Specyfikacja wymagań
na zakup ZINTERGROWANEGO SYSTEMU BEZPIECZEŃSTWA

Spis treści

CZĘŚĆ I. PLATFORMA OCHRONY AUTOMATYCZNEJ

System składa się z dwóch elementów:

- I.a. Systemu ochrony automatycznej,
- I.b. Oprogramowanie zapewniające automatyczną ochronę rozbudowanych sieci.

Ad. I.a. System ochrony automatycznej

- **Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych aplikacji instalowanych na platformach ogólnego przeznaczenia.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie firewall, ochrony w warstwie aplikacji, protokołów routingu dynamicznego.

- **Redundancja, monitoring i wykrywanie awarii:**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

- **Interfejsy:**

W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 7.4 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 500 Mbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 130 Mbps.

- **Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych platform lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

- **Polityki, Firewall:**
  1. System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.
  1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
  2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: Translację jeden do jeden oraz jeden do wielu, Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
  3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- **Połączenia VPN**
  1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
     a. Wsparcie dla IKE v1 oraz v2.
     b. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
     c. Obsługa protokołu Diffie-Hellman grup 19 i 20.
     d. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
     e. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
     f. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
     g. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
     h. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
     i. Mechanizm „Split tunneling" dla połączeń Client-to-Site.
  2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
     a. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
     b. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
- **Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: Routingu statycznego .
    - Policy Based Routingu.
    - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

- **Zarządzanie pasmem**
  1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
  2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
  3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
- **Kontrola Antywirusowa**
  1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
  2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
  3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
  4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
- **Ochrona przed atakami**
  1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
  2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
  3. Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
  4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
  5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
  6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
  7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
- **Kontrola aplikacji**
  1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
  2. Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
  3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
  4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
  5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
- **Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

- **Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
    a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
    b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
    c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

- **Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

- **Logowanie**

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

4. Musi istnieć możliwość logowania do serwera SYSLOG.

- **Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

a. ICSA lub EAL4 dla funkcji Firewall,
b. ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW,
c. ICSA dla funkcji SSL VPN.

- **Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów co najmniej do dnia 31/03/2021. Powinny one obejmować kontrolę aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu Sandbox, antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

- **Gwarancja oraz wsparcie**

System musi być objęty serwisem gwarancyjnym producenta przez okres co najmniej do 31/03/2021. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

- **Szkolenie**

W ramach realizacji zadania zamawiający zobowiąże się do przeprowadzenia jednodniowego (8 godzin) szkolenia produktowego dla trzech pracowników zamawiającego w zakresie użytkowania i administrowania dostarczonym systemem.

Ad. I.b. Oprogramowanie zapewniające automatyczną ochronę rozbudowanych sieci

Wymagania systemu:

- **Licencje i aktualizacje**

Oprogramowanie powinno posiadać możliwość aktualizacji i aktualizacji baz sygnatur do najmniej do 31/03/2023. Oprogramowanie powinno posiadać licencje do zabezpieczenia co najmniej 150 punktów tj. stacji roboczych, serwerów, urządzeń mobilnych

- **Ochrona stacji roboczych - Windows**

1. Pełne wsparcie dla systemu 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**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
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, pojedynczych plików „na żądanie” lub według harmonogramu.
7. 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.
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 priorytetu wykorzystania 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. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
15. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
16. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
17. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
18. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.

19. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
20. 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.
21. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
22. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
23. 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).
24. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
25. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
26. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
27. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
28. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
29. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
30. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
31. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
32. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
33. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
34. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
35. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
36. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
37. 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.
38. 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.

39. 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.
40. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
42. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
43. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
44. 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.
45. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
46. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
47. 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.
48. 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.
49. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
50. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
51. 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.
52. 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.
53. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
54. 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.
55. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
56. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.

57. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
58. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
59. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
60. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
61. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
62. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
63. 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.
64. 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.
65. 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.
66. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
67. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
68. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
69. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
70. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
71. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
72. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
73. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
74. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
75. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
76. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron internetowych i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
77. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
78. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.

79. 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.
80. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
81. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
82. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
83. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
84. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
85. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
86. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
87. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
88. 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.
89. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
90. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
91. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
92. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
93. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
94. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
95. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
96. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
97. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
98. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.

- **Ochrona przed spamem**

1. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.

2. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
3. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
4. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
5. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
6. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
7. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym w programie Microsoft Outlook.
9. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana"
10. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana".
11. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

- **Zapora osobista**

1. Zapora osobista ma pracować w jednym z czterech trybów:
    a. tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    b. tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,
    c. tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    d. tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
2. Program musi oceniać reguły zapory systemu Windows.
3. Możliwość tworzenia list sieci zaufanych.
4. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
5. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
6. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
7. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
8. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
9. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
10. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
11. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
12. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.

13. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
14. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
15. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
16. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
    e. z aplikacją lokalną, którą administrator wskazuje z listy,
    f. z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

- **Kontrola dostępu do stron internetowych**

1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli dostępu do stron internetowych.
2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
3. Aplikacja musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
4. Podstawowe kategorie, w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy,
2. nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
5. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
6. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta.
7. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
8. Aplikacja musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.
9. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.

- **Stacje Robocze Apple Mac OS X**

1. Pełne wsparcie dla systemów Mac OS X 10.9 lub nowszy.
2. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
5. 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.
6. Skanowanie w czasie rzeczywistym otwieranych, tworzonych 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 (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).
9. Możliwość skanowania dysków sieciowych i dysków przenośnych.
10. Skanowanie plików spakowanych i skompresowanych.
11. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
13. 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.
14. 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.
15. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
16. Możliwość wykonania skanowania i wysłania pliku do analizy z poziomu menu kontekstowego.
17. Aktualizacje modułów analizy heurystycznej.
18. 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.
19. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
20. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
21. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
22. Ochrona przed atakami typu „phishing”.
23. Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników: Płyta CD/DVD, Pamięć masowa, Sieć, Drukarka USB, Urządzenie do tworzenia obrazów, Port szeregowy, Urządzenie przenośne.
24. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
25. Aktualizacja modułów programu antywirusowego ma być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy serwera HTTP.
26. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
27. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po wystąpieniu zdarzenia).
28. Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.
29. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

30. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera.
31. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.
32. Program musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP.
33. Program musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP.
34. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy" na modyfikację konfiguracji programu.
35. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
36. Możliwość zdalnego zarządzania programem z poziomu Administracji zdalnej.
37. Ochrona poczty mail:
    a. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej niezależnie od programu pocztowego.
    b. 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).
    c. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
    d. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
    e. Możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu.
    f. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
38. Zapora osobista
    a. Zapora osobista może pracować jednym z 2 trybów:
        i. Automatyczny z wyjątkami - umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
        ii. Interaktywny – dla każdej nieznanej komunikacji generowane jest pytanie dla użytkownika o jej odblokowanie.
    b. Możliwość dezaktywacji funkcji zapory sieciowej.
    c. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
    d. Możliwość odnotowania faktu nawiązania danego połączenia w dzienniku zdarzeń.
    e. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
    f. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla profilu: Publiczny, Praca, Dom.
    g. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
    h. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
    i. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.

j. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
k. Aktywacja stref ma się odbywać min. w oparciu o: interfejs sieciowy w systemie, Sieć WiFi, Podsieć IPv4/IPv6, Zakres adresów IPv4/IPv6, Adres IPv4/IPv6.

39. Kontrola dostępu do stron internetowych
    a. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
    b. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
    c. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
    d. Reguły mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
    e. Aplikacja musi posiadać możliwość filtrowania URL w oparciu o co najmniej 140 kategorii i podkategorii.
    f. Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpozna`ne kategorie oraz elementy niezaliczone do żadnej kategorii.
    g. Lista adresów URL, znajdujących się w poszczególnych kategoriach, musi być na bieżąco aktualizowana przez producenta.
    h. Użytkownik musi posiadać możliwość wyłączenia modułu kontroli dostępu do stron internetowych.

- **Stacje robocze Linux**

1. Pełne wsparcie dla dystrybucji opartych na systemach Debian i RedHat (Ubuntu, OpenSuse, Fedora, Mandriva itp). Dodatkowe wymagania systemowe :
    a. Kernel 2.6.x,
    b. Biblioteki GNU C w wersji 2.3 lub nowszej,
    c. GTK+ 2.6 lub nowszej,
    d. Zalecana kompatybilność z LSB 3.1.
2. Wsparcie dla dystrybucji 32- i 64-bitowych.
3. Wersja programu dostępna zarówno w języku polskim jak i angielskim.
4. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
6. Wbudowana technologia do ochrony przed rootkitami.
7. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
9. 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).
10. Skanowanie plików spakowanych i skompresowanych.
11. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
13. 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.
14. 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.
15. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
16. Możliwość wykonania skanowania z poziomu menu kontekstowego.
17. Aktualizacje modułów analizy heurystycznej.
18. 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.
19. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
20. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
21. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
22. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.
23. Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników: Napęd CD-Rom, Dyskietka, Firewire, USB, HotPlug, Inne.
24. Automatyczna, inkrementacyjna aktualizacja baz sygnatur wirusów i innych zagrożeń.
25. 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).
26. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
27. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po wystąpieniu zdarzenia).
28. Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.
29. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
30. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.
31. Program ma posiadać dwie wersje interfejsu (standardowy – z ukrytą częścią ustawień oraz zaawansowany – z widocznymi wszystkimi opcjami).
32. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz sygnatur wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera.

33. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy” na modyfikację konfiguracji programu.
34. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

- **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.
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).
3. Skanowanie na żądanie:
4. Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji.
5. Informacje o skanowaniu mają być przechowywane w plikach dziennika.
6. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.
7. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.
8. Ochrona przed kradzieżą:
9. Administrator ma mieć możliwość skonfigurowania zaufanej karty SIM.
10. 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.
11. 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.
12. Polityka ustawień:
    a. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej:
        i. połączenie Wi-Fi,
        ii. GPS,
        iii. usługi lokalizacyjne,
        iv. pamięć,
        v. roaming danych,
        vi. roaming połączeń,
        vii. nieznane źródła,
        viii. tryb debugowania,
        ix. komunikacja NFC,
        x. szyfrowanie pamięci masowej,

xi. urządzenie zrootowane.

13. Kontrola aplikacji:
    a. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
    b. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
    c. 22. Blokowanie aplikacji musi być możliwe w oparciu o:
        i. nazwę aplikacji,
        ii. nazwę pakietu,
        iii. kategorię sklepu Google Play,
        iv. uprawnienia aplikacji,
        v. pochodzenie aplikacji z nieznanego źródła.
14. Zabezpieczenia urządzenia:
    a. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
        i. minimalny poziom zabezpieczeń i złożoność blokady ekranu,
        ii. maksymalną dopuszczaną liczbę błędnych prób odblokowania,
        iii. odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie,
        iv. czas, po którym automatycznie nastąpi blokada ekranu,
        v. ograniczenie dostępu do kamery wbudowanej w urządzenie.
15. Aktualizacje sygnatur:
    a. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
    b. 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.
    c. Aplikacja ma posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją.

- **Ochrona serwera - Linux**

Architektura rozwiązania:

1. Skaner antywirusowy i antyspyware.
2. Skanowanie plików, plików spakowanych i archiwów samorozpakowujących.
3. Oprogramowanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów oprogramowania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
4. Oprogramowanie musi posiadać wbudowany mechanizm typu ,,watchdog”. Monitoruje on tzw. stan zdrowia poszczególnych mikro-serwisów i automatycznie przeładowuje je w przypadku wykrycia zakłóceń w pracy mikro-serwisu.
5. Architektura rozwiązania musi pozwalać na uruchamianie poszczególnych mikro-serwisów, tylko na czas realizacji funkcjonalności przez nie realizowanych, co pozwala w znaczącym stopniu ograniczyć wykorzystanie zasobów systemu operacyjnego.
6. Oprogramowanie antywirusowe musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności.
7. Oprogramowanie antywirusowe musi być wyposażone w moduł ochrony systemu plików w czasie rzeczywistym. Moduł nie może wymagać instalowania jakichkolwiek dodatkowych

komponentów w systemie operacyjnym. Wszystkie komponenty muszą być instalowane w systemie, podczas instalacji z dostarczonego instalatora binarnego.

8. Silnik ochrony systemu plików w czasie rzeczywistym musi stanowić dodatkowy moduł jądra systemu Linux i musi być dodawany do jądra, podczas procesu instalacji oprogramowania antywirusowego.
9. Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i obejmuje skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych.
10. Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury.
11. Oprogramowanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie ,,Permissive" jak i ,,Enforcing".
12. Oprogramowanie podczas procesu instalacji, musi dodawać i konfigurować własne polityki modułu SELinux, które są kompatybilne z następującymi dystrybucjami systemów Linux: Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Centos 6, Centos 7.
13. Wszystkie mechanizmy bezpieczeństwa oprogramowania muszą wspierać system informowania o zagrożeniach w czasie rzeczywistym. System ten pozwala na weryfikowanie reputacji plików oraz procesów i identyfikację nowych i nieznanych zagrożeń.
14. Skaner systemu plików w czasie rzeczywistym musi działać dla operacji obsługi plików, dla co najmniej takich operacji jak: dostęp do pliku, utworzenie (zapisanie) pliku.
15. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
17. Oprogramowanie musi być wyposażone we własny wiersz polecenia (CLI). Polecenia muszą być odpowiedzialne co najmniej za: skanowanie na żądanie, konfigurację mechanizmów bezpieczeństwa, uruchamianie aktualizacji, przeglądanie logów aplikacji, konfigurację graficznego interfejsu użytkownika, obsługę kwarantanny plików.
18. Rozwiązanie musi wspierać system plików zamontowany z flagą ,,noexec".
19. Oprogramowanie musi pozwalać na uruchamianie zadań skanowania działających ,,w tle", z możliwością ustawienia dla nich niskiego priorytetu.
20. Zadania skanowania nie mogą zmieniać znacznika dostępu do plików.

- **Interfejs graficzny**

1. Produkt musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna musi działać w oparciu o dynamicznie generowaną zawartość tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5.
3. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
4. Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu o protokół HTTPS.
5. Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP.
6. Logowanie do lokalnej konsoli administracyjnej musi być realizowane, poprzez podanie danych w postaci nazwy użytkownika i zdefiniowanego dla niego hasła.
7. Administrator systemu musi mieć możliwość zdefiniowania dodatkowych kont użytkowników, w lokalnej konsoli administracyjnej.
8. Lokalna konsola administracyjna musi zapewniać funkcjonalność zweryfikowania stanu licencji i informacji na jej temat.

9. Z poziomu lokalnej konsoli administracyjnej musi być możliwość zarządzania, wbudowanym modułem menadżera kwarantanny.
10. Lokalna konsola administracyjna musi zapewniać możliwość przełączenia wersji językowej konsoli, na etapie logowania. Lokalna konsola administracyjna musi posiadać interfejs, co najniej języku: polskim, angielskim, niemieckim, francuskim, hiszpańskim, japońskim.

- **Skanowanie sieciowych systemów plików**

1. Oprogramowanie antywirusowe musi pozwalać na skanowanie plików składowanych i obsługiwanych przez zewnętrzne rozwiązania obsługi danych typu NAS / SAN.
2. Oprogramowanie antywirusowe nie może wymagać instalacji jakichkolwiek dodatkowych modułów na rozwiązaniach typu NAS / SAN, a skanowanie plików musi się odbywać wyłącznie w oparciu o protokół ICAP.
3. Rozwiązanie musi umożliwiać zmianę domyślnego portu protokołu ICAP.
4. Oprogramowanie antywirusowe, do celów skanowania plików na rozwiązaniach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

- **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
16. 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 antywirusowa, 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.
89. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, grupy, zadania, komputery oraz szablony grupy dynamicznych.
90. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta.
91. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.

- **Szkolenie**

W ramach realizacji zadania zamawiający zobowiąże się do przeprowadzenia jednodniowego (8 godzin) szkolenia produktowego dla trzech pracowników zamawiającego w zakresie użytkowania i administrowania dostarczonym systemem.

CZĘŚĆ II. PROAKTYWNE ZAPOBIEGANIE INCYDENTOM

System do cyklicznego testowania zespołu bezpieczeństwa pod kątem możliwości obrony Uczelni przed obecnymi zagrożeniami

1. Licencja na oprogramowanie i dostęp do co najmniej stu uruchomień testów zespołowych.
2. Elementy składowe:
   - Serwer platformy: Serwer ten jest centralnym elementem platformy, przeznaczony do pełnienia następujących ról:
     - panel Zarządzania: aplikacja webowa, wykorzystująca bazę danych służąca do konfiguracji za pośrednictwem API OpenStacka,
     - panel Zarządzania Maszyny wirtualne oraz symulowane operacje i zarządzanie siecią,
     - repozytorium zasobów platformy: zasoby maszyn wirtualnych, archiwum scenariuszy treningowych, kopie zapasowe.
   - Serwer roboczy: odpowiedzialny za prawidłową pracę całego systemu, posiadający wystarczającą moc obliczeniową i zasoby do obsługi symulowanych środowisk treningowych.
   - Interaktywny panel, wraz z dołączonym inteligentnym systemem Windows 10.
3. Wielozadaniowość
   - Platforma oparta o rozwiązania wirtualizacji. Poszczególne środowiska szkoleniowe muszą być logicznie odseparowane od siebie. Środowisko posiada cały niezbędny sprzęt wirtualny ICT: routery, przełączniki, serwery, firewalle, symulowane usługi internetowe. Na platformie można uruchomić treningi.
   - Pełna elastyczność w zakresie uruchamiania różnych scenariuszy dla uczestników treningów (np. możliwość realizacji tego samego scenariusza w osobnych treningach dla różnych grup uczestników).
4. Specyfikacja szczegółowa:
   - realizacja scenariuszy treningowych i testowych.
   - możliwość tworzenia środowisk, które pomagają w praktycznej ocenie skuteczności rozwiązań zabezpieczających zarówno w postaci oprogramowania (AV, SIEM, EDR, itp.), jak i rozwiązań fizycznych (np. Firewall),
   - pełna swoboda w zakresie użycia protokołów sieciowych i systemów operacyjnych, wraz z możliwością łączenia rozwiązań fizycznych,
   - możliwość uruchomienia szkoleń zarówno dla osób odpowiedzialnych za obronę (reagowanie na incydenty, kryminalistyka cyfrowa, analiza danych, analiza złośliwego oprogramowania itp.), jak i za działania ofensywne (etyczny hacking, pentesting, red teaming, emulacja przeciwnika),
   - możliwość oceny użyteczności rozwiązań bezpieczeństwa poprzez realizację zwykłych scenariuszy zaimplementowanych w oprogramowanie,
   - prowadzenie treningów zespołu bezpieczeństwa, które pozwolą na zbudowanie umiejętności zespołowych i poprawę komunikacji,
   - wbudowane mechanizmy komunikacji, takie jak chat,
   - możliwość odbywania treningów w sposób zdalny dzięki dostępowi poprzez aplikację internetową lub połączenie VPN,
   - możliwość zastosowania, jako środowisko testowe, np. możliwość tworzenia pojedynczych maszyn od podstaw lub uploadowania gotowych obrazów maszyn na platformę, możliwość łatwego zbudowania wirtualnego środowiska testowego, które w dużym stopniu odzwierciedla środowisko produkcyjne uczeni (środowisko to może być wykorzystywane do analizy zmian konfiguracji pod kątem ich wpływu na bezpieczeństwo lub do testowania nowych technologii przed wprowadzeniem ich do środowiska produkcyjnego),

- możliwość edycji scenariuszy treningowych oraz kopiowania sieci zawartych w scenariuszu, co pozwala na ich łatwą modyfikację,
- interfejs użytkownika, pozwalający również na prowadzenie szkoleń specjalistycznych szkoleń z zakresu świadomości bezpieczeństwa IT dla odbiorców o mniejszych umiejętnościach technicznych,
- panel trenera pozwalający na zarządzanie każdym scenariuszem testowym i treningowym,
- wersja oprogramowania powinna byś dostosowana do warunków technicznych Uczelni.

5. Instalacja i szkolenie produktowe

W ramach realizacji zadania zamawiający zobowiąże się do:

a. Instalacji produktu na wskazanych serwerach (fizycznych lub VMware),
b. Przeprowadzenia jednodniowego (8 godzin) szkolenia produktowego dla trzech pracowników zamawiającego w zakresie użytkowania i administrowania dostarczonym systemem.
c. Dostarczenia opisu scenariuszy testowych i ćwiczeń w formie pisemnej w języku polskim i angielskim.

CZĘŚĆ III. ANALIZA ŚLEDCZA NOŚNIKÓW PO INCYDENCIE

Opis:

Aplikacja umożliwiająca zespołowi bezpieczeństwa skuteczną analizę incydentu polegającą na:

a. przeprowadzeniu zabezpieczenia danych w znaczeniu informatyki śledczej,
b. wykonaniu analizy śledczej. Aplikacja z musi mieć możliwość akwizycji i analizy zarówno urządzeń komputerowych, urządzeń mobilnych oraz zasobów internetowych.

Wymagania:

- Akwizycja i skanowanie urządzeń mobilnych i komputerowych, chmur. Możliwość pełnego fizycznego odczytu danych i obejścia hasła na urządzeniach wielu producentów, w tym:
  - systemy mobilne:
    - Android
    - iOS
    - Kindle Fire
    - urządzenia wspierające media transfer protocol (MTP)
    - karty SIM,
  - systemy komputerowe:
    - HDD, SSD, USB, SD flash drives,
  - platformy Cloud-based:
    - Amazon Web Services (AWS),
    - Apple,
    - Box.com,
    - Dropbox,
    - IMAP/POP Email,
    - Facebook,
    - Google,
    - Instagram,
    - Lyft,
    - Microsoft,
    - Microsoft Azure,
    - Microsoft Teams,
    - Slack,
    - Twitter,
    - Uber,
    - WhatsApp (Google Drive backups and QR code access).
- Funkcjonalność analizy artefaktów z usuniętych plików w systemach plików NTFS i FAT oraz odtwarzania metadanych, takie jak nazwy plików i sygnatury czasowe. Możliwość odtworzenia artefaktów z zagnieżdżonych archiwów i mobilnych kopii zapasowych. Podczas wyszukiwania danych w zagnieżdżonych archiwach, na przykład pliku .zip w pliku .zip, możliwość wyboru warstw przeszukiwania. Możliwość wyboru opcji skanowania ujawnionych archiwów i kopii zapasowych urządzeń mobilnych, w tym:
  - obrazy bitowe systemów komputerowe:
    - podłączone dyski i udziały,
    - pliki i foldery,
    - obrazy,
    - Volume shadow copies,
    - pliki zrzutów pamięci,
  - obrazy bitowe systemów mobilnych:
    - Android,
    - iOS,

        - Windows Phone,
        - Kindle Fire,
    - źródła Cloud including:
        - AccessData images,
        - Apple warrant returns,
        - Facebook warrant returns,
        - Facebook Download Your Information archives,
        - Instagram warrant returns,
        - archiwa Google Takeout,
        - Google warrant returns,
        - backup iCloud,
        - Microsoft Office 365 Unified Audit Logs.
- Akwizycja i skanowanie chmury. Możliwość uzyskania kontaktów użytkownika Office 365. Pracując w sieci lokalnej (LAN), można teraz łączyć się z Internetem przy użyciu systemu proxy. Możliwość uzyskania kopii zapasowych iCloud z kont, które mają uwierzytelnianie dwuskładnikowe dla systemu iOS w wersji 11.1 i niższej.
- Zaawansowana konfiguracja akcji przeszukiwania danych:
    - dodawanie słów kluczy oraz list słów kluczy,
    - przeszukiwanie archiwów o backupów urządzeń mobilnych,
    - obliczanie funkcji skrótu dla wszystkich plików w obrazie źródłowym,
    - kategoryzowanie obrazów oraz zawartości czatów z użyciem zaawansowanych narzędzi opartych o AI,
    - kategoryzowanie obrazów i wideo w oparciu o bazy hash znanych plików w tym plików .json w projektu VIC i CAID,
    - dynamiczne przeszukiwanie baz SQLite,
    - wyszukiwanie wybranych artefaktów plików.
- Analiza artefaktów z urządzeń mobilnych i komputerów:
    - komunikatory internetowe - [iOS. Android, Windows] - Viber Messages, KakaoTalk, Messenger, inne.
    - historia lokalizacji: Obsługa analizowania i przetwarzania dla buforowanych lokalizacji systemu z obrazu GrayKey,
    - możliwość analizowania z uwzględnieniem podejrzanych adresów URL zidentyfikowanych przez SANS Internet Storm Center (ISC) – Podejrzana lista domen,
    - Prasowanie w celu połączenia aktywności użytkownika P2P z określonym GUID użytkownika,
    - Możliwość analizowania kart płatniczych i zapisanych karnetów, takich jak karty pokładowe, karty członkowskie i inne,
    - Możliwość analizowania informacji o urządzeniach Bluetooth, do które zostały odnalezione przez urządzenie, iOS,
    - możliwość analizy wiadomości iMessage /SMS/MMS w celu odzyskania informacji o nadawcy / odbiorcy, znaczników czasowych i innych.
- Raportowanie

Możliwość eksportu wyników analiz do różnych formatów w celu dostarczenia informacji na poziomie zarządczym lub operacyjnym, w tym:

    - Excel, XML, HTML, PST, PDF, inne,
    - tworzenie tzw. raportów przenośnych w celu umożliwienia przeglądania zawartości dużych zbiorów danych w postaci elektronicznej.

6. Instalacja i szkolenie produktowe

W ramach realizacji zadania zamawiający zobowiąże się do:

a. Instalacji produktu na wskazanych maszynach (VMware),

b. Przeprowadzenia jednodniowego (8 godzin) szkolenia produktowego dla trzech pracowników zamawiającego w zakresie użytkowania i administrowania dostarczonym systemem.

CZĘŚĆ IV. ODTWARZANIE DANYCH PO ATAKU

OPIS:

Aplikacja wraz z wyposażeniem pozwalająca na przeprowadzenie skutecznego odtworzenia (odzyskiwania) danych z większości obecnie używanych nośników danych.

WYMAGANIA:

- system zapewnia narzędzia służące do odzyskiwania danych z nośników danych, które nie są wykrywane lub rozpoznawane przez systemy operacyjne lub dane na nich zapisane padły ofiarą ataku hackerskiego,
- możliwość podłączenia nośników danych z następującymi interfejsami: SATA, ATA, PCI Express, SAS, USB,
- zapewnienie obsługi nowych technologii SSD oraz tradycyjnych HDD,
- możliwość uzyskiwania dostępu do nośników poprzez lokalną sieć LAN:
  - dodatek sieciowy umożliwiający przejęcie kontroli przez sieć LAN, oferując w locie funkcjonalność pobierania danych, skutecznie pozwalając technikom na wybranie określonych plików / folderów do odzyskania przed wykonaniem pełnego klonowania,
- możliwość odtwarzania plików/folderów w systemach plików NTFS, HFS +, APFS, EXT 2/3/4, FAT32, XFS, exFAT,
- obsługa funkcji SATA do diagnostyki dysków i obrazowania, takich jak PHY Control,
- możliwość przetwarzania osobno każdej głowicy, w zależności od stopnia uszkodzenia,
- możliwość dwukierunkowego odczytu dysków,
- możliwość budowania map głowic,
- możliwość wykonania kopii nośnika w trybie odzyskiwania danych standard oraz forensic,
- odtwarzanie danych z niestabilnych nośników USB wersji 2 oraz USB wersji 3:
  - kopiowanie dysków USB 2.0 / 3.0 z wbudowanym złączem USB (takie jak dyski Western Digital, Seagate, Samsung i Toshiba USB 2,5 ”) lub dyski zamontowane w obudowie USB,
  - obsługa komunikacji z napędami USB 2.0 / 3.0 za pośrednictwem protokołów Mass Storage Device Only Bulk Transport i ATA-over-USB
  - kopiowanie per głowica z napędów Western Digital USB
  - odblokowywanie chronionych hasłem dyski USB Western Digital (zablokowane przez WD SmartWare) za pomocą znanego hasła użytkownika
  - odblokowywanie dostępu do ukrytych LBA USB (strefa bezpieczeństwa) znajdujących się na końcu dysków Western Digital
  - obsługa poleceń ATA przez USB, takich jak Wyłącz operacje SMART (Wstępna konfiguracja napędu) i tryb uśpienia napędu
  - obsługa rozbudowanego systemu przesyłania komunikatów o błędach USB-SCSI w celu dodatkowej diagnostyki napędu
  - implementacja natywnego tryb USB tylko do odczytu (blok zapisu)
- odtwarzanie danych z nośników PCIe SSDs w tym M.2 M Key, Macbook 12+16 pin, U.2, NVMe
  - odczyt dysków SSD NVMe i AHCI PCIe w trybie tylko do odczytu,
  - ręczna kontrola szybkość łącza PCIe,
  - ręczna kontrola liczby używanych linii PCIe,
  - możliwość przesyłania różnych typów resetu na poziomie PCIe oraz na poziomie protokołu po przekroczeniu limitu czasu odczytu lub błędu odczytu,
  - ponowne uruchamianie (repower) dysku SSD PCIe jeśli resetowanie jest niewystarczające,
  - możliwość usuwania haseł z obsługiwanych dysków twardych,
  - zapewnianie eksportu odzyskanych danych do dowolnego rodzaju nośnika,

- dodatkowe wyposażenie pozwalające na podłączenie działającego nośnika w trybie forensic (zablokowany zapis):
  - proces kopiowania w trybie zabezpieczania nośnika oryginalnego przez przypadkową zmianą,
  - możliwość usuwania lub przeglądania nieznanych haseł użytkownika i haseł głównych dla większości dysków twardych,
  - możliwość użycia poleceń ATA specyficznych dla dostawców, aby wyłączyć automatyczne przenoszenie uszkodzonych sektorów, dzięki czemu można odzyskać więcej danych,
  - opcja obrazowania dowolnego zdrowego urządzenia pamięci masowej podłączonego do komputera PC do surowego pliku obrazu DD,
  - obrazowanie posektorowe,
  - pełne rejestrowanie każdego działania podjętego przez badacza podczas pracy nad nośnikiem,
  - zwiększone bezpieczeństwo kasowania dysku docelowego.
  - umożliwienie dostępu do ukrytego obszaru DCO,
  - rozszerzenie pozwalające na podłączenie drugiego nośnika docelowego.

7. Szkolenie

W ramach realizacji zadania zamawiający zobowiąże się do przeprowadzenia jednodniowego (8 godzin) szkolenia produktowego dla trzech pracowników zamawiającego pracowników w zakresie użytkowania dostarczonego systemu.