Musi istnieć możliwość zdalnej administracji systemem za pomocą konsoli administracji zdalnej.
63. Do administracji zdalnej musi być wykorzystywany dedykowany agent.
64. Agent musi komunikować się z serwerem administracji zdalnej w bezpieczny sposób uniemożliwiający podsłuch komunikacji.

VII. Pozostałe wymagania:

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. 36 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 7/10),
   b) serwerach (Microsoft Windows Server 2008/2008R2/2012/2012 R2/2016/2019),
   c) urządzeniach mobilnych z systemem Android/IOS.
3. 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.

oraz szczegółowy opis zakresu prac, ich sekwencji oraz wskazania, kto ma je realizować (Zamawiający, Wykonawca) niezbędnych do wdrożenia i konfiguracji systemu równoważnego.

4. 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.
5. Przeprowadzenie szkoleń z instalacji, konfiguracji i zarządzania wdrożonym systemem równoważnym zgodnie z wymogami Zamawiającego.
6. 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.

3. Opis wymagań dotyczących realizacji szkolenia

1. Wykonawca zaplanuje, zorganizuje i przeprowadzi szkolenie dla maksymalnie 36 pracowników Państwowej Inspekcji Pracy, zwanych dalej: „uczestnikami”.
2. Celem szkolenia jest zapoznanie uczestników z wymaganiami w zakresie administracji i obsługi dostarczonego oprogramowania.
3. Szkolenia odbędą się w podziale na grupy, które będą liczyły po 18 uczestników.
4. Szkolenie dla każdej grupy trwać będzie 2 dni. Każde ze szkoleń pierwszego dnia rozpocznie się najwcześniej o godz. 10.00 i zakończy się najpóźniej o godz. 16.00 dnia ostatniego. Dzień szkoleniowy trwać będzie 8 godzin (1 godz. = 45 min.). Łączna liczba godzin szkoleniowych dla każdego szkolenia wynosi 16.
5. Wykonawca zapewni realizację szkoleń zgodnie z obowiązującymi przepisami epidemicznymi, w szczególności z wytycznymi dla organizatorów spotkań biznesowych, szkoleń, konferencji, kongresów i targów w trakcie epidemii SARS-CoV-2.
6. Szkolenia zostaną zorganizowane w jednym z miast wojewódzkich.

7. Szkolenia zostaną przeprowadzone w uzgodnionych terminach, przed terminem dostawy zaoferowanego oprogramowania, w kolejno po sobie następujących dniach od poniedziałku do piątku.
8. Szkolenia mają mieć charakter warsztatów (każdy z uczestników szkolenia samodzielnie wykonuje ćwiczenia pod nadzorem trenerów).
9. Sale muszą mieć powierzchnię dostosowaną do wielkości grup szkoleniowych. Wykonawca zapewni niezbędne oprzyrządowanie do przeprowadzenia szkoleń, w tym w szczególności specjalistyczny sprzęt komputerowy odpowiedni do rodzaju zajęć, m.in. indywidualne stanowisko dla każdego uczestnika szkolenia, infrastruktura sieciowa, zainstalowane i skonfigurowane do zajęć odpowiednie oprogramowanie. Sale szkoleniowe muszą być wyposażone w sprzęt prezentacyjny (m.in. projektor, flipchart, tablica). Sale muszą mieć powierzchnię dostosowaną do wielkości grup szkoleniowych. Budynek oraz sala nie mogą posiadać barier architektonicznych dla osób niepełnosprawnych.
10. Wykonawca ma obowiązek zapewnić minimum dwóch trenerów posiadających odpowiednie kwalifikacje zawodowe do przeprowadzenia zajęć danej grupy, w każdym dniu szkoleniowym. Zamawiający wymaga, by ww. osoby przeprowadziły w okresie ostatnich dwóch lat (licząc wstecz od upływu terminu wyznaczonego na składanie ofert) co najmniej po dwa szkolenia z zakresu szkoleń objętych przedmiotem zamówienia. W przypadku gdyby wykładowca, wskazany w wykazie, o którym mowa w pkt 13 ppkt 3, nie mógł przeprowadzić szkolenia, Wykonawca zobowiązany jest zapewnić innego wykładowcę, posiadającego wymagane kwalifikacje. Informację o zmianie wykładowcy Wykonawca przekaże Zamawiającemu w formie pisemnej, przed rozpoczęciem szkolenia, wraz z opisem jego kwalifikacji. Powyższa zmiana wymaga pisemnej akceptacji Zamawiającego.
11. Wykonawca zapewni każdemu uczestnikowi materiały szkoleniowe, które przekaże uczestnikom poszczególnych szkoleń pocztą elektroniczną oraz w wersji papierowej przed rozpoczęciem każdego szkolenia, a także materiały piśmiennicze (notatnik, długopis) dla każdego uczestnika.
12. Zamawiający przekaże Wykonawcy listy uczestników szkoleń wraz z adresami poczty elektronicznej oraz informacją o korzystaniu z noclegów, najpóźniej 7 dni roboczych po uzyskaniu informacji, o której mowa w pkt 13. Zamawiający zastrzega, że w przypadku choroby lub wyniknięcia innej szczególnej okoliczności może zmienić uczestnika szkolenia lub zmniejszyć/zwiększyć liczbę uczestników danego szkolenia, w tym liczbę osób korzystających z noclegów. Zamawiający informuje, że uiści zapłatę tylko za faktyczną liczbę uczestników szkolenia oraz za faktycznie wykorzystane noclegi. O zmianie osób w poszczególnych grupach Zamawiający poinformuje Wykonawcę przed rozpoczęciem szkolenia dla danej grupy.

Zamawiający może zmniejszyć wskazaną w pkt. 1 liczbę uczestników szkoleń, łącznie ze wszystkich grup, o maksymalnie 2.

13. Wykonawca opracuje i przedstawi Zamawiającemu do akceptacji, na co najmniej 10 dni roboczych przed rozpoczęciem pierwszego szkolenia, na adres wskazany w Umowie, dokumentację szkoleniową zawierającą:
    1) harmonogram szkoleń, obejmujący terminy i miejsca realizacji każdego szkolenia (co najmniej nazwa i adres budynku) oraz miejsce zakwaterowania (nazwa i adres hotelu), ze wskazaniem grupy, której szkolenie dotyczy. Do harmonogramu należy dołączyć informacje o możliwości przemieszczania się komunikacją publiczną: z dworca PKP do miejsca noclegu, z miejsca prowadzenia szkolenia na dworzec PKP oraz z miejsca noclegu do miejsca prowadzenia szkolenia,
    2) program szkolenia, który musi uwzględniać pełny zakres tematyczny szkolenia z podziałem na dni i godziny prowadzenia zajęć i przerw, z podziałem na bloki tematyczne, a w blokach zagadnienia do omówienia,
    3) wykaz wykładowców, o których mowa w pkt 10, wraz z opisem ich kwalifikacji do przeprowadzenia zajęć,
    4) materiały szkoleniowe, które zostaną opracowane w języku polskim,
    5) opis metody badania satysfakcji uczestnictwa w szkoleniu oraz projekt karty oceny zawierającej co najmniej punkty dotyczące stopnia omówienia zagadnień ujętych w programie, oceny wiedzy merytorycznej wykładowcy oraz oceny umiejętności dydaktycznych wykładowcy,
    6) wzór protokołu odbioru szkolenia.

    Zamawiający uprawniony jest do wniesienia uwag do przekazanej dokumentacji szkoleniowej w terminie 3 dni roboczych od jej otrzymania. Uwagi przekazywane będą pocztą elektroniczną (e-mail). Wykonawca zobowiązany jest uwzględnić uwagi Zamawiającego i przekazać dokumentację do ponownej akceptacji Zamawiającego w terminie do 2 dni roboczych od otrzymania ww. uwag.

14. Wykonawca przygotuje formularze badania satysfakcji uczestnictwa w szkoleniu i przeprowadzi badanie, odrębnie dla każdego szkolenia.
15. Wykonawca zobowiązany jest przygotować i wręczyć uczestnikom, w ostatnim dniu szkolenia, dokument potwierdzający udział w szkoleniu (zaświadczenie/certyfikat).
16. Po zakończeniu każdego szkolenia, Wykonawca sporządzi i podpisze protokół odbioru szkolenia w 2 egzemplarzach. Protokoły mają zawierać co najmniej następujące informacje: datę i miejsce przeprowadzenia szkolenia, imię i nazwisko wykładowcy, stwierdzenie, że szkolenie zostało

przeprowadzone zgodnie z zakresem obowiązków określonym przez Zamawiającego, miejsce zakwaterowania i liczbę wykorzystanych noclegów, informację, że uczestnicy szkolenia otrzymali materiały szkoleniowe. Do ww. protokołów mają być załączone oryginały list uczestników szkolenia (podpisane każdego dnia, przez każdego uczestnika szkolenia), wynik badania satysfakcji wraz z wypełnionymi kartami oceny szkolenia oraz kopie wydanych zaświadczeń/certyfikatów. Protokoły wraz z wymaganymi załącznikami dostarczone do siedziby Zamawiającego będą podpisane przez upoważnionego przedstawiciela Zamawiającego. Osobami uprawnionymi do podpisania protokołu odbioru szkolenia są osoby upoważnione do składania oświadczeń woli w imieniu Wykonawcy – zgodnie z zasadami reprezentacji określonej w KRS, ewidencji działalności gospodarczej lub innego właściwego rejestru lub zgodnie z pełnomocnictwem, zaś po stronie Zamawiającego przez dyrektora lub wicedyrektora Departamentu Kadr i Szkoleń PIP GIP.

17. W ramach szkolenia Wykonawca zapewni każdemu uczestnikowi szkolenia, w każdym dniu szkolenia, dwie przerwy kawowe (gorącą kawę i herbatę, cukier, śmietankę oraz wodę i ciasteczka) i jednej przerwy obiadowej (obiady dwudaniowe).
18. Wykonawca zobowiązany jest zapewnić 2 noclegi ze śniadaniami (począwszy od nocy poprzedzającej dzień rozpoczęcia szkolenia) oraz kolacje (w każdym dniu szkolenia z wyjątkiem ostatniego dnia szkolenia), w pokojach jednoosobowych dla uczestników w hotelu o standardzie co najmniej trzygwiazdkowym, usytuowanym w tej samej miejscowości, w której prowadzone będą szkolenia (obiekt zlokalizowany w odległości od miejsca gdzie będą prowadzone szkolenia, umożliwiający dojazd komunikacją miejską w czasie 30 minut; czas dojazdu liczony będzie razem z dojściem do i od przystanku komunikacji miejskiej). Zamawiający dopuszcza, zapewnienie noclegów w motelach, pensjonatach, domach studenckich itp. – pod warunkiem, że będą one spełniały wymagania hotelu trzygwiazdkowego. Budynek oraz pokoje nie mogą posiadać barier architektonicznych dla osób niepełnosprawnych. Zamawiający informuje, że uczestnicy szkolenia z miasta, w którym odbywać się będzie szkolenie, nie będą korzystać z noclegu (natomiast w przypadku oddelegowania na szkolenie osoby zatrudnionej w oddziale danej jednostki organizacyjnej Państwowej Inspekcji Pracy może wystąpić konieczność zapewnienia dla ww. osoby noclegu).
19. Wykonawca uwzględni w ofercie cenowej wszystkie koszty, jakie Państwowa Inspekcja Pracy Główny Inspektorat Pracy będzie zobowiązany ponieść w związku z realizacją szkoleń o których mowa w pkt 5.14. Zamawiający pokryje jedynie koszt dojazdu uczestników na szkolenie (odrębnie).
20. W przypadku niemożności przeprowadzenia szkolenia, w którymkolwiek z terminów, wskazanych w zaakceptowanym przez Zamawiającego harmonogramie szkoleń, Wykonawca

zobowiązuje się niezwłocznie poinformować o powyższym Zamawiającego. W takiej sytuacji Zamawiający ma prawo wskazać termin, w którym ma być przeprowadzone dane szkolenie. Termin wskazany przez Zamawiającego jest wiążący dla Wykonawcy.

21. Wykonawca zobowiązany jest do złożenia protokołu odbioru szkolenia, po przeprowadzeniu szkolenia każdej z grupy, w terminie 3 dni roboczych od daty jego zakończenia, zgodnie z zaakceptowanym wzorem, o którym mowa w pkt 13. Zamawiający zapłaci Wykonawcy wynagrodzenie za szkolenie dla danej grupy, gdy jego ocena merytoryczna, obejmująca stopień omówienia zagadnień ujętych w programie oraz ocenę wiedzy merytorycznej i umiejętności dydaktycznych wykładowcy, obliczona na podstawie kart oceny wyników badania satysfakcji, będzie równa lub wyższa niż 3,8 w skali 1-5. W przypadku, gdy ocena merytoryczna szkolenia, obejmująca stopień omówienia zagadnień ujętych w programie oraz ocenę wiedzy merytorycznej i umiejętności dydaktycznych wykładowcy, obliczona na podstawie kart oceny wyników badania satysfakcji, będzie niższa niż 3,8 pkt w skali 1-5, Strony uznają, że szkolenie dla tej grupy nie zostało wykonane należycie i Wykonawcy, nie przysługuje wynagrodzenie. W przypadku nie załączenia przez Wykonawcę do protokołu odbioru szkolenia danej grupy wyników badania satysfakcji (wraz z wypełnionymi kartami oceny satysfakcji), Zamawiający uzna, że ocena merytoryczna szkolenia na podstawie kart oceny wyników badania satysfakcji była niższa niż 3,8 pkt w skali 1-5 dla danej grupy i Wykonawcy nie przysługuje wynagrodzenie. W przypadkach wskazanych powyżej, Wykonawca zobowiązany będzie przeprowadzić ponownie szkolenie na własny koszt, na warunkach określonych w umowie, w terminie uzgodnionym z Zamawiającym. W takim przypadku, koszt wyjazdu służbowego uczestników szkolenia pokrywa Wykonawca (refundacja kosztu zakupu biletów, ryczałtu za dojazdy samochodem prywatnym, diety i itp.). Podstawą obliczenia ww. kosztów będą rozliczenia kosztów podróży służbowej (rozliczenia delegacji) uczestników szkolenia przedłożone przez Zamawiającego. W przypadkach wskazanych powyżej, Wykonawcy przysługuje wynagrodzenie po ponownym przeprowadzeniu szkolenia z zastrzeżeniem, że jego ocena merytoryczna, obejmująca stopień omówienia zagadnień ujętych w programie oraz ocenę wiedzy merytorycznej i umiejętności dydaktycznych wykładowcy, obliczona na podstawie kart oceny wyników badania satysfakcji, będzie równa lub wyższa niż 3,8 w skali 1-5.
22. Zamawiający oświadcza, że udział pracowników Państwowej Inspekcji Pracy w szkoleniu będzie całkowicie finansowany ze środków publicznych.