OPIS PRZEDMIOTU ZAMÓWIENIA

Rozszerzenie licencji systemu monitorowania incydentów bezpieczeństwa – RSA SIEM.

1) Przedmiot zamówienia:

Zakup rozszerzenia licencji systemu monitorowania incydentów bezpieczeństwa – RSA SIEM obejmujący:

Dostawę licencji RSA Netwitness for Logs SA-SIEM-S-T1 50GB/day + SA-SIEM-S-T1-E1 lub równoważnej, spełniającej wymagania wskazane w Załączniku nr 1 do OPZ.

a) w liczbie 1 (jednej) sztuki;
b) wraz z gwarancją producenta **na okres do dnia 22 lutego 2023 roku;**
c) w terminie do 5 dni roboczych od dnia zawarcia umowy;

2) System SIEM Zamawiającego

1. Zamawiający posiada system SIEM RSA NetWitness for Logs.
2. Obecnie w systemie wykorzystane są licencje RSA Netwitness for Logs - SA-SIEM-S-T1 NW T1 50GB/day, w liczbie 3 trzech sztuk, pozwalających na monitorowanie łącznie 150GB logów dziennie.

3) Gwarancja.

1. W ramach gwarancji wymagane jest wsparcie producenta polegające na:
   a) aktualizacji oprogramowania;
   b) dostępie do nowych wersji oprogramowania oraz poprawek;
   c) dostępie do nowych sygnatur.
2. Zamawiający wymaga, aby mógł dokonywać aktualizacji oprogramowania do najnowszej zalecanej przez producenta wersji przez okres obowiązywania 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

Opis wymagań dla oprogramowania równoważnego do RSA Netwitness for Logs

Zamawiający posiada licencje na oprogramowanie RSA NetWitness for Logs oraz zintegrowane z platformą systemy informatyczne, które korzystają z rozwiązania firmy RSA, w łącznej liczbie ponad 100.
Zamawiający **nie wyraża zgody** na wymianę powyższego oprogramowania na inne w ramach realizacji niniejszego zamówienia.

Jeżeli Zamawiający określił w Opisie przedmiotu zamówienia wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.

I. Zamawiający dopuszcza zaoferowanie produktów równoważnych do oprogramowania RSA Netwitness for Logs

W przypadku dostarczania oprogramowania, równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie przedmiotu zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w Istotnych Warunkach Zamówienia, w szczególności w zakresie:

1. warunków licencji / sublicencji w każdym aspekcie licencjonowania / sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania jak dla oprogramowania RSA NetWitness for Logs,
2. funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w pkt III - „Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego …”,
3. oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem RSA NetWitness for Logs funkcjonującym u Zamawiającego,
4. oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,
5. oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie,
6. oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem,
7. W przypadku dostarczenia rozwiązania równoważnego Wykonawca musi wymienić, na własny koszt, posiadany przez Zamawiającego system kopii zapasowych na oferowany. W tym celu Wykonawca musi skonfigurować zadania kopii zapasowych, przenieść ich specyfikację oraz harmonogramy, przeprowadzić testy odtworzeniowe oraz dostarczyć sprzęt wraz z systemem operacyjnym oraz niezbędne licencje.
8. W przypadku zaoferowania przez Wykonawcę oprogramowania Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.

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

9. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego.
10. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.
11. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w Jego nowszych wersjach.

II. <u>W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:</u>

1. Przeprowadzić Instruktaż dla 4 administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania oprogramowaniem równoważnym, umożliwiającym pełne poznanie produktu równoważnego. Wykonawca w terminie 1 Dnia Roboczego od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogram Instruktażu.
2. Przeprowadzić Instruktaż dla 8 operatorów Zamawiającego z zakresu użytkowania oprogramowania równoważnego, umożliwiającego pełne poznanie produktu równoważnego.
3. Wykonawca w terminie 1 Dnia Roboczego od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogramy Instruktaży.
4. Instruktaże będą realizowane w Dni Robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub w formie zdalnej o ile zostaną spełnione wszystkie wymagania dotyczące Instruktażu. Instruktaże będzie trwał minimum 2 Dni Robocze każdy (łącznie minimum 14 godzin zegarowych każdy).
5. Zainstalować oprogramowanie równoważne w środowisku systemowo-programowym w terminie do 3 Dni Roboczych od dnia podpisania Umowy.
6. Dostarczyć wszelkich dodatkowych licencji - niezbędnych do prawidłowego funkcjonowania oprogramowania równoważnego.

III. <u>Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego w stosunku do oprogramowania RSA NetWitness for Logs</u>

1. Oprogramowanie musi umożliwiać przyjęcie i przetworzenie 50GB logów dziennie.
2. Oprogramowanie musi posiadać możliwość integracji z systemami klasy SIEM, SOAR, ITSM w tym Jira ServiceDesk, SIEM oraz FortiAnalyzer, CyberArk i innymi systemami zarządzania bezpieczeństwem.
3. Oprogramowanie musi definiować precyzyjne uprawnienia administratorów w zakresie monitorowanego obszaru systemu informatycznego oraz dostępnych operacji w systemie. Tożsamość administratorów musi być weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania - co najmniej RADIUS, LDAP i Active Directory. Dostęp do konsoli musi odbywać się za pomocą protokołu HTTPS.

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. Oprogramowanie musi posiadać funkcję zarządzania użytkownikami i uprawnieniami w systemie w oparciu o role „Role Based Access Control" (RBAC) oraz integrować się z LDAP/Active Directory, AzureAD. Zapewnić możliwość definiowania różnych uprawnień do systemu w zależności od wykonywanych czynności oraz ograniczać dostęp do przechowywanych w systemie danych w oparciu o filtry.
5. Oprogramowanie musi posiadać możliwość elastycznej rozbudowy o dodatkowe moduły zwiększające jego wydajność w przypadku niewydolności lub zbyt dużej ilości napływających zdarzeń w ramach zakupionych licencji.
6. W Oprogramowaniu muszą być dostępne raporty dotyczące wewnętrznego stanu systemu oraz raporty związane z incydentami/zdarzeniami bezpieczeństwa.
7. Oprogramowanie musi mieć zaimplementowany mechanizm polityki haseł w celu właściwej ochrony haseł użytkowników systemu monitorującego dla użytkowników lokalnych.
8. Oprogramowanie musi wspierać na platformie Microsoft Windows następujące przeglądarki internetowe w celu logowania do konsoli:
    a) Google Chrome aktualne na dzień składania oferty
    b) Mozilla Firefox aktualne na dzień składania oferty
9. Oprogramowanie musi posiadać zestaw podstawowych reguł, alarmów, raportów dostarczonych przez producenta.
10. Oprogramowanie musi obsługiwać, co najmniej poniższe wskaźniki kompromitacji tzw IOC:
    1) nazwa pliku;
    2) suma kontrolna pliku;
    3) URL;
    4) adres hosta lub domena;
    5) adres IP;
    6) adres email;
    7) nazwa procesu/usługi systemowej;
    8) nazwa/typ zagrożenia.
11. Oprogramowanie musi umożliwiać rozbudowę funkcjonalności o nowe typy wskaźników.
12. Oprogramowanie nie może ograniczać liczby równocześnie zalogowanych użytkowników.
13. Oprogramowanie musi zapewniać log audytowy rejestrujący co najmniej następujące operacje administratorów – logowanie użytkowników, zmiany konfiguracji systemu (w tym co najmniej: zmiany haseł użytkowników, tworzenie/usuwanie/modyfikacja obiektów systemowych).
14. Oprogramowanie musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. health check).
15. Rozwiązanie musi umożliwiać uwierzytelnianie i szyfrowanie połączenia między komponentami systemu.
16. Chwilowe przekroczenie (w ustalonym przez producenta okresie czasu) EPS/FPM nie może skutkować utratą zbieranych danych. Oprogramowanie musi informować o takim przekroczeniu w postaci alarmu i informacji w interfejsie użytkownika.
17. Oprogramowanie musi być skalowalny i umożliwiać (po zakupie dodatkowych licencji) obsługę większej ilość GB surowych danych/EPS/FPM.
18. Wymagania techniczne
19. Oprogramowanie musi pracować w architekturze wysokiej dostępności - HA.
20. W przypadku rozproszonej struktury zarządzanie całości systemu musi odbywać się z jednej konsoli.
21. Oprogramowanie musi mieć możliwość pracy w środowisku wirtualnym Vmware oraz HyperV.

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

22. Oprogramowanie musi zapewnić możliwość implementacji w środowisku rozproszonym.
23. Wymagania w zakresie normalizacji danych
24. Oprogramowanie musi umożliwiać wzbogacanie danych pochodzących z logów, o informacje zawarte w zewnętrznych repozytoriach: katalogi LDAP, dane geolokalizacyjne, DNS itp.
25. Oprogramowanie musi umożliwiać analizowanie logów wielolinijkowych.
26. Oprogramowanie musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość np. „timestamp=2020-01-02 00:00:01" musi tworzyć pole np.: „eventtime" o wartości „2020-01-02 00:00:01".
27. Wymagania w zakresie pozyskiwania danych
28. Oprogramowanie musi posiadać narzędzia integracyjne do budowy kolektorów do podłączenia się do różnych innych nietypowych aplikacji i systemów bez ograniczeń licencyjnych, wolumetrycznych, czasowych.
29. Oprogramowanie musi zapewnić jak najmniejszą ingerencję w monitorowane systemy. Oznacza to możliwość zbierania logów bez konieczności instalacji dedykowanych agentów na źródłach danych urządzeń, poprzez wykorzystanie zaimplementowanych już w systemach mechanizmów bezagentowych.
30. Oprogramowanie musi umożliwiać zbieranie danych z systemów z wykorzystaniem agentów w przypadku gdy dostęp bezagentowy nie zapewnia odpowiedniego poziomu bezpieczeństwa przesyłanych danych lub gdy istnieją inne przesłanki do wykorzystania agentów. Lista systemów opisana w wymaganiu 35.
31. Oprogramowanie musi dostarczać gotowe oprogramowanie agentów do zbierania danych i monitorowania systemów dla platform MS Windows oraz Unix i Linux. Konfiguracja agenta, po podłączeniu do serwera zarządzającego musi odbywać się centralnie. Dopuszcza się zastosowanie dwóch rozwiązań, które łącznie spełniają tę funkcjonalność.
32. Oprogramowanie musi zapewniać szyfrowanie danych w komunikacji pomiędzy agentem a serwerem systemu kolekcjonującym dane. Przykładowe szyfrowanie SSL wersja minimum 1.2
33. Oprogramowanie musi zapewniać buforowanie danych po stronie agenta w przypadku utraty lub niemożności przesłania danych między agentem a serwerem.
34. Pobieranie logów z innych systemów za pomocą wielu metod, nie mniej niż syslog UDP/TCP, trap SNMP, logi i informacje przechowywane w bazach danych Oracle, MS SQL, MySQL, PostgreSQL. Musi istnieć możliwość instalacji sterowników do innych typów baz danych w standardzie JDBC lub ODBC (alternatywnie), pliki tekstowe, Windows EventLog.
35. Oprogramowanie musi posiadać gotowe konektory dostarczone przez producenta systemu do podłączenia i zbierania informacji. Lista takich konektorów musi co najmniej obejmować pozycje przedstawione poniżej:
    - Apache HTTP Server
    - Bitdefender
    - Bluecoat
    - Cisco - Firewall, Switch, AccessPoint
    - Cisco - urządzenia sieciowe
    - Cyberark
    - Cylance
    - DNS BIND
    - ESET Antivirus/Endpoint Security
    - F5 Loadbalancer

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

- FireEye
- FortiNet (FortiAnalyzer, FortiGate, FortiMail, FortiSandbox, FortiAuthenticator)
- IBM DB2
- Kaspersky
- Linux/Unix - minimum Centos, RedHat, Suse
- McAfee EPO
- MS Exchange 2010/2013/2016
- Microsoft IIS
- Microsoft Office 365
- MobileIron
- MS-SQL Server 20XX
- MySQL
- PostgreSQL
- NginX
- Open LDAP
- OpenVPN
- Oracle Database
- PostFix
- SAP
- Sendmail
- Trend Micro
- VMware vCenter
- Windows Server HyperV
- Windows Server R2 HyperV
- MS Windows Server 2008/2012/2016, MS Windows Desktop 7/8.x/10
- AzureAD

36. Przez zbieranie informacji rozumie się:
    a) pobranie logów i zapisanie w bazie systemie
    b) klasyfikację zdarzeń wg typów (np. zalogowanie użytkownika, nawiązanie połączenia, itp.).
37. Oprogramowanie musi posiadać możliwość potwierdzania poprawnego dostarczenia danych od agenta do elementów odpowiedzialnych za przechowywanie danych.
38. Wymagania w zakresie przechowywania danych
39. Oprogramowanie musi mieć możliwość przechowywania zgromadzonych danych w postaci znormalizowanej dla wszystkich źródeł danych.
40. Oprogramowanie musi zawierać mechanizm retencji danych.
41. Wymagana jest obsługa co najmniej dwóch etapów życia danych: WARM i COLD. 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. Dane COLD muszą być dostępne w ten sam sposób co dane WARM.
42. Oprogramowanie musi umożliwiać przechowywanie danych za okres minimum 2 lat. Zapewnienie przechowywania logów i danych historycznych umożliwi korelację zdarzeń z różnych źródeł w różnych okresach, a także zapewni dostęp do zdarzeń historycznych nawet po czasie wygaśnięcia umowy. Dane muszą być przechowywane w sposób zapewniający ochronę ich integralności.

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

43. Przechowywane dane muszą być zabezpieczone przed modyfikacją z wykorzystaniem metod kryptograficznych. Oprogramowanie musi umożliwiać znakowanie danych czasem.
44. Oprogramowanie musi mieć możliwość efektywnego przechowywania logów (np. przez kompresję).
45. Oprogramowanie musi utrzymywać repozytorium logów z możliwością ich przeglądania w formie rzeczywistej (raw) oraz udostępniać użytkownikowi dane w formie znormalizowanej (z uwzględnieniem znaczenia poszczególnych zmiennych/pól logu). Dostęp do danych w formie rzeczywistej jak i znormalizowanej musi być możliwy w oparciu o te same narzędzia.
46. Oprogramowanie musi monitorować przypadki naruszenia bezpieczeństwa oraz posiadać mechanizmy śledzenia statusu rozwiązywania problemów.
47. Oprogramowanie musi analizować dane w czasie rzeczywistym. Dopuszczalne jest opóźnieniem do 15 minut przy granicznym obciążeniu do jednego tysiąca zdarzeń na sekundę (1k EPS). W przypadku przekroczenia 1k EPS czas może rosnąć liniowo o maksymalnie 3 sekundy dla każdego kolejnego kEPS (kilo Event Per Second).
48. Oprogramowanie audytu i monitorowania zdarzeń musi pracować w czasie rzeczywistym i działać (kolekcjonować dane i korelować zdarzenia) nawet w przypadku krótkiej awarii lub czasowego wyłączenia bazy danych zbierającej te informacje.
49. Oprogramowanie musi posiadać konsolę, która na bazie zdefiniowanego filtru pozwala na śledzenie w czasie rzeczywistym wybranych zdarzeń.
50. Oprogramowanie musi mieć możliwości zarządzania powiadomieniami o incydentach w postaci e-mail.
51. Oprogramowanie musi udostępniać możliwość tworzenia własnych reguł pasujących do analizy spływających do systemu informacji w oparciu o wyrażenia regularne przy pomocy wbudowanego narzędzia.
52. Oprogramowanie musi udostępniać narzędzia do analizy przepływów sieciowych NetFlows.
53. Oprogramowanie musi mieć możliwość centralnego wyszukiwania i analizy całości danych zgromadzonych przez wszystkie zainstalowane instancje serwerów systemu.
54. Oprogramowanie musi umożliwiać wyszukiwanie oraz przeglądanie danych bieżących oraz archiwalnych w lokalnym zbiorze danych gromadzonych przez system.
55. Oprogramowanie musi posiadać mechanizm wyszukiwania rozproszonego w sytuacji, gdy w środowisku zainstalowane są dwie lub więcej instancji systemu, a wynik wyszukiwania musi zawierać dane ze wskazanych przez operatora systemu.
56. Oprogramowanie musi zawierać mechanizm detekcji – automatyczne informowanie o zidentyfikowanych w zbiorze danych zgromadzonych wskutek agregacji i korelacji zdarzeniach, mogących świadczyć o występowaniu zdarzeń bezpieczeństwa. Alarmowanie to musi być realizowane poprzez wyświetlanie odpowiednich informacji na konsoli użytkownika systemu, poprzez wysyłanie powiadomień, np. za pośrednictwem poczty elektronicznej, API itp
57. Oprogramowanie musi posiadać możliwość korelacji zdarzeń na podstawie zdefiniowanych reguł, możliwość zaimplementowania gotowych oraz tworzonych ad-hoc wzorców korelacji dla zdarzeń bezpieczeństwa. Rozwiązanie musi zapewniać możliwość korelowania zbieranych zdarzeń w oparciu o reguły powiązane z poszczególnymi zdarzeniami.
58. Oprogramowanie musi być skalowalny w obszarze detekcji zdarzeń co oznacza możliwość uruchomienia więcej niż jednego modułu odpowiedzialnego za obsługę reguł korelacyjnych.
59. Oprogramowanie musi posiadać wbudowane narzędzie do obsługi incydentów bezpieczeństwa obejmujące co najmniej: możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych; możliwość przypisania incydentu do osoby; możliwość zmiany statusu i priorytetu

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

incydentu; możliwość tworzenia komentarzy; możliwość automatycznego i ręcznego modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy;

60. Oprogramowanie musi zawierać moduł, który w czasie rzeczywistym prezentować będzie dane odbiegające od statystycznego wzorca zachowania obserwowanego przez system monitorowania bezpieczeństwa teleinformatycznego źródła danych lub danego typu zdarzeń w całym monitorowanym środowisku – analiza behawioralna.
61. Oprogramowanie musi umożliwiać alarmowanie i raportowanie o anomaliach statystycznych dla dowolnych parametrów liczbowych zawartych w logach polegając na odchyleniach w stosunku do wartości przewidywanych (zarówno w górę, jak i w dół) z uwzględnieniem sezonowości (np. różnic wynikających z pory dnia, czy dnia tygodnia) – analiza behawioralna.
62. Możliwość tworzenia raportów w oparciu o dane pochodzące z podłączonych źródeł danych (np. logów generowanych przez oprogramowanie i aplikacje, przepływów sieciowych, kontroli dostępu, itp.). Możliwość generowania raportów z podziałem na odpowiednio zdefiniowane okresy czasu oraz umożliwienie ich wyeksportowania do elektronicznego formatu pliku minimum: pdf, csv.
63. Oprogramowanie musi posiadać możliwość wprowadzania zmian w raportach domyślnie zainstalowanych w systemie (dostosowanie wzorca graficznego).
64. Oprogramowanie musi umożliwiać podejmowanie automatycznych akcji lub alarmowanie. Dostępne akcje muszą obejmować co najmniej:
    1) utworzenie incydentu w systemie;
    2) wysłanie email;
    3) uruchomienie skryptu.
65. Rozwiązanie musi zawierać API pozwalające na budowanie nowych akcji, w tym przekazanie wybranych pól zdarzenia, jako parametrów akcji.
66. Wyszukiwanie danych musi być możliwe z wykorzystaniem filtrów opartych o dane znormalizowane np. zapytanie o konkretny adres IP występujący jako adres źródłowy połączeń. Oprogramowanie musi również pozwalać na wyszukiwanie danych w oparciu o wyrażenia regularne zastosowane wobec całego logu jak również pojedynczych pól.
67. Oprogramowanie musi umożliwiać korelację zdarzeń pochodzących z różnych systemów źródłowych na podstawie dowolnych pól i zmiennych logu lub dowolnych innych danych wzbogacających log, np. dane o tożsamości, dane o zasobach.
68. Oprogramowanie musi posiadać możliwość automatycznego reagowania na zdarzenie oraz powiadamiania administratorów. Musi istnieć możliwość wysłania wiadomości email oraz możliwość konfigurowania innych akcji w postaci skryptów, do których może być przekazywana dowolna liczba argumentów na podstawie treści alarmu.
69. Oprogramowanie musi pozwalać na definiowanie własnych i modyfikację reguł korelacyjnych, raportów, zapytań i dashboardów dostarczonych przez producenta.
70. Oprogramowanie w ramach dostarczonej licencji musi zapewniać możliwość instalacji nielimitowanej liczby instancji serwerów z oprogramowaniem zbierającym logi tzw. log collector.
71. Dostarczona licencja dla oprogramowania nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z 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