**Zakup systemu DAM (Database Activity Monitoring)**

1. Przedmiotem zamówienia jest :
   1. sprzedaż, dostarczenie, skonfigurowanie i uruchomienie Systemu, zgodnie ze specyfikacją, w tym:
2. przeprowadzenie Wdrożenia, w tym wykonanie i dostarczenie Projektu Technicznego, Planu Testów Akceptacyjnych oraz Dokumentacji powdrożeniowej oraz poinstruowanie 4 przedstawicieli Zamawiającego z zakresu działania Systemu;
   1. zapewnienie Zamawiającemu - prawa do korzystania (na zasadach subskrypcji) z Systemu przez okres 36 miesięcy dla 20 serwerów bazodanowych (serwer bazodanowy rozumiany jako instancja systemu operacyjnego, na której zainstalowany został silnik bazodanowy),
   2. świadczenie Gwarancji dla Systemu przez okres 36 miesięcy , w tym zapewnienie świadczenie wsparcia producenta (Opieki serwisowej), poprzez wydanie odpowiedniego dokumentu na rzecz Zamawiającego, potwierdzającego prawo dostępu do wsparcia producenta w ww. okresie, zgodnie z ogólnymi warunkami producenta;
   3. świadczenie rzecz Zamawiającego Usługi Wsparcia (konsultacji) w maksymalnym wymiarze 2000 roboczogodzin obejmujące konfigurowanie oraz optymalizację Systemu, a także konsultacje w zakresie obsługi generowanych zdarzeń, raportów

**Specyfikacja Systemu**

# Wymagania ogólne

* 1. Wymagane jest dostarczenie dedykowanego Systemu klasy Database Activity Monitoring z możliwością blokowania zdarzeń (Database FireWall).
  2. Działanie Systemu nie może powodować degradacji wydajności i baz danych.
  3. System musi pochodzić tylko z oficjalnych kanałów dystrybucyjnych producenta na terenie Unii Europejskiej.
  4. Wszystkie Moduły Systemu muszą pochodzić od jednego producenta.
  5. 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.
  6. Oferowane rozwiązanie ma stanowić jednolity i kompleksowy System składający się z wymaganych Modułów. Skalowalny i elastyczny w kontekście potencjalnej rozbudowy tj. objęcia ochroną kolejne serwery bazodanowe.
  7. Wymaganiem Zamawiającego jest, aby każdy Moduł posiadał maksymalnie jedną Konsolę zarządzającą.
  8. Oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
  9. Oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
  10. Zamawiający wymaga, aby wszystkie elementy i Moduły dostarczanego Systemu były w najnowszej wersji (tzn. najnowszej udostępnionej przez Producenta rozwiązania) na dzień wdrożenia Systemu.
  11. Żaden z Modułów i elementów oferowanego Systemu na dzień składania ofert nie może być przeznaczony przez Producenta do wycofania z produkcji lub sprzedaży.
  12. Zamawiający wymaga, aby System składał się z minimum trzech wyróżnionych modułów:
      1. Moduł DAM/DBF (Database Activity Monitoring/ Database FireWall),
      2. Moduł wizualizacji logów i zdarzeń bazodanowych
      3. Moduł ML (Machine Learning) – automatycznego wykrywania anomalii w ruchu SQL, i został wdrożony zgodnie z wymaganiami Zamawiającego w zakresie niezbędnym do poprawnego działania tego Systemu.

# 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. Ilość licencji 20 szt. serwerów bazodanowych
3. System musi monitorować bazy danych zainstalowane on-site (w serwerowni Zamawiającego) i współpracować z systemem operacyjnym Redhat 6.6 (i wyższy) oraz Windows Serwer 2016 (i wyższy)
4. 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 v.9, v.10 SE,EE |
| DB2 | 10 i wyższy |
| MySQL | 8.0, 5.7 |
| MariaDB Server | 10.6-2 |
| MSSQL | 2016 |
| 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 |

1. System musi składać się z opisanych poniżej modułów, w skład których wchodzą wskazane komponenty:
   * + **Moduł DAM/DBF musi składać się z:**
2. **Komponentu wykonawczego**, analizującego bazodanowy ruch,
3. **Komponentu zarządzającego DAM/DBF** dla wielu Komponentów wykonawczych,
4. **Agenta bazodanowego** – programu instalowanego na serwerze baz danych,
   * + **Moduł Machine Learning musi składać się z:**
5. **Komponentu analitycznego**, który za pomocą algorytmów machine learning (ML) analizuje zdarzenia pochodzące z ruchu SQL monitorowanych baz danych dostarczone przez Moduł DAM/DBF
6. **Komponentu zarządzającego** dla wielu komponentów analitycznych (ML)
   * + **Moduł wizualizacji logów i zdarzeń bazodanowych**
7. **Komponentu wizualizującego** dane wraz z funkcjonalnością pobierania zdarzeń i logów SQL z natywnych tablic audytowych baz danych oraz z Modułu DAM/DBF.
8. Zamawiający może zainstalować dowolną liczbę modułów i komponentów (pkt. 5 a, b, d, e, f) w ramach wykupionej pojedynczej licencji w modelu subskrypcyjnym dla serwera bazodanowego. W celu zwiększenia wydajności oraz niezawodności Zamawiający może łączyć Komponenty wykonawcze (pkt. 5a) w klastry wydajnościowe.
9. Komponenty Systemu z pkt. 5 (a, b, d, e) muszą zostać dostarczone jako gotowe maszyny wirtualne (ang. virtual appliance) dla wirtualizatora VMWare.

# Wymagania funkcjonalne

1. **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:
   1. Dostępu do bazy danych w niestandardowych godzinach.
   2. Używanie użytkownika bazodanowego (np. administratora baz danych lub innego) kont serwisowych (np. tych, które wykorzystywane są przez aplikacje)
   3. Użytkownik bazodanowy przeglądał rekordy bazodanowe wprowadzone przez innych użytkowników bazodanowych
   4. Inna ilość błędnych logowań do konta bazodanowego niż standardowa ilość.
   5. Użytkownik bazodanowy przeglądał w krótkim czasie rekordy z wielu baz danych.
   6. Przeglądanie przez użytkownika bazodanowego bardzo wielu danych sklasyfikowanych jako wrażliwe (sensitive)
   7. Użytkownik bazodanowy korzysta z danych, które powinny być osiągalne tylko poprzez aplikację - użytkownika serwisowego (aplikacyjnego)
   8. Użytkownik bazodanowy wykonał polecenia SQL, których sposób i cel wykonania jest podejrzany.
   9. Użytkownik bazodanowy przeszukał bazę danych za pomocą dynamicznego SQL w sposób nieprawidłowy.
2. 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.
3. Moduł Machine Learning musi zapewnić możliwość odróżnienia i określenia kto pracuje z systemem oraz z jakich danych korzysta:
   1. Użytkownika/pracownika/administratora
   2. Użytkownika aplikacyjnego
   3. Użytkownika uprzywilejowanego
   4. Metadanych
   5. Danych krytycznych dla firmy
4. Moduł DAM/DBF musi zapewnić poniższe funkcjonalności:
   1. Aktywne wyszukiwanie i klasyfikacja usług bazodanowych w sieci
      1. 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.
      2. 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.
   2. 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

1. Moduł DAM/DBF musi mieć przygotowane testy podatności zgodne ze standardem CIS i DISA STIG dla minimum baz danych ORACLE, MSSQL, MySQL
2. 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.
3. Moduł DAM/DBF musi umożliwić definiowanie polityki monitorowania lub audytowania uwzględniając nie mniej niż następujące kryteria:
   1. użytkownik bazodanowy,
   2. użytkownik aplikacyjny,
   3. tabele, kolumny,
   4. baza danych, schemat bazy danych,
   5. ilość wystąpień zdarzeń w czasie,
   6. dostęp do danych wrażliwych (sklasyfikowanych za pomocą funkcjonalności Wyszukiwanie i klasyfikacja informacji w bazach danych) ,
   7. wielkość odpowiedzi (ilość rekordów) na zapytanie SQL
   8. czas odpowiedzi bazy danych na zapytanie SQL,
   9. źródłowy adres IP
   10. dzień tygodnia i czas dnia
   11. wbudowane i predefiniowane sygnatury (np. CVE), sygnatury własne
   12. Polecenia SQL uprzywilejowane – grant, alter, drop, restore, create, deny, kill, backup, shutdown, truncate, revoke,
   13. Analiza odpowiedzi na zapytanie (SQL response) oraz analiza zmiennych typu Input Bind Variables
4. 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
5. 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.
6. Moduł DAM/DBF musi zapewnić definiowanie reguł dostępu użytkowników do poszczególnych baz danych na poziomie sieciowym.
7. 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:
   1. Zapisane bazy i schematy, z których użytkownik bazodanowy korzysta
   2. Tabele i polecenia SQL (select, insert, update, delete), z których użytkownik bazodanowy korzysta
   3. Parametry połączenia użytkownika:
      1. Adres IP
      2. Aplikacja kliencka
      3. Nazwa komputera (OS Hostname)
      4. Nazwa użytkownika systemu operacyjnego (OS User)
      5. Zapytania SQL

Na podstawie powyższej listy definiowane są reguły polityki bezpieczeństwa.

1. Ruch SQL wykryty przez polityki bezpieczeństwa Modułu DAM/DBF jako zagrożenie nie może być ruchem przekazanym do profilowania.
2. 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.
3. Moduł DAM/DBF musi zapewnić możliwość definiowania oddzielnych reguł dostępu w odniesieniu do tabel z danymi wrażliwymi, sklasyfikowanymi przez zdefiniowanych poprzez funkcjonalność klasyfikacji (za pomocą funkcjonalności Wyszukiwanie i klasyfikacja informacji w bazach danych)
4. 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.
5. 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.
6. Moduł DAM/DBF musi posiadać opcję blokowania ruchu wykorzystującego podatności wykryte w bazach danych poprzez funkcjonalność testowania podatności systemów bazodanowych.
7. Moduł DAM/DBF musi wykrywać komendy wykonywane na systemie zarządzania bazą danych (poza silnikiem SQL) jak np. Export Direct w DB Oracle
8. 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.
9. Musi istnieć możliwość zmiany wszystkich haseł dla natywnych użytkowników oferowanego Modułu DAM/DBF (użytkownicy CLI, GUI, SQL oraz systemowi).
10. 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.
11. 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.
12. **Moduł wizualizacji logów i zdarzeń bazodanowych** musi posiadać co najmniej poniższe funkcjonalności:
13. Pobieranie logów i zdarzeń SQL z tablic natywnego audytu.
14. Pobieranie zebranych logów audytowych z monitorowanych baz danych zebranych przez Moduł DAM/DBF.
15. Generowanie wykresów, raportowanie,
16. Posiadanie predefiniowanych raportów oraz możliwość tworzenia własnych raportów, dashbordów z logami, wykresami.
17. Tworzenie oraz wykonywanie grupy działań i ich argumentów (playbooks),
18. Przeglądanie, analizowanie, filtrowanie zebranych danych,
19. Tworzenie polityk bezpieczeństwa (reguł) służących do wykrywania niezgodnych działań użytkowników bazodanowych.
20. Integracja z Modułem DAM/DBF w celu wymiany informacji o danych, które za pomocą Modułu DAM/DBF zostały sklasyfikowane jako wrażliwie.
21. Logi bazodanowe muszą zostać przekazane do Modułu Machine Learning w celu dalszej analizy
22. Musi istnieć możliwość wyszukiwania i analizy zebranych logów bazodanowych za pomocą języka Search Processing Language lub Piped Processing Language
23. 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)
24. **Agent Modułu DAM/DBF** musi posiadać minimalnie poniższe funkcje:
    1. Agent przesyła kopię ruchu bazodanowego do Komponentu wykonawczego w celu wykonania analizy.
    2. Agent nie może wykonywać analizy ruchu bazodanowego (z uwagi na jak najmniejsze zużycie zasobów serwera bazodanowego).
    3. Agent bazodanowy musi obsługiwać minimum następujące systemy operacyjne:
       1. AIX 7.1, 7.2,
       2. HP-UX 11.31 (Itanium, PARSIC),
       3. RedHat 8.x, 7.x, 6.x, 7 [PowerPC],
       4. SLES SUSE: 15 SP [3,2,1,0], 12 SP [4,3], 11 SP [4,3]
       5. CentOS 8, 7
       6. 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]
       7. Oracle LINUX 8, 7, 6, 5
       8. Solaris 11 [SPARC], 11 [x86\_64]
       9. Windows Server 2019, 2016, 2012 R2, 2012
       10. Ubuntu 20.04; 18.04
       11. IBM z/OS 1.13 lub nowsza
25. Musi zostać dostarczony wraz z aplikacjami monitorującymi ruch lokalnie na serwerach bazodanowych (zwanymi dalej aplikacją agenta). Aplikacja agenta ma na celu wysyłanie informacji o lokalnej aktywności użytkowników do Komponentu wykonawczego. Komponent wykonawczy musi posiadać możliwości weryfikacji stanu działania agenta.
26. 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.
27. Agent 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.
28. Agent musi posiadać możliwość blokowania ruchu w przypadku wykrycia incydentu.
29. Agent musi wykrywać nowo zdefiniowane interfejsy bazy danych i automatycznie dodawać je do reguł monitorowania.
30. Agent musi posiadać możliwość definiowania reguł, zgodnie z którymi agent wybierać będzie ruch który ma był wysyłany do Komponentu wykonawczego monitorowania i ochrony baz danych.
31. Agent musi posiadać możliwość kompresji ruchu przesyłanego do modułów wykonawczych.
32. Agent musi monitorować połączenia szyfrowane – Oracle ASO, MSSQL, PostgreSQL, MySQL
33. Moduł DAM/DBF musi mieć możliwość zarządzania Agentami z funkcjonalnościami nie mniej niż:
    * Wyświetlana informacja: o stanie Agenta, wersja agenta, adres IP, wersja monitorowanej bazy danych, adres IP Komponentu wykonawczego, z którym agent obecnie działa.
    * Raport obciążenia sieci, obciążenie CPU serwera bazodanowego przez Agenta,
    * Wyłącznie, włączenie, restart Agenta
    * Zdalna aktualizacja Agenta
    * Ręczna lub automatyczna konfiguracja interfejsów bazodanowych, które Agent ma monitorować
    * Reguły wykluczające wysyłanie określonego ruchu przez Agenta do Modułu DAM/DBF.
    * Informowanie administratora Systemu o zdarzeniach dotyczących Agenta np. Zmiana stanu (włączony, wyłączony),
    * Pobranie logów Agenta
34. Agent Modułu DAM/DBF musi mieć funkcjonalność działania bez klastrów komponentów wykonawczych jednocześnie działając w redundancji w przypadku awarii Komponentu wykonawczego. W przypadku awarii Komponentu wykonawczego Agent w konfiguracji ma wskazany zapasowy Komponent wykonawczy. Agent automatycznie musi się przepiąć na zapasowy Komponent wykonawczy.
35. **System** 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.
36. 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.
37. Komponenty wykonawcze muszą mieć możliwość zbudowania dwóch typów klastrów n+1:

a. Komponenty wykonawcze muszą 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.

1. Konsole zarządzające oferowanego Systemu muszą być dostępne poprzez interfejs przeglądarki Web w celu eliminacji konieczności instalacji dodatkowego oprogramowania na stacji administratora.
2. Wymagane jest zarządzanie zorientowane zadaniowo. Oznacza to, że musi istnieć mechanizm informowania administratora o wykonaniu/nie wykonaniu na czas zadania zleconego innym użytkownikom Systemu.
3. Aktualizacja Systemu musi być dostępna zarówno poprzez ręczne pobranie zawartości ze strony producenta jak i automatycznie, poprzez zdefiniowanie terminów wykonania procedury aktualizacji.
4. System musi zostać dostarczony w formie kompletnego rozwiązania tj. nie może wymagać do działania żadnego oprogramowania firm trzecich np. zewnętrznych baz danych.
5. Uwierzytelnianie użytkowników i administratorów Systemu musi być możliwe za pomocą:
   1. Użytkownika lokalnego
   2. protokołu RADIUS
   3. poprzez integrację z Active Directory
6. Komponent zarządzający musi posiadać wbudowany mechanizm RBAC, który umożliwia integrację z Active Directory poprzez przypisanie roli w zależności od przynależności do określonej grupy w Active Directory.
7. Całość konfiguracji Systemu oraz repozytorium logów musi być przechowywana na Komponentach zarządzających w Module DAM/DBF lub Module wizualizującym dane.
8. Komponent zarządzający Modułu DAM/DBF musi wyświetlać w czasie rzeczywistym logi na jednej planszy (dashboard):
9. zdarzenia z ruchu bazodanowego, które łamią polityki bezpieczeństwa (security logs).
10. 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 itp.
11. Komponent wykonawczy Modułu DAM/DBF musi zapewnić możliwość monitorowania ruchu SQL w trybach :
12. Transparent In-line Bridge (warstwa L2 ISO/OSI)
13. SPAN (analiza kopii ruchu)
14. Agent (program instalowany na serwerze baz danych, który przesyła kopię ruchu bazodanowego do modułu wykonawczego w celu wykonania analizy). Agent nie wykonuje analizy ruchu bazodanowego.
15. System musi mieć otwarte REST API, które umożliwia konfigurację rozwiązania, pobieranie danych z Systemu oraz możliwość integracji Systemu z innymi aplikacjami.
16. Musi być możliwość uruchomienia centralnego Komponentu zarządzającego Modułu DAM/DBF w przypadku korzystania z wielu Komponentów zarządzających.
17. Komponent zarządzający Modułu DAM/DBF musi posiadać następujące funkcje/opcje:
18. Informacje o wgranej licencji Systemu
19. Zarządzania użytkownikami (administratorami) systemu za pomocą RBAC
20. Zarządzania, ustawiania wielkości budowanego profilu bazodanowego
21. Konfiguracji połączenia z AD w celu logowania się do Systemu za pomocą AD
22. Ustawienia siły hasła: ilość dni ważności hasła, minimalna ilość znaków, wielkie/małe litery, znaki specjalne, inne hasło od poprzedniego (minimum 12 ostatnich).
23. Konfiguracja serwera PROXY http w celu pobierania aktualizacji z sieci Internet.
24. Dołożenia sterowników, za pomocą których można podłączyć się do bazy danych w celu wykonania skanowania podatności i klasyfikacji danych
25. Możliwość definiowania słów kluczowych, które można wykorzystywać np. przy raportach
26. Dodawanie komentarza do polityk bezpieczeństwa i audytu
27. Status zadań cyklicznych w podziale na kategorie: anulowane, wykonywane, zakończone z błędami, zatrzymane, w oczekiwaniu na uruchomienie
28. Eksportowanie konfiguracji Modułu DAM/DBF z poziomu GUI
29. Konfiguracja autoryzacji Komponentów wykonawczych w Komponentach zarządzania za pomocą certyfikatów.

# Raportowanie

1. System musi posiadać gotowe szablony raportów dotyczące:
   1. Alarmów bezpieczeństwa
   2. Zdarzeń systemowych
   3. Zmian w profilach baz danych
   4. Monitorowania aktywności użytkowników w bazach danych
   5. Wykonanych testów podatności systemów, klasyfikacji usług oraz informacji w bazach danych.
   6. 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, XLSX, CSV.