Wymagania funkcjonalne oraz jakościowe Systemu DAM

ID	Spełnia wymaganie (TAK/NIE)	Opis Wymagania
DAM.W.K1		System musi zapewniać automatyczną lub konfigurowalną identyfikację danych wrażliwych, umożliwiać wykorzystanie mechanizmów wykrywania danych, klasyfikacji i raportowania uprawnień
DAM.W.K2		System musi zapewniać możliwość identyfikacji źródeł danych poprzez skanowanie sieci dla minimum: • MSSQL TDS • ORACLE TNS • POSTGRES • MYSQL • MONGODB • PERCONA
DAM.W.K3		Klasyfikacja danych musi bazować na analizie zawartości. System może wykorzystywać metadane jako element pomocniczy (nazwy kolumn, tabel).
DAM.W.K4		Rozwiązanie musi zawierać system analityczny w celu identyfikacji danych osobowych oraz statycznej analizy zidentyfikowanych danych osobowych.
DAM.W.K5		System musi umożliwiać klasyfikację danych niemożliwych do opisania wyrażeniami regularnymi poprzez analizę słownikową i mechanizmy samouczące się. Mechanizmy te muszą umożliwiać rozbudowę o nowe typy danych.
DAM.W.001		System musi wykrywać dostęp użytkowników do bazy danych w niestandardowych godzinach pracy, nieujętych w harmonogramach aktywności.
DAM.W.002		System musi automatycznie wykrywać wykorzystywanie przez użytkownika kont administracyjnych i serwisowych w bazie danych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

DAM.W.003		System musi wykrywać aktywność poszczególnych kont bazodanowych, polegających na przeglądaniu rekordów bazodanowych wprowadzonych przez innych użytkowników bazodanowych.
DAM.W.004		System musi wykrywać zmiany zachowań użytkownika w minimalnym zakresie dotyczącym: • zmiany czasu aktywności, • dostępu do nowo utworzonych obiektów, • ilościowych zmian w dostępie do danych, • dostępu do danych, które powinny być osiągalne tylko poprzez aplikację lub konto techniczne.
DAM.W.005		System musi wykrywać anomalie błędnych logowań do konta bazodanowego innych niż zdefiniowana liczba.
DAM.W.006		System musi umożliwiać identyfikację i klasyfikację z wykorzystaniem mechanizmów wykrywania danych wrażliwych, w sposób konfigurowalny lub predefiniowany.
DAM.W.007		System musi dostarczać mechanizm analizy behawioralnej dla zdarzeń zgromadzonych w systemie centralnego raportowania, w minimalnym zakresie analizy dotyczącej: • identyfikowania nowych wektorów dostępu, • zmiany zachowania użytkowników - zmiana czasu aktywności; dostęp do nowych obiektów; ilościowa zmiana w dostępie do danych, • zmiany w transakcjach - analiza zmian w transakcjach musi charakteryzować się mechanizmem identyfikującym powtarzające się sekwencje zdarzeń i notyfikować zmiany we wzorcach tych sekwencji.
DAM.W.008		System musi zapewnić możliwość odróżnienia i określenia kto pracuje z systemem bazodanowym, np. użytkownik, administrator, aplikacja.
DAM.W.009		Zbudowane wzorce zachowań użytkowników muszą być efektem procesu automatycznej analizy behawioralnej użytkowników bazodanowych.
DAM.W.010		System musi się integrować z usługami LDAP w celu zasilania Systemu informacją o użytkownikach oraz uwierzytelniania w Systemie.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

DAM.W.011		System musi umożliwiać integrację z narzędziami klasy Privilege Access Management, w celu pobierania danych uwierzytelniających.
DAM.W.012		System musi zapewniać monitorowanie agentowe dla systemów zarządzanych samodzielnie we własnej infrastrukturze lub bezagentowo w przypadku systemów poza infrastrukturą własną (np. w chmurze)
DAM.W.013		System monitorowania baz danych musi wyszukiwać i klasyfikować informacje w bazach danych poprzez wykorzystanie wbudowanych wzorców danych jak i poprzez zdefiniowane wzorce.
DAM.W.014		Definiowanie polityki monitoringu musi uwzględniać następujące kryteria: • użytkownik, • tabele, • kolumny, • typ danych, • schemat bazy danych, • liczba wystąpień, • dostęp do danych wrażliwych zdefiniowanych poprzez system wykrywania danych.
DAM.W.015		System musi rozumieć język komunikacji źródła danych i identyfikować w minimalnym zakresie: • adresy IP nadawcy i odbiorcy, • użytkownika nawiązującego połączenie, • nazwy aplikacji klienckich, • port połączenia, • protokół komunikacyjny, • listę poleceń/komend, • nazwy systemu operacyjnego, z których użytkownik ma dostęp do zasobów, • listę obiektów, do których odwołuje się polecenie/komenda na podstawie których będzie możliwe definiowanie reguł polityk bezpieczeństwa.
DAM.W.016		System musi umożliwiać grupowanie parametrów reguł monitoringu, takich jak: • polecenia DCL, DML, DDL, • obiekty (lista tabel wrażliwych, lista plików wrażliwych), • użytkownicy (lista administratorów baz danych, lista kont technicznych),

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

		• adresy IP (np. lista stacji roboczych administratorów).
DAM.W.017		System musi zapewnić monitorowanie wszystkich połączeń do bazy danych oraz zabezpieczać następujące źródła danych, posiadających wsparcie producenta: • Oracle, • PostgreSQL, • MongoDB, • MSSQL, • MySQL, • IBM DB2, • Percona server • wyżej wymienione źródła danych użyte w rozwiązaniach zewnętrznych dostawców usług chmurowych, Jako zabezpieczenie rozumiane jest minimum: • monitorowanie aktywności (audyt), • aktywna ochrona bazy danych, w tym blokowanie zdefiniowanych nieautoryzowanych transakcji, • analiza behawioralna całości ruchu bazodanowego obserwowanego na poziomie silnika bazy danych lub sieciowym.
DAM.W.018		System musi zapewniać mechanizm ilościowej korelacji zdarzeń z możliwością generowania alarmów i notyfikacji do zewnętrznych systemów z wykorzystaniem co najmniej protokołu syslog.
DAM.W.019		System musi umożliwiać wykorzystanie wykrytych informacji przy definiowaniu reguł monitoringu.
DAM.W.020		System musi umożliwiać monitorowanie oparte o pobieranie danych z tablic natywnego audytu oraz zdarzeń.
DAM.W.021		System może umożliwiać monitorowanie: • wszystkich błędnych połączeń i zapytań, • czas wykonania operacji dla baz danych, • liczby zwracanych z zapytania rekordów w przypadku baz danych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

DAM.W.022		Instalacja agenta musi być możliwa na następujących systemach operacyjnych: • RedHat, • CentOS, • SUSE, • Oracle Linux, • Solaris, • AIX, • HP-UX, • Windows Server.
DAM.W.023		Agent musi posiadać możliwość bezpośredniej integracji z silnikiem bazy danych w celu wykrywania nieautoryzowanych transakcji i odpowiednio ich blokowania, bez blokowania innych połączeń do baz danych.
DAM.W.024		System musi posiadać możliwość automatycznego blokowania nieautoryzowanych transakcji bez ingerencji na płynność ruchu na bazach danych z innych aplikacji.
DAM.W.025		Agent musi posiadać możliwość blokowania ruchu bazodanowego w przypadku wykrycia incydentu bez ingerencji na płynność ruchu na bazach danych z innych aplikacji.
DAM.W.026		Agent musi wykrywać nowo zdefiniowane interfejsy bazy danych i automatycznie dodawać je do reguł monitorowania.
DAM.W.027		Agent musi posiadać możliwość definiowania reguł na podstawie których, agent będzie blokował tylko zdefiniowane transakcje bez ingerencji w płynność ruchu na bazach danych z innych aplikacji.
DAM.W.028		Agent musi umożliwiać przechowanie danych zbieranych z systemów bazodanowych w sytuacji niedostępności konsoli zarządzającej .
DAM.W.029		System musi zapewniać usługi samokontroli obejmujące: • identyfikację problemów w transmisji zdarzeń i automatyczne przełączanie do infrastruktury zapasowej, • identyfikację braku aktywności w monitorowanych wektorach i zapewnienie wstępnej analizy przyczyn, • uwzględnienie wpływu agenta monitorującego na system z możliwością zdefiniowania akcji po przekroczeniu progów alarmowych dla agenta.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

DAM.W.030		System musi zapewniać centralne i zdalne zarządzanie agentami dla monitorowania agentowego zapewniając: • rekonfiguracje agenta, • aktualizację agenta.
DAM.W.031		Moduły agentowe muszą posiadać możliwość łączenia w klaster n+1 gdzie wiele agentów komunikuje się z klastrem. Główny serwer węzła ma zadanie loadbalancera. Do budowy klastra może być użyta zewnętrzna infrastruktura, np. wydzielony loadbalancer firmy trzeciej.
DAM.W.033		Moduł agentowy Systemu musi posiadać możliwości weryfikacji stanu działania agenta.
DAM.W.034		System może posiadać moduł testowania podatności systemów bazodanowych oraz analizy pod kątem podatności baz danych: • na znane typy ataków, • na błędy konfiguracyjne, • na braki w aktualizacji oprogramowania, • w kontekście weryfikacji zabezpieczenia kont użytkowników bazodanowych.
DAM.W.035.1		System może zawierać wstępnie zdefiniowane testy oceny podatności baz danych, które obejmują kontrolę dostępu.
DAM.W.035.2		System może zawierać wstępnie zdefiniowane testy oceny podatności baz danych, które obejmują uwierzytelnianie i zarządzanie użytkownikami:
DAM.W.035.3		System może zawierać wstępnie zdefiniowane testy oceny podatności baz danych, które obejmują audyt.
DAM.W.035.4		System może zawierać wstępnie zdefiniowane testy oceny podatności baz danych, które obejmują ogólne informacje o bazie danych.
DAM.W.035.5		System może zawierać wstępnie zdefiniowane testy oceny podatności baz danych, które obejmują testy wewnętrzne.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

DAM.W.035.6		System może zawierać wstępnie zdefiniowane testy oceny podatności baz danych, które obejmują wykrywanie danych wrażliwych.
DAM.W.035.7		System może zawierać wstępnie zdefiniowane testy oceny podatności baz danych, które obejmują ataki oparte na bazie CVE.
DAM.W.035.8		System może zawierać wstępnie zdefiniowane testy oceny podatności baz danych, które obejmują integralność systemu operacyjnego.
DAM.W.035.9		System może zawierać wstępnie zdefiniowane testy oceny podatności baz danych, które obejmują kontrolę zasobów.
DAM.W.035.10		System może zawierać wstępnie zdefiniowane testy oceny podatności baz danych, które obejmują kwestie licencyjne.
DAM.W.036		System musi umożliwiać przechowywanie i przekazywanie danych mające na celu zapobieganie utracie zdarzeń (logów).
DAM.W.037		Logi dotyczące zarejestrowanych naruszeń oraz wykrytych anomalii muszą zawierać co najmniej następujące informacje: • nazwę użytkownika bazodanowego, • dodatkowe dane o użytkowniku pochodzące z zewnętrznych systemów - jeśli zdefiniowano, • źródłowy adres IP, • pełne zapytanie SQL wykonane przez użytkownika.
DAM.W.038		System musi umożliwiać archiwizowane logów dotyczących aktywności użytkowników.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

DAM.W.039		Archiwizowane logi muszą być natywnie zapisywane w postaci zaszyfrowanej i skompresowanej.
DAM.W.040		System musi umożliwić definiowanie reguł dostępu użytkowników do poszczególnych baz danych.
DAM.W.041		System musi umożliwić definiowanie reguł dostępu użytkowników bazodanowych do poszczególnych obiektów w bazie danych poprzez automatyczne tworzenie (na podstawie analizy wykonywanych transakcji lub ruchu sieciowego) listy użytkowników oraz listy zapytań SQL, jakie użytkownik może wykonać w odniesieniu do obiektów baz danych.
DAM.W.042		System musi umożliwić definiowanie oddzielnych reguł dostępu w odniesieniu do tabel z danymi wrażliwymi, sklasyfikowanymi przez moduły Systemu.
DAM.W.043		System musi umożliwić tworzenie list tabel, do których poszczególni użytkownicy bazodanowi mogą mieć dostęp w określonym, zdefiniowanym czasie, (np. definiowanie dni tygodnia oraz godzin, w jakich dany użytkownik może nawiązać połączenie z bazą danych). Zamawiający dopuszcza możliwość tworzenia w Systemie zarówno whitelist (opisanej powyżej) oraz blacklist.
DAM.W.044		System musi umożliwić zablokowanie ruchu wykorzystującego podatności wykryte w bazach danych.
DAM.W.047		Rozwiązanie w ramach funkcji centralnego raportowania, musi dostarczać predefiniowany zestaw raportów.
DAM.W.047		Rozwiązanie w ramach funkcji centralnego raportowania, może umożliwiać graficzną prezentację danych z użyciem REST API.
DAM.W.048		System raportowania musi umożliwić wykorzystanie informacji z następujących źródeł zewnętrznych: • Bazy SQL, • plik CSV, • Active Directory.
DAM.W.049		System musi mieć możliwość generowania własnych raportów, w formie tekstowej oraz graficznej.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

DAM.W.050		System musi zapewnić automatyczne, cykliczne wysyłanie raportów za pomocą poczty elektronicznej (e-mail).
DAM.W.051		System musi posiadać funkcję integracji z systemami typu SIEM.
DAM.W.052		System musi posiadać funkcję wysyłania informacji o zdarzeniach poprzez protokół SNMP, syslog, wiadomość e-mail oraz uruchomienia skryptu per konkretna polityka bezpieczeństwa.
DAM.W.053		Konsola zarządzająca musi wyświetlać w czasie rzeczywistym logi na jednej planszy.
DAM.W.054		Wyświetlane muszą być zdarzenia, które: • łamią polityki bezpieczeństwa, • pokazują działania Systemu (system events np. logowanie/wylogowanie użytkowników, dodanie/usunięcie polityki bezpieczeństwa lub audytu), problemy z modułami Systemu.
DAM.W.055		System musi zostać dostarczony w formie kompletnego rozwiązania tj. nie może wymagać do działania żadnego oprogramowania firm trzecich np. zewnętrznych baz danych.
DAM.W.056		Wszystkie elementy centralnego komponentu zarządzającego muszą być dostarczone przez tego samego producenta co moduły wykonawcze oraz w formie gotowych maszyn wirtualnych (ang. virtual appliance) działających w środowisku VMWare.
DAM.W.057		Całość konfiguracji Systemu oraz repozytorium logów musi być przechowywane na centralnym serwerze zarządzania. W oparciu o przechowywane dane musi istnieć możliwość centralnego raportowania zdarzeń za okres nie krótszy niż 3 lata z zasobu nie mniejszego niż 100TB danych przechowywanych dla tego okresu.
DAM.W.057.2		W oparciu o przechowywane dane może istnieć możliwość centralnego raportowania zdarzeń za okres 5 lat z zasobu nie mniejszego niż 300TB danych przechowywanych dla tego okresu.
DAM.W.058		Wszystkie elementy Systemu muszą być zlokalizowane w infrastrukturze Zamawiającego.
DAM.W.059		System musi obsługiwać serwery bazodanowe zlokalizowane w infrastrukturze Zamawiającego oraz w usługach chmurowych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

DAM.W.060		Serwer 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.
DAM.W.061		Uwierzytelnianie użytkowników oferowanego rozwiązania musi być możliwe minimum za pomocą: • użytkownika lokalnego, • poprzez integrację z Active Directory lub innym serwerem LDAP.
DAM.W.062		System musi umożliwiać zmianę wszystkich haseł użytkowników w Systemie ochrony baz danych.
DAM.W.063		Konsola zarządzająca musi być dostępna poprzez interfejs przeglądarki Web – Chrome, Firefox, Edge, linie poleceń z wykorzystaniem terminala SSH.
DAM.W.065		Wszelkie działania związane z konfiguracją oraz definicją reguł i polityk muszą być możliwe poprzez interfejs przeglądarki Web.
DAM.W.066		System musi posiadać mechanizm informowania administratora o wykonaniu, bądź niewykonaniu na czas zadania zleconego innym użytkownikom Systemu.
DAM.W.067		System musi mieć zapewnione aktualizacje uwzględniające co najmniej: • sygnatury ataków, • listę reguł polityki bezpieczeństwa oraz monitorowania aktywności użytkowników na bazach danych, • listę testów podatności baz danych, • listę raportów.
DAM.W.068		Aktualizacja Systemu musi być dostępna zarówno poprzez ręczne pobranie zawartości ze strony producenta lub automatycznie (w sposób konfigurowalny).
DAM.W.069		W ramach licencji Zamawiający może zainstalować dowolną liczbę modułów wykonawczych.
DAM.W.070		Dostarczona licencja dla oprogramowania Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji w zgromadzonych danych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

DAM.W.071		System musi posiadać możliwość instalacji w środowiskach wirtualnych. W środowisku wirtualnym System musi zapewnić nieograniczone przez producenta zwiększanie zasobów w obrębie pojedynczego wirtualnego modułu.

Wykonawca jest zobowiązany do wypełnienia kolumny „Spełnia wymaganie" poprzez wpisanie TAK lub NIE. W przypadku braku wpisu przy kryterium Fakultatywnym, Wykonawca otrzyma 0 pkt za dane wymaganie.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706