Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup subskrypcji licencji, dostarczenie, wdrożenie, uruchomienie i konfiguracja Systemu informatycznego służącego do monitorowania i ochrony środowisk bazodanowych z zastosowaniem mechanizmów wykrywania wycieków informacji i anomalii klasy Database Activity Monitor (DAM) z opcją blokowania Database FireWall (DBF) zgodnie z poniższą specyfikacją:

1. Maksymalna ilość Agentów bazodanowych do instalacji na serwerach bazodanowych objętych wdrożeniem – 80 szt. – w tym:
    a. Pakiet Virtual: 60 subskrypcji licencji Agenta bazodanowego Systemu. Każdy komponent Systemu w tym pakiecie zostanie dostarczony w wersji wirtualnej zgodnej z platformą wirtualizacją VMWare.
    b. Pakiet Appliance: 20 subskrypcji licencji Agenta bazodanowego Systemu.. Komponent analizujący ruch bazodanowy w trybie L2 ISO/OSI transparent in-line bridge oraz analizujący ruch bazodanowy otrzymany od Agenta Systemu w tym pakiecie zostanie dostarczony w wersji fizycznego serwera appliance, a pozostałe komponenty zostaną dostarczone w zgodnej wersji z platformą wirtualizacją VMWare.
2. Wsparcie techniczne Producenta dla subskrypcji licencji lub subskrypcji licencji i sprzętu na okres 36 miesięcy od dnia podpisania Protokołu Ilościowego Odbioru.
3. Usługi towarzyszące Wykonawcy obejmujące: Usługi Instalacyjno-Wdrożeniowe, Usługi Szkoleniowe
4. Usługi wsparcia eksperckiego Wykonawcy, maksymalnie 5.000 godzin zegarowych do wykorzystania w całym okresie obowiązywania Umowy.

System monitorowania i ochrony środowisk bazodanowych z zastosowaniem mechanizmów wykrywania wycieków informacji i anomalii musi monitorować oraz zabezpieczać systemy baz danych: Jako zabezpieczenie rozumiane jest zarówno monitorowanie aktywności (Database Activity Monitoring) jak i aktywna ochrona bazy danych w tym blokowanie niepożądanych aktywności (Database Firewall), w tym analiza behawioralna całości ruchu bazodanowego obserwowanego na poziomie sieciowym oraz raportowanie.

Zamawiający przewiduje możliwość wdrożenia Systemu w różnych lokalizacjach.

Zamawiający nie dopuszcza Systemu, którego Moduły i komponenty znajdują się, lub będą instalowane w chmurze (cloud).

I.Wymagania ogólne

1. Wymagane jest dostarczenie dedykowanego Systemu klasy Database Activity Monitoring z możliwością blokowania zdarzeń (Database FireWall), przeznaczone do monitorowania i ochrony danych przetwarzanych w bazach danych z zastosowaniem mechanizmów wykrywania wycieków informacji i anomalii.
2. Oferowany System musi posiadać wsparcie techniczne producenta. Nie dopuszcza się rozwiązań open source.

3. Oferowany System musi istnieć na rynku co najmniej 5 lat oraz posiadać wsparcie techniczne producenta w języku polskim.
4. Zamawiający wymaga, aby System składał się z minimum trzech wyróżnionych modułów:
   1)**Moduł DAM/DBF** (Database Activity Monitoring/ Database FireWall),
   2)**Moduł ML** (Machine Learning) – automatycznego wykrywania incydentów i anomalii w ruchu SQL
   3)**Moduł wizualizacji** i analizy logów i zdarzeń bazodanowych
5. Wykonawca zobowiązuje się w szczególności:
   a) dostarczyć, wdrożyć, uruchomić i skonfigurować System składający się z wymaganych Modułów oraz sprzętu, o ile jest niezbędny dla prawidłowego działania Systemu;
   b) wykonać analizę przedwdrożeniową oraz Dokumentację projektu technicznego oraz Dokumentację powdrożeniową
   c) uzgodnić z Zamawiającym harmonogram wdrożenia,
   d) zapewnić subskrypcję licencji na okres 36 miesięcy od dnia podpisania Protokołu Odbioru Ilościowego Licencji, wymaganych do prawidłowego działania Systemu, jako całości, jak i poszczególnych jego elementów dla maksymalnie 80 serwerów bazodanowych. Serwer bazodanowy rozumiany jako instancja systemu operacyjnego, na której zainstalowany został silnik bazodanowy. Licencjobiorcą jest Zamawiający, a podmiotami uprawnionymi do korzystania z Systemu jest Zamawiający oraz są wszystkie Jednostki Zamawiającego w tym Ministerstwo Sprawiedliwości.
   e) przenieść na Zamawiającego autorskie prawa majątkowe do Dokumentacji opracowanej przez Wykonawcę w ramach Umowy.
   f) udzielić Zamawiającemu Gwarancji na wykonane Wdrożenie w ramach Umowy od daty podpisania Protokołu Odbioru Wdrożenia Systemu na okres trwania subskrypcji licencji oraz świadczyć w tym okresie usługi gwarancyjne w zakresie wdrożonego Systemu w ramach wynagrodzenia wynikającego z Umowy.
   g) Udzielić Zamawiającemu Gwarancji na sprzęt o ile jest niezbędny dla prawidłowego działania Systemu od daty podpisania Protokołu Odbioru sprzętu oraz świadczyć w tym okresie usługi gwarancyjne w zakresie dostarczonego sprzętu, w ramach wynagrodzenia wynikającego z Umowy.
6. Oferowany System musi pochodzić tylko z oficjalnych kanałów dystrybucyjnych Producenta na terenie Unii Europejskiej.
7. Wszystkie Moduły Systemu muszą pochodzić od jednego Producenta.
8. Każdy Moduł stanowiący element Systemu musi stanowić jednolite środowisko programowe, tj. współpracować ze sobą bez konieczności stosowania dodatkowych elementów nie będących standardową częścią oferowanego Systemu np. pochodzić od innego Producenta, wymagać wykonania koniecznych integracji, zakupu dodatkowego oprogramowania lub sprzętu.
9. Oferowane rozwiązanie ma stanowić jednolity i kompleksowy System składający się z wymaganych Modułów. Skalowalny i elastyczny w kontekście potencjalnej rozbudowy tj. objęcia ochroną kolejnych serwerów bazodanowych.
10. Wymaganiem Zamawiającego jest, aby System posiadał jedną konsolę zarządzającą lub każdy Moduł Systemu posiadał maksymalnie jedną Konsolę zarządzającą.
11. Oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).

12. Oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
13. Zamawiający wymaga, aby wszystkie elementy i Moduły dostarczanego Systemu były w najnowszej wersji (tzn. najnowszej udostępnionej przez Producenta rozwiązania) na dzień wdrożenia Systemu.
14. Całość przetwarzania danych w Systemie musi odbywać się w infrastrukturze Zamawiającego, Jednostkach lub w Ministerstwie Sprawiedliwości. Zamawiający nie dopuszcza instalacji Modułów i przetwarzania danych Systemu w rozwiązaniach chmurowych.
15. Żaden z Modułów i elementów oferowanego Systemu na dzień składania ofert nie może być przeznaczony przez Producenta do wycofania z produkcji lub sprzedaży.
16. Czynności związane z wdrożeniem i konfiguracją Systemu w infrastrukturze Zamawiającego Systemu muszą być przeprowadzone przez personel Wykonawcy w obecności personelu IT Zamawiającego.
17. Wszystkie niezbędne elementy sprzętowe i programowe wymagane do poprawnego działania Systemu muszą w pełni ze sobą współpracować, być dostarczone wraz z Systemem oraz być w pełni objęte gwarancją Producenta.
18. W przypadku zastosowania Systemu do monitorowania fizycznych serwerów bazodanowych wymagana jest funkcjonalność monitorowania ruchu bazodanowego w trybie L2 transparent in-line bridge z zastosowaniem dedykowanego sprzętu posiadającego funkcjonalność bypass-u kart sieciowych.
19. W przypadku zastosowania Systemu do monitorowania wirtualnych serwerów bazodanowych wymagana jest funkcjonalność monitorowania ruchu bazodanowego w trybie L2 transparent in-line bridge.

II.Pakiet Virtual - Wymagania techniczne i licencjonowania

1. Licencjonowanie wszystkich modułów oferowanego Systemu musi opierać się o licencje liczone na każdy serwer bazodanowy bez względu na wydajność, ilość przetwarzanych danych i przepustowość. Serwer bazodanowy rozumiany jako instancja systemu operacyjnego, na której zainstalowany został silnik bazodanowy.
2. System musi obsługiwać środowiska bazodanowe w zakresie monitorowania, minimum dla wskazanych poniżej silników bazodanowych:

silnik bazodanowy	**wersja silnika bazodanowego**
ORACLE	21, 19c, 12.2, 12.1
MySQL	8.0, 5.7
MariaDB Server	10.6-2
INFORMIX	14.10, 12.10
Percona MySQL	5.7
PostgreSQL	14.x – 10.x
SAP-HANA	2 SPS 5
Teradata	17.05, 16.20, 16.10
Apache Cassandra	4.0
Sybase IQ	16.1 SP4, 16.1 SP2
Sysbase SQL Anywhere	17.0
Sysbase ASE	16.0
Snowflake	Wszystkie wersje

3. Oferowany System musi składać się z opisanych poniżej modułów, w skład których wchodzą wskazane komponenty:
   - **Moduł DAM/DBF musi składać się z:**
     a. **Komponentu wykonawczego**, analizującego ruch bazodanowy w trybie L2 ISO/OSI transparent in-line bridge oraz analizującego ruch bazodanowy otrzymany od Agenta
     b. **Komponentu zarządzającego DAM/DBF** dla wielu Komponentów wykonawczych i Agentów bazodanowych,
     c. **Agenta bazodanowego** – lekka aplikacja instalowana na serwerze baz danych, wysyłająca do analizy kopię ruchu bazodanowego do Komponentu wykonawczego
   - **Moduł Machine Learning musi składać się z:**
     d. **Komponentu analitycznego**, który za pomocą algorytmów machine learning (ML) analizuje zdarzenia pochodzące z ruchu SQL monitorowanych baz danych dostarczone przez Moduł DAM/DBF
     e. **Komponentu zarządzającego** dla wielu komponentów analitycznych (ML)
   - **Moduł wizualizacji logów i zdarzeń bazodanowych musi składać się z:**
     f. **Komponentu wizualizującego** dane, który analizuje dane otrzymane z Komponentu wykonawczego. Komponent ten musi również posiadać funkcjonalność pobierania zdarzeń i logów SQL z natywnych tablic audytowych baz danych.

4. Zamawiający może zainstalować dowolną liczbę modułów i komponentów (pkt. 3 a, b, d, e, f) w ramach wykupionych pakietów licencyjnych dla serwerów bazodanowych. W celu zwiększenia wydajności oraz niezawodności Zamawiający może łączyć Komponenty wykonawcze (pkt. 3a) w klastry wydajnościowe.
5. Komponenty Systemu z pkt. 3 (a, b, d, e) muszą zostać dostarczone jako gotowe maszyny wirtualne (ang. virtual appliance) dla wirtualizatora VMWare.
6. Z uwagi na posiadanie przez Zamawiającego systemów bazodanowych, na których z powodów licencyjnych lub wydajnościowych nie ma możliwości zainstalowania oprogramowania Agenta bazodanowego Zamawiający wymaga aby Komponent wykonawczy w wersji wirtualnej Systemu posiadał poniższe funkcjonalności:
   a. Obsługa trybu sieciowego – L2 In-Line Transparent Bridge, SPAN, wydzielenie interfejsu sieciowego do komunikacji z Agentami DB
   b. Przepustowość ruchu SQL – minimum 1Gbps
   c. Wydajność analizy zapytań SQL na poziomie nie mniejszym niż 20.000TPS
   d. Monitorowanie w trybie L2 In-Line Transparent Bridge ruchu bazodanowego przesyłanego za pomocą połączenia trunk (IEEE 802.1Q)
   e. Preinstalowany System w najnowszej wersji
7. Moduł wizualizacji logów i zdarzeń bazodanowych może zostać dostarczony jako aplikacja do instalacji na systemie operacyjnym lub jako obraz gotowej maszyny wirtualnej.
8. Licencję na system operacyjny, jaki i wszelkie inne oprogramowanie (oprogramowanie firm trzecich) potrzebney do instalacji i poprawnego działania Modułu wizualizacji logów i zdarzeń bazodanowych dostarczy Wykonawca.

III.Pakiet Appliance - Wymagania techniczne i licencjonowania

1. Licencjonowanie wszystkich modułów oferowanego Systemu musi opierać się o licencje liczone na każdy serwer bazodanowy bez względu na wydajność, ilość przetwarzanych danych i przepustowość. Serwer bazodanowy rozumiany jako instancja systemu operacyjnego, na której zainstalowany został silnik bazodanowy.
2. System musi obsługiwać środowiska bazodanowe w zakresie monitorowania, minimum dla wskazanych poniżej silników bazodanowych:

silnik bazodanowy	wersja silnika bazodanowego
ORACLE	21, 19c, 12.2, 12.1
MySQL	8.0, 5.7
MariaDB Server	10.6-2
INFORMIX	14.10, 12.10
Percona MySQL	5.7
PostgreSQL	14.x – 10.x
SAP-HANA	2 SPS 5
Teradata	17.05, 16.20, 16.10
Apache Cassandra	4.0
Sybase IQ	16.1 SP4, 16.1 SP2
Sysbase SQL Anywhere	17.0
Sysbase ASE	16.0
Snowflake	Wszystkie wersje

3. Oferowany System musi składać się z opisanych poniżej modułów, w skład których wchodzą wskazane komponenty:
   - **Moduł DAM/DBF musi składać się z:**
     a. **Komponentu wykonawczego** w wersji fizycznego serwera appliance, analizującego ruch bazodanowy w trybie L2 ISO/OSI transparent in-line bridge oraz analizującego ruch bazodanowy otrzymany od Agenta
     b. **Komponentu zarządzającego DAM/DBF** dla wielu Komponentów wykonawczych i Agentów bazodanowych,
     c. **Agenta bazodanowego** – lekka aplikacja instalowana na serwerze baz danych, wysyłająca do analizy kopię ruchu bazodanowego do Komponentu wykonawczego
   - **Moduł Machine Learning musi składać się z:**
     d. **Komponentu analitycznego**, który za pomocą algorytmów machine learning (ML) analizuje zdarzenia pochodzące z ruchu SQL monitorowanych baz danych dostarczone przez Moduł DAM/DBF
     e. **Komponentu zarządzającego** dla wielu komponentów analitycznych (ML)
   - **Moduł wizualizacji logów i zdarzeń bazodanowych musi składać się z:**
     f. **Komponentu wizualizującego** dane, który analizuje dane otrzymane z Komponentu wykonawczego. Komponent ten musi również posiadać funkcjonalność pobierania zdarzeń i logów SQL z natywnych tablic audytowych baz danych.

4. Zamawiający może zainstalować dowolną liczbę modułów i komponentów (pkt. 3 a, b, d, e, f) w ramach wykupionych pakietów licencyjnych dla serwerów bazodanowych. W celu zwiększenia wydajności oraz niezawodności Zamawiający może łączyć Komponenty wykonawcze (pkt. 3a) w klastry wydajnościowe.
5. Komponenty Systemu:
   - Komponent wykonawczy pkt. 3a musi zostać dostarczony jako fizyczny serwer appliance
   - Komponenty z pkt 3 (a, b, d, e) muszą zostać dostarczone jako gotowe maszyny wirtualne (ang. virtual appliance) dla wirtualizatora VMWare.
6. Z uwagi na posiadanie przez Zamawiającego systemów bazodanowych, na których z powodów licencyjnych lub wydajnościowych nie ma możliwości zainstalowania oprogramowania Agenta bazodanowego Zamawiający wymaga dostarczenia fizycznego serwera (appliance) producenta Systemu o minimalnych parametrach:
   - Wysokość maksymalna 2U

- Redundantne zasilacze sieciowe 220V-230V
- Redundantne dyski HDD/SSD (minimum dwie szt.) obsługiwane przez sprzętowy kontroler RAID z obsługą RAID1, lub RAID5, lub RAID6, lub RAID10
- Karty sieciowe obsługujące bazodanowy ruch sieciowy RJ45 – minimum 16 szt.
- Wszystkie karty sieciowe dla trybu In-Line Transparent Bridge (minimum 8 linii) muszą być wyposażone w fizyczny bypass, który w przypadku awarii serwera appliance, nie będzie blokował ruchu sieciowego lub zablokuje cały ruch sieciowy (w zależności od skonfigurowanych ustawień).
- Wydzielony interfejs RJ45 do sieci zarządzającej (MGMT), wydzielony interfejs RJ45 do podłączenia sieci lokalnej (LAN) lub Agenta bazodanowego
- Obsługa trybu sieciowego – L2 In-Line Transparent Bridge (minimum 8 linii), SPAN (minimum 16 linii), wydzielenie interfejsów do komunikacji z Agentami bazodanowego
- Przepustowość ruchu SQL – minimum 1Gbps
- Karta sprzętowa do deszyfracji ruchu SSL/TLS – np. podczas procesu zaszyfrowanego logowanie się użytkowników do bazy danych
- Karta zarządzania serwerem Intelligent Platform Management Interface (IPMI)
- Monitorowanie w trybie L2 In-Line Transparent Bridge ruchu bazodanowego przesyłanego za pomocą standardów sieciowych – połączenie trunk (IEEE 802.1Q), Link Aggregation Control Protocol (LACP).
- Preinstalowany System w najnowszej wersji

7. Moduł wizualizacji logów i zdarzeń bazodanowych może zostać dostarczony jako aplikacja do instalacji na systemie operacyjnym lub jako obraz gotowej maszyny wirtualnej.
8. Licencje na system operacyjny, jaki i wszelkie inne oprogramowanie (oprogramowanie firm trzecich) potrzebne do instalacji i poprawnego działania Modułu wizualizacji logów i zdarzeń bazodanowych dostarczy Wykonawca.

IV. Wymagania funkcjonalne Systemu

1. Moduł DAM/DBF musi zapewnić poniższe funkcjonalności:
    a. Aktywne wyszukiwanie i klasyfikacja usług bazodanowych w sieci
        i. Wyszukiwanie i klasyfikacja informacji w bazach danych: Klasyfikacja odbywać się musi zarówno poprzez wykorzystanie wbudowanych wzorców danych (jak numery kart kredytowych, dane personalne, dane finansowe, identyfikatory bankowe, dane medyczne etc.) jak i przez definiowanie własnych wyrażeń. Definicja uwzględniać musi nazwy tabel, kolumn oraz rekordy w tabelach przy użyciu wyrażeń regularnych. Musi istnieć możliwość wykorzystania wykrytych informacji przy definiowaniu reguł monitorowania baz danych.
        ii. Testowanie podatności systemów bazodanowych: przy uwzględnieniu analizy podatności systemu operacyjnego oraz baz danych na znane typy ataków, błędy konfiguracyjne, brak aktualizacji oprogramowania, weryfikacja zabezpieczenia kont użytkowników bazodanowych. System musi posiadać funkcję uwierzytelnienia w systemie operacyjnym serwera oraz w bazie danych w celu wykonania powyższych testów. Uwierzytelnienie w systemie operacyjnym obsługiwać powinno nie mniej niż protokoły SSH oraz NTLM. Musi być zawarta licencja na testowanie podatności nie mniej niż 1000 instancji bazodanowych.
    b. musi zawierać co najmniej 1000 wstępnie zdefiniowanych testów oceny podatności na bazy danych, które obejmują następujące kategorie:

- Kontrola dostępu
- Audyt
- Uwierzytelnianie i zarządzanie użytkownikami
- Ogólne informacje o bazie danych
- Wewnętrzne testy
- Znane ataki oparte na CVE
- Licencjonowanie
- Integralność systemu operacyjnego
- Kontrola zasobów
- Wrażliwe wykrywanie danych

2. Moduł DAM/DBF musi mieć przygotowane testy podatności zgodne ze standardem CIS i DISA STIG dla minimum baz danych ORACLE, MSSQL, MySQL
3. Moduł DAM/DBF musi posiadać możliwość zdefiniowania bardzo szczegółowych reguł monitorowania lub audytowania dostępu do danych, zapewniając jednocześnie odpowiedni poziom ochrony dla całości ruchu SQL do bazy z uwzględnieniem języków w DCL, DML, DDL, TCL, procedur składowanych.
4. Moduł DAM/DBF musi umożliwić definiowanie polityki monitorowania lub audytowania uwzględniając nie mniej niż następujące kryteria:
    a. użytkownik bazodanowy,
    b. użytkownik aplikacyjny,
    c. tabele, kolumny,
    d. baza danych, schemat bazy danych,
    e. ilość wystąpień zdarzeń w czasie,
    f. dostęp do danych wrażliwych (sklasyfikowanych za pomocą funkcjonalności Wyszukiwanie i klasyfikacja informacji w bazach danych) ,
    g. wielkość odpowiedzi (ilość rekordów) na zapytanie SQL
    h. czas odpowiedzi bazy danych na zapytanie SQL,
    i. źródłowy adres IP
    j. dzień tygodnia i czas dnia
    k. wbudowane i predefiniowane sygnatury (np. CVE), sygnatury własne
    l. Polecenia SQL uprzywilejowane – grant, alter, drop, restore, create, deny, kill, backup, shutdown, truncate, revoke,
    m. Analiza odpowiedzi na zapytanie (SQL response) oraz analiza zmiennych typu Input Bind Variables
5. Moduł DAM/DBF musi zapewnić dodawanie informacji o użytkowniku wykonującym operacje bazodanowe (np. imię i nazwisko) poprzez pobieranie danych z zewnętrznych systemów: Bazy SQL, plik CSV, Active Directory
6. Moduł DAM/DBF musi zapewnić integrację z narzędziami typu Privilige Access Management, w celu pobierania dynamicznych danych uwierzytelniających do wykonywania aktywnego skanowania podatności serwera baz danych.
7. Moduł DAM/DBF musi zapewnić definiowanie reguł dostępu użytkowników do poszczególnych baz danych na poziomie sieciowym.
8. Moduł DAM/DBF musi zapewnić automatyczne budowanie i uczenie się profilu użytkownika bazodanowego z przeanalizowanego ruchu SQL. Profil powinien składać się z co najmniej poniższych informacji:
    a. Zapisane bazy i schematy, z których użytkownik bazodanowy korzysta
    b. Tabele i polecenia SQL (select, insert, update, delete), z których użytkownik bazodanowy korzysta
    c. Parametry połączenia użytkownika:
        i. Adres IP
        ii. Aplikacja kliencka
        iii. Nazwa komputera (OS Hostname)

iv. Nazwa użytkownika systemu operacyjnego (OS User)
v. Zapytania SQL

Na podstawie powyższej listy definiowane są reguły polityki bezpieczeństwa.

9. Ruch SQL wykryty przez polityki bezpieczeństwa Modułu DAM/DBF jako zagrożenie nie może być ruchem przekazanym do profilowania.
10. Moduł DAM/DBF musi zapewnić definiowanie reguł dostępu użytkowników bazodanowych do poszczególnych obiektów w bazie danych poprzez automatyczne tworzenie (na podstawie analizy ruchu sieciowego) listy użytkowników oraz listy zapytań SQL, jakie użytkownik może wykonać w odniesieniu do obiektów baz danych.
11. Moduł DAM/DBF musi zapewnić możliwość definiowania oddzielnych reguł dostępu w odniesieniu do tabel z danymi wrażliwymi.
12. Moduł DAM/DBF musi zapewnić tworzenie list tabel, do których poszczególni użytkownicy bazodanowi nie mogą mieć dostępu. Musi istnieć funkcja definiowania dni tygodnia oraz godzin, w jakich dany użytkownik może nawiązać połączenie z bazą danych, lub dostęp jest zabroniony.
13. Moduł DAM/DBF musi zapewnić w logach dotyczących zarejestrowanych naruszeń / anomalii co najmniej następujące informacje: nazwa użytkownika bazodanowego, dodatkowe dane o użytkowniku pochodzące z zewnętrznych systemów (np. LDAP, SQL, CSV), źródłowy adres IP, pełne zapytanie SQL wykonane przez użytkownika, ilość pobranych lub zmienionych rekordów.
14. Moduł DAM/DBF musi posiadać opcję blokowania ruchu wykorzystującego podatności wykryte w bazach danych poprzez funkcjonalność testowania podatności systemów bazodanowych.
15. Moduł DAM/DBF musi wykrywać komendy wykonywane na systemie zarządzania bazą danych (poza silnikiem SQL) jak np. Export Direct w DB Oracle
16. Moduł DAM/DBF musi posiadać funkcjonalność archiwizacji logów na zewnętrzny dysk (macierz dyskową), jak również przechowywać je w komponencie wizualizującym przez minimum rok. Archiwizowane logi dotyczące aktywności użytkowników muszą być natywne zapisywane w postaci zaszyfrowanej i skompresowanej. Archiwizowane logi muszą być podpisywane za pomocą certyfikatu.
17. Musi istnieć możliwość zmiany wszystkich haseł dla natywnych użytkowników oferowanego Modułu DAM/DBF (użytkownicy CLI, GUI, SQL oraz systemowi).
18. Moduł DAM/DBF musi posiadać funkcję wysyłania informacji o zdarzeniach poprzez protokół smtp (mail), syslog (SIEM) oraz uruchomienia skryptu jednocześnie ustawianymi per konkretna polityka bezpieczeństwa.
19. Producent musi zapewnić aktualizację Systemu, uwzględniając co najmniej: sygnatury ataków, listę reguł polityk bezpieczeństwa oraz monitorowania aktywności użytkowników na bazach danych, listę testów podatności baz danych oraz listę raportów jak również aktualizacje oprogramowania sprzętu appliance (dot. Pakietów Appliance).
20. Blokowanie ruchu SQL wymagane jest w środowiskach bazodanowych gdzie System monitoruje ruch za pomocą Agenta bazodanowego lub Komponentu wykonawczego w konfiguracji L2 Transparent In-line Bridge.
21. Komponent wykonawczy musi mieć możliwość zbudowania dwóch typów klastrów n+1:
    a. Komponent wykonawczy musi posiadać możliwość łączenia w klaster n+1. Wielu Agentów komunikuje się z klastrem. Główny serwer węzła (Master) ma zadane loadbalancera. Do budowy klastra nie może być użyta zewnętrzna infrastruktura np. wydzielony loadbalancer firm trzecich.
    b. W przypadku, gdy baza danych generuje bardzo duże obciążenie, więcej niż Komponent wykonawczy może obsłużyć, to Komponenty wykonawcze muszą posiadać możliwość łączenia się w klaster n+1, gdzie Agent komunikuje się z klastrem w celu rozłożenia obciążenia na wiele węzłów klastra, która generuje baza danych.
22. Zarządzanie oferowanym Systemem musi być dostępne poprzez interfejs przeglądarki Web w celu eliminacji konieczności instalacji dodatkowego oprogramowania na stacji administratora.

    a. Wymagane jest zarządzanie zorientowane zadaniowo. Oznacza to, że musi istnieć mechanizm informowania administratora o wykonaniu/nie wykonaniu na czas zadania zleconego innym użytkownikom Systemu.
23. Aktualizacja Systemu musi być dostępna zarówno poprzez ręczne pobranie zawartości ze strony producenta jak i automatycznie, poprzez zdefiniowanie terminów wykonania procedury aktualizacji.
24. System musi zostać dostarczony w formie kompletnego rozwiązania tj. nie może wymagać do działania żadnego oprogramowania firm trzecich np. zewnętrznych baz danych lub zewnętrznych load-balancerów.
25. Uwierzytelnianie użytkowników i administratorów Systemu musi być możliwe za pomocą:
    a. Użytkownika lokalnego
    b. protokołu RADIUS
    c. poprzez integrację z Active Directory
26. Wszystkie Komponenty zarządzające Systemu muszą posiadać wbudowany mechanizm RBAC, który umożliwia integrację z Active Directory poprzez przypisanie roli w zależności od przynależności do określonej grupy w Active Directory.
27. Całość konfiguracji Systemu oraz repozytorium logów musi być przechowywana na Komponencie zarządzającym w Module DAM/DBF lub Module wizualizującym dane.
28. Komponent zarządzający Modułu DAM/DBF musi wyświetlać w czasie rzeczywistym logi na jednej planszy (dashboard):
    a. minimum zdarzenia z ruchu bazodanowego, które łamią polityki bezpieczeństwa (security logs).
    b. minimum zdarzenia z działania Modułu DAM/DBF (system events np. logowanie/wylogowanie użytkowników, dodanie/usunięcie polityki bezpieczeństwa lub audytu, problemy z komponentem wykonawczym (np. przeciążenie, uszkodzenie dysku), brak prawidłowej komunikacji z Agentem bazodanowym.
29. Komponent wykonawczy Modułu DAM/DBF musi zapewnić możliwość monitorowania ruchu SQL w trybach :
    a. Transparent In-line Bridge (warstwa L2 ISO/OSI)
    b. SPAN (analiza kopii ruchu)
    c. Agent bazodanowy (program instalowany na serwerze baz danych, który przesyła kopię ruchu bazodanowego do modułu wykonawczego w celu wykonania analizy). Agent bazodanowy nie wykonuje analizy ruchu bazodanowego.
30. System musi mieć otwarte REST API, które umożliwia konfigurację rozwiązania, pobieranie danych z Systemu oraz możliwość integracji Systemu z innymi aplikacjami.
31. Musi być możliwość uruchomienia centralnego Komponentu zarządzającego Modułu DAM/DBF w przypadku korzystania z wielu Komponentów zarządzających.
32. Komponent zarządzający Modułu DAM/DBF musi posiadać następujące funkcje/opcje:
    a. Informacje o wgranej licencji Systemu
    b. Zarządzania użytkownikami (administratorami) systemu za pomocą RBAC
    c. Zarządzania, ustawiania wielkości budowanego profilu bazodanowego
    d. Konfiguracji połączenia z AD w celu logowania się do Systemu za pomocą AD
    e. Ustawienia siły hasła: ilość dni ważności hasła, minimalna ilość znaków, wielkie/małe litery, znaki specjalne, inne hasło od poprzedniego (minimum 12 ostatnich).
    f. Konfiguracja serwera PROXY http w celu pobierania aktualizacji z sieci Internet.
    g. Dołożenia sterowników, za pomocą których można podłączyć się do bazy danych w celu wykonania skanowania podatności i klasyfikacji danych
    h. Możliwość definiowania słów kluczowych, które można wykorzystywać np. przy raportach
    i. Dodawanie komentarza do polityk bezpieczeństwa i audytu
    j. Status zadań cyklicznych w podziale na kategorie: anulowane, wykonywane, zakończone z błędami, zatrzymane, w oczekiwaniu na uruchomienie

k. Eksportowanie konfiguracji Modułu DAM/DBF z poziomu GUI
l. Konfiguracja autoryzacji Komponentów wykonawczych w Komponentach zarządzania za pomocą certyfikatów.

33. **Moduł Machine Learning** musi zapewnić funkcjonalność klasy User Behavior Analytics. Moduł ten musi z wykorzystaniem mechanizmów sztucznej inteligencji i nauczania maszynowego analizować zebrane i przechowywane logi bazodanowe za pomocą komponentów Systemu oraz zapewnić w ten sposób realizacje minimum poniższych scenariuszy detekcji i raportowania anomalii i incydentów:
    a. Dostępu do bazy danych w niestandardowych godzinach.
    b. Używanie użytkownika bazodanowego (np. administratora baz danych lub innego) kont serwisowych (np. tych, które wykorzystywane są przez aplikacje)
    c. Użytkownik bazodanowy przeglądał rekordy bazodanowe wprowadzone przez innych użytkowników bazodanowych
    d. Inna ilość błędnych logowań do konta bazodanowego niż standardowa ilość.
    e. Użytkownik bazodanowy przeglądał w krótkim czasie rekordy z wielu baz danych.
    f. Przeglądanie przez użytkownika bazodanowego bardzo wielu danych sklasyfikowanych jako wrażliwe (sensitive)
    g. Użytkownik bazodanowy korzysta z danych, które powinny być osiągalne tylko poprzez aplikację - użytkownika serwisowego (aplikacyjnego)
    h. Użytkownik bazodanowy wykonał polecenia SQL, których sposób i cel odbiega od normy.
    i. Użytkownik bazodanowy przeszukał bazę danych za pomocą dynamicznego SQL w sposób nieprawidłowy.
34. Moduł Machine Learning musi dokonywać analizy poprzez porównanie normalnego zachowania użytkowników bazodanowych w oparciu o obserwowane modele zachowania specyficzne dla danej grupy użytkowników, dla całości organizacji, dla wybranych grup. Moduł musi dokonywać tej analizy w sposób automatyczny, prezentując wyniki analizy w formie incydentów i anomalii zachowania poszczególnych użytkowników bazodanowych.
35. Moduł Machine Learning musi zapewnić możliwość odróżnienia i określenia kto pracuje z systemem oraz z jakich danych korzysta:
    a. Użytkownika/pracownika/administratora
    b. Użytkownika aplikacyjnego
    c. Użytkownika uprzywilejowanego
    d. Metadanych
    e. Danych krytycznych dla firmy

36. **Moduł wizualizacji logów i zdarzeń bazodanowych** musi posiadać co najmniej poniższe funkcjonalności:
    a. Pobieranie logów i zdarzeń SQL z tablic natywnego audytu.
    b. Pobieranie zebranych logów audytowych z monitorowanych baz danych zebranych przez Moduł DAM/DBF.
    c. Generowanie wykresów, raportowanie,
    d. Posiadanie predefiniowanych raportów oraz możliwość tworzenia własnych raportów, dashbordów z logami i wykresami.
    e. Tworzenie oraz wykonywanie grupy działań i ich argumentów (playbooks),
    f. Przeglądanie, analizowanie, filtrowanie zebranych danych,
    g. Tworzenie polityk bezpieczeństwa (reguł) służących do wykrywania niezgodnych działań użytkowników bazodanowych.
    h. Integracja z Modułem DAM/DBF w celu wymiany informacji o danych, które za pomocą Modułu DAM/DBF zostały sklasyfikowane jako wrażliwie.

i. Logi bazodanowe muszą zostać przekazane do Modułu Machine Learning w celu dalszej analizy
j. Musi istnieć możliwość wyszukiwania i analizy zebranych logów bazodanowych za pomocą języka Search Processing Language lub Piped Processing Language
k. Udostępnić minimum 10 predefiniowanych scenariuszy UEBA z zakresu:
    - Wykrywania próby udzielenia dostępu do danych złośliwym aplikacjom.
    - Wykrywania próby uzyskania dostępu do danych przez atak typu SQL Injection
    - Wykrywania podejrzanych prób umieszczenia metaznaków (metacharacters) we wprowadzanych danych
    - Wykrywania próby utworzenia kont z uprawnieniami dostępu do danych dla nieistniejących lub nieautoryzowanych użytkowników.
    - Wykrywania anomalii w zachowaniu użytkowników aplikacyjnych, technicznych
    - Wykrywania nieoczekiwanych, nietypowych połączeń do bazy danych z niezaufanych źródeł
    - Wykrywania nietypowych ilości poleceń SQL wydawanych przez konta typu superuser w określonej bazie danych
    - Wykrywania prób uzyskania nieautoryzowanego dostępu do bazy danych za pomocą ataków typu brute force.
    - Wykrywania prób dostępu użytkowników w niestandardowych godzinach ich pracy
    - Wykrywanie błędów SQL w operacjach na danych sklasyfikowanych jako wrażliwe (sensitive)

37. **Agent bazodanowy** musi posiadać minimalnie poniższe funkcje:
    a. Agent bazodanowy przesyła kopię ruchu bazodanowego do Komponentu wykonawczego w celu wykonania analizy.
    b. Z uwagi na jak najmniejsze zużycie zasobów serwera bazodanowego, Agent bazodanowy nie może wykonywać analizy ruchu bazodanowego.
    c. Agent bazodanowy musi obsługiwać minimum następujące systemy operacyjne:
        i. AIX 7.1, 7.2,
        ii. HP-UX 11.31 (Itanium, PARSIC),
        iii. RedHat 8.x, 7.x, 6.x, 7 [PowerPC],
        iv. SLES SUSE: 15 SP [3,2,1,0], 12 SP [4,3], 11 SP [4,3]
        v. CentOS 8, 7
        vi. ORACLE LINUX UEK x86_64: 8, 7, 6 [5.4.17; 4.14.35; 4.1.12; 3.8.13; 2.6.39 kernel family]
        vii. Oracle LINUX 8, 7, 6, 5
        viii. Solaris 11 [SPARC], 11 [x86_64]
        ix. Windows Server 2019, 2016, 2012 R2, 2012
        x. Ubuntu 20.04; 18.04
        xi. IBM z/OS 1.13 lub nowsza
    d. Agent bazodanowy ma na celu wysyłanie informacji o lokalnej i sieciowej aktywności użytkowników do Komponentu wykonawczego. Komponent wykonawczy musi posiadać możliwości weryfikacji stanu działania Agenta bazodanowego.
    e. W przypadku gromadzenia zdarzeń zebranych za pomocą Agenta bazodanowego System musi obsługiwać funkcję przechowywania i przekazywania danych lub równoważną funkcjonalność zaprojektowaną w celu zapobiegania utracie zdarzeń (logów) z powodu niedostępności pozostałych komponentów Systemu.
    f. Agent bazodanowy musi posiadać możliwość pracy w trybach sniffing oraz inline. Jako sniffing rozumiany jest tryb pracy bez opóźnień z możliwością terminacji sesji w przypadku wykrycia nadużycia. Tryb inline rozumiany jest, jako wstrzymywanie ruchu od użytkownika do systemu bazodanowego, przesyłanie ruchu do jednostki

wykonawczej oraz oczekiwanie na decyzję czy zapytanie jest zgodne z polityką bezpieczeństwa.

g. Agent bazodanowy musi posiadać możliwość blokowania ruchu w przypadku wykrycia incydentu.
h. Agent bazodanowy musi wykrywać nowo zdefiniowane interfejsy bazy danych i automatycznie dodawać je do reguł monitorowania.
i. Agent bazodanowy musi posiadać możliwość definiowania reguł, zgodnie z którymi agent wybierać będzie ruch który ma był wysyłany do Komponentu wykonawczego monitorowania i ochrony baz danych.
j. Agent bazodanowy musi posiadać możliwość kompresji ruchu przesyłanego do modułów wykonawczych.
k. Agent bazodanowy musi monitorować połączenia szyfrowane – Oracle ASO, MSSQL, PostgreSQL, MySQL
l. Moduł DAM/DBF musi mieć możliwość zarządzania Agentami bazodanowymi z funkcjonalnościami nie mniej niż:
    - Wyświetlana informacja: o stanie Agenta bazodanowego, wersja agenta, adres IP, wersja monitorowanej bazy danych, adres IP Komponentu wykonawczego, z którym Agent bazodanowy obecnie działa.
    - Raport obciążenia sieci, obciążenie CPU serwera bazodanowego przez Agenta bazodanowego,
    - Wyłącznie, włączenie, restart Agenta bazodanowego,
    - Zdalna aktualizacja Agenta bazodanowego,
    - Ręczna lub automatyczna konfiguracja interfejsów bazodanowych, które Agent bazodanowy ma monitorować
    - Reguły wykluczające wysyłanie określonego ruchu przez Agenta bazodanowego do Modułu wykonawczego.
    - Informowanie administratora Systemu o zdarzeniach dotyczących Agenta bazodanowego np. Zmiana stanu (włączony, wyłączony),
    - Pobranie logów Agenta bazodanowego.
m. Agent bazodanowy musi mieć funkcjonalność działania bez klastrów komponentów wykonawczych jednocześnie działając w redundancji w przypadku awarii Komponentu wykonawczego. W przypadku awarii Komponentu wykonawczego Agent bazodanowy w konfiguracji ma wskazany zapasowy Komponent wykonawczy. Agent bazodanowy automatycznie musi się przepiąć na zapasowy Komponent wykonawczy.

V. Raportowanie

1. System musi posiadać gotowe szablony raportów dotyczące:
    a. Alarmów bezpieczeństwa
    b. Zdarzeń systemowych
    c. Zmian w profilach baz danych
    d. Monitorowania aktywności użytkowników w bazach danych
    e. Wykonanych testów podatności systemów, klasyfikacji usług oraz informacji w bazach danych.
    f. Zgodności z wymaganiami regulacji, m.in.: PCI, SOX,
2. Musi istnieć możliwość wykorzystania w raportach informacji z zewnętrznych źródeł co najmniej: Bazy SQL, plik CSV, Active Directory.
3. Musi istnieć możliwość tworzenia własnych raportów, zarówno w formie tekstowej jak i prezentacji graficznej, a także automatycznego, cyklicznego wysyłania raportów drogą e-mail. Raporty muszą być generowane minimum w standardach PDF, MSExcel (XLS), CSV.

VI. Usługi Instalacyjno-Wdrożeniowe

Usługi Instalacyjno-Wdrożeniowe Systemu obejmują:

1. Instalację i konfigurację dostarczonego Oprogramowania, w tym:
   1.1. Wykonanie Dokumentacji, o której mowa w pkt 9 i 10 poniżej,
   1.2. Instalację Oprogramowania Systemu w środowisku Zamawiającego,
   1.3. Skonfigurowanie Systemu zgodnie z Dokumentacją projektową.
2. Wykonanie testów akceptacyjnych wykazujących poprawność wdrożenia Systemu zgodnie z Dokumentacją projektową uzgodnioną na etapie umowy wykonawczej.
3. Przygotowanie procedur obsługi dot. eksploatacji, awarii, wykonania kopii zapasowych oraz ich odtworzenia, administrowania Systemem.
4. Ilości godzin Usług Instalacyjno-Wdrożeniowych będą każdorazowo rozliczane z łącznej puli godzin przeznaczonej na świadczenie Usług.
5. Usługi Instalacyjno-Wdrożeniowe będą realizowane na podstawie zatwierdzonego przez Jednostkę harmonogramu wdrożenia.
6. Na wniosek Wykonawcy Jednostka może wyrazić zgodę w formie elektronicznej (e-mail) lub dokumentowej na wykonanie prac instalacyjno-wdrożeniowych zdalnie w całości lub części, pod warunkiem przestrzegania przez Wykonawcę zasad bezpieczeństwa określonych przez Jednostkę. Jednostka ma prawo odmowy udostępnienia zdalnego dostępu w dowolnym momencie bez podawania przyczyny.
7. Wykonawcy nie przysługuje dodatkowe wynagrodzenie ani zwrot poniesionych jakichkolwiek kosztów z tytułu realizacji prac w siedzibie Zamawiającego.
8. Zamawiający dostarczy niezbędne zasoby informatyczne potrzebne do wdrożenia elementów Systemu.
9. Zamawiający dysponuje i akceptuje tylko platformą wirtualizacyjną Vmware, miejscem w szafie rack w przypadku wykorzystania platformy fizycznej (appliance), niezbędnym okablowaniem oraz wsparciem inżynierów IT w zakresie konfiguracji systemów leżących po stronie Zamawiającego.
10. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy, w zakresie Dokumentacji Projektowej, będzie podpisany bez zastrzeżeń Protokół Odbioru Projektu zawierający w szczególności: odbiór Dokumentacji Projektowej tj. Projektu Wdrożenia Systemu, Dokumentacji Testów Akceptacyjnych.
11. Potwierdzeniem prawidłowej realizacji przedmiotu Umowy w zakresie uruchomienia i skonfigurowania Systemu będzie podpisany bez zastrzeżeń Protokół Odbioru Wdrożenia Systemu zawierający w szczególności:
    11.1. odbiór Systemu ochrony baz danych wraz z wchodzącymi w skład Systemu Modułami i komponentami, na podstawie przeprowadzonych Testów Akceptacyjnych,
    11.2. odbiór Dokumentacji Powykonawczej,
    11.3. odbiór realizacji transferu wiedzy.

VII. Usługi Szkoleniowe

VII.1. Warsztaty wdrożeniowe z obsługi wdrażanego Sytemu

1. Wykonawca przeprowadzi, na etapie wdrożenia Systemu, co najmniej 8 godzinne warsztaty wdrożeniowe w języku polskim dla maks. 6 uczestników w zakresie instalacji, konfiguracji, zawansowanej obsługi i administracji wdrażanego Systemu; w szczególności warsztaty szkoleniowe polegać będą na:

a) zapewnieniu możliwości udziału osób wskazanych przez Zamawiającego przy przeprowadzanym przez inżyniera/inżynierów wdrożenia Systemu po stronie Wykonawcy,
b) udzielaniu odpowiedzi na pytania zadawane przez osoby wskazane przez Zamawiającego w zakresie zagadnień związanych z czynnościami administracyjnymi, funkcjonowaniem wdrożonego Systemu w środowisku produkcyjnym Zamawiającego, w tym omówieniu wraz z przeprowadzeniem praktycznych scenariuszy możliwości Systemu,
c) Zapewnieniu transferu wiedzy w zakresie konfiguracji Systemu i administracji Systemem, który musi być prowadzony na bieżąco w trakcie wdrożenia. Transfer wiedzy przeprowadzony zostanie w języku polskim.

2. Wykonawca zapewni możliwość konsultowania z trenerami tematów omawianych podczas warsztatów oraz opieki merytorycznej nad uczestnikami warsztatów w okresie 5 dni roboczych po zakończeniu warsztatów za pomocą poczty elektronicznej (udzielanie odpowiedzi drogą elektroniczną na pytania lub wątpliwości powstałe podczas warsztatów).
3. Warsztaty wdrożeniowe, będą realizowane w formule on-line z wykorzystaniem narzędzia komunikacji udostępnionego przez Zamawiającego lub w siedzibie Zamawiającego (w takim wypadku koszty dojazdu i pobytu trenera/ów pokrywa Wykonawca).

VII.2. Usługi szkoleniowe po wdrożeniu Systemu

1) Wymagane jest przeprowadzenie dwóch szkoleń dla 4-ech uczestników każde w terminach uzgodnionych z Zamawiającym w okresie obowiązywania umowy.
2) Czas trwania Szkolenia powinien wynosić minimum 40 godzin i być przeprowadzone w języku polskim lub angielskim.
3) Po zakończeniu szkolenia musi być możliwość odbycia egzaminu certyfikacyjnego w terminie uzgodnionym z Zamawiającym w okresie obowiązywania umowy.
4) Wszystkie koszty z wiązane z organizacją, przeprowadzeniem, zapewnieniem ewentualnego transportu uczestników, materiałów szkoleniowych itp. pokrywa Wykonawca.
5) Szkolenie musi zostać przeprowadzone z wykorzystaniem dedykowanego laboratorium treningowego przygotowanego przez Producenta dostarczonego systemu i zostać przeprowadzone przez certyfikowanego trenera przez Producenta.
6) Szkolenie musi obejmować swoim zakresem specjalistyczną wiedzę z dostarczanego systemu i obejmować przygotowanie uczestników w zakresie administrowania systemem, rozwiązywania problemów i utrzymania Systemu w szczególności obejmować tematykę opisaną poniżej:
   a) Architektura Systemu, najlepsze praktyki: scenariusze wdrożeń i konfiguracji,
   b) Elementy przeprowadzania symulowanych ataków na bazy danych: Oracle, MS SQL, MySQL wraz z modelowaniem ochrony przed atakami za pomocą Systemu
   c) Instalacja i konfiguracja najważniejszych elementów Sytemu,
   d) Instalacja Agenta bazodanowego w środowisku testowym na serwerach bazodanowych,
   e) Budowa i optymalizacja profili bazodanowych,
   f) Skanowanie baz danych w celu wyszukania zdefiniowanych danych wrażliwych,
   g) Tworzenie reguł bezpieczeństwa lub audytu. Monitorowanie dostępu do danych wrażliwych,
   h) Tworzenie wyjątków od zainstalowanych reguł,
   i) Skanowanie baz danych w celu znalezienia podatności lub błędów konfiguracyjnych,
   j) Integracja z zewnętrznymi systemami - SIEM, poczta elektroniczna, Active Directory, SQL, CSV,

k) Montowanie zewnętrznych zasobów CIFS,NFS do archiwizacji
l) Archiwizacja zebranych danych z logów
m) Backup środowiska Systemu
n) Raportowanie
o) Tworzenie i zarządzanie rolami i użytkownikami
p) Typowe zadania takie jak: tworzenie obiektów, tworzenie zasad, podstawowe zrozumienie reguł, interpretacja alertów systemowych i generowanie raportów,
q) Automatyzacja zadań administracyjnych,
r) Analiza wykrytych zdarzeń bezpieczeństwa – złamanie polityk bezpieczeństwa, rekcja na wycieki danych, zdarzenia nieuprawnionego dostępu do danych,
s) Troubleshoting - podstawowa obsługa i analiza możliwych błędów związanych z konfiguracją Systemu

VIII. Usługi wsparcia eksperckiego Wykonawcy

1. Usługi wsparcia eksperckiego Wykonawcy będą obejmowały konfigurowanie oraz optymalizację Systemu, a także konsultacje w zakresie obsługi generowanych zdarzeń, raportów, powiadomień.
2. Rodzaj usługi wsparcia eksperckiego Wykonawcy będzie precyzowany na etapie umowy wykonawczej, z zastrzeżeniem pkt 1 powyżej.
3. Ilości godzin usługi wsparcia eksperckiego Wykonawcy będą każdorazowo rozliczane z łącznej puli godzin przeznaczonej na świadczenie Usług
4. usługi wsparcia eksperckiego Wykonawcy będą realizowane na podstawie zatwierdzonego przez Jednostkę harmonogramu świadczenia usługi dostarczonego przez Wykonawcę w terminie do 7 dni kalendarzowych od daty zawarcia Umowy

IX. Wymagania w zakresie Gwarancji i wsparcia technicznego

1. W ramach udzielonej Gwarancji Wykonawca udostępni oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu Zgłoszenia Serwisowego Awarii, oprogramowanie to musi zapewnić Zamawiającemu brak ograniczeń, co do liczby dokonywanych Zgłoszeń Serwisowych w zakresie Awarii.
2. Wszelkie prace wykonywane przez Wykonawcę w Systemie nie mogą skutkować utratą praw gwarancyjnych do Systemu przez Zamawiającego.
3. W ramach udzielonej gwarancji Wykonawca będzie realizował Zgłoszenia Serwisowe Awarii Systemu w następujący sposób:
   3.1. **Awaria Krytyczna**, wada skutkująca nieprawidłowym działaniem dowolnego Modułu Systemu powodująca albo całkowity brak możliwości korzystania z Modułu albo takie ograniczenie możliwości korzystania z niego, że przestaje on spełniać swoje podstawowe funkcje. Czas odnalezienia obejścia lub Naprawy do 12 godzin od chwili Zgłoszenia Serwisowego przez Zamawiającego;
   3.2. **Awaria Niekrytyczna** wada skutkująca nieprawidłowym działaniem Systemu powodująca ograniczenie korzystania z Systemu, nie powodując skutków opisanych dla Awarii Krytycznej. Czas odnalezienia obejścia lub Naprawy do 72 godzin od chwili Zgłoszenia Serwisowego przez Zamawiającego.
4. Wszelkie Awarie będą zgłaszane przez Zamawiającego za pomocą udostępnionego przez Wykonawcę oprogramowania, o którym mowa w punkcie 1 powyżej.

5. W przypadku potrzeby konsultacji z działem wsparcia technicznego Producenta lub wydania poprawki do Systemu przez Producenta, na wniosek Wykonawcy złożony w formie elektronicznej, Zamawiający zawiesi czas usunięcia Awarii do czasu udostępnienia poprawki.
6. Obsługa Zgłoszeń Serwisowych musi obejmować co najmniej:
    a) aktualizację i konfigurację Systemu przez Wykonawcę,
    b) rozwiązywanie przez Wykonawcę zgłaszanych problemów związanych z działaniem i obsługą Systemu.
    c) Wykonawca w ramach udzielonej gwarancji na wezwanie i w terminie uzgodnionym z Zamawiającym zainstaluje poprawki, usprawnienia i nowe wersje oprogramowania dla Systemu, udostępniane przez producenta wdrożonego Systemu.
7. W ramach udzielonej gwarancji Zamawiającemu przysługuje prawo do samodzielnej instalacji i używania wszystkich poprawek, usprawnień i nowych wersji Systemu udostępnianych przez producenta Systemu bez ponoszenia dodatkowych kosztów finansowych przez Zamawiającego. Powyższe nie może skutkować utratą uprawnień gwarancyjnych przysługujących Zamawiającemu.
8. Świadczenia gwarancyjne w zakresie Sprzętu (o ile dotyczy – jeżeli Wykonawca oferuje rozwiązanie oparte o Sprzęt fizyczny) realizowane będą z uwzględnieniem następujących zasad:
    8.1. usługi gwarancyjne będą świadczone przez producenta Sprzętu lub podmiot posiadający autoryzację producenta Sprzętu, w miejscu użytkowania Sprzętu, jeśli jednak naprawa Sprzętu w tym miejscu okaże się niemożliwa, naprawa może zostać wykonana w innym miejscu; usługi gwarancyjne Sprzętu będą świadczone w Dni Robocze, w godzinach od 8:00 do 16:00;
    8.2. w zakres usług gwarancyjnych wchodzi również dojazd i praca osób wykonujących czynności gwarancyjne w imieniu Wykonawcy oraz pozostałe koszty niezbędne do świadczenia usług gwarancyjnych, w tym koszty dostawy i odbioru wymienionych urządzeń, niezależnie od podmiotu wykonującego usługę gwarancyjną;
    8.3. na czas naprawy Sprzętu poza miejscem jego użytkowania Sprzęt zabierany będzie bez dysku twardego lub innych elektronicznych nośników informacji (o ile dotyczy). Po zwrocie naprawionego sprzętu dysk twardy lub inne elektroniczne nośniki informacji zostaną ponownie zamontowane przez Wykonawcę, po czym nastąpi sprawdzenie poprawności funkcjonowania naprawionego Sprzętu;
    8.4. w przypadku nieodwracalnej awarii dysku twardego lub innych elektronicznych nośników informacji (o ile dotyczy) będą one wymienione przez Wykonawcę na nowy, wolny od wad, o parametrach nie gorszych niż te, które uległy awarii. Uszkodzony dysk twardy lub inne elektroniczne nośniki informacji nie będzie podlegał zwrotowi Wykonawcy;
    8.5. Wykonawca zobowiązuje się zapewnić, że każda osoba wykonująca usługi gwarancyjne w miejscu wykorzystywania Sprzętu, będzie posiadała dokument tożsamości i pisemne upoważnienie do wykonywania napraw i czynności objętych gwarancją, potwierdzone przez Wykonawcę oraz będzie zobligowana stosować się do przepisów wewnętrznych Jednostki dotyczących ruchu osobowego i materiałowego w jej siedzibie;
    8.6. Usługi gwarancyjne wykonywane będą przy wykorzystaniu materiałów, sprzętu i narzędzi Wykonawcy, chyba że naprawa zostanie wykonana w punkcie serwisowym producenta nie będącego Wykonawcą;
    8.7. Części lub podzespoły, które zostaną wymienione w ramach usług gwarancyjnych stają się własnością Wykonawcy, który zobowiązuje się do ich bezpośredniego odbioru od Jednostek i utylizacji zgodnie z obowiązującymi przepisami;

8.8. W przypadku wymiany części lub podzespołów, Wykonawca zobowiązuje się dostarczyć kartę gwarancyjną dla wymienionych elementów Sprzętu, (jeżeli ich producent udziela odrębnej gwarancji);

8.9. W przypadku niemożności dotrzymania terminu naprawy Sprzętu, Wykonawca zobowiązany jest do dostarczenia w pierwszym Dniu Roboczym po upływie tego terminu, na swój koszt, do siedziby Jednostki, Sprzętu zastępczego o parametrach nie gorszych niż Sprzęt, który podlega naprawie, na cały okres naprawy Sprzętu, posiadającego stosowne certyfikaty/ dokumenty;

8.10. W razie niedokonania naprawy Sprzętu (usunięcia awarii) w terminie:

a) dopuszcza się dokonanie naprawy siłami własnymi Zamawiającego lub Jednostki na koszt Wykonawcy lub zlecenie naprawy osobie trzeciej na koszt Wykonawcy, z zachowaniem praw wynikających z Gwarancji i rękojmi za wady Sprzętu, bez dodatkowego wezwania Wykonawcy do wykonania usługi gwarancyjnej. W przypadku skorzystania z powyższego uprawnienia, Wykonawca zostanie niezwłocznie powiadomiony w formie pisemnej o tym fakcie oraz zakresie zleconych prac (napraw, zmian, itp.). W takim przypadku Wykonawca zobowiązany jest zapłacić Jednostce – w terminie wskazanym przez tę Jednostkę, nie krótszym jednak niż 14 dni kalendarzowych – kwotę stanowiącą równowartość poniesionego przez Jednostkę kosztów wykonania tych prac.

b) okres Gwarancji przedłuża się o czas trwania naprawy, a w przypadku gdy ten sam element Sprzętu po raz trzeci ulegnie awarii podlegającej naprawie gwarancyjnej, Wykonawca zobowiązany jest dokonać wymiany elementu Sprzętu na nowy, o takich samych lub lepszych funkcjonalnościach oraz takich samych lub lepszych parametrach, bez dodatkowego wezwania Wykonawcy. Wymiana Sprzętu na nowy powinna zostać potwierdzona protokołem, który zawierał będzie co najmniej datę dostawy nowego Sprzętu. W takiej sytuacji termin gwarancji biegnie na nowo od chwili dostarczenia i potwierdzenia protokolarnego dostawy nowego Sprzętu.

8.11. Rozbudowa lub modyfikacje Sprzętu nie mogą prowadzić do utraty uprawnień wynikających z rękojmi za wady urządzenia lub utraty prawa do korzystania z usług gwarancyjnych.

X. Dokumentacja Projektowa

1. Wykonawca w uzgodnieniu z Zespołem Odbiorowym opracuje i dostarczy następującą Dokumentację Projektową:

a) Projekt Wdrożenia Systemu, który musi zawierać, w szczególności: 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 Zamawiającego, harmonogram wdrożenia,

b) Dokumentację Testów Akceptacyjnych wdrożenia Systemu, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z opisem przedmiotu zamówienia. Testy akceptacyjne mają być realizowane w środowisku produkcyjnym, zgodnie ze scenariuszami testowymi opracowanymi przez Wykonawcę i zaakceptowanymi przez Zespół Odbiorowy na etapie odbioru Dokumentacji Projektowej.

3. Dokumentacja musi być dostarczona w wersji elektronicznej i napisana w języku polskim.
Procedury i instrukcje producenta mogą być dostarczone w języku angielskim lub polskim.

XI. Dokumentacja Powykonawcza

Dokumentacja Powykonawcza ma zawierać, w szczególności:

1. Szczegółową konfiguracją oraz opis infrastruktury technicznej wdrażanego Systemu,
2. Opis struktury i konfiguracji Systemu, w tym pliki konfiguracyjne, skrypty uruchomieniowe, skrypty zatrzymujące, itp.,
3. Zalecenia i procedury eksploatacyjne oraz zalecenia w zakresie konserwacji Systemu, w tym przeglądu logów wraz z procedurami.
4. Wykonawca opracuje i dostarczy Dokumentację Powykonawczą, która musi być jednym spójnym dokumentem, bez względu na jej objętość i musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji Systemu, w szczególności:
   a) procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji Systemu,
   b) procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
   c) instrukcje dla użytkowników i administratorów, w tym procedury zarządzania zdarzeniami dotyczącymi bezpieczeństwa,
   d) inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia Systemu, uzgodnione z przedstawicielem Zespołu Odbiorowego
5. Dokumentacja Powykonawcza powinna być dostarczona w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje Producenta mogą być dostarczone w języku angielskim lub polskim

XII. Dysponowanie Sprzętem

1. W przypadku gdy dostarczenie, wdrożenie i uruchomienie Systemu wymagać będzie dostawy Sprzętu, korzystanie z tego Sprzętu będzie miało miejsce tytułem dzierżawy przez czas określony 36 miesięcy od dnia podpisania przez Odbiorcę bez zastrzeżeń Protokołu Odbioru Sprzętu, z uwzględnieniem następujących postanowień:
   1) wynagrodzenie Wykonawcy określone w Umowie obejmuje wszelkie koszty związane z dzierżawą Sprzętu w całym okresie obowiązywania Umowy i Wykonawcy nie będzie przysługiwać dodatkowe wynagrodzenie z tego tytułu;
   2) Zamawiający nie będzie zobowiązany do czynienia jakichkolwiek nakładów na Sprzęt – wszelkie nakłady, w tym niezbędne do prawidłowego działania i funkcjonowania Sprzętu oraz jego zachowania w stanie niepogorszonym obciążają wyłącznie Wykonawcę w ramach udzielonej Gwarancji;
   3) dopuszczalna jest poddzierżawa lub oddanie do bezpłatnego używania Sprzętu na rzecz Jednostek, jeśli wymagać będzie tego korzystanie z Systemu zgodnie OPZ lub Umową;
   4) po upływie terminu wskazanego w zdaniu pierwszym, Wykonawca zobowiązuje się odebrać dostarczony Sprzęt, na swój koszt, swoim staraniem i na własne ryzyko z miejsca, do którego dokonano dostawy Sprzętu; Strony ustalą wspólnie termin odbioru Sprzętu przez Wykonawcę, a w razie braku możliwości dojścia do porozumienia w tym zakresie, Odbiorca wyznaczy Wykonawcy wiążący termin na dokonanie odbioru Sprzętu, nie krótszy niż 7 dni kalendarzowych;
   5) w przypadku niedokonania odbioru Sprzętu w terminie, o którym mowa w pkt 4), Zamawiający nie będzie ponosić odpowiedzialności z tytułu utraty lub uszkodzenia sprzętu, nie jest i nie będzie zobowiązany do ponoszenia żadnych opłat, wynagrodzeń ani

innych kosztów w szczególności z tytułu bezumownego korzystania ani wobec Wykonawcy ani jakichkolwiek podmiotów trzecich;

6) w przypadku niedokonania odbioru Sprzętu, w terminie określonym w pkt 4), Zamawiający będzie użytkował bez kosztowo (tj. Wykonawcy nie będzie z tego tytułu przysługiwało jakiekolwiek wynagrodzenie) Sprzęt zgodnie z dotychczasowym przeznaczeniem lub traktować Sprzęt jako odpad i przeznaczy go do zagospodarowania zgodnie z właściwymi przepisami o odpadach, w tym w szczególności do utylizacji, na koszt Wykonawcy; Wykonawca jednocześnie zobowiązuje się ponieść koszty, o których mowa w niniejszym punkcie, w wysokości określonej przez Zamawiającego;
7) przepisy o dzierżawie albo inne przepisy stosowane odpowiednio do dzierżawy nie mogą być interpretowane w sposób ograniczający lub utrudniający Zamawiającemu korzystanie z Systemu w sposób określony w Umowie lub OPZ, ani powodować powstania z tego tytułu dodatkowych zobowiązań, w tym zobowiązań pieniężnych; W razie wątpliwości, przyjmuje się, że Zamawiającemu, przysługują w tym zakresie wszelkie prawa niezbędne do zrealizowania celu Umowy.
8) W przypadku świadczenia usług gwarancyjnych sprzętu, jeśli naprawa sprzętu będzie wymagała wykonania tej usługi poza siedzibą Zmawiającego, Zamawiający każdorazowo nie wyraża zgody na przekazanie sprzętu do naprawy wraz z zapisanymi danymi tj. wszystkie nośniki danych zainstalowane w sprzęcie nie mogą opuścić lokalizacji Zamawiającego.
9) W przypadku zakończenia okresu dzierżawy sprzętu wszystkie nośniki danych (dyski hdd/ssd ; card memory ; pamięci RAM itp.) pozostają w lokalizacji dostarczenia i użytkowania w/w sprzętu tj. w siedzibie danego sądu.