Ministerstwo Rozwoju i Technologii **Warszawa, 7.10.2025 r.**

ul. Plac Trzech Krzyży 3/5

00-507 Warszawa

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo planuje uruchomić postępowanie przetargowe o udzielenie zamówienia publicznego na zakup Systemu Rozszerzonego Wykrywana i Reagowania (XDR - Extended Detection and Response) wraz z wdrożeniem i instruktażem oraz usługami wsparcia technicznego dla Ministerstwa Rozwoju i Technologii.

Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego zamówienia do wszczęcia postępowania przetargowego.

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia, jest zakup Systemu Rozszerzonego Wykrywana i Reagowania (XDR - Extended Detection and Response) wraz z wdrożeniem i instruktażem oraz usługami wsparcia technicznego dla Ministerstwa Rozwoju i Technologii.

Przedmiot zamówienia składają się następujące działania:

1. Dostarczenie subskrypcji oraz oprogramowania Systemu XDR wraz ze wsparciem producenta na 36 miesięcy.
2. Wdrożenie dostarczonego systemu XDR
3. Usługi asysty technicznej dla wdrożonego Systemu, świadczone na podstawie dodatkowych zleceń Zamawiającego

II. TERMIN REALIZACJI ZAMÓWIENIA

Przedmiot zamówienia zostanie zrealizowany w terminie maksymalnie **do 30 dni** od daty podpisania przez strony umowy **(termin realizacji do uzupełnienia przez Wykonawcę w Formularzu Ofertowym).**

III. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. W ramach realizacji przedmiotu zamówienia zostanie zrealizowana dostawa systemu Rozszerzonego Wykrywana i Reagowania (XDR - Extended Detection and Response) wraz z wdrożeniem i instruktażem oraz usługami wsparcia technicznego dla Ministerstwa Rozwoju i Technologii.
2. W ramach realizacji przedmiotu zamówienia zostaną dostarczone niezbędne elementy i subskrypcje oprogramowania składającego się na zaoferowany system Rozszerzonego Wykrywana i Reagowania (XDR - Extended Detection and Response)
3. Zaoferowane oprogramowanie nie może być przeznaczone przez producenta do wycofania ze sprzedaży.
4. Dostarczone licencje (subskrypcje) muszą być zarejestrowane na Zamawiającego i pochodzić z legalnego kanału dystrybucyjnego producenta na rynek UE oraz nie posiadać wad prawnych, zaś korzystanie z niego przez Zamawiającego nie powinno stanowić naruszenia majątkowych praw autorskich osób trzecich.

5. Prawo do aktualizacji przedmiotowego oprogramowania oraz baz sygnatur musi być zarejestrowane u producenta na użytkownika końcowego (Zamawiającego).
6. Zapewnienie wsparcia i pomocy technicznej przez okres 36 miesięcy od dnia wdrożenia. W ramach wsparcia należy zapewnić dostęp do aktualizacji oprogramowania i sygnatur. Wsparcie powinno być realizowane w języku polskim. W ramach wsparcia zgłoszenia będą realizowane za pomocą systemu informatycznego wykonawcy (całodobowo) lub telefonicznie - w dni robocze w godzinach 8-16.
7. Wykonawca musi zagwarantować przywrócenie funkcjonalności systemu, licząc od momentu zgłoszenia przez Zamawiającego w ciągu 8 godzin roboczych.
8. System musi spełniać wymogi w zakresie ochrony poufności, integralności i dostępności informacji oraz systemów informatycznych zgodnie z polskimi normami i Krajowymi Ramami Interoperacyjności (KRI), w tym aktualizację oprogramowania oraz zarządzanie konfiguracją.
9. System musi współpracować z istniejącą infrastrukturą teleinformatyczną Zamawiającego oraz być zgodny z wymaganiami interoperacyjności systemów publicznych w Polsce.

IV. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE SYSTEMU XDR

1. System XDR musi obejmować kompleksowe wykrywanie, korelowanie, monitorowanie, blokowanie i usuwanie zaawansowanych zagrożeń oraz automatyczne i manualne działania naprawcze na okres określony w formularzu ofertowym.
2. System XDR musi zapewnić zbieranie i korelację zdarzeń:
   a) stacji roboczych;
   b) serwerów;
   c) sieci;
   d) rozwiązań chmurowych – aplikacji SaaS;
   e) poczty elektronicznej;
   f) dotyczących tożsamości *(np. próby eskalacji uprawnień)*
3. System XDR musi być dostarczony w formie lub SaaS. Rozwiązanie SaaS musi posiadać wskaźnik dostępności na poziomie co najmniej 99,9%.
4. Wszystkie moduły funkcjonalne Systemu muszą być dostarczone od jednego producenta.
5. Wszystkie wygenerowane przez system incydenty, zdarzenia bezpieczeństwa, informacje dotyczące wykrytych podatności oraz informacje związane z analizą ryzyka muszą być prezentowane w jednej centralnej konsoli stanowiącej część oferowanego systemu.
6. System musi się składać z wymienionych komponentów:
   a) agentów instalowanych na stacjach roboczych i serwerach
   b) agentów instalowanych na urządzeniach mobilnych
   c) konsoli zarządzającej i analitycznej
7. Dla rozwiązania SaaS wymaga się, aby system był uruchomiony w chmurze publicznej oraz przechowywał i przetwarzał dane na terenie Polski lub Europejskiego Obszaru Gospodarczego.
8. System musi być zgodny z regulacjami RODO/GDPR (ang. General Data Protection Regulation), posiadać certyfikację ISO/IEC 27001:2022,CSA Star Level 2, FedRAMP, PCI DSS CSP, SOC 3, SOC 2 Type 2.
9. System nie może być zabroniony do stosowania ani czasowo wstrzymany do stosowania przez administrację któregokolwiek z państw członkowskich NATO.
10. Skuteczność systemu musi być poświadczona przez co najmniej następujące niezależne instytucje badające rynek rozwiązań EDR/XDR:
    a) System musi być sklasyfikowany jako „Leader” dla raportu Gartner Magic Quadrant for Endpoint Protection Platforms co najmniej za rok 2025.
11. System należy dostarczyć z subskrypcją wraz ze wsparciem producenta na okres określony w formularzu ofertowym umożliwiającą objęcie ochroną:

a) stacje robocze windows 10/11 (w tym VDI)
b) stacje robocze macOS
c) serwery Linux
d) serwery Microsoft Windows Server

12. System musi przechowywać informacje o alarmach i incydentach co najmniej przez 30 dni
13. System musi przechowywać szczegółowe dane telemetryczne z endpointów zabezpieczonych agentem przez co najmniej 30 dni.
14. System musi umożliwiać pobieranie/eksportu kompletnych „surowych" danych telemetrycznych z chmury producenta dla potrzeb długoterminowego przechowywania logów i analityki w lokalnym SIEM. Jeżeli funkcja ta wymaga dodatkowej licencji to należy przewidzieć ją w ofercie. Musi istnieć również możliwość przeszukiwania tych danych.
15. System musi szyfrować dane w trakcie transmisji i w trakcie przechowywania za pomocą protokołów i algorytmów kryptograficznych uznanych powszechnie za bezpieczne. Producent systemu musi zagwarantować, że dostęp do przechowywanych danych posiada tylko i wyłącznie producent i że dostęp do danych nie jest możliwy dla żadnej trzeciej strony. Dane w trakcie przechowywania muszą być szyfrowane algorytmem AES-256.
16. Interfejs API systemu musi umożliwiać co najmniej następujące akcje:
    a) Wykonanie kwerendy do danych telemetrycznych z endpointa i z systemów trzecich
    b) Uruchomienie skryptu na wskazanym hoście
    c) Zarządzanie izolacją sieciową danego hosta
    d) Pobranie informacji o alarmach
    e) Zlecenie skanowania hosta
    f) Pobranie pliku z hosta
17. System musi przechowywać przez 180 dni logi audytowe odnotowujące co najmniej logowanie użytkowników, zmiany wprowadzane w konfiguracji systemu, nawiązywanie zdalnych połączeń do chronionych stacji i wykorzystanie interfejsu API
18. Producent musi dostarczyć zakres danych przetwarzanych w usłudze jako załącznik do dokumentacji powdrożeniowej
19. System musi posiadać możliwość instalacji agenta na co najmniej następujących systemach operacyjnych:
    a) Microsoft:
        - Windows 10
        - Windows 11
        - 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
        - Debian 10, 11 i 12
        - Oracle Linux 7, 8 i 9
        - Red Hat Enterprise Linux 7, 8, 9 i 10
        - Rocky Linux 9 i 10
        - SUSE Linux Enterprise Server 12 i 15
        - Ubuntu, 20.04 LTS, 22.04 LTS, 24.04 LTS
    c) Apple macOS od Ventura 13 (i nowszych wersjach)
    d) Apple iOS/iPadOS od 16.x (i nowszych wersjach)
    e) Android od 9.x (i nowszych wersjach)
20. System musi posiadać możliwość instalacji agenta na systemach VDI.
21. 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

c) W formacie pakietu pkg dla macOS

22. 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
23. 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 lub poprzez generowanie pakietu instalacyjnego agenta
24. Dokumentacja Systemu musi wskazywać adresy IP oraz adresy URL, z którymi komunikuje się agent nawiązując komunikację z konsolą systemu, aby umożliwić udrożnienie komunikacji sieciowej.
25. System musi posiadać możliwość zarządzania przez przeglądarkę internetową. Komunikacja musi być zabezpieczona HTTPS w wariancie co najmniej z TLS1.2.
26. Interfejs webowy Systemu nie może korzystać z komponentów typu Flash, Silverlight, applet Java, ActiveX, wtyczek NPAPI.
27. System musi posiadać możliwość zarządzania oraz integracji z innymi systemami przez interfejs API.
28. System musi posiadać możliwość wskazania listy publicznych adresów IP, z których będzie istniała możliwość zalogowania się do konsoli systemu.
29. System musi umożliwiać integrację z zewnętrznymi katalogami użytkowników z wykorzystaniem SAML 2.0 ze wsparciem dla ADFS.
30. Logowanie do konsoli zarządzającej musi wymagać użycia drugiego składnika - MFA (multi-factor authentication)
31. System musi posiadać wbudowany katalog użytkowników oraz obsługiwać drugi czynnik uwierzytelniający wykorzystujący tokeny TOTP (ang. Time Based One-Time Password).
32. System podczas tworzenia haseł dla lokalnych kont administracyjnych musi wymuszać tworzenie haseł złożonych.
33. System nie może posiadać ograniczenia licencyjnego na liczbę użytkowników (administratorów, analityków, inżynierów bezpieczeństwa) zdefiniowanych w systemie ani ograniczenia na równocześnie zalogowanych w systemie użytkowników. Wszyscy użytkownicy muszą posiadać własne konta imienne. Nie dopuszcza się wykorzystania współdzielonych kont użytkowników.
34. 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 rodzaj (tylko do odczytu, pełen dostęp) oraz jego zakresu (wszystkie lub wybrane hosty).
35. System musi obsługiwać co najmniej 5 poziomów ważności alarmów, np: informacyjny, niski, średni, wysoki i krytyczny.
36. System musi automatycznie grupować powiązane alerty w celu przyspieszenia i ułatwienia triażu i analizy incydentu.
37. 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, ustalenia celu i zakresu ataku oraz zweryfikowania, czy atak się powiódł.
38. System musi posiadać moduł obsługi zgłoszeń (case management)
39. System musi umożliwiać zarządzanie incydentami co najmniej w następującym zakresie:
    a) Przypisanie incydentu do analityka
    b) Zmianę stanu incydentu np: badany, false positive, true positive
    c) Dodawanie notatek
    d) Przypisania priorytetów

40. System musi mapować alarmy do frameworku MITRE ATT&CK minimum w wersji 12
41. System musi posiadać funkcjonalność sprawdzania próbek w piaskownicy tzw. Sandbox.
    a) musi posiadać konfigurowalną możliwość automatycznego uploadowania plików do analizy w sandboxie,
    b) musi umożliwiać wgląd w raport z sandboxa dla plików powiązanych z incydentem i eksport raportu.
42. System musi posiadać możliwość kontroli urządzeń podłączanych do portów USB co najmniej na systemach Windows, Linux i macOS w następującym zakresie:
    a) Określenia jakie urządzenia USB można podłączyć
    b) Określenia zakresu dostępu do pamięci masowej USB:
    c) Brak dostępu
    d) Tylko odczyt
    e) Odczyt i zapis
    f) Odczyt, zapis i uruchamianie
43. System musi posiadać możliwość kontroli host firewalla co najmniej na systemach Windows
44. System musi posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla danych grup hostów.
45. System musi umożliwiać dynamiczne grupowanie hostów z wykorzystaniem co najmniej następujących atrybutów: nazwa hosta, jednostka organizacyjna Organizational Unit wewnątrz Active Directory, system operacyjny, adres IP.
46. System musi umożliwiać nawiązanie zdalnego połączenia konsolowego do hosta chronionego agentem oferując co najmniej następujące funkcje:
    a) Podgląd uruchomionych procesów
    b) Podgląd systemów plików
    c) Wyłączenie wskazanego procesu
    d) Uruchomienie skryptu z biblioteki
    e) Pobranie pliku z hosta
    f) Zrzut pamięci procesu dla systemu Windows
47. System musi umożliwiać zdalną izolację sieciową hosta. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu musi zostać zablokowany.
48. System musi umożliwiać tworzenie biblioteki skryptów oraz ich zdalne uruchamianie na pojedynczym hoście i na grupie hostów. Wymagana jest obsługa co najmniej następujących języków skryptowych:
    a) Systemy windows: powershell
    b) Systemy Linux: skrypty bash lub python
    c) Systemy MacOS: skrypty zsh lub python
49. System musi posiadać możliwość uruchomienia pełnego skanowania hosta na żądanie.
50. System musi umożliwiać integrację z usługą VirusTotal. Wraz z Systemem nie jest wymagane dostarczenie licencji do wskazanego narzędzia.
51. System musi posiadać wbudowane mechanizmy integracji lub umożliwiać integrację za pomocą API z produktami i usługami klasy SIEM i SOAR
52. System musi umożliwiać globalne oraz per grupa hostów blokowanie uruchamiania plików binarnych poprzez wskazanie ich hasha.
53. System musi posiadać możliwość budowania własnych reguł detekcyjno-prewencyjnych.
54. System musi posiadać możliwość budowania własnych list indykatorów (ang. Indicator Of Compromise) w formie nazw domenowych, adresów IPv4 i IPv6 oraz hashy SHA256 poprzez:
    a) Import indykatorów z pliku w formacie STIX
    b) Manualne dodanie indykatorów
    c) Programowe dodanie indykatorów przez interfejs API
    d) Poprzez protokół TAXII
55. System musi umożliwiać definiowanie własnych dashboardów (konsol) z wykorzystaniem predefiniowanych widgetów (kontrolek).

56. System XDR musi zapewnić zbieranie i korelację zdarzeń:
    a) Stacji roboczych
    b) Serwerów
    c) Sieci
    d) Rozwiązań chmury publicznej pracujących w modelu SaaS np. Sharepoint Online, OneDrive
    e) Poczty elektronicznej MS Exchange
    f) Dotyczących tożsamości (np. próby eskalacji uprawnień)
57. System musi umożliwiać przeszukiwanie wszystkich danych telemetrycznych z wykorzystaniem kwerend. Kwerendy muszą umożliwiać łączenie danych telemetrycznych z różnych źródeł, ich filtrowanie, przekształcanie wyników i obsługiwać free text search (wyszukiwanie dowolnego ciągu znaków bez wskazywania konkretnego pola). Reguły tworzenia kwerend muszą być opisane w dokumentacji systemu.
58. System musi umożliwiać zapisanie kwerendy do danych telemetrycznych do biblioteki.
59. System musi umożliwiać zrealizowanie kwerendy do danych telemetrycznych i odczytanie jej wyników via interfejs API.
60. System musi umożliwiać eksport wyników kwerendy do danych telemetrycznych w formie pliku tekstowego lub JSON.
61. System musi umożliwiać eksportowanie alertów oraz logów audytowych w formacie syslog
62. System musi umożliwiać integracje z systemami ticketowymi takimi jak Jira, ServiceDesk Plus
63. System musi umożliwiać uruchamianie kwerendy
64. System musi umożliwiać wykrywanie zasobów podłączonych w sieci wewnętrznej w sposób pasywny.
65. System musi posiadać następujące możliwości przetwarzania logów z systemów trzecich:
    a) Co najmniej 10GB logów dziennie
    b) Wsparcie dla logów w formacie syslog
66. System musi posiadać możliwość rozbudowy o zintegrowany moduł raportowania o podatnościach systemu operacyjnego i o podatnościach zainstalowanych aplikacji na systemach operacyjnych Windows, macOS i Linux. Moduł musi tworzyć inwenturę zainstalowanych aplikacji.
67. System musi posiadać możliwość rozbudowy o zintegrowany moduł ITDR (ang. Identity Threat Detection and Response) co najmniej w zakresie detekcji niebezpiecznych i podejrzanych zdarzeń związanych z kradzieżą tożsamości. Moduł ITDR musi działać co najmniej dla środowiska Active Directory. Wbudowany moduł ITDR musi budować profile zachowania użytkowników i alarmować w przypadku wykrycia podejrzanych anomalii w ich zachowaniu oraz na bieżąco oceniać ryzyko powiązane z użytkownikiem.
68. System musi umożliwiać definiowanie wskaźników kompromitacji w formie: SHA256, nazwy domenowej, adresu IPv4, ścieżki, nazwy pliku. Musi istnieć możliwość dodania znacznika ręcznie, zaimportowania znaczników z pliku i via REST API oraz oznaczenia reputacji, wiarygodności i okresu wygaśnięcia znacznika.
69. System musi umożliwiać definiowanie złożonych wskaźników kompromitacji opisujących zachowanie procesu co najmniej w zakresie: operacji plikowych, uruchamianych procesów i ich parametrów, operacji sieciowych i operacji na rejestrze (tylko windows).
70. System musi posiadać wbudowane modele uczenia maszynowego (Machine Learning) dedykowane do wykrywania ruchu bocznego (lateral movement) w infrastrukturze IT.
71. System dla każdego wprowadzonego i złożonego wskaźnika kompromitacji musi wygenerować alarm(-y):
    a) jeśli znacznik został odszukany w historycznych danych telemetrycznych (zgromadzonych przed dodaniem wskaźnika)
    b) jeśli znacznik zostanie odszukany w nowych danych telemetrycznych
72. System musi umożliwiać przekształcanie złożonych wskaźników kompromitacji w reguły prewencyjne co najmniej dla agenta dla Windows.

73. 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.
74. Wbudowany moduł SOAR musi posiadać możliwość orkiestracji systemów bezpieczeństwa wewnątrz sieci Zamawiającego (systemów on-prem) oraz systemów bezpieczeństwa.
75. Wbudowany moduł SOAR musi umożliwiać zrealizowanie co najmniej następujących scenariuszy:
    a) Wysłanie maila do wskazanych adresatów w odpowiedzi na alarm o wskazanej istotności celem potwierdzenia załączenia izolacji sieciowej hosta.
    b) 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.
    c) W odpowiedzi na alarm o zadanej wartości, w którym zidentyfikowano komunikację z groźnymi publicznymi adresami IP musi nastąpić dodanie w/w adresów IP do listy blokowanych adresów IP na firewallu Fortinet i firewallu Palo Alto Networks. Zgodę na dodanie adresów IP musi wyrazić wskazany operator otrzymując powiadomienie o konieczności podjęcia decyzji w formie powiadomienia wysłanego na wskazany kanał Microsoft Teams lub drogą mailową.

V. Wymagania dla Agenta instalowanego na stacjach roboczych:

1. Agent nie może wykorzystywać Oracle Java JRE/JDK.
2. 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.
3. 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.
4. 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.
5. W trakcie instalacji agenta musi istnieć możliwość wskazania dedykowanego serwera proxy, z którego agent będzie korzystał nawiązując połączenie z systemem.
6. Agent musi wykrywać i blokować próby wyłączenia usługi Volume Shadow Copy Service (VSS) oraz inne próby uszkodzenia migawek VSS.
7. Agent musi bezpośrednio na chronionym hoście zapewniać ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi poprzez lokalną analizę statyczną bazującą na uczeniu maszynowym (ang. Machine learning)
8. Agent musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami w plikach Microsoft Word i Microsoft Excel poprzez lokalną analizę statyczną bazującą na uczeniu maszynowymi (ang. Machine learning)
9. Agent musi realizować ochronę przed zaszyfrowaniem dysku i plików przez złośliwe oprogramowanie (aka ochrona anty-ransomware'owa).
10. Agent musi wykonywać analizę plików binarnych po tym jak zostały zapisane w systemie plików.
11. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu.
12. Agent musi posiadać konfigurowalną opcję umieszczania złośliwych plików w kwarantannie.
13. 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.
14. Agent co najmniej na systemach Windows musi posiadać mechanizm skanowania pamięci RAM w celu wykrywania złośliwego kodu.
15. 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.
16. Agent musi zapewniać ochronę przed atakami mającymi na celu kradzież poświadczeń użytkowników.
17. Agent musi posiadać możliwość automatycznej remediacji złożonych ataków co najmniej poprzez wyłączenie złośliwych procesów, umieszczenie plików w kwarantannie.
18. Agent musi integrować się z Windows Security Center.
19. Agent musi umożliwiać kwarantannę groźnych plików.
20. 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
21. 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)
22. W przypadku braku łączności z systemem agent musi lokalnie przechować dane telemetryczne i wysłać je do systemu po przywróceniu łączności sieciowej.

VI. MINIMALNE WYMAGANIA W ZAKRESIE GWARANCJI SYSTEMU

Gwarancja dla oferowanego systemu musi spełniać niżej opisane wymagania:

1. Minimalny okres gwarancji 36 miesięcy.
2. Gwarancja będzie liczona od daty odbioru przedmiotu umowy i oparta na gwarancji producenta rozwiązania zgodnie z terminami obowiązywania wymaganymi w OPZ.
3. Gwarancja ma być świadczona w reżimie 8x5xNBD. Czas naprawy Awarii liczony jest od czasu przesłania zgłoszenia o awarii do Wykonawcy zgodnie z procedurą przyjmowania zgłoszeń serwisowych.
4. Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub www) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją w godzinach pracy Zamawiającego.
5. W okresie gwarancji Wykonawca w ramach otrzymanego wynagrodzenia udostępni Zamawiającemu możliwość wielokrotnego uaktualniania całego dostarczonego Oprogramowania do najnowszych wersji oferowanych przez producenta oraz patche i programy korekcji błędów.
6. Przez usunięcie Awarii należy rozumieć przywrócenie pierwotnej funkcjonalności Systemu we wszystkich modułach i zaprzestanie stosowania w bieżącej pracy procedur zastępczych.
7. Po usunięciu każdej Awarii, Wykonawca zobowiązuje się do doprowadzenia całego systemu do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych komponentów.
8. W ramach gwarancji Zamawiający będzie miał prawo przez okres wskazany w formularzu ofertowym do:
    a) pobierania i instalowania nowych wersji oprogramowania dla każdego elementu wchodzącego w skład oferty;
    b) Dostępu do bazy wiedzy oraz dokumentacji dostarczonych elementów;
    c) Dostępu do powiadomień/ogłoszeń/alarmów w zakresie dostarczonych elementów;

d) Zgłaszania nieograniczonej liczby awarii systemu w trybie 24x365x7 za pomocą dedykowanego portalu i/lub zgłoszenia telefonicznego.

9. Czasy reakcji/naprawy na zgłoszenie będą na poziomie:
   a) 1 godzina/8 godzin - błąd krytyczny – tj. przerwa w działaniu usług w środowisku produkcyjnym, brak dostępnego obejścia problemu,
   b) 2 godziny/2 dni - błędy wysokie – tj. problem z poprawnym działaniem usługi znacząco utrudniający realizację procesów biznesowych, brak dostępnego obejścia problemu,
   c) 4 godziny/7 dni - błędy średnie - tj. problem z poprawnym działaniem usługi, utrudnienie realizacji procesów biznesowych, dostępne obejście problemu,
   d) 8 godzin/14 dni - błędy niskie – tj. problem z poprawnym działaniem usługi, brak wpływu na realizację procesów biznesowych.
10. Wykonawca w terminie 7 dni od zawarcia Umowy dostarczy Zamawiającemu procedury zgłaszania i obsługi Awarii wraz z listą osób upoważnionych do kontaktów, wykazem adresów poczty elektronicznej i nr telefonów.
11. W okresie gwarancji Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie oprogramowania stanowiącego przedmiot zamówienia, z zastrzeżeniem, że Wykonawca nie ponosi odpowiedzialności za uszkodzenia oprogramowania powstałe z wyłącznej winy Zamawiającego lub osób trzecich działających w jego imieniu.
12. Wymagany tryb zgłaszania wszelkich awarii, wad i błędów. Zgłoszenie następuje w drodze pisemnej mailem na adres podany przez Wykonawcę lub za pośrednictwem telefonicznego zgłaszania awarii, wad i błędów dotyczących sprzętu i oprogramowania w dni robocze w godzinach 8:00-17:00.
13. Zamawiający wymaga obsługi zgłoszeń w języku polskim.

VII. MINIMALNE WYMAGANIA W ZAKRESIE DOKUMENTACJI POWYKONAWCZEJ

Wykonawca po zakończonym wdrożeniu Systemu zobowiązany jest do sporządzenia dokumentacji powykonawczej wdrożonego Systemu. Dokumentacja musi zawierać następujące elementy:

1. Informacje ogólne
   - Tytuł projektu/systemu
   - Zamawiający i wykonawca
   - Zakres wdrożenia
   - Daty realizacji (rozpoczęcia i zakończenia)
   - Osoby kontaktowe/odpowiedzialne
2. Opis systemu
   - Cel i funkcjonalność systemu
   - Zakres objęty wdrożeniem
   - Architektura systemu (np. model warstwowy, serwer-klient, chmura)
   - Schematy lub diagramy (np. diagramy UML, sieciowe, architektury logicznej i fizycznej)
   - Licencje
3. Wykonane prace
   - Opis wykonanych etapów wdrożenia
   - Zastosowane technologie i narzędzia
   - Zainstalowane oprogramowanie i ich wersje
   - Dostarczone komponenty ich specyfikacja
4. Konfiguracja systemu
   - Parametry konfiguracyjne
   - Zastosowane ustawienia (system operacyjny, bazy danych, serwery, aplikacje)
   - Dane dostępowe (jeśli to możliwe) lub procedura ich uzyskania
   - Schematy połączeń (np. sieciowych, zasilania, logiki sterowania)
5. Testy i odbiory

- Protokoły testów funkcjonalnych i integracyjnych
- Wyniki testów
- Protokół odbioru końcowego
- Wykryte i rozwiązane problemy (jeśli były)

6. Instrukcje i procedury
    - Instrukcja użytkownika systemu
    - Instrukcja administratora
    - Procedury awaryjne i odzyskiwania danych (Disaster Recovery)
    - Szczegóły dotyczące kopii zapasowych i przywracania systemu
    - Procedury utrzymaniowe
7. Załączniki
    - Licencje na oprogramowanie
    - Certyfikaty zgodności
    - Rysunki techniczne
    - Zrzuty ekranów lub dokumentacja fotograficzna
    - Raporty z testów

VIII. MINIMALNE WYMAGANIA W ZAKRESIE WDROŻENIA SYSTEMU WRAZ Z PRZEPROWADZENIEM INSTRUKTAŻU

Wdrożenie zostanie wykonane przez następujące działania:

1. instalację subskrypcji oprogramowania;
2. analizę przedwdrożeniową obejmującą rozpoznanie potrzeb i przygotowanie architektury rozwiązania ujętą w projekcie technicznym;
3. konfigurację i uruchomienie systemu XDR;
4. wykonanie dokumentacji technicznej i eksploatacyjnej;
5. przeprowadzenie instruktażu dla administratorów Systemu;
6. konfigurację i implementację polityk bezpieczeństwa, reguł oraz raportów, optymalizację pod kątem wydajności oraz minimalizacji liczby fałszywych alarmów zgodnie z najlepszymi praktykami oraz wytycznymi Zamawiającego;
7. przeprowadzenie testów poprawności instalacji i konfiguracji oraz przygotowanie szablonów powiadomień o incydentach bezpieczeństwa
8. instalację i konfigurację oprogramowania XDR według najlepszych praktyk producenta. Instalację oprogramowania na stacjach roboczych i serwerach wykona Zamawiający na podstawie informacji i dokumentacji dostarczonej przez Wykonawcę.
9. konfigurację autentykacji i autoryzacji do systemów włączając w to integrację z usługami zarządzania tożsamością działających u Zamawiającego.
10. przeprowadzenie pełnej integracji z istniejącymi narzędziami SIEM, IAM, systemami pocztowymi oraz integrację z zewnętrznymi źródłami threat intelligence.
11. skonfigurowanie procesów normalizacji i parsowania danych, aby wszystkie informacje były ujednolicone i gotowe do skutecznej analizy.
12. utworzenie reguł korelacyjnych pozwalających na wykrywanie zaawansowanych scenariuszy ataków i nietypowych aktywności w środowisku.
13. przygotowanie spersonalizowanych dashboardów i raportów, które umożliwią zespołowi SOC szybkie monitorowanie stanu bezpieczeństwa.
14. zdefiniowanie przypadków użycia wraz z ich mapowaniem do standardów takich jak MITRE ATT&CK lub NIST w celu ujednolicenia monitoringu zagrożeń.
15. zrealizowanie integracji XDR z narzędziami zabezpieczeń, systemami ticketowymi, platformami skanowania i urządzeniami sieciowymi w celu umożliwienia automatycznych reakcji.
16. opracowanie i wdrożenie reakcji na incydenty, obejmujących zarówno działania automatyczne, jak i półautomatyczne.

17. przeniesienie (odtworzenie) ustawień z obecnie wykorzystywanego rozwiązania EDR w zakresie migracji polityk (antywirusowych, wykluczeń, polityk zapory ogniowej, polityk kontroli aplikacji).
18. konfigurację i implementację polityk bezpieczeństwa, reguł oraz raportów, optymalizację pod kątem wydajności oraz minimalizację liczby fałszywych alarmów zgodnie z najlepszymi praktykami oraz wytycznymi Zamawiającego.
19. wdrożenie konfiguracji inicjalnej dla min. 5 playbooków w module SOAR.
20. wykonanie testów wydajności, bezpieczeństwa oraz procedur odtwarzania po awarii w celu potwierdzenia gotowości systemów do pracy w środowisku produkcyjnym.
21. wykonanie testów akceptacyjnych (niezawodnościowe oraz funkcjonalne) oraz opracowanie i przedstawienie Raportu w dokumentacji powykonawczej.
22. Wykonawca przeprowadzi instruktaż dla administratorów wskazanych przez Zamawiającego:
    a) Instruktaż zostanie przeprowadzony w terminie uzgodnionym z Zamawiającym (jednak nie później niż 10 dni od daty wdrożenia), w jego siedzibie, tj. Plac Trzech Krzyży 3/5, 00-507 Warszawa lub w formie zdalnej.
    b) Instruktaż powinien obejmować:
        - omówienie dostarczonego oprogramowania (parametry, funkcjonalności),
        - omówienie przeprowadzonych prac instalacyjno-konfiguracyjnych,
        - omówienie i weryfikację przygotowanych i dostarczonych procedur,
        - omówienie scenariuszy w przypadku wystąpienia błędów/awarii
23. Wdrożenie musi odzwierciedlać odwzorowanie struktury organizacji MRIT:
    a) Każdy komputer/serwer musi być przypisany do określonej jednostki organizacyjnej zgodnie ze strukturą AD.
    b) Wskazana grupa administratorów globalnych musi mieć możliwość nadzoru nad wszystkimi urządzeniami, na których jest zainstalowane oprogramowania Systemu XDR
    c) Użytkownik (administartor) musi mieć przypisane odpowiednie uprawnienia w kontekście danej organizacji.
24. Konfigurację i implementację polityk bezpieczeństwa, reguł oraz raportów, optymalizację pod kątem wydajności oraz minimalizacji liczby fałszywych alarmów zgodnie z najlepszymi praktykami oraz wytycznymi Zamawiającego.

IX. MINIMALNE WYMAGANIA W ZAKRESIE ASYSTY TECHNICZNEJ

1. Wykonawca przez cały okres trwania umowy zobowiązany będzie do świadczenia usługi asysty technicznej na każde żądanie Zamawiającego, tj. każdorazowo na podstawie pisemnego zlecenia asysty technicznej, wystawianego przez Zamawiającego.
2. Zakres, sposób oraz termin realizacji zostanie uzgodniony na etapie przedstawienia wymagań przez Zamawiającego i wyceny pracochłonności przez Wykonawcę, poprzedzających zlecenie.
3. Zlecenia będą obejmować w szczególności:
    a) Zapewnienie Zamawiającemu pomocy w rozwiązaniu problemów i incydentów wynikłych w trakcie obsługi dostarczonego systemu XDR tj.:
        - analiza problemów zgłaszanych przez Zamawiającego;
        - asysta przy określaniu i usuwaniu przyczyn oraz skutków zgłaszanych incydentów;
        - dostarczanie, instalacja (po uzyskaniu zgody Zamawiającego) i konfiguracja uaktualnień i nowych wersji oprogramowania lub jego komponentów, oraz związana z tym aktualizacja dostarczonej dokumentacji;
        - przeprowadzanie analiz oraz udzielanie konsultacji Zamawiającemu;
        - dokonywanie zmian konfiguracji oprogramowania;
        - opracowywanie i dostarczanie dokumentacji, w tym aktualizacji dokumentacji oraz dostarczanie dokumentacji wprowadzanych zmian;
        - implementację nowych funkcjonalności lub modyfikację już skonfigurowanych.

b) Wsparcie w przypadku wystąpienia incydentu bezpieczeństwa:
   - wsparcie w zakresie wykonania analizy wykorzystanych podatności;
   - kontakt z ekspertem w zakresie bezpieczeństwa dostarczonego systemu;
   - analizę zakresu kompromitacji systemu;
   - wsparcie w konfiguracji/rekomendacji w celu zabezpieczenia systemu;
   - wsparcie w zakresie usunięcia skutków oraz rozwiązania incydentu bezpieczeństwa;

c) Wsparcie w planowanych pracach serwisowych:
   - Przeprowadzenia standardowych prac serwisowych,
   - Przeprowadzania aktualizacji komponentów systemu,
   - Weryfikacji poprawności konfiguracji,
   - Wsparcia w okresie podwyższonej czujności (np. monitoring środowiska w czasie biznesowo krytycznych wydarzeń).

d) Wsparcie on-site w przypadku braku możliwości rozwiązania problemu zdalnie.
e) Usługi asysty technicznej muszą być realizowane przez inżyniera posiadającego Certyfikat z oficjalnej ścieżki producenta dostarczonego systemu na poziomie eksperckim.

4. Usługi asysty technicznej Wykonawca zobowiązuje się realizować w dwóch formach:

   a) w siedzibie Zamawiającego przez pracowników Wykonawcy na podstawie pisemnego zlecenia Zamawiającego określającego zakres oraz termin wykonania tych usług, uzgodnionych wcześniej z Wykonawcą. Usługi te będą świadczone, przez liczbę godzin wskazanych w zleceniu,
   b) zdalnie przez pracowników Wykonawcy na podstawie pisemnego zlecenia Zamawiającego określającego zakres oraz termin wykonania tych usług, uzgodnionych wcześniej z Wykonawcą. Usługi te będą świadczone, przez określoną liczbę godzin w danym dniu. Wykonawca udostępni narzędzie umożliwiające zdalną komunikację, które w uzgodnieniu z Zamawiającym zostanie uruchomione na stacji roboczej pracownika Zamawiającego.

5. Po wykonaniu usług Wykonawca przedłoży Zamawiającemu protokół z wykonania usług asysty zawierający ich rodzaj, zakres oraz termin.
6. Maksymalna liczba roboczogodzin w trakcie trwania umowy wynosi 200.
7. Zamawiający zastrzega sobie prawo do nie udzielania zleceń na usługi asysty technicznej.
8. Proces realizacji asysty technicznej będzie przebiegał następująco:

   a) Zamawiający przekaże Wykonawcy drogą mailową zlecenie wykonania asysty technicznej. Zgłoszenie zawierać będzie co najmniej:
      - zakres prac do wykonania lub opis problemu do rozwiązania,
      - określenie proponowanego terminu realizacji (opcjonalnie).

   b) W terminie nie dłuższym niż 3 dni robocze od dnia otrzymania zgłoszenia o asystę techniczną Wykonawca skontaktuje się z Zamawiającym w celu ustalenia szczegółowego zakresu prac, terminu realizacji i szacowanego wymiaru godzin realizacji asysty technicznej.