Załącznik nr 2 Szczegółowy opis

Część zamówienia	Nazwa	Ilość	Szczegółowy opis
1	**Laptop**	4	1. Procesor: Procesor (min. 4 rdzeniowy, 8 wątkowy) dedykowany do pracy w laptopach osiągający w teście PassMark - CPU Mark wynik co najmniej 7600 punktów (dopuszcza się przeprowadzenie testów przez oferenta, przy czym wymagane jest potwierdzenie w postaci wydruku dołączonego do oferty). 2. Ilość: 4 szt. 3. Pamięć operacyjna: Min. 16 GB 4. Karta graficzna: zintegrowana 5. Dysk twardy: min. 240 GB SSD M.2, możliwość dodania drugiego dysku SATA 6. Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną 7. Ekran: przekątna min. 17.3'', rozdzielczość min. 1920x1080 pikseli 8. Certyfikaty i standardy: posiada ważną Deklarację zgodności CE oraz spełnia wymogi normy Energy Star. 9. Gwarancja: Minimum 2 lata. Okres gwarancji będzie obowiązywał od dnia podpisania protokołu odbioru. Gwarancja musi być świadczona przez producenta laptopa lub jego partnera/importera. 10. Wsparcie techniczne producenta: Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej laptopa oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Należy podać nr telefonu do wsparcia producenta oraz jego stronę www serwisową. 11. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu laptopa. 12. Wymagania podstawowe: a) Wbudowane porty i złącza: • Min. 3 x USB 3.0 wyprowadzonych na zewnątrz (wymagana ilość i rozmieszczenie portów USB na zewnątrz obudowy laptopa nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.), • Min. 1 x USB C • Min. 1 x HDMI • Port sieciowy RJ-45, • Porty audio: wyjście słuchawkowe/wejście mikrofonowe, b) Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana) c) Karta sieciowa WIFI 802.11 a/b/g/n/ac d) Moduł komunikacyjny Bluetooth e) Płyta główna z chipsetem zalecanym przez producenta procesora 13. System operacyjny: Oferowany system operacyjny musi obsługiwać protokoły w wersji 64-bit oraz być

			kompatybilny z aktualnie funkcjonującym w jednostce Zamawiającego oprogramowaniem Microsoft. 14. Rok produkcji: Wyprodukowano nie wcześniej niż w 2021 r.
2	**Oprogramowanie**	4	Pakiet biurowy - Licencje zarządzane z poziomu producenta - Przeznaczone do celów dydaktycznych w wersji najnowszej Zawartość pakietu: - Edytor tekstu - Arkusz kalkulacyjny - Przygotowanie prezentacji - Program pocztowy - Organizer / Notes - Projektowanie i publikacja treści Zastosowanie: Laptopy multimedialne / Komputery stacjonarne Rodzaj licencji: na min. 4 stanowiska Typ licencji: edukacyjna Rodzaj wersji oprogramowania: nośnik CD/DVD lub elektroniczna wersja oprogramowania Okres ważności licencji: dożywotnia
3	**Program antywirusowy**	4	Program antywirusowy Ilość licencji: 4 szt. Czas trwania licencji: min. 2 lata Ochrona stacji roboczych: 1. Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows 8/Windows 8.1/Windows 10 2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows. 3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim. 4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. 5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim. 6. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives Ochrona antywirusowa i antyspyware 7. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 8. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 9. Wbudowana technologia do ochrony przed rootkitami. 10. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

			11. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 12. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. 13. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania. 14. 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). 15. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 16. Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 17. Możliwość skanowania dysków sieciowych i dysków przenośnych. 18. Skanowanie plików spakowanych i skompresowanych. 19. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 20. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku. 21. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 22. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 23. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera. 24. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 25. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 26. 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. 27. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. 28. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. 29. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

			30. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 32. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. 33. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL. 34. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora. 35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 36. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 37. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe. 38. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta. 39. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. 40. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 41. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym. 42. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 43. 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. 44. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 45. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. 46. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego

			zainstalowanego na komputerze użytkownika. 47. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 48. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 49. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. 50. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. 51. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 52. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji. 53. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. 54. Po instalacji programu, 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 zagrożeń. 55. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. 56. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. 57. Program 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 oraz urządzeń przenośnych. 58. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia. 59. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. 60. Program 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. 61. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 62. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 63. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się

			automatycznie lub za potwierdzeniem przez użytkownika. 64. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 65. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach. 66. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. 67. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 68. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 69. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. 70. Program ma 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 procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 71. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa. 72. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie. 73. Automatyczna, inkrementacyjna aktualizacja silnika detekcji. 74. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. 75. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji. 76. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. 77. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.

			78. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). 79. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 80. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym. 81. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji. 82. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym. 83. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń. 84. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu. 85. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji. 86. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline. 87. Możliwość podejrzenia informacji o licencji, która znajduje się w programie. 88. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji. 89. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 90. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia. 91. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny. 92. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. 93. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki. 94. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. 95. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji. 96. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. 97. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

			98. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia. 99. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup. 100. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny. 101. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”. 102. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 103. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. 104. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. 105. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 106. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet. 107. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. Ochrona stacji roboczych - Mac OSX 1. Procesor 32-bit (x86) / 64-bit (x64), Intel®. 2. Pełne wsparcie dla systemów Mac OS X 10.9 lub nowszy. 3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim. 4. Pomoc w programie (help) w języku polskim oraz angielskim. 5. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 6. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 7. W momencie wykrycia trybu pełnoekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji. 8. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 9. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 10. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności). 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. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 15. 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. 16. 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. 17. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym. 18. Możliwość wykonania skanowania i wysłania pliku do analizy z poziomu menu kontekstowego. 19. Aktualizacje modułów analizy heurystycznej. 20. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 21. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 22. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 23. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 24. Ochrona przed atakami typu „phishing”. 25. Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników: Płyta CD/DVD, Pamięć masowa, karty sieciowe, Drukarka USB, Urządzenie do tworzenia obrazów, Port szeregowy, Urządzenie przenośne. 26. Automatyczna, inkrementacyjna aktualizacja silnika detekcji. 27. Aktualizacja modułów programu antywirusowego ma być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy serwera HTTP. 28. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 29. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po wystąpieniu zdarzenia). 30. Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania syst. operacyjnego. 31. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu

			(antywirus, antyspyware, metody heurystyczne). 32. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera. 33. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień. 34. Program musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP. 35. Program musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP. 36. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy” na modyfikację konfiguracji programu. 37. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 38. Możliwość zdalnego zarządzania programem z poziomu Administracji zdalnej. 39. Ochrona poczty mail: • Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej niezależnie od programu pocztowego. • Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). • Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. • Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie. • Możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu. • Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. Ochrona urządzeń mobilnych opartych o system Android 1. Wspierany system co najmniej Android 5.0. 2. Rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa. 3. Procesor: ARM z obsługą ARMv7 lub x86 Intel Atom. Ochrona antywirusowa: 4. Ochrona plików w czasie rzeczywistym. 5. Ochrona przed atakami typu „phishing”. 6. Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 7. Aplikacja musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 8. Ochrona proaktywna wykrywająca nieznane zagrożenia.

			9. W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie. 10. Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia. 11. Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). Skanowanie na żądanie: 12. Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji. 13. Informacje o skanowaniu mają być przechowywane w plikach dziennika. 14. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania. 15. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia. Ochrona przed kradzieżą: 16. Administrator ma mieć możliwość skonfigurowania zaufanej karty SIM. 17. Dodanie zaufanej karty SIM ma się odbyć w oparciu o kartę wprowadzoną w danym urządzeniu lub w oparciu o wprowadzony ręcznie numer IMSI karty SIM. 18. W przypadku kradzieży urządzenia, Administrator ma mieć możliwość wysłania na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia, d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS. Polityka ustawień: 19. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej: a. połączenie Wi-Fi, b. GPS, c. usługi lokalizacyjne, d. pamięć, e. roaming danych, f. roaming połączeń, g. nieznane źródła, h. tryb debugowania, i. komunikacja NFC, j. szyfrowanie pamięci masowej, k. urządzenie zrootowane.

			Kontrola aplikacji: 20. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji. 21. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji. 22. Blokowanie aplikacji musi być możliwe w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła. Zabezpieczenia urządzenia: 23. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej: a. minimalny poziom zabezpieczeń i złożoność blokady ekranu, b. maksymalną dopuszczaną liczbę błędnych prób odblokowania, c. odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie, d. czas, po którym automatycznie nastąpi blokada ekranu, e. ograniczenie dostępu do kamery wbudowanej w urządzenie. Aktualizacje sygnatur: 24. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji. 25. Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin. 26. Aplikacja ma posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją. Konfiguracja i zdalne zarządzanie: 27. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne. 28. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją. 29. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych. 30. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna. 31. Wdrożenie urządzenia mobilnego z poziomu konsoli zarządzającej musi się odbyć co najmniej na jeden z trzech możliwych sposobów: a. za pomocą kodu QR,

			b. za pomocą unikatowego łącza, c. za pomocą wiadomości e-mail, W ramach aktywacji za pomocą kodu QR musi istnieć możliwość aktywacji w trybie właściciela urządzenia (Android Enterprise Device Owner). Stacje robocze Linux 1. Wymagania sprzętowe: • Procesor 32-bit / 64-bit AMD®, Intel®, • RAM 512MB wolnej pamięci RAM, • HDD 100MB wolnej przestrzeni. 2. Pełne wsparcie dla dystrybucji opartych na systemach Debian i RedHat (Ubuntu, OpenSuse, Fedora, Mandriva itp). Dodatkowe wymagania systemowe : • Kernel 2.6.x, • Biblioteki GNU C w wersji 2.3 lub nowszej, • GTK+ 2.6 lub nowszej, • Zalecana kompatybilność z LSB 3.1. 3. Wsparcie dla dystrybucji 32- i 64-bitowych. 4. Wersja programu dostępna zarówno w języku polskim jak i angielskim. 5. Pomoc w programie (help) w języku polskim. 6. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 7. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 8. Wbudowana technologia do ochrony przed rootkitami. 9. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 10. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 11. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności). 12. Skanowanie plików spakowanych i skompresowanych. 13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 14. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 15. 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. 16. 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. 17. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów. 18. Możliwość wykonania skanowania z poziomu menu kontekstowego. 19. Aktualizacje modułów analizy heurystycznej. 20. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (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. 21. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 22. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 23. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 24. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB. 25. Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników : Napęd CD-Rom, Dyskietka, Firewire, USB, HotPlug, Inne. 26. Automatyczna, inkrementacyjna aktualizacja baz sygnatur wirusów i innych zagrożeń. 27. Aktualizacja systemu antywirusowego ma 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). 28. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 29. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po wystąpieniu zdarzenia). 30. Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego. 31. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 32. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.

			33. Program ma posiadać dwie wersje interfejsu (standardowy – z ukrytą częścią ustawień oraz zaawansowany – z widocznymi wszystkimi opcjami). 34. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz sygnatur wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera. 35. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy" na modyfikację konfiguracji programu. 36. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. Ochrona serwera - Linux 1. Skaner antywirusowy, antyspyware. 2. Skanowanie plików, plików spakowanych, archiwów samorozpakowujących, plików wiadomości e-mail. 3. Konfiguracja wszystkich modułów oprogramowania ma być możliwa poprzez edycję jednego pliku konfiguracyjnego. 4. Możliwość ustawień limitów dla modułu skanującego względem maksymalnego rozmiaru pliku, maksymalnej liczby poziomów kompresji, maksymalnego rozmiaru archiwum, maksymalnego czasu skanowania, rozszerzenia skanowanego pliku. 5. Możliwość skanowania podkatalogów oraz podążania za łączami symbolicznymi (symlinkami) w systemie. 6. Możliwość zdefiniowania częstotliwości aktualizacji programu z dokładnością do jednej minuty. 7. Wbudowany bezpośrednio w program system obsługi plików spakowanych niewymagający zewnętrznych komponentów zainstalowanych w systemie. 8. Brak potrzeby instalacji źródeł jądra systemu oraz kompilacji jakichkolwiek modułów jądra do skanowania plików na żądanie. 9. Możliwość tworzenia przynajmniej pięciu poziomów dokładności czyszczenia zainfekowanych plików. 10. Możliwość skanowania alternatywnych strumieni danych (ADS) obecnych w systemie plików NTFS. 11. Wsparcie dla integracji oprogramowania z modułem Dazuko Access Controll (DAC), który odpowiada za skanowania plików w trybie on-access podczas zdarzeń typu otwarcie, zamknięcie oraz wykonanie pliku. 12. Wsparcie dla skanowania za pośrednictwem biblioteki współdzielonej LIBC, która umożliwia skanowanie plików, które są otwierane, zamykane lub wykonywane przez serwery plików (ftp, Samba), które wykorzystują zapytania do biblioteki LIBC. 13. Możliwość zdefiniowania liczby wątków oraz liczby procesów dla każdego z modułów skanujących. 14. Możliwość tworzenia różnych akcji (przynajmniej 5-ciu różnych) w zależności od typu zdarzenia (w przypadku pliku nieprzeskanowanego, pliku przeskanowanego, pliku zainfekowanego). 15. Logowanie wykonanych akcji na plikach oraz zdarzeń dla poszczególnych modułów oprogramowania. 16. Wsparcie dla zewnętrznego serwera logującgo syslog, możliwość definiowania dowolnego pliku logu w tym co najmniej: daemon, mail, user.

			17. Możliwość zdefiniowania przynajmniej ośmiu poziomów logowania programu. 18. Możliwość uruchomienia interfejsu programu dostępnego przez przeglądarkę webową. 19. Interfejs ma umożliwiać modyfikację ustawień programu oraz jego aktualizację i przeskanowanie dowolnego obszaru systemu plików, a także przegląd statystyk dotychczas przeskanowanych plików. 20. Interfejs programu dostępny przez przeglądarkę webową wykorzystuje wbudowany w program serwer http. 21. Możliwość uruchomienia interfejsu webowego na dowolnym porcie TCP. 22. Możliwość uruchomienia interfejsu webowego na dowolnym interfejsie sieciowym. 23. Możliwość zabezpieczenia dostępu do interfejsu webowego poprzez zdefiniowanie nazwy użytkownika i hasła. 24. Interfejs webowy ma przedstawić administratorowi dokładny wynik skanowania poszczególnych plików w systemie wraz z możliwością pobrania tych wyników w postaci pliku tekstowego celem późniejszej analizy. 25. Możliwość podglądu informacji o licencji bezpośrednio z poziomu interfejsu webowego, która zawiera przynajmniej informacje o liczbie dni do wygaśnięcia licencji, nazwę użytkownika licencji oraz pełną nazwę produktu, którego dotyczy licencja. 26. Program ma być wyposażony w graficzny menadżer kwarantanny dostępny z poziomu interfejsu webowego. Menadżer ma oferować administratorowi możliwość przeglądu, pobrania, dodania i usunięcia plików w kwarantannie. 27. Menadżer kwarantanny ma posiadać możliwość wyszukiwania plików znajdujących się w kwarantannie przynajmniej po nazwie pliku, dacie dodania pliku (możliwość definiowania przedziałów czasowych), rozmiarze (możliwość definiowania minimalnej i maksymalnej wielkości) oraz ilości plików (możliwość definiowania minimalnej i maksymalnej ilości). 28. Interfejs webowy do zarządzania produktem ma opierać się o wbudowane w program biblioteki PHP w wersji nie niższej niż 5.2.8. 29. Interfejs dostępny poprzez przeglądarkę webową ma umożliwiać zarządzanie programem również wtedy, gdy przeglądarka nie obsługuje kodu JavaScript. 30. Możliwość stworzenia lokalnego repozytorium aktualizacji dla przynajmniej dwóch różnych produktów antywirusowych instalowanych na stacjach Windows. 31. Możliwość tworzenia osobnych ustawień skanowania dla poszczególnych użytkowników w systemie. 32. Możliwość definicji użytkownika systemowego z prawami, którego zostanie uruchomiony demon skanujący. 33. Współpraca z mechanizmem automatycznej wysyłki podejrzanych plików do laboratorium producenta. 34. Możliwość uaktywnienia dodatkowych funkcjonalności programu (moduł skanujący pocztę e-mail oraz moduł skanujący dla bram sieciowych), które nie wymagają od użytkownika instalacji dodatkowych zależności ani modułów a jedynie zaczytanie dodatkowych plików licencji. 35. Możliwość instalacji na dowolnym systemie Linux 2.6.x i nowszym. 36. Możliwość instalacji na systemie FreeBSD 6.x, 7.x, 8.x i 9.x. 37. Wsparcie dla platform 32 oraz 64 bitowych.

			38. Architektura programu umożliwia jego uruchomienie i optymalizację zarówno dla systemów jedno jak i wieloprocesorowych. 39. System ma mieć możliwość powiadomienia administratora o wykryciu infekcji oraz powiadomienia o zbliżającym się terminie wygaśnięcia licencji za pośrednictwem poczty e-mail. 40. Możliwość szybkiej konfiguracji oprogramowania poprzez skrypt powłoki. Skrypt umożliwia prostą konfigurację oprogramowania stosownie do wykrytego systemu operacyjnego, w jakim oprogramowanie zostało zainstalowane. 41. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. Ochrona serwera Windows 1. Wsparcie dla systemów: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2008 R2 SP1, Microsoft Windows Server 2008 SP2 (oparty na procesorze x86 i x64), Server Core (Microsoft Windows Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016). 2. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. 3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 5. Wbudowana technologia do ochrony przed rootkitami i exploitami. 6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (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. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 11. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 12. Możliwość skanowania dysków sieciowych i dysków przenośnych. 13. Skanowanie plików spakowanych i skompresowanych. 14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 15. Aplikacja powinna wspierać mechanizm klastrowania.

			16. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 17. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, b. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, d. tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, e. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach. 18. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. 19. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 20. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 21. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. 22. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 23. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze. 24. Program 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 oraz urządzeń przenośnych. 25. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 26. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. 27. Program 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. 28. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 29. Program musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.

			30. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 31. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 32. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 33. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 34. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 35. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 36. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 37. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 38. 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. 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 programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 41. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 42. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 43. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 44. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. 45. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła. 46. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.

			47. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 48. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji. 49. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. 50. Po instalacji programu, 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 zagrożeń. 51. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. 52. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. 53. Program ma 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 procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 54. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa. 55. System antywirusowy ma 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. 56. Automatyczna, inkrementacyjna aktualizacja silnika detekcji. 57. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. 58. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji. 59. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. 60. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. 61. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). 62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 63. Aplikacja musi wspierać skanowanie magazynu Hyper-V. 64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów. 65. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i

			samego oprogramowania. 66. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 67. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”. 68. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 69. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia. 70. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 71. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 72. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. 73. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 74. Program 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. 75. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 76. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. 77. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. Ochrona bezagentowa maszyn wirtualnych 1. Rozwiązanie zapewnia bezagentową ochronę maszyn wirtualnych w wersjach systemu gościa: Windows XP SP3 x32, Windows Server 2003 SP2 x32, Windows Vista x32, Windows 7 x32/x64, Windows Server 2008 x32/x64, Windows Server 2008 R2 x32/x64, Windows Server 2012, Windows Server 2012 R2, Windows 8 x32/x64, Windows 8.1 x32/x64, Windows 10 x32/x64. 2. Rozwiązanie umożliwia ochronę nieograniczonej liczby fizycznych serwerów ESXi w roli hypervisora. 3. Ochrona środowiska wirtualnego zarządzana z jednej, centralnej konsoli administracyjnej, niezależnie od ilości chronionych hostów wirtualnych i serwerów w roli hypervisora. 4. W ramach całego chronionego środowiska wirtualnego wymagane jest uruchomienie tylko jednej maszyny wirtualnej. 5. Wyłączenie serwera z centralną konsolą administracyjną, nie wpływa na działanie mechanizmów ochrony maszyn

			wirtualnych (silniki antywirusowe pozostają aktywne). 6. Wdrożenie rozwiązania do ochrony środowiska wirtualnego jest przeprowadzane w sposób zautomatyzowany z wykorzystaniem dedykowanego narzędzia, niezależnie od liczby systemów wirtualnych. 7. Wdrożenie rozwiązania nie wymaga instalowania jakichkolwiek zewnętrznych składników czy plug-inów na natywnym systemie operacyjnym nadzorcy wirtualnego (hypervisora). 8. Rozwiązanie funkcjonuje bez konieczności instalowania jakiegokolwiek własnego agenta na systemach operacyjnych wirtualnych hostów. 9. Rozwiązanie wspiera środowisko VMware vSphere 5.5 U2 lub nowsze wraz z VMware NSX 6.2.4 10. Ochrona środowiska wirtualnego realizowana jest z wykorzystaniem VMWare EPSec Library. 11. Ochrona środowiska wirtualnego sprzedawana wraz z dwoma możliwymi do wyboru modelami licencjonowania: liczba chronionych hypervisorów lub liczba procesorów serwera hypervisora. 12. Ochrona środowiska wirtualnego dostarczana jest wyłącznie w postaci obrazów maszyn wirtualnych (OVA- Open Virtual Appliance). 13. Rozwiązanie wspiera technologię Vmware vMotion Migration - host wirtualny jest chroniony w trybie ciągłym niezależnie od tego na jakim serwerze fizycznym znajduje się w ramach jednego środowiska vSphere. 14. System ochrony maszyny wirtualnej działa w trybie aktywnym (ochrona systemu w czasie rzeczywistym) jak i pasywnym (realizowanie skanowania na żądanie). 15. Mechanizmy ochrony wirtualnych serwerów i desktopów realizowane są bezagentowo przez silnik producenta uruchomiony na dedykowanym wirtualnym appliance. 16. Aktualizacje baz sygnatur antywirusowych pobierane są wyłączenie przez silnik producenta uruchomiony na dedykowanym wirtualnym appliance. 17. Silnik antywirusowy wykorzystuje mechanizmy weryfikowania w chmurze producenta plików i procesów w czasie rzeczywistym - musi istnieć możliwość zdecydowania, czy funkcja ta ma być włączona, czy też nie. 18. Do mechanizmów ochrony maszyn wirtualnych rozwiązanie wykorzystuje wyłączenie sieć zdefiniowaną programowo (SDN). 19. Wyłączenie adaptera sieci TCP/IP na maszynie wirtualnej w żaden sposób nie wpływa na jej ochronę przez silnik antywirusowy. 20. Administrator ma możliwość zdefiniowania aktywacji ochrony bezagentowej tylko na wybranych maszynach wirtualnych. Administracja zdalna 1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2008 R2, 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. 6. 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. 7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy. 9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6. 10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs. 11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji. 12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 13. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 14. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 15. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 16. Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”. 17. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów. 18. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy. 19. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 20. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 21. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS. 22. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP. 23. 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. 24. Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap. 25. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji

			silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych. 26. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów. 27. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 28. 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, host agenta wirtualnego. 29. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android. 30. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS. 31. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywir., zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci. 32. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 33. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające. 34. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania. 35. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 36. 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. 37. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play. 38. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 39. 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. 40. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego. 41. 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. 42. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 43. 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. 44. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 45. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej. 46. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany. 47. 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. 48. 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. 49. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych. 50. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. 51. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej. 52. 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. 53. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 54. 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. 55. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania. 56. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.

			57. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta. 58. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej. 59. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji. 60. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce. 61. Serwer administracyjny musi posiadać minimum 170 szablonów raportów, przygotowanych przez producenta. 62. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów. 63. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie. 64. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy. 65. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania. 66. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów. 67. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny. 68. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF, CSV oraz PS. 69. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 70. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów. 71. Powiadomienia mailowe mają być wysyłane w formacie HTML. 72. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń. 73. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. 74. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. 75. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji. 76. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego,

			pliku offline licencji oraz konta systemu zarządzania licencjami. 77. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych. 78. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu. 79. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. 80. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan. 81. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. 82. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli. 83. 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. 84. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta. 85. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli. 86. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania. 87. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie. 88. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.