Załącznik Nr 2
do zaproszenia do składania ofert INF.1330.1.2024
z dnia 28.02.2025r.

SZCZEGÓŁOWY OPIS ZAMÓWIENIA

Zakup oprogramowania typu XDR w ramach projektu „Cyberbezpieczny Samorząd”

Specyfikacja oprogramowania

Producent: …….

Pełna nazwa oprogramowania ……..

XDR dla 200 użytkowników

Czas licencjonowania 24 miesięcy

Czas wsparcia technicznego 24 miesięcy

Wdrożenie i konfiguracja w siedzibie zamawiającego

LP	Wymagania dla dostawcy	Spełnia/ nie spełnia	UWAGI
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 któregokolwiek z państw członkowskich NATO.		
6	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 **Leaders** dla raportu Forrester Wave For Extended Detection and Response Platforms Q2 2024. 2. System musi być sklasyfikowany przynajmniej jako Leader dla raportu Gartner Magic Quadrant for Endpoint Protection Platforms co najmniej za rok 2023 i 2024		
7	System należy dostarczyć z subskrypcją na okres 24 miesięcy umożliwiającą objęcie ochroną 200 urządzeń.		
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 do chronionych stacji.		
11	1. System musi posiadać możliwość instalacji agenta na co najmniej następujących systemach operacyjnych: a. Microsoft: i. Windows 10 (x86-64 oraz arm64) ii. Windows 11 (x86-64 oraz arm64) iii. Server 2016 i Server Core 2016 iv. Server 2019 i Server Core 2019 v. Server 2022 i Server Core 2022 b. Linux i. CentOS 6, 7 i 8 ii. Debian 9,10, 11 i 12 iii. Oracle Linux 6, 7, 8 i 9 iv. Red Hat Enterprise Linux 6, 7, 8 i 9 v. Red Hat Enterprise CoreOS 4 vi. Rocky Linux 8 i 9 vii. SUSE 11, 12 i 15 viii. Ubuntu 14, 16, 18, 20 i 22 c. Apple macOS i. macOS Monterey 12 ii. macOS Ventura 13 iii. macOS Sonoma 14 iv. macOS Sequoia 15 d. Apple iOS 15.x, 16.x, 17.x i 18.x e. Android 12.x, 13.x i 14.x		
12	System musi posiadać możliwość instalacji agenta na systemach VDI		
13	System musi umożliwiać wygenerowanie i pobranie pakietu instalacyjnego: a. W formacie msi lub exe dla systemów Microsoft b. W formacie pakietu rpm i deb dla systemów Linux W formacie pakietu pkg dla macOS		
14	System musi umożliwiać instalację agenta dla systemów iOS i Android za pośrednictwem systemu MDM lub odpowiednio ze sklepu Apple Store i Google Play.		
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 wariancie 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 5 poziomów ważności alertów, np: 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.		
	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. Tempa propagacji aktualizacji c. Możliwość zdefiniowania wersji: najnowsza wersja, najnowsza przedostatnia wersja, statycznie wskazana wersja		
30	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.		
31	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		
32	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.		
33	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 lub python b. Systemy Linux: skrypty bash lub python c. Systemy MacOS: skrypty zsh lub python		
34	System musi posiadać możliwość uruchomienia pełnego skanowania endpointa na żądanie i w odpowiedzi na zarejestrowany alarm.		
35	System musi umożliwiać bezpośrednią integrację z usługą VirusTotal.		
36	System musi umożliwiać globalne oraz per grupa endpointów blokowanie uruchamiania plików binarnych poprzez wskazanie ich hasha SHA256.		
37	System musi posiadać możliwość budowania własnych reguł detekcyjno-prewencyjnych bazujących co najmniej na określeniu łańcucha przyczynowo-skutkowego procesów wraz z określeniem parametrów linii poleceń.		
38	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		
39	System musi umożliwiać definiowanie własnych dashboardów (konsol) z wykorzystaniem predefiniowanych widgetów (kontrolek) oraz kontrolek definiowanych samodzielnie poprzez kwerendy do danych telemetrycznych.		
40	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.		
41	System musi umożliwiać zapisanie kwerendy do danych telemetrycznych do globalnej biblioteki dostępnej dla wszystkich innych użytkowników.		

42	System musi umożliwiać zrealizowanie kwerendy do danych telemetrycznych i odczytanie jej wyników via API.		
43	System musi umożliwiać eksport wyników kwerendy do danych telemetrycznych w formie pliku tekstowego.		
44	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.		
45	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.		
46	System musi posiadać następujące możliwości przetwarzania logów z systemów trzecich: a. Co najmniej 10GB logów dziennie b. Okres retencji logów co najmniej 7 dni c. Wsparcie co najmniej dla następujących systemów i. firewalli Palo Alto Networks ii. firewalli Fortinet iii. Proofpoint Email Security iv. Cisco Secure Email Gateway v. VMware ESXi vi. Microsoft Azure Event Hubs vii. Microsoft Exchange Online viii. Microsoft Graph API ix. Vectra AI x. ZScaler xi. Uniwersalny Http Event Collector		
47	Agent nie może wykorzystywać Oracle Java JRE/JDK.		
48	Instalacja agenta nie może wymagać restartu systemu operacyjnego.		
49	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		
50	Agent musi posiadać mechanizmy ochronne uniemożliwiające wyłączenie agenta lub wpłynięcie na jego poprawne funkcjonowanie nawet przez użytkowników z podwyższonymi uprawnieniami (ang. anti-tampering).		
51	Odinstalowanie agenta musi być chronione unikalnym hasłem dla każdej chronionej stacji, tak aby uniemożliwić odinstalowanie agenta nawet użytkowników z podwyższonymi uprawnieniami		
52	W trakcie instalacji agenta musi istnieć możliwość nadania agentowi nieusuwalnego z konsoli znacznika, który może zostać wykorzystany jako atrybut do grupowanie endpointów.		
53	W trakcie instalacji agenta musi istnieć możliwość wskazania dedykowanego serwera proxy, z którego agent będzie korzystał nawiązując połączenie z systemem.		
54	Agent musi wykrywać i blokować próby wyłączenia usługi Volume Shadow Copy Service (VSS) oraz inne próby uszkodzenia migawek VSS.		
55	Agent musi realizować ochronę przed atakami klasy Bring Your Own Vulnerable Driver poprzez wykrywanie i blokowanie prób ładowania podatnych sterowników.		

56	Agent musi bezpośrednio na chronionym endpontcie 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)		
57	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 maszynowymi (ang. Machine learning)		
58	Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel.		
59	Agent musi realizować ochronę przed zaszyfrowaniem dysku i plików przez złośliwe oprogramowanie (jak ochrona anty-ransomware'owa).		
60	Agent musi wykonywać analizę plików binarnych po tym jak zostały zapisane w systemie plików.		
61	Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu.		
62	Agent musi posiadać konfigurowalną opcję umieszczania złośliwych plików w kwarantannie.		
63	Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB.		
64	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.		
65	Agent musi zapewniać ochronę przed atakami mającymi na celu kradzież poświadczeń użytkowników.		
66	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.		
67	Agent musi integrować się z Windows Security Center.		
68	Agent musi działać: a. W jądrze systemu (używać sterownika) na systemach Windows b. W jądrze systemu (jak kernel space) lub poza jądrem systemu (jak user space) na systemach Linux c. Poza jądrem systemu na systemach MacOS		
69	Agent na systemy Linux musi posiadać możliwość automatycznego przełączenia się do pracy w trybie bez sterownika (jak user space), jeśli sterownik nie został poprawnie załadowany.		
70	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 dotyczące uwierzytelnienia. e. Operacje na rejestrze (tylko systemy Windows)		
71	W przypadku braku łączności z systemem agent musi lokalnie przechować dane telemetryczne i wysłać je do systemu po przywróceniu łączności sieciowej.		
72	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.		
73	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. Raz na dobę wysyłanie powiadomienia mailowego o serwerach, na których agent jest offline		
74	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).		
75	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		
76	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		
77	Agent co najmniej na systemach Windows musi wspierać sprzętową akceleracją skanowania pamięci, aby zminimalizować wpływ tego procesu na obciążenie chronionego endpointa i nie wpływać negatywnie na wydajność usług serwerowych i aplikacji użytkowych		

*** Uwaga: Prawą stronę tabeli, należy wypełnić stosując słowa „spełnia” lub „nie spełnia”, zaś w przypadku wyższych wartości niż minimalne- wykazane w tabeli należy wpisać**

oferowane wartości techniczno-użytkowe. W przypadku, gdy Wykonawca w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości oferta zostanie odrzucona, gdyż jej treść nie odpowiada treści SIWZ (art. 89 ust 1 pkt 2 ustawy PZP).

……..
/podpis i pieczęć osoby uprawnionej
do reprezentowania Wykonawcy/