Opis Przedmiotu Zamówienia

1. **Przedmiot zamówienia**
2. Przedmiotem zamówienia jest:
3. wdrożenie Systemu klasy XDR (Extended\Endpoint Detection and Response – zaawansowanie oprogramowanie ochrony stacji roboczych przed zagrożeniami cyberbezpieczeństwa posiadające m.in. funkcjonalność ochrony antywirusowej, możliwość gromadzenia informacji o zdarzeniach oraz rozbudowane funkcje reakcji na incydenty).
   1. umożliwiającego zapewnienie:
      1. aktywnej ochrony stacji końcowych i serwerów przed działaniem złośliwego oprogramowania i innych zaawansowanych cyberzagrożeń,
      2. detekcji zagrożeń, identyfikacji działań cyberprzestępców oraz zdarzeń z kategorii APT (Advanced Persistent Threats),
      3. aktywnej reakcji i odpowiedzi na wykryte zdarzenie oraz incydenty
      4. realizacji działań proaktywnych w tym to aktywnego wyszukiwania intruzów w infrastrukturze informatycznej,
   2. dostawa licencji dla 90 tysięcy stacji roboczych i serwerów,
   3. zakup usługi wsparcia dla rozwiązania XDR na okres 36 miesięcy,
   4. organizacja i realizacja warsztatów dla wskazanych przez Zamawiającego pracowników
   5. dostawa usług konsultingowych z obszaru monitorowania, analizy i reagowania na incydenty w ramach wdrożonego Systemu klasy XDR w wysokości 2000 godzin,
4. **Wymagania ogólne**
5. W ramach przedmiotu zamówienia Wykonawca MUSI w szczególności: 
   1. dostarczyć, wdrożyć, uruchomić i skonfigurować System;
   2. wykonać Dokumentację wdrożeniową i powdrożeniową,
   3. wykonać transfer wiedzy dla osób wskazanych przez Odbiorcę dla maksymalnie 15 osób z zakresu funkcjonowania dostarczonego Systemu i działań utrzymaniowych i rozwojowych w obszarze administrowania nim,
   4. udzielić lub zapewnić udzielenie wszelkich licencji wymaganych do prawidłowego działania Systemu, jako całości jak i poszczególnych jego elementów dla 90 tysięcy użytkowników w rozproszonej infrastrukturze informatycznej Zamawiającego. Licencjobiorcą jest Odbiorca, a podmiotami uprawnionymi do korzystania z Systemu są Jednostki.
   5. przenieść na Odbiorcę autorskie prawa majątkowe do Dokumentacji opracowanej przez Wykonawcę w ramach Umowy.
   6. udzielić Odbiorcy Gwarancji na dostarczony w ramach Umowy System, w tym gwarancji na Oprogramowanie, na okres 36 miesięcy od podpisania Protokołu Odbioru Dostawy Systemu oraz świadczyć w tym okresie usługi gwarancyjne w zakresie wdrożonego Systemu, w ramach wynagrodzenia wynikającego z Umowy.
   7. przeprowadzić warsztaty szkoleniowe związane z oferowanym rozwiązaniem (Systemem) w zakresie i na warunkach opisanych w Rozdziale VIII niniejszego dokumentu.
   8. zapewnić usługi asysty technicznej w języku polskim w maksymalnej ilości 2000 godzin w okresie obowiązywania umowy.
6. Wymagane jest, aby Odbiorca przekazał wszystkie niezbędne zasoby informatyczne potrzebne do wdrożenia elementów Systemu. Zakres integracji wdrażanego Systemu z Systemami Odbiorcy polegać będzie co najmniej na przekazaniu przez Wykonawcę wymaganych do prawidłowego działania Systemu informacji o koniecznych zmianach w konfiguracji Systemów Odbiorcy w postaci instrukcji, opisu konfiguracji itp.
7. W ramach wdrożenia Systemu wymaga się od Wykonawcy dostawy, instalacji i konfiguracji Systemu, zgodnie z zaakceptowanym przez Zespół Zamawiającego Projektem Wdrożenia Systemu.
8. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy, w zakresie Dokumentacji Projektowej, będzie podpisany bez zastrzeżeń Protokół Odbioru Projektu zawierający co najmniej: odbiór Dokumentacji Projektowej tj. Projektu Wdrożenia Systemu, Dokumentacji Testów akceptacyjnych.
9. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy w zakresie uruchomienia i skonfigurowania Systemu MUSI być podpisany bez zastrzeżeń Protokół Odbioru Wdrożenia Systemu zawierający co najmniej:
   1. odbiór Systemu w infrastrukturze Zamawiającego,
   2. odbiór Dokumentacji Powykonawczej,
   3. odbiór realizacji transferu wiedzy.
10. **Wymagania techniczne dotyczące oferowanego rozwiązania**
11. System MUSI być dostarczony w formie SaaS (Software as a Service), Producent Systemu MUSI posiadać certyfikację minimum SOC 2 type 2 (procedura audytowa, której efektem jest raport szczegółowo opisujący w jaki sposób dostawca usług zarządza powierzonymi mu danymi. W skład SOC 2 wchodzą dwa raporty: Type 1 – opisuje System zarządzania bezpieczeństwem informacji i ocenia jego adekwatność w kontekście punktów kontrolnych standardu. Type 2 – ocenia czy System zarządzania bezpieczeństwem informacji faktycznie funkcjonuje) oraz gwarantować dostępność usługi w ramach SLA (Service Level Agreement ) co najmniej na poziomie minimum 99,9%.
12. Dokumentacja Systemu POWINNA być opublikowana przez producenta na jego stronie internetowej co najmniej w języku angielskim.
13. System MUSI obsłużyć co najmniej 90000 hostów, z licencją pozwalającą na instalacje na dowolnym typie maszyny, w tym:
    1. stacje robocze typu windows
    2. stacje robocze typu macOS
    3. serwery typu Linux
    4. serwery typu Microsoft Server
    5. urządzenia mobilne typu Android
    6. urządzenia mobilne typu IOS
14. System MUSI przechowywać informacje o alarmach i incydentach minimum przez okres 180 dni, ale także powinien umożliwiać jego dowolne wydłużenie poprzez standardową zmianę w konfiguracji z poziomu konsoli Systemu, w zależności od posiadanej licencji.
15. System MUSI przechowywać szczegółowe dane telemetryczne z wszystkich zabezpieczonych agentem systemów przez co najmniej 30 dni.
16. System MUSI szyfrować dane w trakcie transmisji i w trakcie przechowywania za pomocą protokołów i algorytmów kryptograficznych uznanych za powszechnie 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 ze stron trzecich .
17. Cały system, wraz z gromadzonymi danymi analitycznymi musi być szyfrowany kluczami szyfrującymi wygenerowanymi i zarządzanymi przez zamawiającego i w taki sposób, aby była możliwość w każdej chwili odwołania bądź zmiany użytych kluczy szyfrujących.
18. System musi być skwalifikowany przez niezależne instytucje badające rynek rozwiązań EDR/XDR przynajmniej w jednym z:
    1. System wg ewaluacji MITRE Engenuity: Mitre Attack z 2022 (https://attackevals.mitre-engenuity.org/enterprise/wizard-spider-sandworm/) MUSI posiadać skuteczność na poziomie minimum 95% w następujących kategoriach:
       1. widoczności zagrożeń (sekcja Visibility)
       2. analityki zagrożeń (sekcja Analytics Coverage)
    2. System MUSI być sklasyfikowany przynajmniej jako „Strong Performers” dla raportu Forrester Wave For EDR Providers Q2 2022.
    3. System MUSI być sklasyfikowany przynajmniej jako „Leader” dla raportu 2022 Gartner Magic Quadrant for Endpoint Protection Platforms
19. System MUSI umożliwiać zarządzanie przez pojedynczy interfejs z wykorzystaniem graficznej przeglądarki internetowej oraz przez API. Oba dostępne po https (co najmniej z uwzględnieniem TLS 1.2).
    1. Zamawiający nie dopuszcza, aby webowy interfejs graficzny korzystał z technologii flash, silverlight lub java.
20. Wszystkie składniki Systemu MUSZĄ być konfigurowalne i zarządzane przez jeden spójny interfejs. Nie dopuszcza się, aby składniki Systemu posiadały oddzielne pulpity/konsole do zarządzania konkretnymi funkcjami bezpieczeństwa, a dostęp do nich realizowany jest przez pojedyncze logowanie (Single Sign-On).
21. 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
22. System MUSI posiadać możliwość ograniczenia logowania do Systemu tylko ze wskazanych publicznych adresów IP.
23. System MUSI umożliwiać integrację z zewnętrznym katalogiem użytkowników (ze wsparciem dla ADFS) oraz posiadać możliwość definiowania lokalnych użytkowników, których logowanie jest zabezpieczone hasłem oraz dodatkowym czynnikiem uwierzytelniającym.
    1. System jako dodatkową metodę uwierzytelnienia MUSI wspierać co najmniej tokeny w formie jednorazowych kodów generowanych w aplikacji mobilnej wg. algorytmu Time-based One-Time Password algorithm (ang. TOTP-based) lub wykorzystywać klucze fizyczne działające według standardu FIDO2.
    2. Zamawiający dopuszcza zastosowanie Google Authenticator lub Microsoft Authenticator na platformy Android i iOS dla aplikacji mobilnej służącej jako dodatkowa metoda uwierzytelnienia.
24. System podczas tworzenia haseł dla lokalnych kont administracyjnych MUSI uwzględniać założenia polityki, która wymaga ustawienie hasła spełniającego o następujących kryteriach:
    1. co najmniej 14 znaków, MUSI zawierać małe i duże litery łacińskie, cyfry i znaki specjalne.
25. System MUSI umożliwiać przypisywanie użytkowników do grup użytkowników.
26. Każdy użytkownik Systemu (administrator, operator, analityk) MUSZĄ posiadać indywidualne konta pozwalające na jego jednoznaczną identyfikację i rozliczalność.
27. 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).
28. System w ramach roli MUSI umożliwiać określenie dostępu do co najmniej następujących obszarów Systemu:
    1. Ustawienia Systemu
    2. Zarządzanie hostami
    3. Zarządzanie politykami
    4. Zarządzanie regułami detekcyjnymi
    5. Zarządzania wykluczeniami
    6. Zarządzanie incydentami
    7. Uruchamianie odpowiedzi na incydent
    8. Nawiązywanie połączenia do linii poleceń
    9. Uruchamianie co najmniej skryptów python lub powershell
    10. Zarządzanie kwerendami do danych
    11. Zarządzanie raportami
    12. Zarządzenie dashboardami/kokpitami
29. System musi umożliwiać pracę w trybie multi-tenant (środowisko wielu podmiotów).
30. Środowisko multi-tenant musi umożliwiać utworzenie wydzielonych od siebie instancji gdzie dostęp do każdego z nich będzie limitowany odpowiednimi uprawnieniami.
31. Środowisko multi-tenant musi umożliwiać zarządzani poszczególnymi instancjami z pojedynczej konsoli zarządzania.
32. Każdy tenant musi mieć możliwość udzielenia limitowanego dostępu przynajmniej w zakresie
    1. Incydenty
    2. Alerty
    3. Tworzenie kwerend i zapytań do danych
    4. Wyświetlanie wszystkich zapytań i ich wyników
    5. Widok szczegółów zdarzeń w osi czasu
33. System MUSI posiadać możliwość definiowania własnych ról i profili.
34. System MUSI posiadać zestaw predefiniowanych dashboardów (pulpitów) informujących co najmniej:
    1. O liczbie i poziomie ważności incydentów
    2. O liczbie incydentów przypisanych do analityków
    3. O hostach z największą liczbą incydentów
    4. O liczbie agentów z rozbiciem na wersję agenta
    5. O liczbie agentów z rozbiciem na agentów offline i online
    6. O liczbie agentów z rozbiciem na wersję aktualizacji modułów bezpieczeństwa
    7. O liczbie agentów z rozbiciem na status ochrony
35. System MUSI umożliwiać definiowanie własnych dashboardów (konsol) z wykorzystaniem predefiniowanych widgetów (kontrolek) oraz kontrolek definiowanych samodzielnie poprzez kwerendy do danych telemetrycznych.
36. System MUSI umożliwiać skonfigurowanie okna czasu, po którym użytkownik zostanie automatycznie wylogowany z Systemu oraz posiadać możliwość automatycznego zawieszania kont użytkowników, którzy nie logowali się dłużej niż określona liczba dni.
37. System MUSI co najmniej przez 365 dni przechowywać logi audytowe dokumentujące wszystkie akcje podejmowane przez użytkowników zalogowanych do Systemu oraz logi audytowe dotyczące funkcjonowania agentów.
38. System MUSI posiadać możliwość eksportu wybranych logów audytowych via syslog po SSL/TLS w formacie CEF. W dokumentacji Systemu MUSI być wskazany adres IP lub zakres adresów IP, z których nawiązywane będzie połączenie do serwerów syslog.
39. System MUSI posiadać możliwość alarmowania o wskazanych zdarzeniach zapisanych w logach audytowych poprzez wysłanie korespondencji mailowej na wskazane skrzynki poczty elektronicznej.
40. System MUSI posiadać możliwość integracji z Microsoft Active Directory w zakresie synchronizacji struktury organizacyjnej katalogu AD zarówno z lokalnym AD jak również z Azure AD na potrzeby automatycznego wzbogacania informacji na temat hostów i użytkowników oraz tworzenia dynamicznych grup hostów celem różnicowania konfiguracji agentów.
41. System MUSI posiadać funkcjonalność wykrywania niezarządzanych hostów w środowisku sieciowym Zamawiającego w oparciu o wykorzystanie mechanizmów skanowania obiektów kont komputerów Active Directory.
42. System po integracji z Active Directory, MUSI mieć możliwość wyświetlenia widoku wszystkich komputerów obsługiwanych przez Active Directory Zamawiającego z możliwością ich filtrowania per dana jednostka (Organization Unit -OU).
43. System MUSI posiadać możliwość określenia strefy czasowej wykorzystywanej do reprezentowania znaczników czasowych w interfejsie zarządzania oraz formatu tego znacznika co najmniej w takim zakresie, aby uwidaczniał on strefę czasową.
44. System MUSI posiadać możliwość instalacji oprogramowania agenta co najmniej dla następujących Systemów operacyjnych i środowisk:
    1. Windows 7, 8, 10 i 11 (włącznie ze środowiskiem Persistent oraz Non-Persistent VDI)
    2. Windows Server 2012 R2, 2016 standard i core, 2019 standard i core oraz 2022,
    3. Linux
       1. Red Hat Enterprise Linux 7, 8 i 9
       2. SUSE Linux Enterprise Server 11, 12 i 15
       3. Ubuntu 18.04 LTS, 20.04 LTS i 22.04 LTS
       4. Oracle Linux 6 i 7
       5. CentOS 6,7 i 8
       6. Debian 9, 10 i 11
    4. macOS 11.x, 12.x i 13.x
    5. środowisko klastrów Kubernetes
    6. Android 10,11 i 12
    7. iOS 15.x i 16.x
45. System MUSI umożliwiać wygenerowanie i pobranie pakietu instalacyjnego:
    1. W formacie msi dla Systemów Windows
    2. W formacie rpm, deb i sh dla Systemów Linux
    3. W formacie dpkg dla Systemów macOS
    4. W formacie helm dla klastrów kubernetes
46. System powinien umożliwiać uruchomienie lokalnego komponentu pośredniczącego dla danych przez który agenci zainstalowani na hostach będą się komunikować do konsoli Systemu bez konieczności nawiązywania komunikacji bezpośredniej z Systemem.
47. Pakiet instalacyjny agenta dla Systemów Windows, macOS, Linux i klastrów Kubernetes MUSI posiadać możliwość:
    1. Przypisanie do hosta nieusuwalnego znacznika (w procesie instalacji agenta) , który może być wykorzystany do tworzenia dynamicznych grup hostów i określenia zakresu dostępu jaki posiada rola użytkownika
    2. Skonfigurowania komponentu pośredniczącego w komunikacji z Systemem
48. Instalacja agenta i jego aktywacja w Systemie nie może wymagać restartu Systemu operacyjnego.
49. Komunikacja pomiędzy agentem a Systemem MUSI być zabezpieczona z wykorzystaniem protokołu https (co najmniej TLS 1.2) i w zależności od konfiguracji MUSI być realizowana w sposób bezpośredni lub pośredni via dedykowany komponent pośredniczący tego samego producenta, który:
    1. MUSI umożliwiać uruchomienie w formie maszyny wirtualnej
    2. MUSI obsługiwać funkcję proxy chaining dla http z uwierzytelnieniem
    3. MUSI umożliwiać cache’owanie (buforowanie) aktualizacji oprogramowania agenta i aktualizacji komponentów bezpieczeństwa agenta
50. Komunikacja pomiędzy komponentem pośredniczącym a Systemem MUSI być zabezpieczona z wykorzystaniem protokołu https (co najmniej TLS 1.2). Komponent pośredniczący MUSI posiadać możliwość manualnej lub automatycznej aktualizacji. System MUSI umożliwiać centralne zarządzanie ustawieniami komponentu pośredniczącego.
51. Dla rozwiązania SaaS (Software as a Service) w dokumentacji Systemu MUSZĄ być wskazane publiczne adresy IP oraz adresy URL niezbędne do zapewnienia poprawnej komunikacji między agentami i Systemem oraz pomiędzy komponentem pośredniczącym a Systemem. Komunikacja MUSI być zawsze nawiązywana w kierunku od agenta/komponentu pośredniczącego do Systemu.
52. System MUSI posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup hostów. Polityka automatycznej konfiguracji agenta MUSI umożliwiać określenie:
    1. Dnia tygodnia i zakresu czasu, w którym wykonywana jest aktualizacja
    2. Maksymalnej liczby równolegle aktualizowanych agentów
    3. Możliwość zdefiniowania zakresu: tylko aktualizacje naprawcze, tylko aktualizacje naprawcze w ramach wskazanej nowej wersji , najnowsza wersja, najnowsza przedostatnia wersja
    4. Opóźnienie aktualizacji o wskazaną liczbę dni od publikacji nowej wersji
    5. Globalnego limitu na wykorzystanie pasma przy bezpośrednim pobieraniu z Systemu
    6. Źródła: bezpośrednio z Systemu, z komponentu pośredniczącego, peer-to-peer pomiędzy agentami
53. System MUSI umożliwiać odnotowanie w logach Systemu w przypadku, gdy:
    1. Moduły bezpieczeństwa agenta nie będą funkcjonowały poprawnie
    2. Agent zostanie odinstalowany
54. System MUSI umożliwiać różnicowanie konfiguracji agenta i modułów bezpieczeństwa poprzez przypisanie różnych profili konfiguracyjnych do wybranych grup hostów lub pojedynczych hostów.
55. System MUSI umożliwiać przetwarzanie i przechowywanie danych telemetrycznych i alarmów z urządzeń firewall co najmniej znaczących producentów takich jak: Check Point, Fortinet, Cisco i Palo Alto Networks.
56. System MUSI umożliwiać przetwarzanie i przechowywanie danych telemetrycznych co najmniej z następujących Systemów: Microsoft Office 365, Azure Event Hub.
57. System MUSI umożliwiać przetwarzanie i przechowywanie danych telemetrycznych w formacie NetFlow v9 i IPFIX.
58. System MUSI umożliwiać przetwarzanie i przechowywanie danych telemetrycznych przesyłanych przez syslog w formacie CEF i LEEF a w przypadku nieustrukturyzowanych danych umożliwiać ich analizę i mapowanie.
59. System MUSI umożliwiać przetwarzanie i przechowywanie danych telemetrycznych przesyłanych w ramach mechanizmu Windows Event Forwarding.
60. Wszystkie dane telemetryczne (pochodzące zarówno od agentów jak i rozwiązań trzecich) MUSZĄ być przechowywane przez System w centralnym i umożliwiającym wyszukiwanie wymaganych informacji w repozytorium danych.
61. 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.
62. System MUSI umożliwiać zapisanie kwerendy do danych telemetrycznych do prywatnej biblioteki kwerend danego użytkownika lub do globalnej biblioteki kwerend dostępnej dla wszystkich innych użytkowników.
63. System MUSI umożliwiać zrealizowanie kwerendy do danych telemetrycznych i odczytanie jej wyników via API.
64. System MUSI umożliwiać eksport wyników kwerendy do danych telemetrycznych w formie pliku tekstowego.
65. System MUSI umożliwiać uruchamianie kwerendy cyklicznie zgodnie z podanym harmonogramem lub jeden raz o określonym czasie.
66. System MUSI umożliwiać wizualizację wyników kwerendy do danych telemetrycznych w formie tabelarycznej i w formie wykresu: liniowego, słupkowego i kołowego.
67. System MUSI umożliwiać wykorzystanie wyników kwerendy do tworzenia periodycznie generowanych raportów.
68. System MUSI umożliwiać wykorzystanie wyników kwerend do wizualizacji danych w konsoli.
69. System MUSI umożliwiać przekształcenie kwerendy do danych telemetrycznych w uruchamianą zgodnie z zadanym harmonogramem regułę korelacyjną generującą alarmy, jeśli kwerenda zwróciła jakiekolwiek rekordy.
70. System MUSI umożliwiać definiowanie pojedynczych wskaźników kompromitacji w formie: SHA256, nazwy domenowej, adresu IPv4, adresu IPv6, ścieżki, nazwy pliku. MUSI istnieć możliwość dodania znacznika ręcznie, zaimportowania znaczników z pliku i via API oraz oznaczenia reputacji, wiarygodności i okresu wygaśnięcia znacznika.
71. 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).
72. System dla każdego wprowadzonego pojedynczego i złożonego wskaźnika kompromitacji MUSI wygenerować alarm(-y):
    1. jeśli znacznik został odszukany w historycznych danych telemetrycznych (zgromadzonych przed dodaniem wskaźnika)
    2. jeśli znacznik zostanie odszukany w nowych danych telemetrycznych
73. System MUSI umożliwiać przekształcanie złożonych wskaźników kompromitacji w warunki reguł prewencyjnych co najmniej dla agenta dla Windows, macOS i Linux.
74. System MUSI umożliwiać bezpośrednią integrację z usługą VirusTotal.
75. System MUSI umożliwiać globalne blokowanie uruchamiania/ładowania plików binarnych z wykorzystaniem funkcji skrótu SHA256.
76. System w ramach odpowiedzi na incydent MUSI umożliwiać:
    1. Reakcje (remediację) ze wskazaniem kroków, które mogą być podjęte automatycznie i kroków, które należy zrealizować manualnie. MUSI istnieć możliwość wyboru kroków reakcji na incydent (remediacyjnych), które zostaną wykonane automatycznie.
    2. Uruchomienie co najmniej skryptu python lub powershell na hoście.
    3. Nawiązanie interaktywnego połączenia do linii poleceń na hoście.
    4. Wstrzymanie procesu na hoście.
    5. Wyłączenie procesu na hoście.
    6. Izolację sieciową hosta.
    7. Dodanie adresu IP do listy publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi Systemami bezpieczeństwa.
    8. Dodanie nazwy domenowej do publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi Systemami bezpieczeństwa.
    9. Zmianę w rejestrze (tylko Systemy Windows).
    10. Usunięcie pliku na hoście.
    11. Przeniesienie pliku na hoście do kwarantanny.
    12. Wyszukanie pliku na innych hostach.
    13. Zrzucenie pamięci procesu dla hosta.
77. System MUSI posiadać mechanizm wykrywania anomalii w ruchu sieciowym i w zachowaniu użytkownika i procesów.
78. System MUSI obsługiwać co najmniej następujące typy ważności alertów: informacyjny, niski, średni, wysoki i krytyczny.
79. System MUSI automatycznie grupować powiązane alerty w celu przyspieszenia i ułatwienia triażu i analizy incydentu.
80. W ramach incydentu System MUSI umożliwiać grupowanie:
    1. powiązanych z incydentem użytkowników
    2. Hostów
    3. Plików
    4. Domen
    5. Adresów IP
81. 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, tak aby analityk mógł w łatwy sposób przeanalizować wykorzystywane techniki, określić zakres ataku, ustalić potencjalny cel ataku i zweryfikować, czy cel został osiągnięty.
82. System MUSI umożliwiać wgląd w raport z modułu sandboxa dla plików powiązanych z incydentem i eksport raportu.
83. System MUSI umożliwiać zarządzanie incydentami co najmniej w następującym zakresie:
    1. Przypisanie incydentu do analityka
    2. Zmianę stanu incydentu: badany, false positive, true positive, duplikat, testy
    3. Dodawanie notatek
    4. Komunikacja z innymi analitykami
    5. Raportowanie czasu MTTR
84. System MUSI mapować alerty do matrycy taktyk, technik i procedur w ramach framewarku (metodyki) MITRE ATT&CK bezpośrednio w konsoli alertu.
85. Zamawiający nie dopuszcza, aby agent wykorzystywał komponenty Oracle Java JRE/JDK.
86. Agent dla Systemów operacyjnych z rodziny Windows:
    1. MUSI posiadać możliwość pobierania aktualizacji agenta i aktualizacji modułów bezpieczeństwa:
       1. Bezpośrednio z Systemu
       2. Od innych hostów w tej samej podsieci (peer-to-peer)
    2. MUSI posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Wyłączenie modułów bezpieczeństwa i odinstalowanie agenta MUSI wymagać podania hasła, które może być skonfigurowane per grupa hostów lub indywidualnie dla danego hosta po stronie Systemu. Nie dopuszcza się rozwiązań, w których hasło jest statyczne i podawane w trakcie uruchamiania instalatora. Operacja deinstalacji agenta i wyłączenia modułów bezpieczeństwa MUSI zostać zapisana w dzienniku audytowym Systemu.
    3. MUSI umożliwiać:
       1. Ukrycie ikony agenta w zasobniku Systemowym
       2. Wyłączenie powiadomień o zablokowanych zagrożeniach
       3. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej
       4. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego
       5. Użycie komunikatów i powiadomień w języku Polskim
       6. Zarządzanie host firewallem hosta z wykorzystaniem Windows Filtering Platform
       7. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu
       8. Weryfikację stanu szyfrowania dysków
       9. Wyszukiwanie plików po skrócie SHA256 i po ścieżce włączając w to pliki, które zostały usunięte
       10. Usuwanie plików po SHA256 i po wskazaniu ścieżki do pliku
    4. MUSI posiadać możliwość wykonywania periodycznego skanowania hosta w zakresie zainstalowanych aplikacji, automatycznie uruchamiających się aplikacji, dysków, użytkowników, grup użytkowników i przypisania użytkowników do grup oraz zestawienia tych danych z wynikami poprzednich skanów.
    5. Powinien posiadać wbudowany moduł obsługujący skrypty python w wersji 3.7 lub nowszy i możliwość uruchamiania wbudowanych i własnych skryptów python.
    6. MUSI posiadać możliwość wyszukania plików we wskazanej ścieżce przy pomocy reguł yara.
    7. W ramach działań zabezpieczenia dowodu cyfrowego MUSI posiadać możliwość zrzucenia pamięci wskazanego procesu.
    8. MUSI integrować się z Windows Security Center.
    9. MUSI posiadać możliwość blokowania uruchamiania programów z zewnętrznej pamięci masowej podłączonej na porcie USB i z napędów optycznych.
    10. MUSI posiadać możliwość blokowania uruchamiania programów ze wskazanych lokalizacji w Systemie plików.
    11. MUSI posiadać możliwość blokowania uruchamiania programów z zasobów sieciowych poza wybranymi ścieżkami.
    12. Do kolekcji danych telemetrycznych MUSI używać sterownika (działać w jądrze Systemu operacyjnego).
    13. W ramach działań zabezpieczenia dowodu cyfrowego MUSI posiadać możliwość zrzucenia pamięci Systemu operacyjnego
    14. W ramach działań zabezpieczenia dowodu cyfrowego MUSI posiadać możliwość zebrania historii przeglądarek internetowych
    15. W ramach działań zabezpieczenia dowodu cyfrowego MUSI posiadać możliwość wglądu w tablicę MFT (Master File Table) Systemu plików
    16. MUSI wykonywać monitoring wywołań API Systemu operacyjnego (tzw. syscall hooking) w trybie kernela, aby uniemożliwić usunięcie hooków z poziomu programów działających w trybie użytkownika. Co najmniej następujące wywołania API Systemu operacyjnego muszą być monitorowane:
        1. NtLoadDriver
        2. NtReadVirtualMemory
        3. NtAllocateVirtualMemory i NtAllocateVirtualMemoryEx
        4. NtWriteVirtualMemory
        5. NtQuerySystemInformation
        6. NtOpenCreateFile
        7. NtUserSetWindowsHookEx
        8. RegNtPreSetValueKey
        9. RegNtPreCreateKey
        10. RegNtPreDeleteKey
    17. MUSI zbierać co najmniej następujące dane telemetryczne:
        1. Utworzenie nowego procesu i zakończenie procesu
        2. Wszystkie operacje na plikach: tworzenie, zapisywanie, kasowanie, zmiana nazwy, przesunięcie, modyfikacja, link symboliczny
        3. Ładowanie bibliotek DLL
        4. Wstrzykiwanie kodu do procesu
        5. Wszystkie operacje na socketach sieciowych dla TCP i UDP: accept, connect, create, listen, close, bind
        6. Statystyki połączeń sieciowych
        7. Praca z rejestrem: skasowanie wartości, ustawienie wartości, utworzenie klucza, kasowanie klucza, zmiana nazwy klucza
        8. Wywołania RPC
        9. Windows Event Log:
           1. Security:
              1. Np. Successful logon (4624), Failed logon (4625), Special privileges attempted login (4672), Kerberos TGT request (4768), Kerberos service ticket requested (4769), Kerberos service ticket renewal (4770), Kerberos pre-authentication failed (4771), Domain controller validation attempt (4776), Session was reconnected to a Windows station (4778), A user account was created (4720), A user account was enabled (4722), An attempt was made to change an account's password (4723), An attempt was made to reset an account’s password (4724), A user account was deleted (4726), Group member additions (4728, 4732, 4756), NTLM authentication failed (4822, 4823), Kerberos pre-authentication failed (4824), User denied access to Remote Desktop (4825),
           2. Microsoft-Windows-DNS-Client/Operational: DNS Query Completed (3008) without local machine name resolution events and without empty name resolution events
           3. Microsoft-Windows-PowerShell/Operational: PowerShell executes block activity (4103), Remote Command (4104), Start Command (4105)
    18. MUSI wysyłać zgromadzone dane telemetryczne do Systemu nie rzadziej niż co 5 minut, przy czym wymagane jest, aby agent posiadał możliwość wymuszenia wysłania danych telemetrycznych na żądanie. Jeśli z powodu braku łączności sieciowej agent nie może wysłać danych telemetrycznych, to dane telemetryczne muszą zostać lokalnie przechowane i wysłane do Systemu po przywróceniu łączności sieciowej.
    19. MUSI zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika exploitacji.
    20. MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi umożliwiając skonfigurowanie co najmniej następujących mechanizmów:
        1. Weryfikacja sha256 w bazie threat intelligence producenta Systemu
        2. Analiza dynamiczna w sandboxie chmurowym lub lokalnym producenta Systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym hoscie)
        3. Lokalna analiza statyczna
        4. Weryfikacja podpisu pliku binarnego
        5. Przeniesienie pliku binarnego do kwarantanny
        6. Zablokowanie uruchomienia/załadowania złośliwego pliku binarnego
        7. Zablokowanie uruchomienia pliku z przenośnej pamięci masowej USB
        8. Zablokowanie uruchomienia pliku z innych lokalizacji sieciowych niż wskazane
        9. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego
        10. Wykrywanie shellcodu’u ładowanego do pamięci
        11. Wykrycie i przerwanie próby szyfrowania plików na dysku (ochrona przeciw ransomware).
    21. MUSI wykrywać i blokować próbę wyłączenia Volume Shadow Copy Service (VSS).
    22. MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami co najmniej w plikach Microsoft Word i Microsoft Excel umożliwiając skonfigurowanie co najmniej następujące mechanizmy:
        1. Weryfikacja sha256 w bazie threat intelligence producenta Systemu
        2. Analiza dynamiczna w sandboxie chmurowym lub lokalnym producenta Systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym host)
        3. Lokalna analiza statyczna
    23. MUSI zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia Systemowe w podejrzany sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie taktyk, technik i procedur stosowanych przez cyberprzestępców.
    24. MUSI umożliwiać zablokowanie całego ruchu sieciowego (izolacji sieciowej) poza połączeniem do Systemu.
    25. MUSI posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z Systemem. Wyłączenie izolacji sieciowej MUSI być zabezpieczone hasłem. Każdy host MUSI posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło MUSI być automatycznie rotowane przez System nie rzadziej niż co dwa tygodnie.
87. Agent dla Systemów operacyjnych z rodziny macOS:
    1. MUSI posiadać możliwość pobierania aktualizacji agenta i aktualizacji modułów bezpieczeństwa:
       1. Bezpośrednio z Systemu
       2. Od innych hostów w tej samej podsieci (peer-to-peer)
    2. MUSI posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Wyłączenie modułów bezpieczeństwa i odinstalowanie agenta MUSI wymagać podania hasła, które może być skonfigurowane per grupa hostów lub indywidualnie dla danego hosta po stronie Systemu. Nie dopuszcza się rozwiązań, w których hasło jest statyczne i podawana w trakcie uruchamiania instalatora. Operacja deinstalacji agenta i wyłączenia modułów bezpieczeństwa MUSI zostać zapisana w dzienniku audytowym Systemu.
    3. MUSI umożliwiać:
       1. Ukrycie ikony agenta w zasobniku Systemowym
       2. Wyłączenie powiadomień o zablokowanych zagrożeniach
       3. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej
       4. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego
       5. Użycie komunikatów i powiadomień w języku Polskim
       6. Zarządzanie firewallem hosta
       7. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu
       8. Weryfikację stanu szyfrowania dysków
       9. Wyszukiwanie plików po skrócie SHA256 i po ścieżce włączając w to pliki, które zostały usunięte
       10. Usuwanie plików po SHA256 i po ścieżce
    4. MUSI posiadać możliwość wykonywania periodycznego skanowania hosta w zakresie zainstalowanych aplikacji, automatycznie uruchamiających się aplikacji, dysków, użytkowników, grup użytkowników i przypisania użytkowników do grup oraz zestawienia tych danych z wynikami poprzednich skanów.
    5. Powinien posiadać wbudowany moduł obsługujący skrypty python w wersji 3.7 lub nowszy i możliwość uruchamiania wbudowanych i własnych skryptów python
    6. MUSI posiadać możliwość wyszukania plików we wskazanej ścieżce przy pomocy reguł yara
    7. W ramach działań zabezpieczenia dowodu cyfrowego MUSI posiadać możliwość zrzucenia pamięci wskazanego procesu.
    8. MUSI zbierać co najmniej następujące dane telemetryczne:
       1. Utworzenie nowego procesu i zakończenie procesu,
       2. Wszystkie operacje na plikach: tworzenie, zapisywanie, kasowanie, zmiana nazwy, przesunięcie, otwarcie,
       3. Wszystkie operacje na socketach sieciowych dla TCP i UDP: accept, connect, connect failure, disconnect, listen,
       4. Statystyki połączeń sieciowych,
       5. Zdarzenia z event logu dotyczącego uwierzytelnienia.
    9. MUSI wysyłać zgromadzone dane telemetryczne do Systemu nie rzadziej niż co 5 minut, przy czym wymagane jest, aby agent posiadał możliwość wymuszenia wysłania danych telemetrycznych na żądanie. Jeśli z powodu braku łączności sieciowej agent nie może wysłać danych telemetrycznych, to dane telemetryczne muszą zostać lokalnie przechowane i wysłane do Systemu po przywróceniu łączności sieciowej.
    10. MUSI zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika eksploitacji.
    11. MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:
        1. Weryfikacja sha256 w bazie threat intelligence producenta Systemu
        2. Analiza dynamiczna w sandboxie chmurowym lub lokalnym producenta Systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym host)
        3. Lokalna analiza statyczna
        4. Weryfikacja podpisu pliku binarnego
        5. Przeniesienie pliku binarnego do kwarantanny
        6. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego
    12. MUSI zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia Systemowe w podejrzany sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie taktyk, technik i procedur stosowanych przez cyberprzestępców.
    13. MUSI umożliwiać zablokowanie całego ruchu sieciowego (izolacja sieciowa) poza połączeniem do Systemu.
    14. MUSI posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z Systemem. Wyłączenie izolacji sieciowej MUSI być zabezpieczone hasłem. Każdy host MUSI posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło MUSI być automatycznie rotowane przez System nie rzadziej niż co dwa tygodnie.
88. Agent dla Systemów operacyjnych z rodziny Linux i klastrów Kubernetes:
    1. MUSI posiadać możliwość pobierania aktualizacji agenta i aktualizacji modułów bezpieczeństwa:
       1. Bezpośrednio z Systemu
       2. Od innych hostów w tej samej podsieci (peer-to-peer)
    2. Operacja deinstalacji agenta i wyłączenia modułów bezpieczeństwa MUSI zostać zapisana w dzienniku audytowym Systemu.
    3. MUSI posiadać wsparcie dla rozszerzenia eBPF.
    4. MUSI posiadać możliwość wykonywania periodycznego skanowania hosta w zakresie zainstalowanych aplikacji, automatycznie uruchamiających się aplikacji, dysków, użytkowników, grup użytkowników i przypisania użytkowników do grup oraz zestawienia tych danych z wynikami poprzednich skanów.
    5. MUSI posiadać wbudowany moduł obsługujący skrypty python w wersji 3.7 lub nowszy i możliwość uruchamiania wbudowanych i własnych skryptów python.
    6. MUSI posiadać możliwość wyszukania plików we wskazanej ścieżce przy pomocy reguł yara.
    7. W ramach działań zabezpieczenia dowodu cyfrowego MUSI posiadać możliwość zrzucenia pamięci wskazanego procesu
    8. MUSI zbierać co najmniej następujące dane telemetryczne:
       1. Utworzenie nowego procesu i zakończenie procesu
       2. Informacje o kontenerach (co najmniej docker i containerd)
       3. Wszystkie operacje na plikach: tworzenie, otwarcie, zapisywanie, kasowanie, kopiowanie, zmiana nazwy, zmiana właściciela, zmiana atrybutów
       4. Wszystkie operacje na socketach sieciowych dla TCP i UDP: listen, accept, connect, connect failure, disconnect
       5. Zdarzenia z event logu dotyczącego uwierzytelnienia
    9. MUSI wysyłać zgromadzone dane telemetryczny do Systemu nie rzadziej niż co 5 minut, przy czym wymagane jest, aby agent posiadał możliwość wymuszenia wysłania danych telemetrycznych na żądanie. Jeśli z powodu braku łączności sieciowej agent nie może wysłać danych telemetrycznych, to dane telemetryczne muszą zostać lokalnie przechowane i wysłane do Systemu po przywróceniu łączności sieciowej.
    10. MUSI zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika eksploitacji:
    11. MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:
        1. Weryfikacja sha256 w bazie threat intelligence producenta Systemu
        2. Analiza dynamiczna w sandboxie chmurowym lub lokalnym producenta Systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym host)
        3. Lokalna analiza statyczna
        4. Przeniesienie pliku binarnego do kwarantanny
        5. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego
        6. Wykrywanie webshelli
    12. MUSI zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia Systemowe w podejrzany sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie taktyk, technik i procedur stosowanych przez cyberprzestępców.
    13. MUSI umożliwiać zablokowanie całego ruchu sieciowego (izolacji sieciowej) poza połączeniem do Systemu.
    14. MUSI posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z Systemem. Wyłączenie izolacji sieciowej MUSI być zabezpieczone hasłem. Każdy host MUSI posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło MUSI być automatycznie rotowane przez System nie rzadziej niż co dwa tygodnie.
89. Agent dla Systemów operacyjnych Android:
    1. MUSI umożliwiać automatyczną instalację via System MDM i manualną via Google Play.
    2. Operacja deinstalacji agenta MUSI zostać zapisana w dzienniku audytowym Systemu i wygenerować alarm.
    3. MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi aplikacjami wykorzystując co najmniej następujące mechanizmy:
       1. Weryfikacja sha256 w bazie threat intelligence producenta Systemu
       2. Analiza dynamiczna w sandboxie chmurowym lub lokalnym producenta Systemu
90. Agent dla Systemów operacyjnych iOS:
    1. MUSI umożliwiać automatyczną instalację via System MDM i manualną via App Store.
    2. Operacja deinstalacji agenta MUSI zostać zapisana w dzienniku audytowym Systemu i wygenerować alarm.
    3. MUSI weryfikować i raportować integralność Systemu operacyjnego (wykrywanie tzw. jail break).
    4. MUSI zapewniać ochronę przed podejrzanymi wiadomościami tekstowymi przez weryfikację linków url (ochrona przeciw smishingowa).
    5. MUSI zapewniać ochronę przed podejrzanymi połączeniami głosowymi (ochrona przeciw vishingowa).
    6. MUSI umożliwiać użytkownikowi raportowanie podejrzanych wiadomości tekstowych.
    7. MUSI mieć opcję okresowego przypominania o konieczności restartu telefonu.
91. **Wymagania w zakresie Gwarancji Systemu**
92. W ramach udzielonej Gwarancji Wykonawca udostępni oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu Zgłoszenia Serwisowego Awarii, oprogramowanie to MUSI zapewnić Odbiorcy brak ograniczeń, co do liczby dokonywanych Zgłoszeń Serwisowych w zakresie Awarii.
93. Wszelkie prace wykonywane przez Wykonawcę w Systemie nie mogą skutkować utratą praw gwarancyjnych do Systemu przez Odbiorcę.
94. W ramach udzielonej gwarancji Wykonawca będzie realizował Zgłoszenia Serwisowe Awarii Systemu w następujący sposób:

3.1. Awaria Krytyczna, wada skutkująca nieprawidłowym działaniem Systemu powodująca całkowity brak możliwości korzystania z Systemu przez co najmniej jednego użytkownika końcowego albo takie ograniczenie możliwości korzystania z niego, że przestaje on spełniać swoje podstawowe funkcje. Czas Naprawy do 12 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę;

3.2. Awaria Niekrytyczna wada skutkująca nieprawidłowym działaniem Systemu powodująca ograniczenie korzystania z Systemu, nie powodując skutków opisanych dla Awarii Krytycznej: Czas Naprawy do 72 godzin od chwili Zgłoszenia Serwisowego przez Odbiorcę.

3.3. Wszelkie Awarie będą zgłaszane przez Odbiorcę za pomocą udostępnionego przez Wykonawcę oprogramowania, o którym mowa w punkcie 1 powyżej.

3.4. W przypadku potrzeby wydania poprawki do Systemu przez Producenta, na wniosek Wykonawcy złożony w formie elektronicznej, Odbiorca może zawiesić czas usunięcia Awarii Niekrytycznych, maksymalnie na 40 dni kalendarzowych.

3.5. Obsługa Zgłoszeń Serwisowych MUSI obejmować co najmniej:

a) rozwiązywanie przez Wykonawcę zgłaszanych problemów związanych z działaniem i obsługą Systemu.

b) w ramach udzielonej gwarancji Odbiorcy przysługuje prawo do samodzielnej instalacji i używania wszystkich poprawek, usprawnień i nowych wersji Systemu udostępnianych przez Producentów elementów wchodzących w skład Systemu bez ponoszenia dodatkowych kosztów finansowych przez Odbiorcę. Powyższe nie może skutkować utratą uprawnień gwarancyjnych przysługujących Odbiorcy.

1. **Wymagania w zakresie dokumentacji**
2. W ramach projektu MUSZĄ zostać stworzone przez Wykonawcę i zaakceptowane przez Zamawiającego dokumenty obejmujące minimum wszystkie niżej wymienione zagadnienia, dotyczące wdrażanego rozwiązania:
3. przedstawienia szczegółowego opisu architektury wybranego rozwiązania,
4. przedstawienia elementów rozwiązania wykorzystanych w Projekcie,
5. projekt Wdrożenia Systemu, który musi zawierać co najmniej: opis funkcjonalny Systemu, wykaz wymaganych elementów Systemu, sposób ich wdrożenia i konfiguracji, wykaz licencji niezbędnych dla działania Systemu jako całości, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Odbiorcy,
6. szczegółowy harmonogram wdrożenia
7. wykonawca opracuje i przekaże Dokumentację Powykonawczą, która MUSI być jednym spójnym dokumentem, MUSI zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji Systemu, w tym co najmniej:
8. procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji Systemu,
9. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
10. instrukcje dla użytkowników i administratorów, w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa,
11. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione z przedstawicielem Zespołu Odbiorowego.
12. Dokumentacja MUSI być przekazana w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje Producenta mogą być przekazane w języku angielskim lub polskim.
13. **Wymagania w zakresie transferu wiedzy**
14. W ramach wdrożenia Wykonawca umożliwi Odbiorcy w siedzibie i w środowisku Odbiorcy transfer wiedzy maksymalnie 15 osób wskazanych przez Odbiorcę polegający na możliwości uczestniczenia ww. osób przy wdrażaniu, konfiguracji i administracji Systemem. Transfer wiedzy polegać będzie na:
15. zapewnieniu możliwości udziału osób wskazanych przez Odbiorcę przy przeprowadzanym przez inżyniera/inżynierów wdrożenia Systemu po stronie Wykonawcy,
16. udzielaniu odpowiedzi na pytania zadawane przez osoby wskazane przez Odbiorcę w zakresie zagadnień związanych z czynnościami administracyjnymi, analizą zdarzeń i incydentów oraz funkcjonowaniem wdrażanego Systemu w środowisku produkcyjnym Odbiorcy.
17. zapewnieniu transferu wiedzy w zakresie konfiguracji i administracji Systemu oraz działań operacyjnych w obszarze monitorowania, wykrywania i reagowania na generowane zdarzenia i incydenty w ramach Systemu, który musi być prowadzony na bieżąco w trakcie wdrożenia. Transfer wiedzy przeprowadzony zostanie w języku polskim.
18. potwierdzeniem prawidłowej realizacji transferu wiedzy będzie podpisany bez zastrzeżeń przez Zespół Projektowy Odbiorcy Protokół Odbioru Wdrożenia Systemu.
19. **Warsztaty szkoleniowe**
20. Wykonawca przeprowadzi warsztaty szkoleniowe dla administratorów i analityków, Systemu XDR zawierające:
    1. Architektura, instalacja i konfiguracja Systemu,
    2. Modyfikacja (rozbudowa) architektury Systemu,
    3. Utrzymanie i administrowanie Systemem (w tym patchowanie i podnoszenie wersji Systemu/aplikacji),
    4. Integracja Systemu z Systemami zewnętrznymi,
    5. Zarządzanie uprawnieniami użytkowników,
    6. Procedury bezpiecznej eksploatacji,
    7. Procedury odtwarzania po katastrofie i awarii,
    8. Codzienne obowiązki administracyjne,
    9. Inne istotne funkcjonalności z punktu widzenia administratora Systemu.
    10. Zarzadzanie assetami i ich poprawnym funkcjonowaniem
    11. Zarządzanie politykami i funkcjonalnościami w zakresie monitorowania, wykrywania i reagowania
    12. Tworzenie, modyfikowanie, strojenie poszczególnych konfiguracji, reguł, polityk, mechanizmów odpowiedzialnych za warstwę monitorowania, wykrywania, reagowania
    13. Obsługa poszczególnych modułów i ich konfiguracja
    14. Analiza zdarzeń i incydentów
    15. Obsługa działań w obszarze głębokiej analizy „drill down”
    16. Działania proaktywne w tym Threat Hunting
    17. Raportowanie oraz budowa przykładowych raportów
    18. Wykorzystanie API
    19. Generowanie statystyk, trendów, dashbordów
21. Każde z przeprowadzonych warsztatów powinny zostać przeprowadzone dwukrotnie, w terminach i grupach wskazanych przez Zamawiającego.
22. W zależności od planowanej obsady stanowisk Zamawiający wskaże ilości osób biorących udział w każdych warsztatach. Należy przyjąć, że jednorazowo ilość osób na poszczególnych warsztatach nie przekroczy 10 osób, a całościowa liczba osób biorących udział w warsztatach autoryzowanych wyniesie 20 osób.
23. Każdy uczestnik warsztatów niezależnie, jakiego zakresu dotyczyły warsztaty powinien otrzymać od Wykonawcy zaświadczenie/certyfikat uczestnictwa oraz materiały warsztatowe w języku polskim lub angielskim w formie papierowej i elektronicznej obejmujące zagadnienia będące przedmiotem warsztatów. W przypadku warsztatów autoryzowanych – certyfikatów producenta.
24. Warsztaty zostaną przeprowadzone w terminie uzgodnionym pomiędzy stronami.
25. Materiały warsztatowe przekazane będą zarówno w formie papierowej jak i elektronicznej.
26. **Testy akceptacyjne**

Przeprowadzenie testów akceptacyjnych ma na celu weryfikację prawidłowości implementacji w Systemie wymaganych przez Zamawiającego w opisie przedmiotu zamówienia funkcjonalności Systemu oraz poprawności jego wdrożenia i funkcjonowania zgodnie z projektem technicznym. Pozytywny wynik testów akceptacyjnych jest podstawą odbioru przez Zamawiającego prac zrealizowanych przez Wykonawcę w ramach wdrożenia.