

Załącznik Nr 5b do SWZ – Opis przedmiotu zamówienia dla Zadania 2: „Dostawa oprogramowania na potrzeby Powiatowego Urzędu Pracy”

Numer sprawy: IT.I.272.1.6.2025

Zintegrowane rozwiązanie cyberbezpieczeństwa ochrony punktów końcowych wraz z wdrożeniem i przeszkoleniem administratorów

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 w całości musi być dostarczony 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 oraz zgodność z SOC 2 Type 2.
- 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) System wg ewaluacji MITRE Engenuity Enterprise Evaluations z ostatnich dwóch lat musi posiadać skuteczność na poziomie minimum **95%** w następujących kategoriach:
 - Detekcje techniki ataku (procent detekcji ze wskazaniem techniki)
 - Prewencja (procent zablokowanych podkroków)
 - b) System musi być sklasyfikowany przynajmniej jako „**Strong Performers**”/”**Leaders**” dla raportu Forrester Wave For Extended Detection and Response Platforms Q2 2024;
 - c) System musi być sklasyfikowany przynajmniej jako „Leader” dla raportu 2024 Gartner Magic Quadrant for Endpoint Protection Platforms.
- 7) System należy dostarczyć z subskrypcją na okres **12** miesięcy umożliwiającą objęcie ochroną **10** serwerów i **72** stacji roboczych, tj. **do 30.06.2026 r.**
- 8) System musi przechowywać informacje o alarmach i incydentach co najmniej przez 90 dni;
- 9) System musi przechowywać przez 365 dni i umożliwiać przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów (ang. Indicators of Compromise): hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe domena;
- 10) System musi przechowywać przez 365 dni logi audytowe odnotowujące co najmniej logowanie użytkowników, zmiany wprowadzane w konfiguracji systemu oraz nawiązywanie zdalnych połączeń;

- 11) System musi posiadać możliwość instalacji agenta na co najmniej następujących systemach operacyjnych:
- a) Microsoft:
 - Windows 7 SP1
 - Windows 10 (x86-64 oraz arm64)
 - Windows 11 (x86-64 oraz arm64)
 - Server 2008 R2 SP1
 - Server 2012 i 2012 R2
 - Server 2016 i Server Core 2016
 - Server 2019 i Server Core 2019
 - Server 2022 i Server Core 2022
 - Server 2025 I Server Core 2025
 - b) Linux:
 - CentOS 7 i 8
 - Debian 9,10, 11 i 12
 - Oracle Linux 6, 7, 8 i 9
 - Red Hat Enterprise Linux 7, 8 i 9
 - Red Hat Enterprise CoreOS 4
 - Rocky Linux 8 i 9
 - SUSE 12 i 15
 - Ubuntu 16, 18, 20, 22 I 24
 - c) Apple macOS:
 - macOS Ventura 13
 - macOS Sonoma 14
 - macOS Sequoia 15
- 12) System musi posiadać możliwość instalacji agenta na systemach Windows 7 SP1 nieobjętych rozszerzonym wsparciem producenta;
- 13) System musi posiadać możliwość instalacji agenta na systemach VDI;
- 14) System musi umożliwiać wygenerowanie i pobranie pakietu instalacyjnego:
- a) W formacie exe dla systemów Microsoft;
 - b) W formacie pakietu rpm i deb dla systemów Linux;
 - c) W formacie pakietu pkg dla macOS.
- 15) Wymagana jest ocena na poziomie min „A+” dla wszystkich serwisów, z których korzysta oferowane rozwiązanie. Ocena będzie weryfikowana przy pomocy ogólnodostępnego narzędzia <https://www.ssllabs.com>
- 16) Komunikacja między agentem a konsolą systemu musi być realizowana z wykorzystaniem protokołu HTTPS w wariantach co najmniej z TLS1.2 i odbywać się:
- a) Bezpośrednio;
 - b) Pośrednio przez proxy systemowe;

- c) Pośrednio przez proxy wskazane w trakcie instalacji.
- 17) Dokumentacja systemu musi wskazywać adresy IP oraz adresy URL, z którymi komunikuje się agent nawiązując komunikację z konsolą systemu;
 - 18) System musi posiadać możliwość zarządzania przez przeglądarkę internetową. Komunikacja musi być zabezpieczona HTTPS w wariancie co najmniej z TLS1.2;
 - 19) System musi posiadać możliwość zarządzania przez API;
 - 20) System musi posiadać możliwość wskazania listy publicznych adresów IP, z których będzie istniała możliwość zalogowania się do konsoli systemu;
 - 21) System musi umożliwiać integrację z zewnętrznymi katalogami użytkowników z wykorzystaniem SAML 2.0;
 - 22) System musi posiadać wbudowany katalog użytkowników oraz obsługiwać drugi czynnik uwierzytelniający wykorzystujący tokeny TOTP (ang. Time Based One-Time Password);
 - 23) System podczas tworzenia haseł dla lokalnych kont administracyjnych musi spełniać minimalnie następujące wymagania złożoności hasła: co najmniej 12 znaków, musi zawierać małe i duże litery, cyfry i znaki specjalne;
 - 24) 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);
 - 25) System musi obsługiwać co najmniej następujące poziomy ważności alertów: informacyjny, niski, średni, wysoki i krytyczny;
 - 26) System musi automatycznie grupować powiązane alerty w celu przyspieszenia i ułatwienia triażu i analizy incydentu;
 - 27) System dla alertów 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 techniki, określenia zakres ataku, ustalenia celu i zakresu ataku oraz zweryfikowania, czy cel został osiągnięty;
 - 28) System musi umożliwiać zarządzanie incydentami co najmniej w następującym zakresie:
 - a) Przypisanie incydentu do analityka
 - b) Zmianę stanu incydentu: badany, false positive, true positive, duplikat, testy
 - c) Dodawanie notatek
 - 29) Rozwiązanie musi mapować alerty do frameworku MITRE ATT&CK.
 - 30) System musi posiadać możliwość kontroli urządzeń podłączanych do portów USB co najmniej na systemach windows i macOS w następującym zakresie:
 - a) Określenia jakie urządzenia USB można podłączyć;
 - b) Określenia zakresu dostępu do pamięci masowej USB:
 - Brak dostępu
 - Tylko odczyt
 - Odczyt i zapis

- Odczyt, zapis i uruchamianie
- 31) System musi posiadać możliwość definiowania i kontroli polityk firewall co najmniej na systemach windows i macOS w następującym zakresie:
- a) Definiowania akcji domyślnej dla ruchu niezdefiniowanego przez polityki:
 - ruch przychodzący – akcje: blokuj/zezwól
 - ruch wychodzący – akcje: blokuj/zezwól
 - b) Włączenia polityki w tryb monitoringu;
 - c) Określenia co najmniej parametrów dla każdej reguły:
 - Nazwa
 - Opis
 - Kierunek
 - Protokół
 - Lokalny adres IP i port
 - Zdalny adres IP i port
 - FQDN
- 32) System musi posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup endpointów. Polityka automatycznej konfiguracji agenta musi umożliwiać określenie:
- a) Dnia tygodnia i zakresu czasu, w którym aktualizacja nie będzie wykonywana;
 - b) Liczby aktualizowanych endpointów;
 - c) Możliwość zdefiniowania wersji: najnowsza wersja, najnowsza przedostatnia wersja, statycznie wskazana wersja.
- 33) System musi umożliwiać dynamiczne grupowanie endpointów z wykorzystaniem co najmniej następujących atrybutów: nazwa endpointa, domena Active Directory, pojemnik Organizational Unit wewnątrz Active Directory, system operacyjny, adres ip, podsieć ip, wersja kernela, znacznik.
- 34) System musi umożliwiać nawiązanie zdalnego połączenia konsolowego do endpointa chronionego agentem oferując co najmniej następujące funkcje:
- a) Podgląd uruchomionych procesów
 - b) Podgląd systemów plików
 - c) Podgląd stanu socketów sieciowych
 - d) Wyłączenie wskazanego procesu
 - e) Uruchomienie skryptu z biblioteki
 - f) Pobranie pliku z endpointa
 - g) Wgranie pliku na endpointa
 - h) Zrzut pamięci procesu
 - i) Zrzut pamięci systemu operacyjnego
 - j) Wyłączenie i restart systemu

- 35) 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;
- 36) System musi umożliwiać tworzenie biblioteki skryptów oraz ich zdalne uruchamianie na pojedynczym endpointcie lub na grupie endpointów. Wymagana jest obsługa co najmniej następujących języków skryptowych:
- a) Systemy windows: powershell
 - b) Systemy Linux: skrypty bash
 - c) Systemy MacOS: skrypty zsh
- 37) System musi posiadać możliwość uruchomienia pełnego skanowania endpointa na żądanie i w odpowiedzi na zarejestrowany alarm;
- 38) System musi umożliwiać bezpośrednią integrację z usługą VirusTotal;
- 39) System musi umożliwiać globalne oraz per grupa endpointów blokowanie uruchamiania plików binarnych poprzez wskazanie ich hash SHA256;
- 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 (ang. Indicator Of Compromise) w formie nazw domenowych, adresów IPv4 i IPv6 oraz hashy SHA256 i MD5 poprzez:
- a) Import indykatorów z pliku
 - b) Manualne dodanie indykatorów
 - c) Programowe dodanie indykatorów przez API
- 42) System musi obsługiwać co najmniej następujące poziomy istotności alarmów: informacyjny, niski, średni, wysoki i krytyczny.
- 43) Dodatkowo ochrona MFA dla nawiązywania połączenia zdalnego, system przed nawiązaniem zdalnego połączenia konsolowego musi żądać od administratora ponownego wprowadzenia hasła MFA celem dodatkowego potwierdzenia jego tożsamości w celu podwyższenia odporności systemu na ataki wynikające z kradzieży tożsamości.
- 44) Wbudowany system do automatyzacji i orkiestracji
- System musi posiadać wbudowany system do automatyzacji i orkiestracji, przy pomocy którego można zrealizować co najmniej następujące scenariusze:
- a) Wysłanie powiadomienia mailowego i via Microsoft Teams w przypadku, gdy mechanizmy detekcyjno-prewencyjne agenta przestały funkcjonować poprawnie.
 - b) Włączenie skanowania endpointa w odpowiedzi na alarm o wskazanej istotności.
 - c) Wysłanie maila do wskazanych adresatów w odpowiedzi na alarm o wskazanej istotności celem potwierdzenia załączenia izolacji sieciowej endpointa.
 - d) 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.

- e) Raz na dobę wysyłanie powiadomienia mailowego o serwerach, na których agent jest offline.

45) Wbudowany Cyber Threat Intelligence

System musi powiązywać indykatory IOC oraz techniki, taktyki i procedury z informacją co najmniej na temat grup cyber przestępczych i grup APT (Advanced Persistent Threat).

46) Wbudowana integracja z Microsoft Teams

System musi posiadać wbudowaną integrację z Microsoft Teams, która musi:

- a) umożliwiać wysyłanie powiadomień co najmniej o alarmach, incydentach i zdarzeniach z logu audytowego.
- b) umożliwiać dwustronną komunikację z analitykiem w celu potwierdzenia włączenia izolacji sieciowej

47) Skanowanie pamięci z akceleracją sprzętową

Agent co najmniej na systemach Windows musi wspierać sprzętową akcelerację skanowania pamięci, aby zminimalizować wpływ tego procesu na obciążenie chronionego endpointa i nie wpływać negatywnie na wydajność usług serwerowych i aplikacji użytkowych.

2. Wymagania dla agenta:

- 1) Agent nie może wykorzystywać Oracle Java JRE/JDK;
- 2) Instalacja agenta nie może wymagać restartu 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;
- 4) Agent musi posiadać mechanizmy ochronne uniemożliwiające wyłączenie agenta lub wpłynięcie na jego poprawne funkcjonowanie nawet przez użytkowników z podwyższonymi uprawnieniami (ang. anti-tampering);
- 5) Odinstalowanie agenta musi być chronione unikalnym dla każdej chronionej stacji, tak aby uniemożliwić odinstalowanie agenta nawet użytkownikom z podwyższonymi uprawnieniami;
- 6) W trakcie instalacji agenta musi istnieć możliwość nadania agentowi nieusuwalnego z konsoli znacznika, który może zostać wykorzystany jako atrybut do grupowania endpointów;
- 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 endpointzie zapewniać ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi co najmniej w następujący sposób:
 - a) Weryfikacja reputacji pliku w bazie threat intelligence producenta systemu

- b) 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:
 - a) Weryfikacja reputacji makra w bazie threat intelligence producenta
 - b) Lokalna analiza statyczna bazująca na uczeniu maszynowym (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 (aka ochrona anty-ransomware'owa);
- 14) Agent musi wykonywać analizę plików binarnych po tym jak zostały zapisane w systemie plików;
- 15) Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu;
- 16) Agent musi posiadać konfigurowalną opcję umieszczania złośliwych plików w kwarantannie;
- 17) Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB;
- 18) 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;
- 19) Agent musi zapewniać ochronę przed atakami mającymi na celu kradzież poświadczeń użytkowników;
- 20) 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;
- 21) Agent musi integrować się z Windows Security Center;
- 22) Agent musi działać:
 - a) W jądrze systemu (używać sterownika) na systemach Windows
 - b) W jądrze systemu (aka kernel space) lub poza jądrem systemu (aka user space) na systemach Linux
 - c) Poza jądrem systemu na systemach MacOS
- 23) Agent na systemy Linux musi posiadać możliwość automatycznego przełączenia się do pracy w trybie bez sterownika (aka user space), jeśli sterownik nie został poprawnie załadowany;
- 24) Agent dla systemów Windows, MacOS i Linux musi zbierać i wysyłać do systemu co najmniej następujące dane telemetryczne:
 - a) Utworzenie nowego procesu i zakończenie procesu
 - b) Operacje na socketach sieciowych dla TCP i UDP

- c) Operacje na plikach
 - d) Zdarzenia z event logu dotyczącego uwierzytelnienia.
 - e) 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.