Wymagania funkcjonalne oraz jakościowe Systemu DAM

ID	Kryteria O- obligatoryjne F-fakultatywne	Opis Wymagania
Scenariusze detekcji i raportowania anomalii oraz incydentów		
DAM.W.001	O	System musi wykrywać dostępu do bazy danych w niestandardowych godzinach pracy.
DAM.W.002	O	System musi wykrywać wykorzystywanie przez użytkownika kont administracyjnych i serwisowych w bazie danych.
DAM.W.003	O	System musi wykrywać przeglądanie przez użytkownika rekordów bazodanowych wprowadzonych przez innych użytkowników bazodanowych.
DAM.W.004	O	System musi wykrywać anomalie błędnych logowań do konta bazodanowego innych niż standardowa ilość.
DAM.W.005	O	System musi wykrywać, że użytkownik bazodanowy przeglądał w krótkim czasie rekordy z wielu baz danych.
DAM.W.006	O	System musi wykrywać przeglądanie przez użytkownika bazodanowego wielu danych sklasyfikowanych jako wrażliwe.
DAM.W.007	O	System musi wykrywać, że użytkownik bazodanowy korzysta z danych, które powinny być osiągalne tylko poprzez aplikację lub użytkownika serwisowego.
DAM.W.008	O	System musi wykrywać wykonanie przez Użytkownika bazodanowego poleceń SQL, których sposób i cel wykonania jest podejrzany.

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.009	O	System musi wykrywać użytkownik bazodanowy przeszukał bazę danych za pomocą dynamicznego zapytania SQL w sposób nieprawidłowy.
DAM.W.010	O	System powinien analizować zachowania użytkowników poprzez porównanie do wzorca zachowania użytkowników bazodanowych zbudowanego w oparciu o obserwowane modele zachowań specyficzne dla danej grupy użytkowników, dla całości organizacji, dla wybranych grup. Musi to być dokonywane w sposób automatyczny, a efekt analizy powinien być przedstawiony w formie incydentów i anomalii zachowań poszczególnych użytkowników bazodanowych.
DAM.W.011	O	System musi zapewnić możliwość odróżnienia i określenia kto pracuje z systemem bazodanowym, np. użytkownik, administrator, aplikacja/API
DAM.W.012	O	Budowanie wzorców powinno opierać się na informacjach takich jak nazwy tabel, kolumn, rekordy w tabelach, przy zastosowaniu wyrażeń regularnych
DAM.W.013	O	System musi umożliwiać wykorzystania wykrytych informacji przy definiowaniu reguł monitoringu.
DAM.W.014	O	System musi umożliwiać dodawanie informacji o użytkowniku wykonującym operacje bazodanowe poprzez pobieranie danych z zewnętrznych systemów takich jak: Active Directory, LDAP, systemy bazodanowe SQL jak i danych dostarczonych w postaci pliku.
DAM.W.015	O	System musi umożliwiać pobieranie danych z tablic natywnego audytu oraz zdarzeń.
DAM.W.016	O	System musi umożliwiać integrację z narzędziami typu Priviliege Access Management, np. CyberArk, w celu pobierania danych uwierzytelniających.
Monitorowanie		
DAM.W.017	O	Moduł monitorowania baz danych powinien aktywnie wyszukiwać i klasyfikować usługi bazodanowe.
DAM.W.018	O	Moduł monitorowania baz danych powinien wyszukiwać i klasyfikować informację w bazach danych poprzez wykorzystanie wbudowanych wzorców danych jak i poprzez zdefiniowane wzorce.
DAM.W.019	O	Definiowanie polityki monitoringu musi uwzględniać przynajmniej następujące kryteria:

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

		• użytkownik, • tabele, • kolumny, • typ danych, • schemat bazy danych, • ilość wystąpień, • dostęp do danych wrażliwych zdefiniowanych poprzez system wykrywania danych.
DAM.W.020	O	System musi umożliwiać automatyczne tworzenie list: • źródłowych adresów IP, • nazw aplikacji klienckich, • nazw systemu operacyjnego, z których użytkownik ma dostęp do zasobów. • na podstawie których będzie możliwe definiowane reguł polityk bezpieczeństwa.
DAM.W.021	O	System musi umożliwiać zdefiniowania bardzo szczegółowych reguł monitoringu dostępu do danych, zapewniając jednocześnie odpowiedni poziom ochrony dla całości ruchu do bazy z uwzględnieniem: • DCL, • DML, • DDL, • TCL, • procedur składowanych.
DAM.W.022	O	System musi wykrywać komendy wykonywane na systemie zarządzania bazą danych (poza silnikiem) jak np. Export Direct w DB Oracle.
DAM.W.023	O	System musi monitorować oraz zabezpieczać, co najmniej, następujące systemy 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

		• Oracle, • PostgreSQL, • Percona PostgreSQL, • MongoDB, • Percona MongoDB, • MSSQL, • MySQL, • Percona MySQL, • Sybase, • Teradata, • IBM DB2, • Elasticsearch Jako zabezpieczenie rozumiane jest, minimum: • monitorowanie aktywności (audyt), • aktywna ochrona bazy danych, w tym blokowanie niepożądanych aktywności (DataBase Firewall), • analiza behawioralna całości ruchu bazodanowego obserwowanego na poziomie sieciowym nawet niepoddanego monitorowaniu.
DAM.W.024	O	System musi zostać dostarczony wraz z aplikacją monitorującą ruch lokalnie na serwerach bazodanowych - agent. Aplikacja agent ma na celu wysyłanie informacji o lokalnej aktywności użytkowników do modułu wykonawczego.
DAM.W.025	O	Instalacja agenta musi być możliwa na następujących systemach operacyjnych: • RedHat, • CentOS,

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

		• SUSE, • Oracle Linux, • Solaris, • AIX, • HP-UX, • Windows Server.
DAM.W.026	O	Agent musi posiadać możliwość pracy w trybie nasłuchu - sniffing. Jako nasłuch rozumiany jest tryb pracy bez opóźnień z możliwością terminacji sesji w przypadku wykrycia nadużycia.
DAM.W.027	O	Agent musi posiadać możliwość pracy w trybie in-line. 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.
DAM.W.028	O	Agent musi posiadać możliwość blokowania ruchu w przypadku wykrycia incydentu.
DAM.W.029	O	Agent musi wykrywać nowo zdefiniowane interfejsy bazy danych i automatycznie dodawać je do reguł monitorowania.
DAM.W.030	O	Agent musi posiadać możliwość definiowania reguł na podstawie których, agent będzie wybierać ruch, który ma być wysyłany do modułu wykonawczego monitorowania i ochrony baz danych.
DAM.W.031	O	Agent musi umożliwiać przechowanie danych zbieranych z systemów bazodanowych w sytuacji niedostępności modułu centralnego.
Moduł wykonawczy		
DAM.W.032	O	Moduły wykonawcze muszą mieć możliwość zbudowania dwóch typów klastrów n+1.

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.033	O	Moduły wykonawcze muszą posiadać możliwość łączenia w klaster n+1 - wielu agentów komunikuje się z klastrem. Główny serwer węzła ma zadane loadbalancera. Do budowy klastra nie może być użyta zewnętrzna infrastruktura, np. wydzielony loadbalancer firm trzecich.
DAM.W.034	O	Moduły wykonawcze muszą posiadać możliwość łączenia się w klaster n+1, gdzie tylko jeden agent komunikuje się z klasterem w celu rozłożenia obciążenia na wiele węzłów klastra, które generuje baza danych. Ma to miejsce np. w przypadku gdy jedna baza danych generuje obciążenie, które nie może zostać obsłużone przez jeden moduł wykonawczy.
DAM.W.035	O	Moduł wykonawczy Systemu musi posiadać możliwości weryfikacji stanu działania agenta.
DAM.W.036	O	System musi posiadać moduł testowania podatności systemów bazodanowych oraz analizy pod kątem podatności systemu operacyjnego i baz danych na znane typy ataków, błędy konfiguracyjne, braki w aktualizacji oprogramowania, czy też weryfikacji zabezpieczenia kont użytkowników bazodanowych.
DAM.W.037	O	Rozwiązanie musi zawierać co najmniej 1000 wstępnie zdefiniowanych testów oceny podatności baz danych, które obejmują następujące kategorie: • kontrola dostępu, • uwierzytelnianie i zarządzanie użytkownikami, • audyt, • ogólne informacje o bazie danych, • testy wewnętrzne, • wykrywanie danych wrażliwych. • ataki oparte na bazie CVE, • integralność systemu operacyjnego, • kontrola zasobów, • kwestie licencyjne.

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.038	O	System musi umożliwiać przechowywanie i przekazywanie danych mające na celu zapobiegania utracie zdarzeń (logów).
DAM.W.038	O	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.040	O	System musi umożliwiać archiwizowane logów dotyczących aktywności użytkowników.
DAM.W.041	O	Archiwizowane logi muszą być natywnie zapisywane w postaci zaszyfrowanej i skompresowanej.
Ochrona baz danych		
DAM.W.042	O	System musi umożliwić definiowanie reguł dostępu użytkowników do poszczególnych baz danych na poziomie sieciowym.
DAM.W.043	O	System musi umożliwić definiowania 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.
DAM.W.044	O	System musi umożliwić definiowanie oddzielnych reguł dostępu w odniesieniu do tabel z danymi wrażliwymi, sklasyfikowanymi przez moduł wykrywania.
DAM.W.045	O	System musi umożliwić tworzenie list tabel, do których poszczególni użytkownicy bazodanowi nie mogą mieć dostępu, np. definiowanie dni tygodnia oraz godzin, w jakich dany użytkownik może nawiązać połączenie z bazą danych.
DAM.W.046	O	System musi umożliwić zablokowania ruchu wykorzystującego podatności wykryte w bazach 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

Raportowanie		
DAM.W.047	O	System musi posiadać gotowe szablony raportów dotyczące: • alarmów bezpieczeństwa, • zdarzeń systemowych, • zmian w profilach baz danych, • monitorowania aktywności użytkowników na bazach, • wykonanych testów podatności systemów, • klasyfikacji usług • informacji w bazach danych, • zgodności z wymaganiami regulacji.
DAM.W.048	O	System musi umożliwić wykorzystania informacji ze źródeł zewnętrznych.
DAM.W.049	O	System musi mieć możliwość generowanie własnych raportów, w formie tekstowej jak i graficznej.
DAM.W.050	O	System musi zapewnić automatyczne, cykliczne wysyłanie raportów za pomocą poczty elektronicznej (e-mail)
DAM.W.052	O	System musi posiadać funkcję integracji z systemami typu SIEM
DAM.W.052	O	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	O	Komponent zarządzający musi wyświetlać w czasie rzeczywistym logi na jednej planszy – dashboard.
DAM.W.054	O	Wyświetlane muszą być zdarzenia: • które łamią polityki bezpieczeństwa,

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

		• działania Systemu (system events np. logowanie/wylogowanie użytkowników, dodanie/usunięcie polityki bezpieczeństwa lub audytu), problemy z modułem wykonawczym.
Wymagania techniczne		
DAM.W.055	O	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	O	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	O	Całość konfiguracji Systemu oraz repozytorium logów musi być przechowywane na centralnym serwerze zarządzania.
DAM.W.058	O	Wszystkie elementy systemu muszą być zlokalizowane w infrastrukturze Zamawiającego
DAM.W.059	O	System musi obsługiwać serwery bazodanowe zlokalizowane w infrastrukturze Zamawiającego oraz w usługach chmurowych.
DAM.W.060	O	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	O	Uwierzytelnianie użytkowników oferowanego rozwiązania musi być możliwe minimum za pomocą: • użytkownika lokalnego, • poprzez integrację z Active Directory.
DAM.W.062	O	System musi umożliwiać zmianę wszystkich haseł użytkowników w Systemie ochrony baz danych.
DAM.W.063	O	Serwer zarządzający oferowanego rozwiązania musi być dostępny wyłącznie poprzez interfejs przeglądarki Web – Chrome, Firefox, Edge.
DAM.W.064	O	Wszelkie działania związane z konfiguracją oraz definicją reguł i polityk muszą być możliwe poprzez interfejs przeglądarki Web.

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.065	O	Wymagany jest mechanizm zarządzania zorientowane na zadania. Musi istnieć mechanizm informowania administratora o wykonaniu, bądź niewykonaniu wykonaniu na czas zadania zleconego innym użytkownikom Systemu.
DAM.W.066	O	Producent System musi zapewnić aktualizację modułów, uwzględniając co najmniej: • sygnatury ataków, • listę reguł polityki bezpieczeństwa oraz monitorowania aktywności użytkowników na bazach danych, • listę testów podatności baz danych, • listę raportów.
DAM.W.067	O	Aktualizacja systemu musi być dostępna zarówno poprzez ręczne pobranie zawartości ze strony producenta, jak i automatycznie.
Moduł fizyczny		
DAM.W.068	F	Możliwość dostarczenia urządzenia w postaci serwera sprzętowego producenta Systemu o poniższych parametrach: • Wysokość maksymalna 2U • Dwa redundantne zasilacze sieciowe 220-240V • Minimum dwa dyski w systemie RAID1 (mirror) • karty sieciowe do obsługi ruchu bazodanowego – minimum 16 portów • karta sieciowa do obsługi ruchu do sieci zarządzania – minimum 1 port • karta sieciowa dla sieci LAN – minimum 1 port • Obsługa ruchu sieciowego w trybie L2 In-Line Transparent Bridge dla minimum 8 linii. • Obsługa ruchu sieciowego w trybie SPAN dla minimum 16 linii • Wydzielenie interfejsu do komunikacji z agentami

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

		• Wsparcie monitorowania w trybue L2 In-Line Transparent Bridge ruchu bazodanowego z uwzględnieniem standardów IEEE 802.1Q (trunk) oraz Link Aggregation Protocol (LACP). • Moduł (karta) umożliwiająca zarządzanie serwerem w ramach Intelligent Platform Management Interface (IPMI) • Moduł wspierający deszyfrację zaszyfrowanego ruchu sieciowego w standardzie SSL/TLS. • Fizyczny bypass w kartach sieciowych umożliwiający, w przypadku awarii urządzenia, przepuszczenie ruchu bez inspekcji lub jego zablokowanie. • Obsługa ruchu bazodanowego na poziomie 5 000 TPS przy założeniu minimalnego ruchu sieciowego 500Mbps. • Preinstalowany System w najnowszej wersji bez konieczności dokupienia dodatkowych lub dedykowanych licencji.
Licencjonowanie		
DAM.W.069	O	System powinien być licencjonowany per serwer bazodanowy.
DAM.W.070	O	Dostarczony licencje pozwolą na wdrożenie Systemu umożliwiającego monitorowanie minimum 25 serwerów bazodanowych
DAM.W.071	O	W ramach licencji Zamawiający może zainstalować dowolną liczbę modułów wykonawczych.
DAM.W.072	O	Dostarczona licencja dla oprogramowania Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji w zgromadzonych danych.
DAM.W.073	F	Dostarczona licencja jest licencją czasową – subskrypcja
DAM.W.074	F	Dostarczona licencja jest licencją bezterminową – perpetual

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