OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa licencji na system służący do przechowywania i zarzadzania logami systemowymi oraz zarzadzania zdarzeniami i informacjami bezpieczeństwa (system klasy SIEM – Security Information and Event Management), zwanego dalej SIEM lub system.

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

1. Przedmiot zamówienia obejmuje:

1.1. Dostawę licencji na system klasy SIEM wraz z 12 miesięcznym wsparciem producenta/Wykonawcy ważnym od dnia podpisania przez Zamawiającego protokołu odbioru tych licencji.

1.2. Oferowany system, musi być rozwiązaniem istniejącym na rynku co najmniej 5 lat, pochodzący z oficjalnego kanału sprzedaży.

1.3. Nie dopuszcza się rozwiązań typu open surce.

1.4. Oferowane dodatkowe moduły, dostępne w ramach platformy muszą być sprawdzonymi rozwiązaniami dostępnymi na rynku, co najmniej przez okres jednego roku przed faktem nabycia licencji.

1.5. Oferowany system, musi posiadać możliwość rozbudowy o dodatkowe moduły realizujące funkcje monitorowania infrastruktury IT oraz infrastruktury OT.

1.6. W przypadku zwiększenia zapotrzebowania dowolnego modułu czy komponentu systemu na zasoby systemowe, które pozwolą zniwelować potencjalne problemy wydajnościowe, rozwiązanie powinno posiadać możliwość zwielokrotnienia poprzez rozbudowę (np. zwielokrotnienia ilości węzłów) bez konieczności zakupu dodatkowych modułów, czy licencji.

1.7. Oferowany system, musi mieć możliwość wydajnego parsowania logów co najmniej na poziomie 500 zdarzeń na sekundę lub 5 GB dziennie.

1.8. Przekroczenie ww. parametrów nie może skutkować żadną utratą danych. System SIEM, powinien informować o takim przekroczeniu w postaci alarmu i informacji w interfejsie użytkownika.

1.9. Rozbudowa systemu, poprzez dokupienie dodatkowych licencji musi umożliwiać powiększenie wydajności parsowania logów przez dokupienie na obsługę kolejnych zdarzeń na sekundę lub GB dziennie.

1.10. System przechowywania danych logów i zdarzeń musi chronić przed nieuprawnionym usunięciem całości lub części danych, raportów i innych informacji oraz gwarantować, że dostęp do nich mają tylko uprawnieni, uwierzytelnieni użytkownicy.

1.11. Podłączona liczba urządzeń lub systemów, z których można pobierać logi, nie może być ograniczona, a system musi być w stanie przetwarzać jednocześnie zdarzenia z szybkością co najmniej 500 zdarzeń na sekundę.

1.12. Oferowany system, musi działać w czasie rzeczywistym i umożliwiać użytkownikom modyfikację sposobu normalizacji danych w razie potrzeby (poprzez dodawanie nowych pól, zmianę przeznaczenia istniejących, zmianę ich nazwy, itp.) bez konieczności całkowitej przebudowy bazy danych. System SIEM, musi obsługiwać jednocześnie korzystanie z wielu metod normalizacji logów.

1.13. Licencja systemu, nie może ograniczać liczby komponentów gromadzących oraz analizujących logi.

1.14. Oferowany system, musi wspierać mechanizm planowego przenoszenia danych na pamięci masowe niższego poziomu (np. inne, wolniejsze lub tańsze w eksploatacji nośniki danych) na podstawie czasu lub okresu.

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

1.15. Oferowany system, musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej na bazie protokołu CIFS/NFS w celu przechowywania danych archiwalnych. Dane archiwalne powinny być dostępne w systemie w analogiczny sposób jak dane dostępne on-line z wykorzystaniem tej samej konsoli zarządzania danymi.

1.16. Oferowany system, musi zapewniać kontrolę dostępu na poziomie RBAC (Role-Based Access Control) w granulacji określonej na poziomie wartości poszczególnych, identyfikowanych danych.

1.17. Licencja musi dopuszczać, dowolne kształtowanie architektury systemu, w szczególności stosowanie dowolnej liczby komponentów poszczególnych funkcji. Rozbudowa oferowanej Platformy o kolejne elementy przetwarzające, analizujące, zbierające, nie może wiązać się z żadnymi kosztami licencyjnymi. Licencja nie może też ograniczać w żaden sposób liczby podłączanych urządzeń.

1.18. Architektura systemu, musi dopuszczać rozdzielenie na osobne serwery funkcjonalności:

- warstwy analitycznej oraz interfejsu użytkownika,
- przechowywania, wyszukiwania i zarządzania bazą zebranych logów,
- pobierania danych.

1.19. Oferowany system, musi umożliwiać tworzenie własnych, nieuwzględnionych przez producenta w wersji bazowej systemu funkcjonalności związanych z analizą danych, takich jak:

- dodatkowe funkcje analityczne,
- raporty,
- formularze,
- mechanizmy pobierania danych czy powiadomienia.

Realizacja tych funkcjonalności nie może wymagać konieczności angazowania producenta i nie może naruszać praw autorskich.

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

1.20. Oferowany system, musi posiadać możliwość uruchomienia w architekturze zapewniającej wysoka dostępność (HA).

1.21. Oferowany system, musi umożliwiać wyszukiwanie zdarzeń w logach/danych o zadanych wartościach pól, w oparciu o wyrażenia regularne (REGEX) lub gotowych wzorców wyboru np.: adres IP źródłowy/docelowy, port, protokół.

1.22. Wszystkie dostarczone licencje, musza mieć możliwość przenoszenia, tj. pozwalać na instalację dodatkowych instancji systemu SIEM oraz dowolne przypisywanie posiadanych licencji pomiędzy tymi instancjami jak również łączenie w jedną większa instancję (np. w przypadku zakupu kolejnych licencji) w przypadku kolejnych zakupów na kolejną dostawę licencji.

1.23. Oferowany system, musi zawierać co najmniej 100 stworzonych i dostarczonych przez producenta oferowanego systemu, wbudowanych reguł korelacyjnych działających na danych ze źródeł logów systemowych i aplikacyjnych. Reguły te powinny być aktualizowane przez producenta oraz mieć możliwość zarządzania poprzez ich dodawanie, usuwanie oraz edycję.

1.24. Oferowany system, musi samodzielnie zarządzać retencją danych. Wymagana jest obsługa co najmniej dwóch etapów życia danych: dane dostępne online i archiwalne. Z każdym etapem związane jest miejsce przechowywania danych. Migracja danych musi następować automatycznie po określonym czasie (wiek danych) lub osiągnięciu określonej objętości. Musi istnieć możliwość stworzenia różnych schematów retencji dla różnych typów danych. System musi umożliwiać wydajną pracę: użytkowników przeglądających zdarzenia i generujących raporty i wyszukiwania dla zgromadzonych danych obejmujących minimum 90 dni. Po upływie 90 dni system powinien automatycznie przenosić dane do wskazanego archiwum.

1.25. Oferowany system, musi być odporny na ataki sieciowe. W tym celu niezbędne jest zabezpieczenie/utwardzenie systemu obejmujący usunięcie niepotrzebnego/nieużywanego oprogramowania systemowego, kont użytkowników, wyłączenia zbędnych usług oraz włączenia filtrowania ruchu IP.

1.26. Oferowany system, musi umożliwiać wykorzystywanie w innych obszarach niż zarządzanie informacją bezpieczeństwa w oparciu o wspólne dane w szczególności w zakresie:

- Zbierania i analizy logów,
- Monitorowa usług,
- Wydajności aplikacji.

Oferowane funkcjonalności, musza mieć pokrycie w oficjalnie dostępnej dokumentacji technicznej producenta, którą Wykonawca udostępni na żądanie Zamawiającego wraz ze wskazaniem punktów odnoszących się do danej funkcjonalności.

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

2. Wymagania funkcjonalne – pozyskiwanie danych:

2.1. Oferowany system musi umożliwiać zaprojektowanie i wdrożenie przesyłania, parsowania, korelowania i przechowywania logów i innych danych z co najmniej następujących typów źródeł:

- Systemy bezpieczeństwa,
- Systemy sieciowe i bezprzewodowe,
- Systemy operacyjne: Linux (wszystkie dystrybucje), Microsoft,
- Serwery: DNS, DHCP, WWW (Apache, IIS, Nginx),
- Systemy pocztowe: Microsoft,
- Usługi katalogowe: Active Directory (AD), OpenLDAP,
- Bazy danych: Oracle, Microsoft SQL Server, MySQL, PostgradeSQL, Maria DB. Musi istnieć możliwośćinstalacji sterowników do innych typów baz danych w standardize JDBC lub ODBC (alternatywnie),
- Systemy wirtualizacyjne: VMware, vSphere, Hyper-V,
- Logi Windows Events (Application, Security, System I inne),
- Logi z ruchu sieciowego wysyłane poprzez NetFlow oraz IP Flow Information Export (IPFIX),
- Logi z system kontroli dostępu.

Poprzez pozyskiwanie logów rozumie się:

- Pobieranie logów i zapisywanie w bazie systemu SIEM,
- Klasyfikację zdarzeń wg. typów (np. Zalogowanie użytkownika, nawiązanie połączenia, itp.).
- Normalizację logów, czyli nadanie kontekstów znaczeniowych dla poszczególnych fragmentów logu, np. Username, source_ip, itp.

2.2. Oferowany system musi umożliwiać pobieranie logów/danych zapisanych w plikach (dziennikach) jak również w postaci komunikatów wychwytywanych z portów TCP/UDP oraz z wykorzystaniem następujących mechanizmów:

- Wysyłanie logów/danych ze źródła systemu, na wskazany port TCP/UDP serwera, będącego częścią wdrażanego systemu (np. Syslog),
- System musi wspierać zbieranie danych z formacie CEF oraz przyjmowanie logów z Syslog Relay,
- Wskazanie w interfejsie użytkownika wdrażanego systemu na znajdujący się lokalnie plik/katalog,
- Wykonywanie przez system zapytań SQL w zewnętrznych bazach danych i pobieranie wyników takich zapytań (alternatywnie musi istnieć możliwość komunikacji z bazami w standardzie JDBC lub ODBC),
- Windows Management Instrumentation (WMI),
- Pliki tekstowe,

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

- Logi JMS, JMX,
- Dane z systemów wirtualizacji,
- Dane z systemów kontenerowych,
- Dane z systemów chmurowych,
- Span port,
- NetFlow v5 i v9, sFlow, jFlow, IPFIX,
- Zbiory wskazane w katalogach.

Pobieranie danych z ww. protokołów musi być możliwe bez wykorzystania agenta dla monitorowanych urządzeń i serwerów.

2.3. Oferowany system musi pozwalać na analizę standardowych logów infrastrukturalnych generowanych przez systemy operacyjne, dostęp webowy/proxy, systemy bezpieczeństwa, urządzenia sieciowe (routery, switche, punkty bezprzewodowe, itp.).

2.4. Oferowany system musi umożliwiać parsowanie logów o długości co najmniej 10 000 znaków oraz zawierających więcej niż jedną linię.

2.5. Oferowany system musi umożliwiać tworzenie bazy definicji formatów logów.

2.6. Oferowany system musi pozwalać na modyfikację mechanizmów klasyfikacji i normalizacji logów dostarczonych razem z produktem (otwarty kod dostarczonych mechanizmów normalizacji). Aktualizacje oprogramowania nie mogą nadpisywać ww. modyfikacji.

2.7. Oferowany system musi pozwalać na analizę niestandardowych logów, takich jak: logi wygenerowane przez oprogramowanie dedykowane, przez aplikacje własne (autorskie) lub utworzone przez użytkowników.

2.8. Oferowany system musi umożliwiać integrację danych gromadzonych z różnych źródeł: aplikacji, baz użytkowników, w tym katalogu Active Directory. Dane powinny być dostępne jako spójna informacja na poziomie interfejsu analitycznego systemu.

2.9. Oferowany system musi umożliwiać stosowanie agentów na monitorowanych serwerach i stacjach roboczych. Agent musi również umożliwiać pobieranie informacji zarówno z systemu, na którym został zainstalowany, jak również z zewnętrznych systemów (np. w celu obsłużenia logów w lokalizacjach zdalnych). Konfiguracja agenta, po podłączeniu do serwera zarządzającego musi odbywać się centralnie. Agent musi zapewniać możliwość szyfrowania i uwierzytelnienia komunikacji z serwerem centralnym.

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

3. Wymagania funkcjonalne – normalizacja danych:

3.1. Oferowany system musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu (np. dodanie nowych pól, zmianę znaczenia lub nazwy istniejących, itp.) bez konieczności przeprowadzenia ponownego odbudowywania bazy danych. System musi pozwalać na równoległe używanie różnych sposobów normalizacji logów.

3.2. Reguły korelacji powinny być tworzone i zarządzane w interfejsie systemu, bez potrzeby użycia dodatkowych narzędzi firm trzecich.

3.3. Oferowany system musi umożliwiać obsługę logów w formacie XML, CEF, JSON bez konieczności tworzenia parserów. Nazwy pól powinny być określone zgodnie z ich strukturą (XML, CEF, JSON).

3.4. Oferowany system musi umożliwiać obsługę logów w formacie CSV bez konieczności tworzenia parserów. Nazwy pól powinny być wierszem nagłówkowym CSV. Musi istnieć możliwość obsługi różnych delimiterów (przecinek, kropka, średnik, tabulator, itp.) oraz wartości pól w cudzysłowach.

3.5. Proces odpowiedzialny za parsowanie logów musi analizować poszczególne logi/dane i wyszukiwać w nich informacje o logowanym zdarzeniu, między innymi:

- Data i czas zdarzenia,
- Nazwa użytkownika,
- Nazwa systemu logującego,
- Nazwa/adres IP systemu,
- Nazwa źródła logów,
- Rodzaj zdarzenia (np. zalogowanie/wylogowanie/zablokowanie użytkownika, przepuszczenie/zablokowanie ruchu sieciowego, wykrycie szkodliwego kodu, itp.).

3.6. Oferowany system musi wspierać geolokalizację zdarzeń na bazie adresów IP. Dane geolokalizacyjne (np. kraj) mają służyć w narzędziu do prezentacji na mapie, jak również umożliwiać ich wykorzystywanie w wyszukiwaniu wartości pól oraz w regułach korelacyjnych.

3.7. Oferowany system musi umożliwiać analizę logów w różnych językach, w tym co najmniej w języku angielskim i polskim. Znaki w logach źródłowych kodowane przy użyciu różnych stron kodowych musza być konwertowane do wspólnego kodowania (preferowane UTF8 lub UTF16).

3.8. Oferowany system musi umożliwiać wykrywanie sytuacji niestandardowej niezgodnej z poprzednio zarejestrowanym wzorcem (np. w celu wykrycia ataku DoS/DDoS, wykrycia wewnętrznego ruchu sieciowego, niewystępującej wcześniej aplikacji, pojawienia się nowego użytkownika, itp.).

3.9. W celu ograniczenia zajętości przestrzeni dyskowej, dane wzbogacające nie mogą być przechowywane razem z logami, a wzbogacenie powinno odbywać w locie, w trakcie odczytu danych ze źródeł zewnętrznych, a nie w trakcie zapisu.

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

4. Wymagania funkcjonalne – narzędzia analityczne:

4.1. Oferowany system musi umożliwiać przeglądanie (w jednej konsoli systemu) logów pobieranych/dostarczanych do systemu oraz sprawdzania statusu połączenia (przepuszczenie, zablokowanie) w celu uniknięcia konieczności logowania się do każdego monitorowanego systemu osobno. Filtrowanie w czasie rzeczywistym musi dopuszczać wyszukiwanie informacji za pomocą wyrażeń regularnych (REGEX) lub gotowych wzorców, np.: adres IP źródłowy/docelowy, port, protokół.

4.2. Oferowany system musi umożliwiać alarmowanie i raportowanie o anomaliach statystycznych dla docelowych parametrów liczbowych zawartych w logach polegając na odchyleniu w stosunku do wartości przewidywanych (zarówno w górę, jak i w dół) z uwzględnieniem sezonowości (np. różnic wynikających z pory dnia, czy tygodnia).

4.3. Oferowany system musi umożliwiać łatwe i samodzielne tworzenie reguł parsowania logów/danych, tworzenie widoków/raportów kolejnych/nowych dowolnych źródeł danych przez pracowników Zamawiającego.

4.4. Oferowany system musi posiadać możliwość tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być tworzone w wielu formatach – minimum PDF, CSV, JPG.

4.5. Oferowany system musi posiadać predefiniowane widoki dedykowane dla specjalistów odpowiedzialnych za poszczególne obszary bezpieczeństwa, np.:

- Wykrywanie i przeciwdziałanie złośliwemu oprogramowaniu,
- Wykrywanie i obsługa podatności,
- Analiza ruchu sieciowego,
- Analiza oraz śledzenie wykorzystywanych portów i protokołów sieciowych,
- Analiza oraz śledzenie aktualizacji oprogramowania w ramach organizacji,
- Analiza i śledzenie uprawnień dostępu.

4.6. Zestaw funkcjonalności analitycznych musi uwzględniać co najmniej następujące funkcje:

- Statystyki typu suma, średnia, mediana, odchylenie standardowe, najstarszy, najnowszy dla zadanego klucza (np. średni godzinny wolumen danych dla adresu źródłowego),
- Funkcje wykrywania anomalii dla dowolnych parametrów zawartych w logach, a nie tylko parametrów ruchu sieciowego,
- System musi wykrywać rzadkie wystąpienia wartości i zdarzeń w określonym podzbiorze,
- Budowanie korelacji w oparciu o zdarzenia zawierające jednakowe wartości danych pól,
- Badanie zmian wartości danego pola i alarmowanie lub raportowanie w oparciu o zmianę tej wartości (np. wzrost liczby niepoprawnych zalogowań o 50%).

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

4.7. Komponenty oferowanego systemu w obszarze analityki biznesowej, raportowania, monitoringu infrastruktury teleinformatycznej oraz zarządzania i monitoringu logów systemowych i aplikacyjnych nie muszą pochodzić od jednego producenta, jednak nie mogą to być rozwiązania open source.

4.8. Oferowany system musi wspierać pracę użytkowników w różnych rolach i w następujących obszarach:

- Analiza zdarzeń w obszarze bezpieczeństwa teleinformatycznego,
- Analiza pracy systemów informatycznych w zakresie wydajności i awarii systemów informatycznych w zakresie wydajności i awarii systemów/urządzeń teleinformatycznych,
- Analiza pracy aplikacji własnych (autorskich) lub utworzonych przez użytkowników.

4.9. Oferowany system musi umożliwiać tworzenie reguł korelacyjnych o długim okresie działania (czas pomiędzy najstarszym, a najnowszym zdarzeniem w ramach grupy zdarzeń powiązanych ze sobą). Okres ten nie może być ograniczany żadnymi innymi limitami, poza dostępnością danych w systemie.

4.10. Oferowany system musi zapewniać rozliczalność działań użytkowników, w szczególności rejestrowanie dostępu do przetwarzanych logów/danych, także jednoczesną prace analityczną, dla co najmniej 10 użytkowników. Licencja powinna uwzględniać możliwość utworzenia kont w systemie dla co najmniej 25 użytkowników. Użytkownicy z przypisanymi różnymi rolami, powinni mieć odseparowane środowiska.

4.11. Oferowany system musi posiadać możliwość rozbudowy funkcjonalności o wizualizacje dostarczane przez zewnętrzne biblioteki komercyjne lub dostępne na zasadzie otwartego kodu. Musi istnieć możliwość umieszczania takich wizualizacji na standardowych dashboardach systemu.

4.12. Oferowany system musi posiadać możliwość tworzenia interaktywnych dashboardów zawierających elementy interfejsu użytkownika takie jak np. pola tekstowe, listy wyboru, checkbox, itp. Pozwalające na parametryzowanie wyświetlanych informacji. Musi istnieć możliwość tworzenia ich bez konieczności programowania (z wykorzystaniem narzędzi graficznych).

4.13. Oferowany system musi posiadać możliwość definiowania akcji typu drill down powiązanych z różnymi typami zdarzeń oraz pól. Dostępne akcje powinny obejmować zewnętrzny URL lub raport/dashboard w samym systemie. Dla zewnętrznych URL musi istnieć możliwość przekazania parametru lub parametrów na podstawie wartości pół, których dotyczy akcja drill down. Musi istnieć możliwość przekazania parametrów metodami GET i POST.

4.14. Oferowany system musi posiadać możliwość automatycznego reagowania na zdarzenie oraz powiadomienia administratorów. Musi istnieć możliwość wysyłania e-mail oraz możliwość konfigurowania innych akcji w postaci skryptów, do których może być przekazana dowolna liczba argumentów na podstawie treści alarmu.

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

5. Wymagania techniczne i bezpieczeństwa:

5.1. Komunikacja użytkownika z systemem SIEM, musi odbywać się przy użyciu przeglądarki internetowej (wsparcie, dla co najmniej Microsoft Edge, Firefox, Chrome). Nie jest dopuszczalne wymaganie instalacji jakiegokolwiek dedykowanego oprogramowania klienckiego na stacjach roboczych użytkowników w tym wtyczek i środowisk uruchomieniowych w rodzaju Adobe Flash, Java lub Microsoft Silverlight.

5.2. Oferowany system musi umożliwiać komunikację z nim za pomocą urządzeń mobilnych Apple IOS i Google Android, i pozwalać na integrację alarmów z powiadomieniami na ww. urządzenia.

5.3. Oferowany system musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healthcheck).

5.4. Oferowany system musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów – logowanie/wylogowywanie, uruchamianie zapytania i zmiany konfiguracji systemu SIEM.

5.5. Oferowany system musi umożliwiać uwierzytelnienie oraz szyfrowanie połączenia między komponentami systemu SIEM.

5.6. W przypadku zaoferowania Zamawiającemu systemu SIEM budowanego w oparciu o rozwiązanie techniczne typu appliance, dostarczony appliance musi posiadać możliwość odpowiedniego zwiększenia wydajności do parsowania logów/danych, których wielkość może dojść do 20 GB dziennie lub 2000 zdarzeń na sekundę, nie może wtedy dochodzić do utraty logów/danych. Zamawiający przewiduje 3 krotny wzrost zapotrzebowania wydajności rozwiązania w okresie eksploatacji i oferowany w takim przypadku appliance nie może uniemożliwiać osiągnięcie tego celu. Zdarzenia musza być przechowywane na oferowanym appliance, przez co najmniej 12 miesięcy.

5.7. Zamawiający dostarczy niezbędną infrastrukturę i środowisko (serwery, systemy operacyjne, system wirtualizacji) niezbędne na potrzeby instalację systemu SIEM. Wykonawca dostarczy wszystkie niezbędne licencje i komponenty do działania prawidłowego systemu SIEM, zgodnego z wymaganiami Załącznika nr 1.

6. Termin realizacji:

6.1. Dostawa licencji na wymagany system SIEM musi nastąpić w terminie do 10 dni roboczych od zawarcia umowy.

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

7. Wsparcie producenta/Wykonawcy:

7.1. W ramach wsparcia producenta/Wykonawcy wymagany jest:

- dostęp do aktualizacji oprogramowania;
- dostęp do nowych wersji oprogramowania oraz poprawek;
- dostęp do nowych sygnatur bezpieczeństwa;
- dostęp do bazy wiedzy producenta.

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