

Załącznik 1 do swz

PZ.271.1.25.2026

Opis przedmiotu zamówienia

pn. „Dostawa oprogramowania antywirusowego wraz z oprogramowaniem wspomagającym”

I. Przedmiot zamówienia:

Główny kod CPV:

48761000-0: Pakiety oprogramowania antywirusowego

Dodatkowe kody CPV:

48730000-4: Pakiety oprogramowania zabezpieczającego

48732000-8: Pakiety oprogramowania do zabezpieczania danych

72263000-6: Usługi wdrażania oprogramowania

ZAMÓWIENIE:

Przedmiotem zamówienia jest dostawa i wdrożenie oprogramowania antywirusowego **Falcon Endpoint Protection**

Enterprise Flexible Bundle lub równoważne wraz z oprogramowaniem wspomagającym oraz udzieleniem licencji na to oprogramowanie **na okres 12 miesięcy od dnia 06.12.2026 r.** w poniższym zakresie:

I.1) Oprogramowanie:

1. Falcon Endpoint Protection Enterprise Flexible Bundle (Prevent, Insight, Falcon for Mobile, Insight for Mobile) lub równoważne dla 540 stacji roboczych 16 serwerów oraz 220 urządzeń mobilnych.
2. Falcon Firewall Management lub równoważne dla 540 stacji roboczych i 16 serwerów.
3. Falcon Next-Gen SIEM lub równoważne dla 13 GB logów dziennie z retencją 12 miesięcy.
4. Falcon Spotlight lub równoważne dla 556 urządzeń.
5. Falcon Data Protection for Endpoint lub równoważne dla 556 urządzeń.

I.2) Wdrożenie

W ramach wdrożenia Wykonawca będzie zobowiązany do:

- pełnego wdrożenia i konfiguracji: Instalacji, konfiguracji i pełnego uruchomienia wszystkich modułów w środowisku Zamawiającego, na poziomie funkcjonalnym zgodnie z ilościami podanymi w pkt. I.1)
- migracji polityk i reguł: reguł bezpieczeństwa, polityk DLP (w tym reguł klasyfikacji danych), parserów i reguł korelacji w systemie SIEM oraz reguł zapór sieciowych
- dostosowania infrastruktury: wykonania wszelkich niezbędnych modyfikacji, zmian konfiguracyjnych w usługach sieciowych i systemowych Zamawiającego
- ciągłości ochrony i braku „okien bezbronności”: przeprowadzenia migracji w sposób gwarantujący brak przerw w monitorowaniu i ochronie infrastruktury IT (tzw. ochrona zakładkowa). Niedopuszczalne jest pozostawienie systemów Zamawiającego bez aktywnej ochrony antywirusowej, EDR lub DLP w trakcie przełączania systemów,

- przeprowadzenia:
 - analizy obecnej konfiguracji,
 - inwentaryzacja polityk,
 - mapowania polityk starego systemu na nowy,
 - migracji reguł,
 - migracji wyjątków,
 - migracji obiektów,
 - migracji integracji,
 - migracji agentów,
 - migracji danych historycznych, zapewnienia integralności danych wraz z możliwością wyszukiwania
 - migracji dashboardów i raportów,
 - migracji kont i uprawnień,
 - testów powdrożeniowych każdego z elementów systemu,
- zapewnić ciągłość działania mechanizmów bezpieczeństwa w zakresie nie mniejszym niż zapewniany przez rozwiązanie obecnie eksploatowane. Niedopuszczalne jest prowadzenie migracji powodujące jednoczesne wyłączenie lub ograniczenie krytycznych mechanizmów ochronnych dla więcej niż określonego 1% zasobów (endpointów) oraz 0% dla systemów krytycznych (serwerów, urządzeń brzegowych).
- Wykonawca zobowiązany jest stosować się do uwag i zaleceń Zamawiającego w trakcie wykonywania prac
- Wykonawca zobowiązany jest udzielić dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej nieprzewanego przez cały okres wdrżania.

- Wdrożenie realizowane będzie w siedzibie Zamawiającego Plac Na Stawach 1, 30 – 107 Kraków, w dni robocze od poniedziałku do piątku w godzinach 8:00 – 16:00,
- Wdrożenie odbywać się będzie pod ciągłym nadzorem administratorów systemów informatycznych Zamawiającego oraz systematyczną weryfikację prawidłowości realizowanych działań. Proces ten obejmuje bieżące monitorowanie stosowania przyjętych procedur, kontrolę zgodności podejmowanych działań z obowiązującymi wymaganiami, harmonogramem wdrożenia oraz identyfikację ewentualnych nieprawidłowości. W przypadku stwierdzenia odchyień bądź też zagrożeń administrator systemów informatycznych może wydawać wiążące polecenia w celu ochrony bezpieczeństwa systemu informatycznego WUP oraz zapewnienia ciągłości jego działania.
- Od dnia zakończenia wdrożenia do dnia wygaśnięcia obecnie posiadanych licencji wykonawca zobowiązany jest zapewnić licencję tymczasową/wdrożeniową /testową zapewniającą pełne bezpieczeństwo i funkcjonalność działania oraz asystę techniczną w godzinach pracy urzędu.
- Wdrożenie przeprowadzane będzie zgodnie z uzgodnionym i zatwierdzonym przez Zamawiającego harmonogramem wdrożenia
- Wykonawca zobowiązuje się do przedstawienia harmonogramu wdrożenia, zwanego dalej również „harmonogramem” w ciągu 1 dnia od podpisania umowy. Zamawiający zatwierdzi, bądź wniesie uwagi do przedłożonego harmonogramu w ciągu 1 dnia roboczego od daty jego otrzymania. Wskazany wyżej okres uzgadniania harmonogramu nie wlicza się do deklarowanego w ofercie Okresu wdrożenia.
- Harmonogram, o którym mowa wyżej sporządzony będzie w sposób zapewniający dotrzymanie przez Wykonawcę deklarowanego w ofercie terminu wdrożenia oraz obejmować będzie, co najmniej następujące etapy:

- Etap 1: analiza i przygotowanie: inwentaryzacja urządzeń, reguł i wyjątków, analiza intergacji, plan migracji, procedury wycofania zmian
- Etap 2: konfiguracja i testy techniczne: konfiguracja polityk bezpieczeństwa, ról i uprawnień, przygotowanie instalatorów agentów, testy integracji, alertów i logowania.
- Etap 3 pilotaż : wdrożenie na testowej grupie komputerów, serwerów i telefonów. Testy wykrywania zagrożeń, blokowania, kwarantanny i reakcji EDR. Testy DLP, skanowania podatności i reguł firewall. Analiza wpływu na wydajność i pracę użytkowników.
- Etap 4 wdrożenie produkcyjne: Instalacja agenta na wszystkich komputerach, serwerach, telefonach. Przenoszenie polityk, reguł i wyjątków.
- Etap 5 optymalizacja systemu: Usuwanie konfliktów polityk, fałszywych alarmów i problemów wydajnościowych. Kontrola pokrycia agentami na grupie komputerów, serwerów i telefonów. Testy obsługi incydentów. Przygotowanie dokumentacji operacyjnej zgodnie z OPZ i przeprowadzenie szkolenia administratorów systemów informatycznych 3 – 5 osób.
- Etap 6 odbiór końcowy: Potwierdzenie spełnienia wymagań, formalny odbiór przygotowanej dokumentacji i podpisanie protokołu odbioru.
- W przypadku niepowodzenia wdrożenia w terminie wskazanym w umowie, Zamawiający wymaga przywrócenia przez Wykonawcę środowiska informatycznego do stanu sprzed wdrożenia w terminie 1 dnia roboczego.
- Poprzez niepowodzenie uznaje się w szczególności: niedotrzymanie któregośkolwiek z terminów wskazanych w umowie, niespełnienie któregośkolwiek z wymagań określonych w OPZ, nieosiągnięcie wymaganego poziomu pokrycia zasobów objętych wdrożeniem, występowanie błędów uniemożliwiających prawidłowe i bezpieczne użytkowanie rozwiązania w środowisku produkcyjnym, brak przekazania dokumentacji, konfiguracji, procedur

administracyjnych lub innych elementów wymaganych do samodzielnej eksploatacji rozwiązania przez Zamawiającego, brak przeprowadzenia szkolenia administratorów systemów informatycznych.

II. Wymagania dotyczące oprogramowania równoważnego:

Zamawiający dopuszcza zaoferowanie rozwiązań równoważnych wobec oprogramowania wskazanego przez Zamawiającego w pkt. I.1) w następującym zakresie (KRYTERIA RÓWNOWAŻNOŚCI):

II.1) Wymagania ogólne:

1. System musi posiadać centralną konsolę realizowaną w formie usługi SaaS (ang. Software-as-a-Service) o dostępności co najmniej 99,9% a do ochrony stacji i serwerów wykorzystywać agenta.
2. System musi pochodzić od jednego producenta.
3. System musi przechowywać i przetwarzać dane na terenie Europejskiego Obszaru Gospodarczego.
4. System musi być zgodny z regulacjami GDPR (ang. General Data Protection Regulation), posiadać certyfikację ISO/IEC 27001:2022 lub równoważny oraz zgodność z SOC 2 Type 2 lub równoważny.
5. System nie może być zabroniony do stosowania ani czasowo wstrzymany do stosowania przez administrację któregośkolwiek z państw członkowskich NATO.
6. Dojrzałość i skuteczność systemu musi być poświadczona przez co najmniej następujące niezależne instytucje badające rynek rozwiązań EDR/XDR:
 - a. Oferowane rozwiązanie musi osiągać skuteczność nie niższą niż 95% w zakresie wskazanych kategorii/technik w niezależnych testach MITRE ATT&CK Enterprise Evaluations, przeprowadzonych w okresie ostatnich 24 miesięcy, o ile producent rozwiązania uczestniczył w odpowiedniej edycji ewaluacji. W przypadku gdy producent oferowanego

rozwiązania nie uczestniczył w odpowiedniej edycji MITRE ATT&CK Enterprise Evaluations w okresie ostatnich 24 miesięcy, wykonawca może wykazać spełnienie wymogu poprzez przedstawienie wyników niezależnego testu bezpieczeństwa przeprowadzonego przez podmiot niezależny od producenta, którego metodologia testowa jest publicznie dostępna i obejmuje techniki oraz scenariusze ataku porównywalne z zakresem właściwej ewaluacji MITRE ATT&CK Enterprise. Przedstawiony raport musi umożliwiać jednoznaczne ustalenie procentowego poziomu detekcji oraz/lub prewencji dla technik objętych wymaganiem..

Kategorie:

- detekcje techniki ataku (procent detekcji ze wskazaniem techniki),
- prewencja (procent zablokowanych podkroków).

b. Oferowane rozwiązanie musi być sklasyfikowane przez firmę Gartner jako „Leader” w raporcie „Gartner Magic Quadrant for Endpoint Protection”, opublikowanym w 2026 roku, lub spełniać równoważne wymaganie renomowanego podmiotu zewnętrznego, obejmującym ocenę rozwiązań klasy Endpoint Protection.

7. System musi przechowywać informacje o alarmach i incydentach co najmniej przez 90 dni.
8. System musi przechowywać logi przez 365 dni i umożliwiać przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów: hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe.
9. System musi przechowywać przez 365 dni logi audytowe odnotowujące co najmniej logowanie użytkowników, zmiany wprowadzane w konfiguracji systemu oraz nawiązywanie zdalnych połączeń.
10. System musi posiadać możliwość instalacji agenta na co najmniej następujących systemach operacyjnych:
 - a. Microsoft:
 - Windows 11 (x86-64 oraz arm64)
 - Windows Server 2019 i Server Core 2019

Windows Server 2022 i Server Core 2022

Windows Server 2025 i Server Core 2025

b. Linux

CentOS 8

Debian 10, 11 i 12

SUSE 12 i 15

Ubuntu 18, 20, 22 i 24

c. Apple macOS

macOS Sonoma 14

macOS Sequoia 15

macOS Tahoe 26

d. Android

Android 10.x, 11.x, 12.x, 13.x, 14.x, 15.x, 16.x

e. iOS

iOS 17.x, 18.x, 26.x

11. System musi posiadać możliwość instalacji agenta na systemach VDI.

12. System musi umożliwiać wygenerowanie i pobranie pakietu instalacyjnego w formacie:

- msi lub exe dla systemów Microsoft
- pakietu rpm i deb dla systemów Linux
- pakietu pkg dla macOS

13. Komunikacja między agentem a konsolą systemu musi być realizowana z wykorzystaniem protokołu HTTPS w wariantach co najmniej z TLS1.2 i odbywać się:
- bezpośrednio
 - pośrednio przez proxy systemowe
 - pośrednio przez proxy wskazane w trakcie instalacji
14. Dokumentacja systemu musi wskazywać adresy IP oraz adresy URL, z którymi komunikuje się agent nawiązując komunikację z konsolą systemu.
15. System musi posiadać możliwość zarządzania przez przeglądarkę internetową. Komunikacja musi być zabezpieczona HTTPS w wariantach co najmniej z TLS1.2.
16. System musi posiadać możliwość zarządzania przez API.
17. System musi posiadać możliwość wskazania listy publicznych adresów IP, z których będzie istniała możliwość zalogowania się do konsoli systemu.
18. System musi umożliwiać integrację z zewnętrznymi katalogami użytkowników z wykorzystaniem SAML 2.0.
19. System musi posiadać wbudowany katalog użytkowników oraz umożliwiać uwierzytelnianie tych użytkowników z wykorzystaniem wieloskładnikowego uwierzytelniania (MFA), obejmującego drugi czynnik w postaci kodów jednorazowych generowanych zgodnie ze standardem TOTP (ang. Time-Based One-Time Password).
20. System podczas tworzenia haseł dla lokalnych kont administracyjnych musi spełniać minimalnie następujące wymagania złożoności hasła: co najmniej 11 znaków, musi zawierać małe i duże litery, cyfry i znaki specjalne.
21. System musi umożliwiać określenie zakresu dostępu z wykorzystaniem matrycy ról i ich przypisania do użytkownika lub do grupy użytkowników. Rola musi definiować dostęp do określonego obszaru administracyjnego systemu, jego rodzaju (tylko do odczytu, pełen dostęp) oraz jego zakresu (wszystkie lub wybrane hosty).

22. System musi obsługiwać co najmniej pięć poziomów ważności alertów, np. informacyjny, niski, średni, wysoki i krytyczny.
23. System musi automatycznie grupować powiązane alerty w celu przyspieszenia i ułatwienia triażu i analizy incydentu.
24. System musi automatycznie grupować powiązane alerty w ramach pojedynczego incydentu oraz tworzyć dla incydentu interaktywny łańcuch przyczynowo-skutkowy (graf zależności), przedstawiający zależności pomiędzy procesami i zdarzeniami związanymi z atakiem oraz powiązane z nimi dane telemetryczne. Mechanizm musi umożliwiać analizę przebiegu ataku, identyfikację wykorzystanych technik, określenie zakresu i celu ataku oraz weryfikację, czy zamierzony cel ataku został osiągnięty.
25. System musi umożliwiać zarządzanie incydentami co najmniej w następującym zakresie:
- przypisanie incydentu do administratora
 - zmianę stanu incydentu: badany, false positive, true positive, duplikat, testy
 - dodawanie notatek
26. Rozwiązanie musi mapować alerty do frameworku MITRE ATT&CK.
27. System musi posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup endpointów. Polityka automatycznej konfiguracji agenta musi umożliwiać określenie:
- dnia tygodnia i zakresu czasu, w którym aktualizacja nie będzie wykonywana
 - liczby aktualizowanych endpointów
 - możliwość zdefiniowania wersji: najnowsza wersja, najnowsza przedostatnia wersja, statycznie wskazana wersja
28. System musi umożliwiać dynamiczne grupowanie endpointów z wykorzystaniem co najmniej następujących atrybutów: nazwa endpointa, domena Active Directory, Organizational Unit wewnątrz Active Directory, system operacyjny, adres IP, podsieć IP, wersja kernela, znacznik.

29. System musi umożliwiać nawiązanie zdalnego połączenia konsolowego do endpointa chronionego agentem oferując co najmniej następujące funkcje:

- podgląd uruchomionych procesów
- podgląd systemów plików
- podgląd stanu socketów sieciowych
- wyłączenie wskazanego procesu
- uruchomienie skryptu z biblioteki
- pobranie pliku z endpointa
- wgranie pliku na endpointa
- zrzut pamięci procesu
- zrzut pamięci systemu operacyjnego
- wyłączenie i restart systemu

30. System musi umożliwiać zdalną izolację sieciową endpointa. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany.

31. System musi posiadać możliwość kontroli urządzeń podłączanych do portów USB co najmniej na systemach windows i macOS w następującym zakresie:

- określenia jak typ urządzenia USB można podłączyć
- określenia zakresu dostępu do pamięci masowej USB:
 - brak dostępu
 - tylko odczyt
 - odczyt i zapis

➤ odczyt, zapis i uruchamianie

32. System musi posiadać możliwość kontroli pamięci masowej podłączanej przez wbudowane (podłączone przez PCIe) czytniki kart SD co najmniej na systemach windows i macOS w następującym zakresie:

- brak dostępu
- tylko odczyt
- odczyt i zapis
- odczyt, zapis i uruchamianie

33. System musi zapewniać możliwość zarządzania host firewallem na platformach Windows, macOS i Linux.

34. System musi umożliwiać tworzenie biblioteki skryptów oraz ich zdalne uruchamianie na pojedynczym endpointcie lub na grupie endpointów.

35. Wymagana jest obsługa co najmniej następujących języków skryptowych:

- systemy windows: powershell
- systemy Linux: skrypty bash
- systemy MacOS: skrypty zsh

36. System musi posiadać możliwość uruchomienia pełnego skanowania endpointa na żądanie i w odpowiedzi na zarejestrowany alarm.

37. System musi umożliwiać bezpośrednią integrację z usługą VirusTotal lub równoważną.

38. System musi umożliwiać globalne oraz per grupa endpointów blokowanie uruchamiania plików binarnych poprzez wskazanie ich hash SHA256.

39. System musi oceniać chronione zasoby pod względem podatności na zagrożenia dla co najmniej 500 systemów i informować co najmniej o:

- metryce CVSS
- dodatkowej metryce na podstawie co najmniej:
 - dostępności exploitów
 - znanych przypadki wykorzystania luki na bazie telemetrii dostawcy
 - popularności oprogramowania (exposure)
 - aktywne wykorzystywanie przez grupy APT
- krokach naprawczych
- szczegółowych dowodach na to, że wersja produktu jest podatna na ataki (klucze rejestru, metadane plików itp.)
- źródłach exploitów (linki)
- mapować luki w zabezpieczeniach do znanych grup cyberprzestępców

40. System musi posiadać możliwość budowania własnych reguł detekcyjno-prewencyjnych bazujących co najmniej na określeniu łańcucha przyczynowo-skutkowego procesów wraz z określeniem parametrów linii poleceń.

41. System musi posiadać możliwość budowania własnych list indykatorów w formie nazw domenowych, adresów IPv4 i IPv6 oraz hashy SHA256 i MD5 poprzez:

- import indykatorów z pliku
- manualne dodanie indykatorów
- programowe dodanie indykatorów przez API

42. System musi umożliwiać definiowanie własnych dashboardów (konsol) z wykorzystaniem predefiniowanych widgetów (kontrolek) oraz kontrolek definiowanych samodzielnie poprzez kwerendy do danych telemetrycznych.

43. System musi umożliwiać przeszukiwanie wszystkich danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem kwerend. Kwerendy muszą umożliwiać łączenie danych telemetrycznych z różnych źródeł, ich filtrowanie i przekształcanie wyników. Reguły tworzenia kwerend muszą być opisane w dokumentacji systemu.
44. System musi umożliwiać zapisanie kwerendy do danych telemetrycznych do globalnej biblioteki dostępnej dla wszystkich innych użytkowników.
45. System musi umożliwiać zrealizowanie kwerendy do danych telemetrycznych i odczytanie jej wyników via API.
46. System musi umożliwiać eksport wyników kwerendy do danych telemetrycznych w formie pliku tekstowego.
47. System musi umożliwiać uruchamianie kwerendy cyklicznie zgodnie z podanym harmonogramem lub jeden raz o określonym czasie i wysyłać mailowe powiadomienie na wskazane adresy email wraz z załączonym plikiem tekstowym zawierającym wynik kwerendy.
48. System musi umożliwiać przekształcenie kwerendy do danych telemetrycznych w uruchamianą zgodnie z podanym harmonogramem regułę korelacyjną generującą alarmy, jeśli kwerenda zwróciła więcej niż jeden rekord.
49. System przed nawiązaniem zdalnego połączenia konsolowego musi żądać od administratora ponownego wprowadzenia hasła MFA celem dodatkowego potwierdzenia jego tożsamości.
50. System musi przetrzymywać i korelować co najmniej 13 GB danych dziennie z firm trzecich (np. firewall, brama mailowa) bezpośrednio w interfejsie EDR.
51. Dane z firm trzecich muszą być przetrzymywane przez okres co najmniej 365 dni.
52. System musi umożliwiać, w przypadku gdy dostępne dane Threat Intelligence pozwalają na przypisanie aktywności do określonego podmiotu, powiązanie wskaźników kompromitacji (IOC), technik, taktyk i procedur (TTP) oraz obserwowanych aktywności z konkretną grupą cyberprzestępczą, grupą APT lub grupą hakywistyczną. Informacja o

przypisaniu musi być prezentowana wraz ze wskazaniem źródła lub poziomu pewności atrybucji, jeżeli takie informacje są dostępne.

II.2) Wymagane minimalne parametry dla agenta:

1. Jeden wspólny agent do AV/EDR, Firewall, zarządzanie podatnościami, DLP.
2. Agent nie może wykorzystywać Oracle Java JRE/JDK.
3. Instalacja agenta nie może wymagać restartu systemu operacyjnego.
4. Agent musi weryfikować poprawność certyfikatu w trakcie nawiązywania połączenia z systemem w celu ochrony przed atakami man-in-the-middle z wykorzystaniem mechanizmu certificate pinning.
5. Agent musi posiadać mechanizmy ochronne uniemożliwiające wyłączenie agenta lub wpłynięcie na jego poprawne funkcjonowanie nawet przez użytkowników z podwyższonymi uprawnieniami (ang. anti-tampering).
6. Odinstalowanie agenta musi być chronione unikalnym dla każdej chronionej stacji hasłem, tak aby uniemożliwić odinstalowanie agenta nawet użytkownikom z podwyższonymi uprawnieniami.
7. W trakcie instalacji agenta musi istnieć możliwość nadania agentowi nieusuwalnego z konsoli znacznika, który może zostać wykorzystany jako atrybut do grupowania endpointów.
8. W trakcie instalacji agenta musi istnieć możliwość wskazania dedykowanego serwera proxy, z którego agent będzie korzystał nawiązując połączenie z systemem.
9. Agent musi wykrywać i blokować próby wyłączenia usługi Volume Shadow Copy Service (VSS) oraz inne próby uszkodzenia migawek VSS.
10. Agent musi realizować ochronę przed atakami klasy Bring Your Own Vulnerable Driver poprzez wykrywanie i blokowanie prób ładowania podatnych sterowników.

11. Agent musi bezpośrednio na chronionym endpointzie zapewniać ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi co najmniej w następujący sposób:
 - weryfikacja reputacji pliku w bazie threat intelligence producenta systemu
 - lokalna analiza statyczna bazująca na uczeniu maszynowym
12. Agent musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami w plikach Microsoft Word i Microsoft Excel co najmniej w następujący sposób:
 - weryfikacja reputacji makra w bazie threat intelligence producenta
 - lokalna analiza statyczna bazująca na uczeniu maszynowym
13. Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel.
14. Agent musi zapewniać ochronę przed szyfrowaniem dysku i plików przez złośliwe oprogramowanie, w szczególności przed atakami typu ransomware.
15. Agent musi wykonywać analizę plików binarnych po tym, jak zostały zapisane w systemie plików.
16. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu.
17. Agent musi posiadać konfigurowalną opcję umieszczania złośliwych plików w kwarantannie.
18. Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB.
19. Agent, poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców, musi zapewnić ochronę przed atakami klasy Living of The Land wykorzystującymi legalne narzędzia systemowe w groźny sposób.
20. Agent musi zapewniać ochronę przed atakami mającymi na celu kradzież poświadczeń użytkowników.

21. Agent musi posiadać możliwość automatycznej remediacji złożonych ataków co najmniej poprzez wyłączenie złośliwych procesów, umieszczenie plików w kwarantannie, usunięcie zadań z harmonogramu i wpisów z rejestru.
22. Agent musi integrować się z Windows Security Center.
23. Agent musi działać:
- w jądrze systemu (używać sterownika) na systemach Windows
 - w jądrze systemu (kernel space) lub poza jądrem systemu (user space) na systemach Linux
 - poza jądrem systemu na systemach MacOS
24. Agent na systemy Linux musi posiadać możliwość automatycznego przełączenia się do pracy w trybie bez sterownika (user space), jeśli sterownik nie został poprawnie załadowany.
25. Agent dla systemów Windows, MacOS i Linux musi zbierać i wysyłać do systemu co najmniej następujące dane telemetryczne:
- utworzenie nowego procesu i zakończenie procesu
 - operacje na socketach sieciowych dla TCP i UDP
 - operacje na plikach
 - zdarzenia z event logu dotyczącego uwierzytelnienia.
 - operacje na rejestrze (tylko systemy Windows)
26. W przypadku braku łączności z systemem agent musi lokalnie przechować dane telemetryczne i wysłać je do systemu po przywróceniu łączności sieciowej.

II.3 Wymagane minimalne parametry dla modułu ochrony przed wyciekiem danych:

1. Zintegrowany moduł ochrony przed wyciekiem danych będzie posiadać co najmniej możliwość analizy zawartości plików kopiowanych na przenośne nośniki danych oraz danych uploadowanych do aplikacji webowych dla co najmniej 500 systemów.
2. Zintegrowany moduł ochrony przed wyciekiem danych będzie posiadać wbudowane klasyfikatory co najmniej dla następujących rodzajów danych: numer PESEL, numer karty kredytowej, certyfikat x509v3, token JWT.
3. Zintegrowany moduł ochrony przed wyciekiem danych będzie posiadać opcję budowania własnych klasyfikatorów danych w oparciu o wyrażenia regularne.
4. Zintegrowany moduł ochrony przed wyciekiem danych będzie posiadać możliwość budowania reguł kontrolujących kopiowanie danych. Reguły w swoich kryteriach dopasowania muszą umożliwiać:
 - zdefiniowanie typu pliku (np. Plik PDF, plik MS Word, skrypt python, plik tekstowy, etc)
 - wskazanie klasyfikatora danych
 - wskazanie źródłowej aplikacji webowej (np. dane pochodzą z usługi microsoft 365)
 - wskazanie konkretnego użytkownika lub grupy użytkowników z Active Directory
5. Reguły kontrolujące przepływ danych w ramach zintegrowanego modułu ochrony przed wyciekiem danych będą posiadać możliwość skonfigurowania następujących akcji:
 - blokada kopiowania danych na urządzenie przenośne.
 - blokada ładowania danych do aplikacji webowej
 - cichy alarm (tj. akcja nie jest zatrzymana, ale odnotowana w konsoli systemu)
 - wyświetlenie okna dialogowego dla użytkownika z prośbą o uzasadnienie wykonywanej operacji

6. Zintegrowany moduł ochrony przed wyciekiem danych będzie obsługiwać inspekcję schowka w celu zachowania ciągłości ochrony w przypadku, w którym użytkownik próbuje wykorzystać schowek systemowy do ominięcia mechanizmów kontroli danych..
7. Zintegrowany moduł ochrony przed wyciekiem danych będzie wykrywać próby obchodzenia mechanizmów kontroli danych realizując co najmniej:
 - inspekcję schowka systemowego
 - inspekcję tworzenia zaszyfrowanych archiwów danych
8. Zintegrowany moduł ochrony przed wyciekiem danych będzie posiadać opcję zbierania dowodu cyfrowego, tj. umożliwiać operatorowi systemu pobrać plik, który spowodował naruszenie polityki ochrony danych.
9. Zintegrowany moduł ochrony przed wyciekiem danych będzie posiadać możliwość personalizacji komunikatów wyświetlanych użytkownikom w przypadku wykrycia naruszenia polityki ochrony danych.
10. Zintegrowany moduł ochrony przed wyciekiem danych będzie posiadać możliwość wykrywania anomalii w sposobie w jaki użytkownicy posługują się danymi, w tym co najmniej anomalie w ilości operacji kopiowania danych i anomalie w wolumenie danych.
11. Zintegrowany moduł ochrony przed wyciekiem danych będzie posiadać wsparcie co najmniej dla systemów Windows i macOS.

II.4. Wymagane minimalne parametry dla systemu automatyzacji i orkiestracji

1. System musi posiadać wbudowany system do automatyzacji i orkiestracji, przy pomocy którego można zrealizować co najmniej następujące scenariusze:

- wysłanie powiadomienia mailowego i via Microsoft Teams w przypadku, gdy mechanizmy detekcyjno-prewencyjne agenta przestały funkcjonować poprawnie
- włączenie skanowania endpointa w odpowiedzi na alarm o wskazanej istotności
- wysłanie maila do wskazanych adresatów w odpowiedzi na alarm o wskazanej istotności celem potwierdzenia załączenia izolacji sieciowej endpointa.
- założenie zgłoszenia w odpowiedzi na alarm o wskazanej istotności lub alternatywnie wywołanie konfigurowalnego webhooka w odpowiedzi na alarm o wskazanej istotności celem integracji z systemem do śledzenia zgłoszeń.
- raz na dobę wysyłanie powiadomienia mailowego o serwerach, na których agent jest offline.

II.5. Oprogramowanie równoważne: W przypadku zaoferowania oprogramowania równoważnego, Wykonawca w ramach wdrożenia zobowiązany będzie do przeprowadzenia autoryzowanych szkoleń technicznych dla 6 administratorów Zamawiającego. Szkolenia muszą przygotować kadrę do pełnego, samodzielnego administrowania, konfigurowania, monitorowania, utrzymywania i rozwiązywania problemów dotyczących zaoferowanego rozwiązania. Zakres szkolenia musi obejmować co najmniej:

- architekturę rozwiązania,
- konfigurację,
- zarządzanie użytkownikami,
- konfigurację polityk,
- zarządzanie wyjątkami,
- monitorowanie,

- analizę zdarzeń,
- obsługę alarmów,
- reakcję na incydenty,
- troubleshooting,
- aktualizacje,
- zarządzanie certyfikatami,
- integracje/API,
- procedury awaryjne,
- procedury odtworzeniowe,
- bezpieczeństwo samego systemu.

Szkolenie musi obejmować część praktyczną.

W przypadku zaoferowania oprogramowania równoważnego, Wykonawca zapewni dedykowaną, osobistą lub zdalną asystę techniczną inżyniera wdrożeniowego przez okres 90 dni od dnia podpisania protokołu odbioru końcowego, w celu dostrajania polityk bezpieczeństwa i eliminacji błędnych detekcji,

III. Wymagania związane z cyberbezpieczeństwem:

Zamawiający wymaga, aby oferowane świadczenie, w tym wszystkie produkty ICT, usługi ICT oraz procesy ICT wykorzystywane do realizacji zamówienia, zarówno jako elementy główne, jak i komponenty, elementy środowiska świadczenia usługi lub rozwiązania towarzyszące, nie obejmowało:

- produktów ICT, usług ICT lub procesów ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa;
- produktu ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ani usług ICT lub procesów ICT określonych w tej decyzji.