**Załącznik nr 3 do OPZ**
**Kryteria równoważności dla oprogramowania antywirusowego**
**na potrzeby Urzędu Miasta i Gminy Budzyń**

**Wspierane systemy operacyjne**

**System Operacyjny Windows:**

**Systemy Operacyjne Komputerów**

- Windows 11 October 2024 Update (24H2)
- Windows 11 October 2023 Update (23h2)
- Windows 10 November 2022 Update (22H2)
- Windows 11 September 2022 Update (22H2)
- Windows 11 (initial release)
- Windows 10 November 2021 Update (21H2)
- Windows 10 May 2021 Update (21H1)
- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10 (initial release)

**Systemy operacyjne serwera**

Windows Server 2025 64x
Windows Server 2022 Core
Windows Server 2022
Windows Server 2019 Core
Windows Server 2019
Windows Server 2016
Windows Server 2016 Core

**Systemy Operacyjne Linux i wersja kernel**

Oparte o RPM

RHEL 7.x - 3.10.0 (build 957) 64-bit
RHEL 8.x - 4.18.0 64-bit
RHEL 9.x - 5.14.0 64-bit
Oracle Linux 7.x (UEK) - 4.18.0 64-bit
Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit
Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit
Oracle Linux 8.x (RHCK) – 4.18.0 64-bit
Oracle Linux 9.x (UEK) – 5.15.0 64-bit
Oracle Linux 9.x (RHCK) – 5.14.0 64-bit
CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit
CentOS 8 Stream - 4.18.0 64-bit
CentOS 9 Stream - 5.14.0 64-bit
Fedora 37 – 40 – wsparcie do wygaśnięcia. 64-bit
AlmaLinux 8.x - 4.18.0 64-bit
AlmaLinux 9.x - 5.14.0 64-bit
Rocky Linux 8.x - 4.18.0 64-bit
Rocky Linux 9.x - 5.14.0 64-bit
CloudLinux 7.x - 3.10 (build 957) 64-bit

CloudLinux 8.x - 4.18.0 64-bit
Miracle Linux 8.x - 4.18.0 64-bit
Kylinv10 RHEL - 4.19.90 64-bit

Oparte o Debian
Debian 9 - 4.9.0 32-bit/64-bit
Debian 10 - 4.19 32-bit/64-bit
Debian 11 - 5.10 32-bit/64-bit
Debian 12 – 6.1.0 64-bit
Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit
Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit
Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit
Ubuntu 22.04.x - 5.15 / 5.19 64-bit
Ubuntu 23.04.x – 6.2.0 64-bit
Ubuntu 24.04.x – 6.8.0 64- bit
PopOS 22.04.x – 6.2.6 64-bit
Pardus 21 – 5.10.0 64-bit
Mint 20.x – 5.4.0 64-bit
Mint 21.x – 5.15.0 64-bit
Mint 22.x – 6.8.0.x 64-bit
Zorin OS – 6.5.x 64-bit
Linux Mint Debian Edition 6 – 6.1.x 64-bit

**Ochrona środowisk wirtualnych (SVE)**

1. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej.
2. Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie:
   a) OVA
   b) VHD
   c) VHDX
   d) VMDK

   Środowiska wspierane:
   - VMware vSphere and vCenter Server:
     - version 6.5
     - version 6.7, including update 1, update 2a and update 3
     - version 7.0, including update 1, update 2, update 2b, update 2c and update 2d
     - version 8.0, including update 1, update 2
   - VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
   - VMware Workstation 11.x, 10.x, 9.x, 8.0.6
   - VMware Player 7.x, 6.x, 5.x
   - Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor)

**Ochrona antywirusowa i antyspyware**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Interfejs oraz pomoc techniczna świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
5. Wbudowana technologia do ochrony przed rootkitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".

8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Możliwość ustawienia zadania skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich.
13. Możliwość dodawania wykluczeń na podstawie:
    a) Plik
    b) Folder
    c) Rozszerzenie
    d) Proces
    e) Hash pliku
    f) Hash certyfikatu
    g) Nazwa zagrożenia
    h) Wiersz poleceń
    i) IP/maska
14. Skanowanie poczty opartej o protokoły POP3 i SMTP w czasie rzeczywistym.
15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie w przeglądarce.
16. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
17. Wsparcie przeglądarek Internet Explorer 8+, Mozilla Firefox 30+, Google Chrome 34+, Safari 4+, Microsoft Edge 20+ i Opera 21+ bez konieczności zmian w konfiguracji.
18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH.
19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
20. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
21. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i godziny.
22. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
23. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
24. Administrator musi mieć możliwość ukrycia ikony oprogramowania w obszarze powiadomień systemu Windows.
25. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows i macOS.
26. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
27. Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
28. System musi umożliwiać kontrolę dostępu do urządzeń na podstawie interfejsów, do których zostały one podłączone.
29. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej na podstawie ich wykrycia lub wpisanych ręcznie ID urządzenia lub ID produktu.
30. Funkcja blokowania informacji wysyłanych przez HTTP lub SMTP jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.).
31. Funkcja blokowania wysyłanych informacji konfigurowana zdalnie przez administratora.
32. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
33. Wbudowany IDS.

34. Możliwość wykorzystania funkcji skanowania lokalnego lub hybrydowego ze sprawdzaniem reputacji plików w chmurze.
35. Możliwość tworzenia list sieci zaufanych.
36. Możliwość dezaktywacji funkcji zapory sieciowej.
37. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
38. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa).
39. Komunikacja między konsolą zarządzającą, a punktami końcowymi jest szyfrowana.
40. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:
    a) Możliwość wymuszenia funkcji DEP systemu Windows.
    b) Możliwość wymuszenia relokacji modułów (ASLR) dla Windows.
41. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:
    -Pierwszy dostęp.
    -Dostęp do poświadczeń.
    -Wykrycie.
    -Crimeware.
    -Ruch boczny.
42. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików, a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznie.
    Formaty plików jakie mogą być odzyskane:
    3fr, ai, arw, bay, cdr, cer, cr2, crt, crw, dcr, der, dll, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, exe, indd, jpe, jpeg, jpg, mdf, mef, mrw, nef, nrw, odb, odc, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pdf, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, png, r3d, raf, rtf, rw2, rwl, sr2, srf, srw, wb2, wpd, wps, x3f, xlk, xls, xlsb, xlsm, xlsx, msg, py, ini, xml, msi, cab, tsf, dgn, log, gif, csv, avi, mov, mp4
43. System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym z Windows i Linux.
44. Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows.
45. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.
46. System musi umożliwiać skanowanie oprogramowania układowego UEFI.
47. System umożliwia przechwytywanie TLS handshake pozwalając na skanowanie ruchu sieciowego bez konieczności deszyfracji.
48. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows i macOS do SIEM Splunk (wymaga TLS 1.2 lub wyższy) lub z systemem Windows i Linux do serwera Syslog (JSON).
49. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników naruszeń bezpieczeństwa (IOC).

**Stacje robocze i serwery Windows**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.

4. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
5. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
6. Produkt i zawartość zabezpieczeń powinny być aktualizowane nie rzadziej niż raz na godzinę.
7. Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.
8. Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
9. Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików.
10. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows po doinstalowaniu odpowiedniego modułu. Zmiana ustawień zabezpieczona jest hasłem.
11. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji „O programie”, możliwość wyświetlenia danych do pomocy technicznej tj: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.
12. Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.

**Ochrona Exchange**

1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w ciągu określonego czasu.
3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz niemożliwych do przeskanowania.
4. Możliwość skanowania w poszukiwaniu potencjalnie niechcianych aplikacji (PUA).
5. Możliwość skanowania malware wewnątrz archiwów.
6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowanie maila do konkretnej skrzynki pocztowej.
11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

**Konsola zdalnej administracji**

1. Centralny System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów.
2. Możliwość integracji wielu domen Active Directory.

3. Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych.
4. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
5. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi.
6. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego.
7. Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu.
8. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
9. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
10. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) oraz wyeksportowanie ich do formatu: pdf i csv. Również zbiorczo w formie archiwum zip.
11. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie.
12. Możliwość generowania raportu co godzinę.
13. Pierwsza aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
14. Możliwość dodania etykiety do stacji roboczej.
15. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
16. Możliwość przechowywania kwarantanny maksymalnie 180 dni.
17. Możliwość definiowania, czy pliki z kwarantanny mają być przesyłane do producenta i co ile godzin ma się ta czynność odbywać.
18. Po aktualizacji zawartości bezpieczeństwa opcja automatycznego przeskanowania kwarantanny.
19. Wsparcie techniczne mailowe i telefoniczne w j. polskim od poniedziałku do piątku w godzinach 8:00-16:00. W pozostałych godzinach możliwość bezpośredniego kontaktu z producentem (24/7) w j. angielskim.
20. Po integracji z lokalnym Active Directory możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
21. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji. Określenie lokalizacji na podstawie:
    -Zakres adresów IP/IP.
    -Adres bramy.
    -Adres serwera WINS.
    -Adres serwera DNS.
    -Połączenie DHCP sufiksów DNS.
    -Punkt końcowy może rozwiązać hosta.
    -Typ sieci.
    -Nazwa hosta.
22. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238.
23. Możliwość naprawy instalacji agenta z poziomu konsoli.
24. Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz na określenie godziny, o której te maszyny będą usuwane.
25. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
26. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
27. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux lub MacOS

28. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
29. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.
30. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M oraz osobnego pakietu dla systemów Windows z Intel x86 oraz oddzielnego dla architektury ARM.
31. System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej.
32. Możliwość wygenerowania i zapisania logów na stacji roboczej z poziomu konsoli zarządzającej.
33. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
34. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
35. Ochrona proaktywna oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie. Ochrona ta musi wykrywać zagrożenia takie jak:
    a) Ukierunkowane ataki.
    b) Podejrzane pliki i ruch w sieci.
    c) Exploity.
    d) Ransomware.
    e) Grayware.
36. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego.
37. Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na:
    a) Tolerancyjny.
    b) Normalny.
    c) Agresywny.
38. Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku:
    a) Plik może zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora.
    b) Możliwość ręcznego przesłania archiwum zabezpieczonego hasłem.
    c) Możliwość ręcznego przesłania adresu URL.
    d) W przypadku ręcznego przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.
39. Wbudowany sandbox musi działać w trybie monitorowania i blokowania.
40. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja, przeniesienie do kwarantanny lub tylko raportowanie.
41. Wbudowany sandbox musi oferować opcję wstępnego filtrowania plików z kategorii aplikacje, dokumenty, skrypty, archiwa, maile zapisane do pliku pod kątem podejrzanego zachowania.
42. Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
43. Minimalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 1KB.
44. Maksymalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 50MB.
45. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100, gdzie liczba mniejsza stanowi mniejsze ryzyko, a liczba większa większe ryzyko. System ponadto musi posiadać:
    a) Funkcję, która pozwala wyszukiwać podatności ustawień punktów końcowych oraz naprawiać je lub ignorować z podziałem na typ wykrytej konfiguracji:

-Przeglądarka
-Sieć
-System operacyjny
-Luki
System ponadto musi określać nasilenie zagrożenia wynikłego z wykrytej podatności w oparciu o punkty procentowe oraz posiadać funkcję cofnięcia wprowadzonych zmian w ustawieniach systemów.

b) System zarządzania ryzykiem powinien określać luki w wykrytym zainstalowanym oprogramowaniu podając przy tym numer CVE tych luk.
c) System pozwala na śledzenie i wykrywanie ryzykownych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem o liczbie użytkowników, których takie działanie dotyczy oraz jaka jest jego szkodliwość.
d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.
e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich szkodliwość wyrażona w procentach.
f) System pozwala na wykrywanie podatności w oparciu o standardy zgodności CISv8, SOC 2, ISO/IEC 27001:2022, GDPR (EU) oraz NIS2.

46. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
47. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
48. Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
49. Funkcja pojedynczego logowania – Single Sign-on (SSO) przy integracji z Microsoft Azure.
50. Raport podsumowujący - Możliwość podglądu raportu, który streszcza stan środowiska firmowego w ciągu ostatnich 24h, 7 dni lub 30 dni. Z rozróżnieniem na takie sekcje jak:
    a) Zarządzane punkty końcowe.
    b) Ilość zajętych miejsc w licencji z rozróżnieniem na stacje robocze Windows, serwery Windows, macOS, Linux oraz fizyczne punkty końcowe i maszyny wirtualne.
    c) Pięć rodzajów najczęściej blokowanych zagrożeń.
    d) Podział zagrożeń na urządzenia takie jak stacje robocze i serwery.
    e) Status incydentów bezpieczeństwa, które wystąpiły.
    f) Stan modułów punktów końcowych.
    g) Ocena ryzyka firmy.
    h) Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.
    i) Zablokowane techniki ataku sieciowego z podziałem na takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware.
51. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:
    a) Firmy
    b) Raporty
    c) Licencjonowanie
    d) Konta
    e) Pakiety
    f) Incydenty
    g) Sieć
    h) Kwarantanna
    i) Integracje
    j) Event Push Service
    k) Polityki
52. Early access – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu powinny umożliwiać

testowanie najnowszych funkcji oprogramowania, których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.

53. Możliwość utworzenia konsoli typu Partner, która pozwala na zarządzanie wieloma firmami z poziomu jednej scentralizowanej konsoli zarządzającej, konsola partnerska musi umożliwiać:
    a) Pobieranie przez partnera plików z kwarantanny podległych firm.
    b) Zarządzanie systemem ochrony firm podrzędnych przez Partnera z jednej konsoli lub tworzenie bezpośrednich dostępów użytkowników dla tych firm.
    c) Odseparowanie przez administratora konsoli podrzędnej od konsoli partnera nadrzędnego.
54. Profil firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej. Dostępne są kategorie m.in: Lotnictwo, Budownictwo, Edukacja, Służba zdrowia, Handel i inne.
55. System musi umożliwiać wybór trzech poziomów obciążenia procesora dla zadań określonych w harmonogramie skanowania na systemach Linux i macOS.
56. System musi posiadać funkcję wstrzymywania skanowania podczas pracy na baterii.
57. Wbudowany sandbox musi posiadać możliwość przesyłania pliku do analizy z komputera zdalnego za pomocą podanej ścieżki. Wielkość pliku nie może przekraczać 100MB.
58. Filtrowanie wykrytych incydentów bezpieczeństwa m.in. na podstawie:
    a) ID.
    b) Ostatnia aktualizacja.
    c) Status.
    d) Osoba przydzielająca.
    f) Data utworzenia.
    g) Priorytet.
    h) Ocena szkodliwości w skali 0-100.
    i) Podmioty.
    j) Zasoby.
    k) Ostatnia faza killchain.
    l) Wykonane czynności.
    m) Skorelowane incydenty.
    n) Typ incydentu.
59. System umożliwia wygenerowanie i pobranie zestawu informacji z chronionych punktów końcowych w formie archiwum. Funkcja powinna być dostępna dla systemów Windows, Linux oraz macOS. Archiwum musi zawierać co najmniej informacje:
    a) Windows
        - Logi zainstalowanego agenta.
        - Dziennik zdarzeń Windows.
        - Informacje o systemie.
        - DnsCache.
        - Webcache.
        - Informacje z głównych katalogów rejestru (SYSTEM, SOFTWARE, DEFAULT, DRIVERS, SAM, SECURITY).
        - Harmonogram zadań.
        - Historia Powershell (jeśli włączono).
    b) Linux
        - Podstawowy log pomocy technicznej zainstalowanego agenta.
        - Certyfikaty.
        - Autorun i usługi.
        - Informacje sieciowe.
        - Informacje systemowe.
        - Zainstalowane pakiety.
    c) macOS
        - Podstawowy log pomocy technicznej zainstalowanego agenta.
        - Autorun.
        - Lista procesów.
        - Informacje sieciowe.

- Informacje o systemie.

60. Oprogramowanie musi umożliwiać przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez tworzenie zapytań pod kątem wykrywania:
    a) historia powłoki.
    b) wczytywanie bibliotek .dll z podejrzanej lokalizacji.
    c) Sesje logowania z użyciem jawnych danych uwierzytelniających.
    d) Arp cache.
    e) Ip forwarding.
    f) Lista zamontowanych nośników.
    g) Konfiguracja ip tables.
    h) Połączenia TLS które używają certyfikatów self-signed.
    i) Używane rozszerzenia w przeglądarce Chrome.
    j) Używane rozszerzenia w przeglądarce Firefox.
    k) Używane rozszerzenia w przeglądarce Safari.
    l) Źródła apt w systemach Linux.
    m) Wyświetlanie zainstalowanych pakietów DEB.
    n) Wyświetlanie zainstalowanych pakietów RPM.
    o) Pakiety Python zainstalowane w systemie.
    p) Lista użytkowników, którzy zostali utworzeni w ciągu ostatnich 30 dni (Linux).
    q) Wykrywanie czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS.
    r) Wykrywanie czy Kontrola Kont Użytkowników (UAC) jest wyłączona.
    s) Wykrywanie czy SecureBoot jest włączony.
    t) Lista zapamiętanych sieci bezprzewodowych.
    u) Wykrywa, czy zmienił się domyślny folder startowy użytkownika.
    w) Wykrywa, czy zmienił się domyślny folder startowy maszyny.
61. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych reguł, po spełnieniu których może zostać wygenerowany incydent bezpieczeństwa. Funkcja ta powinna:
    a) Oferować opcję podjęcia automatycznych działań po spełnieniu warunków tj.: izolacja punktu końcowego, wygenerowanie archiwum diagnostycznego, przesłanie pliku do analizy sandbox, zakończenie procesu i innych.
    b) Automatyczne działania zapobiegawcze są zależne od wyboru kategorii.
    c) Tworzenie reguł musi być określone poprzez wybór operatora np. „to”, „zawiera”, „jest jednym z” itp.
    d) Dotyczyć określonych kryteriów tj. proces, plik, rejestr, połączenia.
    e) Zapewniać możliwość tworzenia zapytań YARA.
    f) Umożliwiać określenie priorytetu kolejności automatyzacji.
    g) Administrator powinien mieć możliwość wyboru poziomu szkodliwości potencjalnie wygenerowanych incydentów (wysokie, średnie i niskie).

**EDR-Endpoint Detection and Response**

Produkt zapewnia szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze.

**Wspierane systemy operacyjne**

A. Systemy desktopowe
    a) Windows 11 October 2024 Update (24H2)
    b) Windows 11 October 2023 Update (23H2)
    c) Windows 10 November 2022 Update (22H2)
    d) Windows 11 September 2022 Update (22H2)
    e) Windows 11 (initial release)
    f) Windows 10 November 2021 Update (21H2)
    g) Windows 10 May 2021 Update (21H1)

h) Windows 10 October 2020 Update (20H2)
i) Windows 10 May 2020 Update (20H1)
j) Windows 10 May 2019 Update (19H1)
k) Windows 10 October 2018 Update (Redstone 5)
l) Windows 10 April 2018 Update (Redstone 4)
m) Windows 10 Fall Creators Update (Redstone 3)
n) Windows 10 Creators Update (Redstone 2)
o) Windows 10 Anniversary Update (Redstone 1)
p) Windows 10 November Update (Threshold 2)
q) Windows 10 (initial release)

B. Systemy operacyjne dla serwerów:
a) Windows Server 2025 64x
b) Windows Server 2022 Core
c) Windows Server 2022
d) Windows Server 2019 Core
e) Windows Server 2019
f) Windows Server 2016
g) Windows Server 2016 Core

C. Linux
Oparte o RPM
RHEL 7.x - 3.10.0 (build 957) 64-bit
RHEL 8.x - 4.18.0 64-bit
RHEL 9x - 5.14.0 64-bit
Oracle Linux 7.x (UEK) - 4.18.0 64-bit
Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit
Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit
Oracle Linux 8.x (RHCK) – 4.18.0 64-bit
Oracle Linux 9.x (UEK) – 5.15.0 64-bit
Oracle Linux 9.x (RHCK) – 5.14.0 64-bit
CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit
CentOS 8 Stream - 4.18.0 64-bit
CentOS 9 Stream - 5.14.0 64-bit
Fedora 37 – 40 – wsparcie do wygaśnięcia. 64-bit
AlmaLinux 8.x - 4.18.0 64-bit
AlmaLinux 9.x - 5.14.0 64-bit
Rocky Linux 8.x - 4.18.0 64-bit
Rocky Linux 9.x - 5.14.0 64-bit
CloudLinux 7.x - 3.10 (build 957) 64-bit
CloudLinux 8.x - 4.18.0 64-bit
Miracle Linux 8.x - 4.18.0 64-bit
Kylin v10 RHEL - 4.19.90 64-bit
Oparte o Debian
Debian 9 - 4.9.0 32-bit/64-bit
Debian 10 - 4.19 32-bit/64-bit
Debian 11 - 5.10 32-bit/64-bit
Debian 12 – 6.1.0 64-bit
Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit
Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit
Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit
Ubuntu 22.04.x - 5.15 / 5.19 64-bit
Ubuntu 23.04.x – 6.2.0 64-bit
Ubuntu 24.04.x – 6.8.0 64- bit

PopOS 22.04.x – 6.2.6 64-bit
Pardus 21 – 5.10.0 64-bit
Mint 20.x – 5.4.0 64-bit
Mint 21.x – 5.15.0 64-bit
Mint 22.x – 6.8.0.x 64-bit
Zorin OS – 6.5.x 64-bit
Linux Mint Debian Edition 6 – 6.1.x 64-bit

Cloud based Linux
AWS Bottlerocket 2020.03 - 5.4.x, 5.10.x 64-bit
Amazon Linux v2 - 4.14.x / 4.19.x / 5.10 64-bit
Amazon Linux 2023 – 6.1.x 64-bit
Google COS Milestones 77, 81, 85 - 4.19.112 / 5.4.49 64-bit
Azure Mariner 2 - 5.15 64-bit

**Komponenty EDR**

Główne elementy:
1. Sensor EDR, który gromadzi i przetwarza dane dotyczące punktu końcowego i zachowania aplikacji w celu ich raportowania.
2. Analityka Bezpieczeństwa, komponent służący do interpretacji metadanych gromadzonych przez sensor EDR.
3. Możliwość instalacji dodatkowego, dedykowanego agenta z sensorem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną równolegle ochronę świadczoną przez innego producenta oprogramowania antywirusowego.

**Wykrywanie podejrzanej aktywności**

Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.
1. Bazowanie na systemach opartych o techniki MITRE ATT&CK i własnej inteligencji.
2. Zgłaszanie naruszeń jako incydent w module EDR.

**Badanie incydentów i wizualizacja**
1. Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym czasie.
2. Produkt integruje się z bazą wiedzy MITRE ATT&CK i odpowiednio oznacza zdarzenia bezpieczeństwa.
3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi danymi lub działaniami z następującymi informacjami:
   a) Karta podsumowująca zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.
   b) Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.
   c) System gromadzi informacje o działaniach podejmowanych przez produkt w związku ze zdarzeniem bezpieczeństwa.

**Incydenty**
1. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i chronologicznej linii zdarzeń oraz daje możliwość:
   a) Filtrowania zdarzeń.
   b) Zakończenia procesów.
   c) Dodania procesów do czarnej listy.
   d) Dodania procesów do białej listy.
   e) Izolacji hosta.
   f) Przesłania pliku do Sandbox.
   g) Sprawdzenia informacji o pliku w Google.

h) Sprawdzenia informacji o pliku w VirusTotal.

2. Możliwość szybkiego podglądu incydentów za pomocą spersonalizowanych widoków list lub widoku domyślnego.
3. Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie.
4. System umożliwia blokowanie na podstawie utworzonych reguł czarnej listy przy pomocy kategorii:
5. a) Hash MD5 lub SHA256.
   b) Pełna ścieżka do aplikacji.
   c) Reguła połączenia.
6. Możliwość importu reguł czarnej listy dla hash, ścieżek do aplikacji oraz reguł połączeń z pliku CSV.
7. System musi oferować szeroki zakres filtrowania dodanych reguł blokowania minimum po nazwie pliku, hash pliku, typu hash, ścieżce, protokole porcie/zakresie portów, daty dodania.