Załącznik nr 1 do Zapytania

Opis przedmiotu zamówienia

Przedmiot zamówienia**: Rozszerzenie funkcjonalności systemu typu SIEM -dostawa oprogramowania służącego do masowego zbierania logów maszynowych, ich wstępnej obróbki oraz analizy w czasie rzeczywistym**

Zamówienie obejmuje:

1) dostawę rozwiązania zapewniającego rozszerzenie funkcjonalności posiadanego przez Zamawiającego systemu typu SIEM służącego do masowego zbierania logów maszynowych i ich wstępnej obróbki oraz analizy w czasie rzeczywistym
2) wdrożenie,
3) gwarancję
4) warsztaty szkoleniowe.

1. Wymagania dla oprogramowania służącego do masowego zbierania logów maszynowych, ich wstępnej obróbki oraz analizy w czasie rzeczywistym:

1.1. Przyjmowanie danych pochodzących z różnych źródeł: systemów operacyjnych, urządzeń sieciowych, aplikacji, baz danych.
1.2. System musi obsługiwać standard logowania Syslog.
1.3. System musi umożliwiać zbierania ruchu Netflow.
1.4. System musi umożliwiać zbieranie logów z plików płaskich.
1.5. System ma mieć możliwość parsowania zdarzeń z różnych źródeł danych, dodawania predefiniowanych obiektów i atrybutów do struktury logów.
1.6. Agregowane dane powinny być Indeksowanie w Systemie z wykorzystaniem pełno tekstowego silnika wyszukiwania.
1.7. System musi mieć możliwość wizualizacji agregowanych danych w czasie rzeczywistym oraz z perspektywy czasu.
1.8. System musi mieć możliwość tworzenia zaawansowanych filtrów przeszukiwania danych i korelacji zdarzeń.
1.9. System musi posiadać możliwość definiowania polityk dla wskazanych źródeł danych, np. czas retencji logów, wielkość indeksu itp.
1.10. System musi umożliwiać generowanie raportów wedle wskazanych reguł/filtrów.
1.11. System musi posiadać możliwość przesyłania przefiltrowanych danych do systemu SIEM (RSA NetWitness, IBM Qradar).
1.12. Dostęp do danych oraz obsługa systemu muszą być możliwe przy pomocy interfejsu www.

Architektura Systemu.

1.13. W przypadku dostarczenia Systemu jako maszyny wirtualnej muszą być wspierane środowiska Hyper-V oraz VMware.

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

1.14. W przypadku systemu operacyjnego na którym będzie instalowany produkt jako oprogramowanie, muszą być wpierane co najmniej systemy operacyjne: Windows Server 2012 R2 /2016 (64 bit), CentOS w wersji 7.
1.15. System musi wspierać pracę w środowisku rozproszonym, klastrze (na potrzeby wdrożenia minimum 3 węzły), z możliwością dołączania kolejnych węzłów danych.
1.16. System powinien posiadać mechanizmy kolejkowania zdarzeń na wypadek awarii/przestoju działania silnika wyszukiwania.
1.17. Komunikacja pomiędzy wszystkimi komponentami Systemu musi być szyfrowana.
1.18. System może być zarządzany poprzez dedykowaną aplikację własną lub też poprzez najnowsze wersje popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox).
1.19. W przypadku dostępu do Internetu System ma umożliwiać aktualizację (oprogramowania) w sposób automatyczny jak również ręczny z poziomu systemu operacyjnego.
1.20. System musi integrować się z posiadanymi przez Zamawiającego rozwiązaniami firmy RSA: NetWitness.
1.21. System musi obsługiwać przestrzeń dyskową minimum 4 TB.
1.22. System powinien zapewniać mechanizmy retencji danych na następujących zasadach:
1.22.1. dane hot: 3 miesiące,
1.22.2. dane warm: 6 miesięcy,
1.22.3. dane cold: 24 miesiące.
1.23. System musi zapewnić wysoką dostępność w dostępie do procesowanych danych.
1.24. Na wypadek awarii System musi być możliwość przywrócenie działania Systemu z wykorzystaniem backupu konfiguracji.

Wydajność Systemu.

1.25. System powinien wspierać strumień danych w ujęciu ilościowych do 500GB danych dziennie i powinien umożliwić skalowanie do większej ilości
1.26. System powinien umożliwić przyjęcie logów z minimum 5 tysięcy źródeł.

Zarządzanie Systemem

1.27. System musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika / administratora Systemu.
1.28. Musi być możliwość określenia polityki haseł dla użytkowników Systemu.
1.29. System musi integrować się z systemem Active Directory (uwierzytelnienie, autoryzacja).
1.30. System musi umożliwiać konfigurowanie zakresu uprawnień w Systemie np. z wykorzystaniem predefiniowanych ról wewnętrznych (np. dostęp tylko do wybranych indeksów, danych, mechanizmów raportowania itp.).
1.31. System musi zapisywać (logować) zdarzenia dotyczące:
1.32. Istotnych operacji wykonywanych w Systemie przez użytkowników.
1.33. Zmian w zakresie kont oraz uprawnień wewnętrznych systemu.
1.34. Zdarzenia (logi) muszą być zapisywane w logach systemowych bądź w dedykowanym logu aplikacyjnym.
1.35. Musi być zapewniona możliwość zapisywania logów w formacie Syslog/CEF oraz zewnętrznego ich przekierowywania/składowania.
1.36. Wszystkie typy zdarzeń zapisywane w logach przez System muszą być udokumentowane w dokumentacji technicznej systemu.

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. Wdrożenie Systemu obejmuje:

2.1. Analizę aktualnych źródeł danych w CeZ i przygotowanie projektu technicznego rozwiązania (architektury systemu) zawierającego plan i harmonogram wdrożenia oraz proponowane scenariusze testów funkcjonalnych, wydajnościowych oraz akceptacyjnych.
2.2. Uruchomienie Systemu w środowisku Zamawiającego (on-premise).
2.3. Przygotowanie konfiguracji Systemu w tym elementów towarzyszących niezbędnych do działania Systemu, polityk propagacji i retencji zdarzeń.
2.4. Podpięcie unikalnych źródeł danych w CeZ wskazanych przez Zamawiającego do Systemu w ilości nie przekraczającej 50. Źródłami danych będą urządzenia sieciowe, bazy danych, systemy Windows, Linux oraz systemy własne posługujące się standardowym mechanizmem zapisu logów – syslog, pliki płaskie
2.5. Integrację wdrażanego Systemu z systemem SIEM Zamawiającego.
2.6. Przeprowadzenie testów funkcjonalnych i akceptacyjnych zainstalowanego Systemu zgodnie z zaakceptowanymi scenariuszami.
2.7. Przygotowanie powdrożeniowej dokumentacji technicznej oraz dokumentacji użytkownika Systemu zawierającej architekturę rozwiązania, spis wszystkich wdrożonych polityk bezpieczeństwa oraz retencji zdarzeń, opis konfiguracji Systemu (w tym nietypowe ustawienia), mechanizm budowania parserów, zapytań i raportów oraz instrukcję dla użytkownika/administratora Systemu w języku polskim, w formie elektronicznej – PDF oraz Word.
2.8. Za pełne wdrożenie Systemu uznaje się wykonanie wszystkich czynności opisanych w pkt. 2.1 do 2.7.

3. Gwarancja dla Systemu

3.1. Definicje:
Awaria - uszkodzenie jednego lub więcej elementów Systemu, ograniczające wydajność lub funkcjonalność lub uniemożliwiające korzystanie z Systemu zgodnie z jego specyfikacją techniczną
Błąd - każde zdarzenie, które nie jest częścią standardowego działania Systemu
Zgłoszenie - poinformowanie Wykonawcy przez przedstawiciela Zamawiającego za pomocą telefonu, wiadomości e-mail, strony internetowej lub system do zgłoszeń udostępnionego przez Wykonawcę na potrzeby realizacji Umowy o zaistniałym wydarzeniu powodującym konieczność podjęcia przez niego interwencji serwisowej. Zgłoszenie może być o zwykłym albo krytycznym priorytecie
Zgłoszenie o krytycznym priorytecie - oznacza wystąpienie Awarii w Systemie, który uniemożliwia wykorzystywanie podstawowych funkcji Oprogramowania w szczególności uniemożliwiających logowanie do Systemu, przeprowadzania skanowania bezpieczeństwa, pobierania aktualizacji i sygnatur
Zgłoszenie o zwykłym priorytecie - oznacza wystąpienie wszystkich innych Błędów niż wskazane w zgłoszeniu o krytycznym priorytecie

3.2. System musi być objęty gwarancją Wykonawcy przez okres co najmniej 24 miesięcy, od daty podpisania protokołu końcowego, która obejmuje:

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

3.2.1. Zapewnienie wsparcia producenta Systemu.

3.2.2. Zapewnienie polskojęzycznego wsparcia telefonicznego i mailowego w zakresie obsługi i konfiguracji Systemu oraz rozwiązywania problemów związanych z funkcjonalnościami Systemu.

3.2.3. Dostęp do nowych wersji oprogramowania Systemu.

3.2.4. Dostęp do aktualizacji baz zagrożeń.

3.2.5. Dostęp do bazy wiedzy i dokumentacji Systemu.

3.2.6. Zapewnienie informacji o zidentyfikowanych przez producenta Systemu podatnościach w terminie do 3 dni roboczych od momentu publikacji takiej informacji przez producenta.

3.2.7. Umożliwienie zgłaszania problemów za pomocą telefonu, wiadomości e-mail, strony internetowej lub system do zgłoszeń udostępnionego przez Wykonawcę w trybie 24/7/365.

3.2.8. Wsparcie z zakresie obsługi zgłoszeń serwisowych, a w szczególności:

3.2.8.1. Zgłoszenie o zwykłym priorytecie w zakresie Błędów związanych z Systemem z czasem reakcji maksymalnie 72 godziny od chwili wysłania zgłoszenia oraz czasem na przedstawienie propozycji rozwiązania do 5 Dni Roboczych od dnia przyjęcia zgłoszenia (przez Dni Robocze rozumie się dni od poniedziałku do piątku w godzinach 9:00-17:00, z wyjątkiem dni ustawowo wolnych od pracy i dni wolnych od pracy u Zamawiającego).

3.2.8.2. Zgłoszenie o krytycznym priorytecie - obejmujące pomoc przy wykryciu na serwerach produkcyjnych Awarii, konfiguracji Systemu, z czasem reakcji maksymalnie 2 godziny Dnia Roboczego od chwili wysłania zgłoszenia oraz czasem na przedstawienie propozycji rozwiązania do 3 Dni Roboczych od momentu przyjęcia zgłoszenia.

3.2.8.3. Rozwiązanie problemów będzie realizowane w formie rozmowy telefonicznej lub za pomocą środków online (e-mail, telekonferencja). W przypadku konieczności rozwiązania zgłoszenia w siedzibie Zamawiającego, Wykonawca zobowiązany jest zrealizować zgłoszenie w fizycznej lokalizacji Zamawiającego.

3.2.8.4. Rozwiązanie problemu o priorytecie zwykłym przez Wykonawcę nastąpi w terminie nie przekraczającym 20 Dni Roboczych od potwierdzenia przyjęcia Zgłoszenia.

3.2.8.5. Rozwiązanie problemu o priorytecie krytycznym przez Wykonawcę nastąpi w terminie nie przekraczającym 5 Dni Roboczych od potwierdzenia przyjęcia Zgłoszenia.

4. Przeprowadzenie warsztatów szkoleniowych

4.1. Zakres warsztatów powinien obejmować przynajmniej:

4.1.1. Omówienie architektury i funkcji wdrażanego Systemu

4.1.2. Omówienie konfiguracji Systemu wymaganej do prawidłowego działania Systemu

4.1.3. Działanie mechanizmu wysyłania, pobierania i analizy logów procesowanych przez System

4.1.4. Integracja Systemu z systemem SIEM Zamawiającego

4.1.5. Zarządzanie logami Systemu

4.1.6. Mechanizmy kontroli w zakresie dostępu do zdarzeń

4.1.7. Zarządzanie politykami retencji logów w zakresie poszczególnych struktur logicznych danych (indeksy)

4.1.8. Monitorowanie działania Systemu

4.1.9. Tworzenie kopii zapasowej Systemu i odtwarzanie w razie awarii

4.1.10. Stworzenie wybranego parsera, wskazanego przez Zamawiającego

4.2. Czas trwania warsztatów: co najmniej 8 godzin, podzielonych na min. dwa spotkania

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

4.3. Zajęcia powinny być przeprowadzone w języku polskim
4.4. Warsztaty powinny się odbyć w formie telekonferencji na platformie udostępnionej przez Zamawiającego w dni robocze w godzinach 9.00 – 16.00
4.5. Uczestnikom zapewnione zostaną materiały dydaktyczne w formie elektronicznej, a przebieg warsztatów zostanie zarejestrowany przy wykorzystaniu mechanizmów platformy telekonferencyjnej celem późniejszego wykorzystania przez Zamawiającego do szkoleń wewnętrznych.

5. Termin realizacji

Umowa zostanie zrealizowana w terminie maksimum 20 dni roboczych (w tym terminie Wykonawca dostarczy, wdroży System oraz przeprowadzi warsztaty, udzieli prawa do korzystania z systemu i gwarancji) , zgodnie ze złożoną ofertą, od momentu podpisania Umowy.
Gwarancja będzie udzielona na okres 24 miesięcy, od daty podpisania protokołu końcowego.

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