

Szczegółowy Opis Przedmiotu Zamówienia

Dostawa i wdrożenie systemów cyberbezpieczeństwa – SIEM/SOAR w związku z realizacją przez Gminę Starachowice zadania w ramach realizacji grantu pn. „Cyberbezpieczny Samorząd”.

Rozdział I. Założenia początkowe oraz wymagania ogólne

I.1 Wprowadzenie

1. Przedmiot zamówienia jest realizowany w ramach grantu pn. „Cyberbezpieczny Samorząd” współfinansowanego ze środków Unii Europejskiej: Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.
2. Realizacja grantu ma na celu podniesienie cyberbezpieczeństwa oraz zdolności do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego w Gminie Starachowice

I.2 Ogólny opis przedmiotu zamówienia

1. Przedmiot zamówienia obejmuje **dostawę i wdrożenie system SIEM/SOAR**
2. Przedmiot zamówienia musi być dostarczony, wdrożony i zainstalowany w całości w siedzibie Zamawiającego we wskazanym miejscu.
3. Wszystkie dostarczane Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem przedmiotu zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach) oraz Komponenty (rozumiane jako integralna część dostawy i wdrożenia przedmiotu zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.
4. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca musi przeprowadzić zgodnie z postanowieniami niniejszego OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
5. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami OPZ oraz Umowy.
6. Ilekroć w niniejszym OPZ Zamawiający użył w opisie oznaczeń norm, aprobat, specyfikacji technicznych i systemów odniesienia, o których mowa w art. 101 ust. 1-3 ustawy Pzp należy je rozumieć jako przykładowe. Zamawiający zgodnie z art. 101 ust. 4 ustawy Pzp dopuszcza rozwiązanie równoważne opisywanym w treści OPZ. Jeżeli zapisy zawarte w OPZ wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający, zgodnie z art. 101 ust. 4 ustawy Pzp dopuszcza składanie ofert na rozwiązania równoważne. Wszelkie „produkty” pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim musi odpowiadać produkt, aby spełnić wymagania

stawiane przez Zamawiającego stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dot. minimalnych wymagań parametrów jakościowych Zamawiający rozumie wymagania materiałów, sprzętu i urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami producentów /produktów/ ma wyłącznie charakter przykładowy. Zamawiający, przy opisie przedmiotu zamówienia, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, wykazujących spełnienie przez produkty równoważne ww. parametrów i cech.

I.3 Termin realizacji Przedmiotu Zamówienia

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie do 5 miesięcy od daty zawarcia umowy.

I.4 Organizacja wdrożenia

I.4.1 Założenia podstawowe

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram wdrożenia, który musi być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia. Wykonawca musi przedstawić Harmonogram wdrożenia w terminie 14 dni od daty podpisania umowy.
2. Wykonawca w Harmonogramie wdrożenia musi w szczególności uwzględnić podział na zadania takie jak: projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich realizowanych przez niego pracach w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji i wdrożeniu i testowaniu).
4. Wykonawca zobowiązany jest do udziału w cyklicznych naradach przeglądu prac w siedzibie Zamawiającego. Dopuszcza się narady prowadzone w trybie zdalnym z wykorzystaniem narzędzi komunikacji elektronicznej, które zapewni Wykonawca. Zamawiający przewiduje częstotliwość narad maksymalnie 1 raz w miesiącu, narad zdalnych maksymalnie 3 razy w miesiącu, chyba że nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań w siedzibie lub odbywanych zdalnie.
5. Wykonawca zobowiązany jest przeprowadzić prace wdrożeniowe przedmiotu zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.

6. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie przedmiotu zamówienia.
7. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
8. W ramach wdrożenia Wykonawca musi przygotować informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującej się realizacją przedmiotu zamówienia, w ramach której muszą zostać powołane minimum następujące role:
 - 1) Kierownik Projektu ze strony Wykonawcy,
 - 2) Zespół Wdrożeniowy ze strony Wykonawcy.
9. Wdrożenie, z zastrzeżeniami wskazanymi poniżej muszą realizować osoby wymienione w ofercie Wykonawcy, przy czym:
 - 1) Osoby Zespołu Wykonawcy muszą być dyspozycyjne w trakcie wykonywania prac,
 - 2) Wykonawca musi przekazać Zamawiającemu wykaz numerów telefonów kontaktowych do kluczowych osób biorących udział w realizacji Przedmiotu Zamówienia po stronie Wykonawcy.

I.4.2 Przygotowanie Dokumentacji

1. W ramach realizowanych prac Wykonawca musi opracować dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:
 - 1) Harmonogram Wdrożenia,
 - 2) Dokumentacja Analizy Przedwdrożeniowej (DAP),
 - 3) Dokumentacja Powykonawcza.
2. Dokumentacja powyższa musi zawierać bazowe zapisy opisujące budowane rozwiązania oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach przedmiotu zamówienia. Dokumenty te wraz ze OPZ z załącznikami będą stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia i DAP warunkuje rozpoczęcie prac Wykonawcy.
4. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z Harmonogramem wdrożenia muszą być opracowane w oparciu o wymagania określone w niniejszym OPZ.

I.4.3 Analiza Przedwdrożeniowa

Analiza Przedwdrożeniowa obejmuje wszystkie czynności do wykonania przez Wykonawcę mające na celu analizę oraz wdrożenie środowiska informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy Przedwdrożeniowej Wykonawca przedstawi Zamawiającemu Dokumentację Analizy Przedwdrożeniowej (zwana dalej DAP) oraz harmonogram wdrożenia, na podstawie której organizacyjnie i technicznie będzie realizowany przedmiot zamówienia. DAP będzie podlegała uzgodnieniu i akceptacji Zamawiającego. Termin wykonania analizy został określony w umowie.

1. DAP musi zawierać w szczególności:

ZAWARTOŚĆ DOKUMENTACJI ANALIZY PRZEDWDROŻENIOWEJ DAP	
1. Wymagane dane ZARZĄDCZE:	
1)	plan i sposób komunikacji Stron.
2)	harmonogram wdrożenia
2. Wymagane dane dotyczące systemów cyberbezpieczeństwa:	
1)	podział przedmiotu zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty,
2)	analiza wymagań przedmiotu zamówienia zawierająca opis sposobu realizacji wymagań, sposób testowania i odbioru,
3)	Wykonawca określi w Analizie przedwdrożeniowej zalecaną specyfikację i optymalną konfigurację środowiska dla Systemu SIEM/SOAR m.in. pamięć, liczbę procesorów, ilość i wielkość dysków.
4)	Dla systemu cyberbezpieczeństwa SIEM/SOAR Wykonawca opracuje: <ol style="list-style-type: none"> a) Architekturę rozwiązania b) Wersję oprogramowania wchodzące w skład Systemu c) Konfigurację Systemu d) Zastosowane licencje/subskrypcje.
5)	Procedura testowania – scenariusze testowe dla wdrażanych systemów
6)	Harmonogram wdrożenia
7)	opis instalacji i wdrożenia oprogramowania
8)	szczegółowy zakres i zawartość pozostałej Dokumentacji.

I.4.4 Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. W szczególności dokumentacja ta musi zawierać:
 - a. Schemat infrastruktury i architekturę rozwiązania wraz z opisem.
 - b. Zasady licencjonowania dostarczonych elementów.
 - c. Konfigurację sprzętową i logiczną elementów infrastruktury dla wdrożonych systemów.
 - d. Procedury uruchamiania, zatrzymywania wdrożonych systemów oraz elementów infrastruktury.
 - e. Procedury wykonywania odtworzenia wdrożonych systemów z kopii zapasowej.
 - f. Procedury uruchamiania wdrożonych systemów w przypadku awarii dowolnej z dwóch lokalizacji Zamawiającego
 - g. Procedury opisujące standardowe działania administracyjne.
 - h. Procedury odzyskania wdrożonych systemów po awarii.
 - i. Wytyczne (dobre praktyki) dla administratorów.
 - j. Spis dokumentacji zewnętrznej do której odwołuje się Dokumentacja Powykonawcza.

I.4.5 Odbiór Etapu/Dokumentacji/Końcowy

1. Odbiory Etapów/Dokumentacji będą się odbywać po zakończeniu określonych prac danego Etapu/Dokumentacji.
2. Odbiór końcowy przedmiotu zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy, w tym odebrania wszystkich Komponentów i Etapów oraz dostarczenia wymaganej zamówieniem Dokumentacji.
3. Odbiory będą odbywać się zgodnie z zapisami w Umowie.

I.4.6 Testy

1. W ramach odbioru przedmiotu zamówienia muszą zostać przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji przedmiotu zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób i podmiotów zewnętrznych.
2. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad jest niezbędne, aby dla poszczególnych Komponentów oraz całego przedmiotu zamówienia dokonać odbiorów w ramach poszczególnych Etapów i Odbioru Końcowego.
3. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
4. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed Odbiorem Końcowym przedmiotu zamówienia.
5. Zamawiający wymaga aby Wykonawca przeprowadził testy odbiorcze z zakresu:
 - a) Uruchamianie i zatrzymywanie wdrożonych systemów
 - b) Weryfikacja wdrożonych systemów zgodnie ze scenariuszami opisanymi w dokumentacji.
 - c) Weryfikacja poprawności działania procedur.
 - d) Symulację awarii wdrożonych systemów w jednej lokalizacji.

I.4.7 Dodatkowe zobowiązania Wykonawcy

1. Wykonanie przedmiotu zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
2. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającymi na każdym etapie realizacji.
3. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
4. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
5. Współdziałanie z osobami wskazanymi przez Zamawiającego.

Rozdział II. Szczegółowy opis przedmiotu zamówienia

II.1. System SIEM/SOAR

Przedmiotem zamówienia jest dostarczenie systemu SIEM z wsparciem technicznym na okres do 20 czerwca 2026 r.

System w ramach jednej konsoli będzie oferował rozbudowane mechanizmy zbierania, analizy i raportowania danych z różnych źródeł w tym z laptopów, komputerów stacjonarnych, serwerów, kontenerów lub maszyn wirtualnych umożliwiając szybką identyfikację i reakcję na potencjalne ataki oraz incydenty bezpieczeństwa.

System powinien być dostarczony dla min 1200 monitorowanych obiektów (assets). System powinien być tak zskalowany aby obsłużyć w przyszłości kolejne 1000 obiektów.

System wdrożony ma być na maszynie wirtualnej na zasobach Zamawiającego. Obecnie Zamawiający dysponuje środowiskiem wirtualnym VMWare.

System będzie pracował w środowisku rozproszonym (sieć MAN).

System ma monitorować infrastrukturę Zamawiającego znajdującą się na terenie Gminy Starachowice (jednostki organizacyjne Gminy Starachowice).

Po zakończeniu wdrożenia, Wykonawca przeprowadzi szkolenie dla administratorów w zakresie co najmniej niezbędnym do prawidłowego użytkowania, konfiguracji i zarządzania problemami występującymi we wdrożonym systemie. Szkolenie musi być przeprowadzone w języku polskim, w formie zrozumiałej dla administratorów. Przekazane materiały szkoleniowe muszą być sporządzone w języku polskim. Szczegółowy zakres, plan wdrożenia i szkolenia zostanie określony podczas analizy przedwdrożeniowej.

II.1.1. Wymagania funkcjonalne

1. System musi bazować na rozwiązaniu open source , którego kod źródłowy jest publicznie dostępny oraz rozwijany przez aktywną społeczność i niezależnego producenta
2. System musi umożliwiać:
 - a. gromadzenie, korelację zdarzeń przesyłanych lub pobieranych z innych systemów
 - b. Monitorowanie zdarzeń bezpieczeństwa
 - c. Analiza logów i detekcja anomalii
 - d. Reakcja na zagrożenia i alertowanie personelu odpowiedzialnego za bezpieczeństwo
 - e. Kompatybilność z istniejącą infrastrukturą IT
 - f. Możliwość łatwego rozszerzenia funkcjonalności w przyszłości
 - g. Zapewnienie zgodności z obowiązującymi regulacjami takimi jak: PCI DSS, HIPAA, NIST 800-53, TSC GDPR
 - h. Skonfigurowanie zbierania logów z różnych źródeł

- i. Analiza zachowań i detekcja anomalii
 - j. Zdefiniowanie zestawu reguł detekcji zgodnych z branżowymi standardami
 - k. Generowanie alertów na podstawie wykrytych zagrożeń
 - l. Skonfigurowanie reakcji automatycznych na określone zdarzenia
 - m. Integracja z systemami ITSM
 - n. Analiza trendów i podejrzanych wzorców
 - o. Mechanizmy szyfrowania dla komunikacji między komponentami.
 - p. Odpowiednie zabezpieczenia dostępu do systemu.
 - q. Intuicyjny interfejs do konfiguracji i zarządzania systemem.
 - r. Możliwość łatwej aktualizacji i rozbudowy.
- 3. Oprogramowanie SIEM zostanie dostosowane na potrzeby zbierania informacji i informowania o incydentach z systemów oraz urządzeń
 - 4. System SIEM będzie wspierać integrację z różnymi systemami i narzędziami, w tym serwerami, firewallami, systemami IDS, systemami NAC, systemami kontroli dostępu, systemami zarządzania tożsamością w tym Active Directory
 - 5. SIEM będzie obsługiwać różne protokoły transmisji logów, takie jak Syslog, SNMP, WMI i inne. Dopuszcza się realizację obsługi wybranych protokołów poprzez zastosowanie integratorów, agentów lub komponentów pośrednich, pod warunkiem zapewnienia pełnej funkcjonalności i zgodności z wymaganiami niniejszego OPZ
 - 6. SIEM umożliwi zbieranie, normalizację i korelację logów z różnych źródeł w jednolitym formacie
 - 7. System musi umożliwiać przypisanie poziomów krytyczności do monitorowanych zasobów
 - 8. System musi umożliwiać mapowanie zdarzeń korelacyjnych na framework Mitre ATT&CK
 - 9. System w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji umożliwi automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email.
 - 10. Rozwiązanie musi umożliwić korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE.
 - 11. Wbudowane mechanizmy detekcji zagrożeń pozwalają na szybkie reagowanie na potencjalne ataki.
 - 12. Integracja się z różnymi źródłami logów, zarówno systemowymi, jak i aplikacyjnymi.
 - 13. System zapewnia normalizację logów, co ułatwia analizę i porównywanie informacji pochodzących z różnych źródeł.
 - 14. Rozwiązanie musi posiadać natywnie zintegrowany moduł HIDS (host-based intrusion detection system) zapewniający analizę integralności plików, monitorowanie logów systemowych w czasie

rzeczywistym oraz mechanizmy aktywnej odpowiedzi (active response) dostępne bez dodatkowych płatnych wtyczek.

15. Wykrywanie podejrzanych aktywności, takich jak próby włamań, ataki brute-force czy nieautoryzowane zmiany w plikach systemowych
16. Posiadanie funkcji detekcji na poziomie sieci (NIDS), które monitorują ruch sieciowy i identyfikują potencjalne zagrożenia.
17. Analizowanie ruchu w czasie rzeczywistym, a także przeszukiwanie archiwalnych danych.
18. centralne zarządzanie konfiguracją i politykami bezpieczeństwa.
19. Umożliwia jednolitą konfigurację dla wielu agentów w środowisku.
20. Integracja z narzędziami Elastic Stack (Elasticsearch, Logstash, Kibana), co umożliwia zaawansowaną analizę i wizualizację danych bezpieczeństwa.
21. funkcje raportowania i wizualizacji, które pozwalają na szybkie zrozumienie stanu bezpieczeństwa w organizacji.
22. Możliwość tworzenia niestandardowych raportów i widoków.
23. Wbudowany system monitorowania integralności plików (FIM) sprawdza, czy pliki systemowe i konfiguracyjne nie uległy nieautoryzowanym zmianom.
24. Możliwość konfiguracji zautomatyzowanych reakcji na wykryte zagrożenia, co przyspiesza proces reagowania na incydenty.
25. Obsługa różne protokoły bezpieczeństwa, takie jak Syslog, SNMP, czy JSON, co ułatwia integrację z różnymi systemami.
26. moduły i rozszerzenia, które umożliwiają dostosowanie systemu do specyficznych potrzeb organizacji.
27. System musi umożliwiać generowanie raportów na żądanie oraz raportów okresowych.
28. Raporty powinny być konfigurowalne i dostosowane do potrzeb różnych grup odbiorców (np. zarząd, dział IT, audyt).
29. System musi zapewniać bezpieczne przechowywanie zebranych logów i zdarzeń przez określony czas (np. 1 rok).
30. Dane powinny być chronione przed nieautoryzowanym dostępem i modyfikacją.

II.1.2. Wymagania нефункционалне

1. Wydajność

- a. • System musi zapewniać wysoką wydajność i skalowalność, aby obsłużyć dużą ilość danych i zdarzeń.
- b. • System musi zapewniać redundancje maszyn. W przypadku awarii maszyny głównej jej rolę i funkcjonalności przejmuje maszyna zapasowa.

2. Bezpieczeństwo

- a. • System musi spełniać wysokie standardy bezpieczeństwa, w tym szyfrowanie danych w transzycie i w spoczynku.
- b. • System powinien być odporny na ataki typu DDoS oraz inne próby naruszenia jego integralności.

3. Łatwość Użycia

- a. • Interfejs użytkownika powinien być intuicyjny i łatwy w obsłudze

4. Wykonanie dokumentacji analizy przedwdrożeniowej obejmującej całość wdrożenia w oparciu o analizę istniejącego środowiska Zamawiającego

- a. Wykonawca opracuje analizę przedwdrożeniową realizacji uzgodnionej koncepcji, uwzględniający najlepsze praktyki i rekomendacje wdrożenia SIEM. W projekcie muszą być zawarte:
 1. • Architektura wdrożenia
 2. • Usługi i systemy monitorowanie przez SIEM
 3. • Wykaz logów zbieranych przez SIEM
 4. • Wykaz wymaganych przez SIEM portów
 5. • Opcje instalacji agentów SIEM
 6. • Opcje podłączenia urządzeń sieciowych do SIEM
 7. • szczegółowy harmonogram realizacji prac migracyjnych, uwzględniający specyfikę organizacji Zamawiającego
 8. Projekt musi zostać przedstawiony do analizy Zamawiającemu który decyduje o jego akceptacji lub zwraca do uzupełnienia z pisemnym wskazaniem obszarów do uzupełnienia.

5. **Wdrożenie i dostosowanie SIEM oraz wykonanie dokumentacji powykonawczej.**

W ramach zadania Wykonawca wykona instalację i konfigurację rozwiązania SIEM w tym:

1. Instalacja SIEM
2. Konfigurację portów wymaganych przez SIEM
3. Instalację agenta SIEM na systemach Windows
4. Instalację agenta SIEM na posiadanym przez Zamawiającego środowisku wirtualnym
5. Instalację agenta SIEM na systemach Linux
6. Utworzy reguły dla poszczególnych grup agentów
7. Podłączy urządzenia sieciowe do SIEM
8. Dostosuje reguły zbierania logów z urządzeń
9. Dostosuje reguły zbierania logów z systemów Windows
10. Dostosuje reguły zbierania logów z systemów Linux
11. Utworzy reguły normalizacji logów, jeśli będzie taka potrzeba
12. Skonfiguruje moduł integralności plików oraz rejestru na systemach Windows monitorowanych przez SIEM
13. Utworzy reguły wykrywania ataków
14. Utworzy reguły wykrywania ataków Pass-the-Hash
15. Utworzy reguły wykrywania ataków Pass-the-ticket
16. Utworzy reguły wykrywania ataków DCSync
17. Utworzy reguły wykrywania ataków Golden Ticket
18. Utworzy reguły wykrywania ataków Kerberoasting
19. Utworzy reguły wykrywania ataków na poświadczenia Windows
20. Utworzy reguły wykrywania ataków na bazę haseł z Ntds.dit
21. Utworzy reguły wykrywania połączeń PsExec w systemach Windows
22. Utworzy reguły wykrywania ataków Ransomware
23. Skonfiguruje listy IP allow i IP block dla SIEM
24. Skonfiguruje moduł blokujący połączenia do hostów monitorowanych przez SIEM
25. Uruchomi moduł wykrywający podatności CVE na systemach monitorowanych przez SIEM

26. Skonfiguruje moduł wykrywający poziom bezpieczeństwa na systemach monitorowanych przez SIEM
27. Utworzy raporty wskazane przez Zamawiającego
28. Skonfiguruje backup rozwiązania SIEM oraz procedury Disaster Recovery

Rozdział III. Gwarancja

III.1 Okres gwarancji i wsparcia technicznego

Wykonawca zapewni w ramach wdrożenia kompleksowe wsparcie techniczne realizowane przez producenta systemu świadczonego minimalnie w godzinach 9-17 w dni robocze z czasem reakcji na zgłoszenie minimum 8 godzin realizowane do 20 czerwca 2026 r.. Wsparcie będzie oferowało nielimitowaną ilość zgłoszeń i zapytań w tym konsultacji technicznych. W ramach wsparcia producent wykona analizę poprawności działania. W ramach wsparcia zapewnione zostaną aktualizacje do najnowszych wersji systemu.

Wykonawca dostarczy wydruk bezpośrednio ze strony producenta potwierdzający, że oferowany poziom serwisu spełnia wymagania Zamawiającego (w przypadku braku takiej informacji na stronie Zamawiający zaakceptuje oświadczenie wystawione przez producenta oprogramowania).

1. Wykonawca w ramach realizacji przedmiotu zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją”) na okres 12 miesięcy
2. Bieg terminów gwarancji określonych w ust. 1 będą rozpoczynać się z dniem Protokołu Końcowego bez uwag przez Zamawiającego.
3. Dostarczone system muszą być objęte gwarancją (serwisem) producenta przez okres wskazany w ust.1. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

III.2 Reżimy realizacji usług serwisowych

W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia rozumianych jako Awaria lub Usterka zgodnie z definicjami, jak poniżej:

- 1) **Awaria** - Kategoria Wady powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiające jego użytkowanie. Sytuacja, w której Oprogramowanie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia.
- 2) **Usterka** - Należy przez to rozumieć kategorię Wady oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SOPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	niezwłocznie, nie później niż 12 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 4 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 4 dni robocze od czasu zgłoszenia
USTERKA	24/7/365	niezwłocznie, nie później niż 3 dni od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 10 dni roboczych od czasu zgłoszenia

1. Dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną.
2. Casy naprawy mogą być inne niż wskazane w powyższych tabelach, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 1).
3. W przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego.
4. Wykonawca w okresie trwania gwarancji, do 5 dnia każdego miesiąca, przedstawi Zamawiającemu raport zawierający co najmniej: numer zgłoszenia, kwalifikację zgłoszenia, godzinę i datę zgłoszenia, temat zgłoszenia, status zgłoszenia, godzinę i datę usunięcia Wady, czas naprawy.

Rozdział IV – Warunki udziału w postępowaniu

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:

1. Nie podlegają wykluczeniu
2. Spełniają warunki udziału w postępowaniu, dotyczące:
zdolności technicznej lub zawodowej, tj. w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, minimum dwie dostawy i wdrożenie systemu klasy SIEM i obsługujący min. 500 urządzeń klienckich, o wartości nie mniejszej niż 50 000 zł brutto każda.
3. dysponuje lub będzie dysponował osobami zdolnymi do realizacji przedmiotowego zamówienia, posiadającymi kwalifikacje niezbędne do wykonania zamówienia tj. minimum jedną osobą

posiadającą imienny certyfikat ukończenia oficjalnego szkolenia producenta rozwiązania, potwierdzający nabycie kompetencji na poziomie co najmniej inżyniera wdrożeniowego w zakresie konfiguracji, administracji i integracji oferowanego systemu. Wszystkie osoby, o których mowa powyżej, powinny biegle posługiwać się językiem polskim (w mowie i piśmie), w przeciwnym wypadku Wykonawca musi zapewnić tłumacza zapewniającego stałe tłumaczenie dla potrzeb realizacji zamówienia

Dokumenty potwierdzające spełnienie warunków udziału w zapytaniu Wykonawca dołączy do oferty.