***Załącznik nr 3*** *do SWZ*

*znak:* ***Szp/243-342/2025***

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Spis treści:

[1 Wprowadzenie 3](#_Toc216963485)

[1.1 Wymagania ogólne 3](#_Toc216963486)

[2 Opis wymagań 4](#_Toc216963487)

**Spis Tabel**

[Tabela 1. Wymagane parametry systemu 4](#_Toc216963496)

[Tabela 2. Wykaz elementów stanowiących przedmiot zamówienia. 12](#_Toc216963497)

# Wprowadzenie

Przedmiotem niniejszego postępowania jest pozyskanie zaawansowanego systemu wykrywania i reagowania dla punktów końcowych z obszaru cyberbezpieczeństwa dostarczanego w modelu SaaS, który zapewni kompleksową ochronę infrastruktury informatycznej organizacji. Wymagane jest, aby system ten oferował scentralizowaną konsolę zarządzania, gwarantował wysoką dostępność oraz wspierał szeroki zakres urządzeń, obejmujący serwery, stacje robocze oraz urządzenia mobilne. Wszystkie moduły i funkcje systemu muszą pochodzić od jednego producenta. Dane przetwarzane w systemie muszą być zgodne z wymogami regulacji RODO (GDPR) oraz standardem ISO/IEC 27001:2022 lub równoważnym. Dodatkowo, system powinien być sklasyfikowany jako wiodące rozwiązanie w uznanych raportach branżowych, takich jak Gartner Magic Quadrant for Endpoint Protection Platforms oraz Forrester Wave for Extended Detection and Response Platforms.

## Wymagania ogólne

1. Niniejszy opis przedmiotu zamówienia (OPZ) nie podlega interpretacji. Jeśli zapisy specyfikacji są zdaniem Wykonawcy niejasne, niepełne, nieprecyzyjne lub błędne, to Wykonawca ma obowiązek zadać pytanie przed złożeniem oferty.

# Opis wymagań

Tabela 1. Wymagane parametry systemu

| **L.p.** | **Parametry wymagane przez Zamawiającego** | Oferowane przez Wykonawcę  (potwierdzenie spełnienia)  **WYPEŁNIA WYKONAWCA** *(uzupełnić brakujące lub skreślić niepotrzebne)* |
| --- | --- | --- |
|  | **Wymagania ogólne**   1. Zdolność spełnienia wymagań musi być potwierdzona poprzez weryfikację dokumentacji systemowej, testów, certyfikatów oraz prawnie wiążących oświadczeń producenta. 2. System musi dysponować centralną konsolą, realizowaną w formie usługi SaaS (Software-as-a-Service), zapewniającą dostępność na poziomie co najmniej 99,9%, a do ochrony stacji roboczych i serwerów wykorzystywać agenta. 3. System musi być zaoferowany i dostarczony w wersji ogólnodostępnej (ang. General Availability). Nie dopuszcza się dostarczenia systemu w wersji, która nie jest wersją ogólnodostępną komercyjnie. 4. Wszystkie moduły funkcjonalne systemu muszą zostać dostarczone przez jednego producenta. Jest to niezbędne w celu zapewnienia spójności technologicznej oraz integralności architektury systemu. 5. System musi zapewnić, że wszystkie dane są przechowywane i przetwarzane wyłącznie w granicach Europejskiego Obszaru Gospodarczego, co jest wymogiem wynikającym z regulacji dotyczących ochrony danych osobowych, takich jak RODO. 6. System musi spełniać wymogi Ogólnego Rozporządzenia o Ochronie Danych Osobowych (RODO) oraz posiadać certyfikację ISO/IEC 27001:2022 lub równoważną lub wykazywać zgodność z SOC 2 Type 2. Wymogi te są niezbędne do zapewnienia należytej ochrony danych osobowych oraz ciągłości bezpieczeństwa informacji, minimalizując ryzyko naruszeń i sankcji regulacyjnych. 7. Dojrzałość i skuteczność system musi być poświadczona przez co najmniej następujące niezależne instytucje badające rynek rozwiązań EDR/XDR:    1. System musi być sklasyfikowany przynajmniej jako **lider** (ang. leader) dla raportu Forrester Wave For Extended Detection and Response Platforms Q2 2024.    2. System musi być sklasyfikowany przynajmniej jako **lider** (ang. leader) dla raportu Gartner Magic Quadrant for Endpoint Protection Platforms co najmniej za rok 2023 i 2024. 8. System ma zostać dostarczony z **60-miesięczną** subskrypcją obejmującą ochronę dla **1000** serwerów, **4000** stacji roboczych i **500** urządzeń mobilnych. Wszystkie moduły funkcjonalne systemu muszą być dostarczone z takim samym okresem licencji. 9. System musi zapewnić przechowywanie informacji o alarmach i incydentach przez co najmniej 90 dni. 10. System musi przechowywać szczegółowe dane telemetryczne pochodzące z chronionych systemów (serwerów, stacji roboczych, urządzeń mobilnych) oraz z zewnętrznych źródeł. Dane te muszą być dostępne do ręcznego przeszukiwania zarówno w konsoli systemu, jak i za pośrednictwem interfejsu API przez co najmniej 30 dni. Należy zapewnić brak jakichkolwiek ograniczeń licencyjnych dotyczących ręcznego przeszukiwania tych danych w konsoli. 11. System musi archiwizować logi audytowe przez okres 365 dni, rejestrując co najmniej zdarzenia logowania użytkowników, modyfikacje konfiguracji systemu, inicjacje zdalnych połączeń do chronionych stacji oraz wykorzystanie interfejsu API, w celu zapewnienia integralności danych i zgodności z wymogami regulacyjnymi. 12. System musi posiadać wsparcie i możliwość instalacji agenta na co najmniej następujących systemach operacyjnych:     1. Microsoft:        1. Windows 10 (x86-64 oraz arm64) i Windows 11 (x86-64 oraz arm64)        2. Windows 7 SP1        3. Windows Server 2012 i 2012 R2        4. Windows Server 2016, 2019, 2022 i 2025        5. Windows Server Core 2016, 2019, 2022 i 2025     2. Linux        1. CentOS 8        2. Oracle Linux 7, 8, 9 i 10        3. Red Hat Enterprise Linux 7, 8, 9 i 10        4. Rocky Linux 8, 9 i 10        5. SUSE Linux Enterprise Server 15.3 do 15.7        6. OpenSUSE Leap 15.3 do 15.6        7. Ubuntu 18, 20, 22 i 24        8. Debian 9, 10, 11 i 12        9. Windows Subsystem for Linux 2 (WSL 2)     3. Apple macOS 14, 15 i 26     4. Apple iOS/iPadOS 17.x, 18.x i 26.x     5. Android od 10.x do 15.x 13. System obligatoryjnie musi zapewniać możliwość instalacji agenta na platformach Windows 7 SP1 oraz Windows 10, niezależnie od statusu wsparcia rozszerzonego ze strony producenta. Wersja agenta przeznaczona dla wymienionego systemu operacyjnego musi pozostawać w aktywnym cyklu wsparcia technicznego producenta oraz regularnie otrzymywać aktualizacje mechanizmów detekcyjnych i prewencyjnych. 14. System powinien umożliwiać instalację agenta na infrastrukturze VDI. 15. System musi udostępniać pakiety instalacyjne w następujących formatach:     1. Dla systemów Microsoft: msi lub exe     2. Dla systemów Linux: pakiet rpm i deb     3. Dla macOS: pakiet pkg 16. System musi zapewniać możliwość dystrybucji agenta na platformy mobilne iOS/iPadOS i Android za pośrednictwem systemu MDM lub odpowiednio ze sklepu Apple Store i Google Play, przy czym proces instalacji może być realizowany za pośrednictwem platformy Mobile Device Management (MDM) lub bezpośrednio z autoryzowanych sklepów aplikacji, odpowiednio Apple App Store i Google Play Store 17. Komunikacja między agentem a konsolą systemu musi być realizowana przy użyciu protokołu HTTPS w wariancie co najmniej TLS 1.2 i odbywać się:     1. Bezpośrednio     2. Pośrednio przez proxy systemowe     3. Pośrednio przez proxy wskazane w trakcie instalacji 18. Dokumentacja systemu musi wskazywać adresy IP oraz adresy URL, z którymi komunikuje się agent nawiązując komunikację z konsolą systemu, aby umożliwić udrożnienie komunikacji sieciowej. 19. System musi oferować interfejs zarządzania dostępny przez przeglądarkę internetową. Komunikacja z tym interfejsem musi być zabezpieczona protokołem HTTPS, wykorzystującym co najmniej TLS1.2. Interfejs webowy systemu nie może zawierać komponentów takich jak Flash, Silverlight, aplety Java, ActiveX czy wtyczki NPAPI. 20. System musi umożliwiać zarządzanie poprzez interfejs API. Uwierzytelnianie do interfejsu API platformy musi być oparte na protokole OAuth2 i zapewniać granularną autoryzację dostępu klienta OAuth2 do poszczególnych obszarów funkcjonalnych Systemu. 21. Interfejs API systemu musi umożliwiać co najmniej następujące akcje:     1. Wykonanie kwerendy do danych telemetrycznych z endpointa i z systemów trzecich     2. Pobranie pliku instalacyjnego agenta     3. Uruchomienie skryptu na wskazanym hoście     4. Zarządzenia izolacją sieciową danego hosta     5. Przywrócenie pliku z kwarantanny     6. Pobranie informacji o alarmach     7. Zlecenie skanowania hosta     8. Pobranie pliku z hosta 22. System musi umożliwiać określenie listy publicznych adresów IP, z których możliwe będzie logowanie do konsoli systemu oraz nawiązywanie połączeń z interfejsem API. 23. System musi umożliwiać integrację z zewnętrznymi katalogami użytkowników z wykorzystaniem protokołu SAML 2.0 oraz SCIM. 24. System musi posiadać wbudowany katalog użytkowników oraz obsługiwać drugi czynnik uwierzytelniający wykorzystujący tokeny TOTP (ang. Time Based One-Time Password). 25. System musi egzekwować następujące minimalne wymagania dotyczące złożoności haseł podczas tworzenia lokalnych kont administracyjnych: hasło musi mieć co najmniej 11 znaków i zawierać małe oraz duże litery, cyfry i znaki specjalne. 26. System nie może narzucać ograniczeń licencyjnych na liczbę użytkowników (administratorów, analityków, inżynierów bezpieczeństwa) ani na równoczesne logowania. Wszyscy użytkownicy muszą korzystać z indywidualnych kont imiennych w celu zapewnienia pełnej rozliczalności akcji podejmowanych w systemie. 27. System musi umożliwiać określenie zakresu dostępu z wykorzystaniem matrycy ról i ich przypisania do użytkownika lub do grupy użytkowników (ang. Role Based Access Control). Rola musi definiować dostęp do określonego obszaru administracyjnego systemu, jego rodzaj (tylko do odczytu, pełen dostęp) oraz jego zasięg (wszystkie lub wybrane hosty). 28. System powinien obsługiwać minimum pięć poziomów ważności alarmów, takich jak: informacyjny, niski, średni, wysoki i krytyczny. 29. System musi automatycznie grupować powiązane alerty w celu przyspieszenia i ułatwienia triażu i analizy incydentu. 30. System dla alarmów zgrupowanych w ramach incydentu musi automatycznie tworzyć łańcuchy przyczynowo skutkowe reprezentujące zależności pomiędzy procesami wykorzystywanymi w trakcie ataku i powiązane dane telemetryczne, celem ułatwienia przeanalizowania wykorzystywanych technik, określenia zakres ataku, ustalenia celu i zakresu ataku oraz zweryfikowania, czy atak się powiódł. 31. System musi umożliwiać zarządzanie incydentami co najmniej w następującym zakresie:     1. Przypisanie incydentu do analityka     2. Zmianę stanu incydentu np: badany, false positive, true positive, duplikat, testy     3. Dodawanie notatek     4. Określenia minimalnego czasu na podjęcie analizy incydentu przez analityka wraz ze ścieżką eskalacji, jeśli ten czas zostanie przekroczony. 32. System musi mapować alarmy do frameworku MITRE ATT&CK. 33. System musi umożliwiać tworzenie wyjątków dla reguł prewencyjnych co najmniej na podstawie certyfikatu producenta oprogramowania i ścieżki do pliku. 34. System musi posiadać konfigurowalną możliwość automatycznego uploadowania plików do analizy w sandboxie oraz umożliwiać upload do sandboxa arbitralnych próbek przez interfejs API i interfejs webowy. Wymaga się dostarczyć licencję umożliwiającą upload co najmniej **250** próbek miesięcznie. 35. System musi umożliwiać wgląd w raport z sandboxa dla plików powiązanych z alarmem i eksport raportu. 36. System musi posiadać możliwość kontroli urządzeń podłączanych do portów USB co najmniej na systemach windows i macOS w następującym zakresie:     1. Określenia jak typ urządzenia USB można podłączyć     2. Określenia zakresu dostępu do pamięci masowej USB:        1. Brak dostępu        2. Tylko odczyt        3. Odczyt i zapis        4. Odczyt, zapis i uruchamianie 37. 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:     1. Brak dostępu     2. Tylko odczyt     3. Odczyt i zapis     4. Odczyt, zapis i uruchamianie 38. System musi zapewniać możliwość zarządzania host firewallem na platformach Windows, macOS i Linux. 39. System musi umożliwiać konfigurację manualnych i automatycznych aktualizacji agenta dla określonych grup hostów. Polityka aktualizacji agenta musi umożliwiać wskazanie:     1. Dnia tygodnia i zakresu czasu, w którym aktualizacja nie będzie wykonywana     2. Wersji agenta: względnie wobec najnowszych wydanych lub bezwzględnie (konkretna wersja) 40. System musi umożliwiać kontrolę nad procesem pobierania aktualizacji mechanizmów detekcyjno-prewencyjnych przez agenta, obejmując co najmniej następujące aspekty:     1. Agent pobiera aktualizację natychmiast po opublikowaniu przez producenta     2. Agent pobiera aktualizację z określonym opóźnieniem od momentu publikacji przez producenta 41. System musi umożliwiać dynamiczne grupowanie hostów z wykorzystaniem co najmniej następujących atrybutów: nazwa hosta, system operacyjny, adres ip, podsieć ip, znacznik, atrybuty Active Directory (co najmniej nazwa domeny i pojemnik OU). 42. System musi umożliwiać nawiązanie zdalnego połączenia konsolowego do hosta chronionego agentem oferując co najmniej następujące funkcje:     1. Podgląd uruchomionych procesów     2. Podgląd systemów plików     3. Podgląd stanu socketów sieciowych     4. Wyłączenie wskazanego procesu     5. Uruchomienie skryptu z biblioteki     6. Pobranie pliku z hosta     7. Wgranie pliku na hosta     8. Zrzut pamięci procesu     9. Zrzut pamięci systemu operacyjnego     10. Wyłączenie i restart systemu 43. System musi zapewniać możliwość zdalnej izolacji sieciowej hosta, blokując cały ruch sieciowy z wyjątkiem połączeń z systemem oraz protokołu DHCP, na czas trwania izolacji. 44. System musi umożliwiać budowanie biblioteki skryptów oraz ich zdalne uruchamianie zarówno na pojedynczych hostach, jak i na grupach hostów. Niezbędne jest zapewnienie obsługi co najmniej wymienionych języków skryptowych:     1. Systemy windows: powershell lub python     2. Systemy Linux: skrypty bash lub python     3. Systemy MacOS: skrypty zsh lub python 45. System musi umożliwiać bezpośrednią integrację z usługą VirusTotal oraz DomainTools. Wraz z Systemem nie jest wymagane dostarczenie licencji do żadnego z w/w narzędzi. 46. System musi zapewniać możliwość blokowania uruchamiania plików binarnych na podstawie ich wartości skrótu (hasha), zarówno globalnie, jak i dla określonych grup hostów. 47. System musi umożliwiać tworzenie własnych reguł detekcyjno-prewencyjnych. Reguły te muszą opierać się co najmniej na określeniu łańcucha przyczynowo-skutkowego procesów oraz na parametrach linii poleceń. 48. System musi posiadać możliwość budowania własnych list indykatorów (ang. Indicator Of Compromise) w formie nazw domenowych, adresów IPv4 i IPv6 oraz hashy SHA256 i MD5 poprzez:     1. Manualne dodanie indykatorów     2. Programowe dodanie indykatorów przez interfejs API     3. Import indykatorów z pliku 49. System powinien oferować możliwość tworzenia niestandardowych kokpitów (dashboardów). Użytkownicy mogą w tym celu korzystać zarówno z gotowych kontrolek (ang. widgetów), jak i definiować własne kontrolki za pomocą własnych zapytań do danych telemetrycznych. 50. System musi zapewniać możliwość przeszukiwania wszystkich danych telemetrycznych zarówno za pomocą kreatorów, jak i manualnie, przy użyciu zapytań. Zapytania muszą umożliwiać łączenie i filtrowanie danych telemetrycznych z różnych źródeł, przekształcanie wyników oraz obsługę wyszukiwania pełnotekstowego (ang. free text search), czyli wyszukiwanie dowolnego ciągu znaków bez konieczności wskazywania konkretnego pola. Zasady tworzenia zapytań muszą być jasno opisane w dokumentacji systemowej. 51. System musi zapewniać funkcjonalność zapisywania zapytań do danych telemetrycznych w bibliotece zapytań. 52. System musi umożliwiać wykonywanie zapytań do danych telemetrycznych i pobieranie wyników za pośrednictwem interfejsu API. 53. System musi zapewniać funkcję eksportu wyników kwerendy do pliku tekstowego zawierającego dane telemetryczne. 54. System musi umożliwiać transformację kwerendy dotyczącej danych telemetrycznych w regułę korelacyjną. Reguła ta, uruchamiana zgodnie z określonym harmonogramem, będzie generować alarmy, jeśli kwerenda zwróci więcej niż jeden rekord. 55. System musi posiadać możliwość pobierania zgodnie z żądanym harmonogramem list indykatorów ze wskazanych adresów URL oraz oferować możliwość ich wykorzystania do budowy reguł korelacyjnych.. W szczególności musi posiadać możliwość pobierania indykatorów publikowanych przez CERT Polska w ramach listy ostrzeżeń przed niebezpiecznymi stronami. 56. System musi umożliwiać eksport danych z systemu do systemu SIEM w posiadaniu Zamawiającego co najmniej w następującym zakresie:     1. Wszystkie dane telemetryczne rejestrowane przez agenta     2. Informacja o detetekcjach     3. Załączenie izolacji sieciowej     4. Informacje o logowaniu do systemu     5. Informacja o nawiązaniu połączenia przez zdalną konsolę     6. Dodanie lub zmiana polityki konfiguracyjnej 57. System musi posiadać następujące możliwości przetwarzania logów z systemów trzecich:     1. Co najmniej **15 GB** logów dziennie     2. Okres retencji logów co najmniej 30 dni     3. Dedykowany kolektor do logów (maszyna wirtualna lub oprogramowanie)     4. Gotowe parsery i reguły korelacyjne co najmniej dla następujących systemów:        1. Firewalli Cisco ASA        2. Firewalli Cisco FirePower        3. Cisco Identity Services Engine        4. FortiMail        5. VMware ESXi        6. Microsoft Entra ID        7. Microsoft Exchange Online     5. Wspierany przez Sztuczną Inteligencję wbudowany generator parserów dla logów z systemów trzecich innych niż wskazane w punkcie podpunkcie d. 58. Konsola systemu musi umożliwiać centralne zarządzanie konfiguracją oraz aktualizacją dedykowanego kolektora do logów z systemów trzecich. 59. System musi umożliwiać wykrywanie zasobów podłączonych w sieci wewnętrznej w sposób pasywny (analiza tablicy ARP) oraz poprzez integrację ze środowiskiem Active Directory. 60. System musi posiadać wbudowany moduł raportowania o podatnościach systemu operacyjnego i o podatnościach zainstalowanych aplikacji na systemach operacyjnych Windows, macOS i Linux oraz tworzyć inwenturę zainstalowanych aplikacji i dodatków do przeglądarek. 61. System musi posiadać możliwość alarmowania wskazanych administratorów systemu w przypadku instalacji oprogramowania spoza listy dopuszczonego oprogramowania. 62. System musi posiadać wbudowany moduł SOAR (ang. Security Orchestration, Automation and Response) umożliwiający automatyczną obsługę alarmów w tym m.in. możliwość zmiany konfiguracji (orkiestracji) innych systemów bezpieczeństwa i rozszerzenie kontekstu alarmu poprzez integrację z systemami trzecimi. Wbudowany moduł SOAR musi umożliwiać budowanie spersonalizowanych scenariuszy obsługi (ang. playbooki) z wykorzystaniem graficznego narzędzia bez potrzeby pisania kodu. 63. Wbudowany moduł SOAR musi posiadać możliwość orkiestracji systemów bezpieczeństwa wewnątrz sieci Zamawiającego (systemów on-prem) oraz systemów bezpieczeństwa dostarczanych w formie usługi chmurowej (systemy SaaS). 64. Wbudowany moduł SOAR musi umożliwiać zrealizowanie co najmniej następujących scenariuszy (ang. playbooków):     1. Wysłanie powiadomienia mailowego i via Microsoft Teams w przypadku, gdy mechanizmy detekcyjno-prewencyjne agenta przestały funkcjonować poprawnie.     2. Włączenie skanowania hosta w odpowiedzi na alarm o wskazanej istotności.     3. Wysłanie maila do wskazanych adresatów w odpowiedzi na alarm o wskazanej istotności celem potwierdzenia załączenia izolacji sieciowej hosta.     4. Założenie zgłoszenia w systemie Jira 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.     5. Raz na dobę wysyłanie powiadomienia mailowego o serwerach, na których agent jest offline.     6. Wyszukuje wszystkie maszyny, na których działa lub działał proces o wskazanym sha256 a następnie zatrzymuje proces (jeśli ciagle działa) i usuwa plik o wskazanym sha256. 65. System musi zawierać zintegrowany moduł asystenta oparty na generatywnej Sztucznej Inteligencji (Generative Artificial Intelligence), oferujący co najmniej następujące możliwości:     1. Promptowanie (tj. wydawanie poleceń) w języku naturalnym. Wymagana jest obsługa promptów co najmniej w języku polskim i angielskim.     2. Generowanie kwerend do danych telemetrycznych     3. Wsparcie w zadaniach konfiguracyjnych i przeszukiwaniu dokumentacji     4. Analiza zaciemnionych (aka zobfuskowanych) linii poleceń     5. Generowanie playbooków dla modułu SOAR | Oferowany parametr spełnia wszystkie wymagania ogólne:  Tak / Nie |
|  | **Wymagania dla agenta**   1. Agent nie może używać środowiska Oracle Java JRE/JDK. 2. Instalacja agenta nie może wymagać ponownego uruchomienia systemu operacyjnego. 3. 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 lub podobnego. 4. Agent musi posiadać mechanizmy ochronne uniemożliwiające wyłączenie agenta lub wpłynięcie na jego poprawne funkcjonowanie nawet przez użytkowników z podwyższonymi uprawnieniami (ang. anti-tampering) na systemach Windows, macOS i Linux. 5. Odinstalowanie agenta musi być chronione unikalnym hasłem dla każdej chronionej stacji, tak aby uniemożliwić odinstalowanie agenta nawet użytkowników z podwyższonymi uprawnieniami na systemach Windows, macOS i Linux. 6. W trakcie instalacji agenta musi istnieć możliwość nadania agentowi nieusuwalnego bezpośrednio z konsoli systemu znacznika, który może zostać wykorzystany jako atrybut do grupowanie hostów. 7. W trakcie instalacji agenta musi istnieć możliwość wskazania dedykowanego serwera proxy, z którego agent będzie korzystał nawiązując połączenie z systemem. 8. Agent musi wykrywać i blokować próby wyłączenia usługi Volume Shadow Copy Service (VSS) oraz inne próby uszkodzenia migawek VSS. 9. Agent musi realizować ochronę przed atakami klasy Bring Your Own Vulnerable Driver poprzez wykrywanie i blokowanie prób ładowania podatnych sterowników. 10. Agent musi bezpośrednio na chronionym hoście zapewniać ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi co najmniej w następujący sposób:     1. Weryfikacja reputacji pliku w bazie threat intelligence producenta systemu     2. Lokalna analiza statyczna bazująca na uczeniu maszynowym (ang. Machine learning) 11. Agent musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami w plikach Microsoft Word i Microsoft Excel co najmniej w następujący sposób:     1. Weryfikacja reputacji makra w bazie threat intelligence producenta     2. Lokalna analiza statyczna bazująca na uczeniu maszynowymi (ang. Machine learning) 12. Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel. 13. Agent musi realizować ochronę przed zaszyfrowaniem dysku i plików przez złośliwe oprogramowanie (ochrona anty-ransomware’owa) w scenariuszu gdzie próba szyfrowania podejmowana jest bezpośrednio na chronionym systemie i pośrednio z wykorzystaniem sieci. 14. Agent musi wykonywać analizę plików binarnych po tym jak zostały zapisane w systemie plików. 15. Agent musi zapewniać ochronę anty-exploitową. 16. Agent musi posiadać możliwość umieszczania złośliwych plików w kwarantannie. 17. Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB lub musi blokować próby intencjonalnego i automatycznego uruchomienia plików wykonywalnych z pamięci masowej. 18. Agent musi posiadać mechanizm skanowania pamięci RAM w celu wykrywania złośliwego kodu. 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 obsługiwać następujące tryby pracy:     1. W jądrze systemu (używać sterownika) na systemach Windows     2. W jądrze systemu (używać kernel modułu) lub poza jądrem systemu (aka user space) na systemach Linux     3. Poza jądrem systemu na systemach MacOS 24. Agent dla systemów Windows, MacOS i Linux musi zbierać i wysyłać do systemu co najmniej następujące dane telemetryczne:     1. Utworzenie nowego procesu i zakończenie procesu     2. Operacje na socketach sieciowych dla TCP i UDP     3. Operacje na plikach     4. Zdarzenia z event logu dotyczące uwierzytelnienia.     5. Operacje na rejestrze (tylko systemy Windows) 25. W przypadku braku łączności z systemem agent musi lokalnie przechować dane telemetryczne i wysłać je do systemu po przywróceniu łączności sieciowej. | Oferowany parametr spełnia wszystkie wymagania ogólne:  Tak / Nie |
|  | Gwarancja:   1. Wykonawca wsparcia serwisowego, opartego na świadczeniu serwisowym producenta, w okresie:  * 60 miesięcy liczonych od dnia podpisania protokołu odbioru.  1. Naprawy odbywać się będą bez dodatkowych opłat za transport i dojazd, przez serwis producenta przedmiotu umowy, co zapewnia Wykonawca. Wymóg wykonywania czynności serwisowych przez serwis przedmiotu. 2. Ustala się czas reakcji serwisu producenta przedmiotu umowy na awarię: 3. od chwili zgłoszenia, w zależności od poziomu krytyczności zgłoszenia:  |  |  | | --- | --- | | Poziomy krytyczności zgłoszenia | Sytuacja | | 1 | Poważne problemy, uniemożliwiające Zamawiającemu wykonywanie krytycznych dla niego funkcji. | | 2 | Zamawiający jest zdolny do wykonywania swoich funkcji, ale wydajność  pracy jest obniżona lub poważnie ograniczona. | | 3 | Problem nie ma wpływu na większość funkcji Zamawiającego. | | 4 | Minimalny wpływ na system; w tym prośby o rozbudowanie funkcjonalności  i inne niekrytyczne pytania. |  |  |  |  | | --- | --- | --- | |  | Poziomy krytyczności zgłoszenia | Czas Reakcji | | Zgłoszenie | 1 | 60 minut | | 2 | 4 godziny | | 3 | 4 godziny | | 4 | w lokalnych godzinach pracy od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy |  1. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: przez portal internetowy oraz z wykorzystaniempoczty elektornicznej. 2. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. | Oferowany parametr spełnia wszystkie wymagania ogólne:  Tak / Nie |

**Tabela 2. Wykaz elementów stanowiących przedmiot zamówienia.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Producent/nazwa** | **Liczba sztuk** | **Opis wymagań** | **Cena jednostkowa netto**  **(PLN)** | **Wartość netto**  **(PLN)**  **(kolumna 3x5)** |
|  | **2** | **3** | **4** | *5* | *6* |
|  | *Wypełnia Wykonawca* |  |  | *Wypełnia Wykonawca* | |
| 1 | …………………………………………….. | 1000 | Tabela 1 |  |  |
| 2 | …………………………………………….. | 4000 | Tabela 1 |  |  |
| 3 | …………………………………………….. | 500 | Tabela 1 |  |  |
| **Cena ogółem netto:**  *(suma wartości netto – kolumny 6)* | | | | |  |
| **Wartość VAT (23%):** | | | | |  |
| **Oferowana cena ogółem brutto za całość przedmiotu zamówienia [„Cena” - C]:**  *(suma wartości neto powiększona o wartość vat)* | | | | |  |