GUS
Dyrektor Generalny Głównego Urzędu Statystycznego
Anna Borowska

Warszawa, dnia 11.09.2020 r.

Modyfikacja i wyjaśnienia SIWZ

Działając na podstawie art. 38 ust. 1, 2, 4 i 4a ustawy Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843, z późn. zm.), Zamawiający odpowiada na pytania do SIWZ zadane przez wykonawców oraz dokonuje modyfikacji SIWZ w postępowaniu o udzielenie zamówienia pn.: „Dostawa i wdrożenie systemu do zarządzania informacją i zdarzeniami bezpieczeństwa klasy SIEM (ang. Security Information and Event Management), gromadzącego i korelującego informacje z systemów, aplikacji oraz urządzeń; numer sprawy: 41/ST/KSZBI/POPC/PN/2020, ogłoszenie o zamówieniu numer 2020/S 162-392310 z dnia 21-08-2020 r.

Pytanie 2:
Treść SIWZ
1) System SIEM realizował:
   a) obsługę, co najmniej 5000 (pięć tysięcy) zdarzeń na sekundę (ang. event per second, EPS),
   b) obsługę minimum 100GB dziennego przyrostu danych przetwarzanych w podsystemie analizy i korelacji zdarzeń,
   c) obsługę minimum 100 dniowego okresu retencji danych przetwarzanych w podsystemie analizy i korelacji zdarzeń Systemu SIEM, danych dostępnych online,
   d) obsługę minimum 250GB dziennego przyrostu danych surowych przetwarzanych w podsystemie zbierania i zarządzania logami,

Czy podane wartości dziennego przyrostu danych odnoszą się do danych surowych, nie kompresowanych w żaden sposób, otrzymywanych bezpośrednio z urządzeń?
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że podane dane wartości dziennego przyrostu danych odnoszą się do danych surowych, nie kompresowanych w żaden sposób, otrzymywanych bezpośrednio z urządzeń.

Pytanie 3:
Treść SIWZ
1) System SIEM został tak zaplanowany i dostarczony, aby w przyszłości bez konieczności rozbudowy sprzętowej i aplikacyjnej, środowisko sprzętowo-programowe (nie dotyczy licencji na EPS lub licencji równoważnych) pozwalało na obsługę 10000 (dziesięć tysięcy) zdarzeń na sekundę (10000 EPS) oraz 200GB/dzień przyrostu danych filtrowanych w Systemie SIEM;
   Zamawiający nie wymaga w tym zamówieniu, dostarczania stałej licencji dla Systemu SIEM o wartości 10000 EPS oraz 200GB/dzień lub równoważnej.

Prosimy o podanie parametrów wydajnościowych dla funkcji LogManager, w szczególności ilość odbieranych logów na sekundę. Jest to niezbędne przy licencjonowaniu systemu SIEM.
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że wymaga dla funkcji LogManager, następujących parametrów wydajnościowych: zgodnie z pkt. II 1. 1) d) Opisu przedmiotu zamówienia obsługę minimum 250GB dziennego przyrostu danych surowych oraz zgodnie z pkt. II 1. 2) OPZ, 10000 (dziesięć tysięcy) zdarzeń na sekundę (10000 EPS).

Pytanie 4:
Treść SIWZ:
2) System SIEM realizował następujące zadania:

a) korelację danych (informacji) pochodzących z różnych źródeł, w czasie rzeczywistym, w celu wykrycia zaawansowanych zagrożeń i/lub eliminacji fałszywych alarmów,
b) zbieranie, zapisywanie i przechowywanie logów na czas określony przez prawo i regulaminy wewnętrzne, na zasadach gwarantujących ochronę ich integralności,
c) wykrywanie zagrożeń, awarii i innych problemów na podstawie logów i metryk pozyskiwanych z urządzeń i systemów informatycznych.
d) weryfikację funkcjonowania zasad bezpieczeństwa i stosowanych środków kontrolnych,
e) zapewniał mechanizmy monitorujące pracowników i innych użytkowników infrastruktury teleinformatycznej,

Prosimy o potwierdzenie, że zamawiający oczekuje pełnej funkcjonalności monitorowania użytkowników. Przykłady funkcji:

- Łączenie tożsamości z różnych logów (email, login, ID, etc) do jednego konta użytkownika w oparciu o dane zewnętrzne jak Active Directory
- Uczenie się zachowania i profilowania użytkowników o mechanizmy np. Machine Learning lub reguł anomalii
- Rozróżnianie nowych kont
- Brak aktywności istniejących kont
- Zmiany parametrów działania (lokalizacja, system źródłowy, etc)

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że wymaga zaoferowania funkcjonalności monitorowania użytkowników co najmniej w zakresie danych z systemu Active Directory oraz Radius.

Pytanie 5:

Treść SIWZ:

3) architektura rozwiązania umożliwiała rozdzielenie, na co najmniej następujące osobne serwery funkcji rozumiane, jako rozwiązania zarówno sprzętowe, programowe jak i sprzętowo – programowe, w tym rozwiązania oparte o wirtualizację lub tzw. appliance:
   a) serwer funkcji SRV-LM-1 realizujący pierwszy poziom zbierania logów – danych źródłowych, stanowiący komponent zbierania i zarządzania logami (log manager) świadczący usługi przechowywania, wyszukiwania i zarządzania zebranymi logami surowymi (danymi źródłowymi), przy czym:
      i. gromadzi, wstępnie przetwarza i przesyła istotne logi – dane źródłowe, zdefiniowane w ramach projektu, do komponentu SIEM realizującego funkcję konsolidacji, analizy i korelacji zdarzeń,
      ii. wymagana minimalna retencja danych 7 dni;
      iii. wymagane jest zastosowanie rozwiązania w trybie pracy klastra niezawodnościowego (HA);
   b) serwer funkcji SRV-LM-2 realizujący drugi poziom zbierania logów – danych źródłowych stanowiący komponent zarządzania logami (log manager) świadczący usługi przechowywania, wyszukiwania i zarządzania zebranymi logami surowymi (danymi źródłowymi), przy czym:
      i. wymagana minimalna retencja danych 730 dni,
      ii. ii. nie jest wymagane stosowanie rozwiązania klastra niezawodnościowego;
   c) serwer funkcji SRV-SIEM-1 realizujący zadania SIEM: konsolidacji danych z różnych źródeł, monitorowania, analizowania oraz korelowania zdarzeń, przy czym:
      i. wymagana jest minimalna retencja danych wynosząca 100 dni,
      ii. nie jest wymagane zastosowanie rozwiązania klastra niezawodnościowego.

Zamawiający wymaga, aby proponowane rozwiązanie uwzględniało możliwość zastosowania mechanizmów kompresji danych, w procesie przechowywania logów, w celu ograniczania potrzebnej do retencji danych przestrzeni dyskowej.

Mając na uwadze złożenie najbardziej korzystnej oferty oraz zachowując poziomy funkcjonalne prosimy o zmianę treści punktu 3 na zdefiniowane wymagań bez definiowania szczegółowej struktury systemu charakterystycznej dla konkretnego producenta. Proponowana zmiana treści tego punktu została przedstawiona poniżej:

Architektura rozwiązania musi spełniać co najmniej wymagania:

a) Funkcja zarządzania logami (log manager) świadczący usługi przechowywania, wyszukiwania i zarządzania zebranymi logami surowymi (danymi źródłowymi) oraz polami charakterystycznymi (logi znormalizowane), przy czym:
   a. gromadzi, wstępnie przetwarza i przesyła istotne logi – dane źródłowe, zdefiniowane w ramach projektu, do komponentu SIEM realizującego funkcję konsolidacji, analizy i korelacji zdarzeń,
   b. wymagana minimalna retencja danych 7 dni;

   c. wymagane jest zastosowanie rozwiązania w trybie pracy klastra niezawodnościowego (HA);
b) Funkcja zarządzania logami (log manager) świadczący usługi przechowywania, wyszukiwania i zarządzania zebranymi logami surowymi (danymi źródłowymi) oraz polami charakterystycznymi (logi znormalizowane), przy czym:
   a. wymagana minimalna retencja danych 730 dni;
c) funkcji SIEM: konsolidacji danych z różnych źródeł, monitorowania, analizowania oraz korelowania zdarzeń, przy czym:
   a. wymagana jest minimalna retencja danych wynosząca 100 dni,
   b. nie jest wymagane zastosowanie rozwiązania klastra niezawodnościowego.

Wszystkie logi zarówno z funkcji log manager jak i SIEM muszą być widziane w jednej konsoli operatora i muszą mieć możliwość wykonywania tych samych zapytań i filtrów. Logi źródłowe musza być poddane normalizacji (parsowaniu) przez jeden mechanizm i wzorzec. Niedopuszczalne jest powtórne przetwarzanie danych źródłowych przez poszczególne stopnie przetwarzania w celu optymalizacji zarządzania normalizowaniem jak i optymalizacji wydajności systemu. Dane surowe jak i znormalizowane muszą być przechowywane w systemie bez duplikacji, niezależnie od funkcji realizowanej na tych danych.

Zamawiający wymaga, aby proponowane rozwiązanie uwzględniało możliwość zastosowania identycznych mechanizmów kompresji danych, w procesie przechowywania logów, w celu ograniczania potrzebnej do retencji danych przestrzeni dyskowej niezależnie od funkcji.

Architektura proponowanego rozwiązania musi być dostarczona od jednego producenta i w pełni przez niego wspierana.

Odpowiedź Zamawiającego:

Zamawiający dokonuje modyfikacji zapisów pkt II.1.5) OPZ poprzez dodanie ppkt d), w brzmieniu:

d) Zamawiający uzna za równoważne zamodelowanie architektury Systemu SIEM, inne niż wskazane w pkt II.1.5) ppkt a) – c) pod warunkiem, że zostaną spełnione parametry pojemnościowe oraz niezawodnościowe (równoważne):
   i. minimalna retencja danych wynosząca 730 dni dla logów surowych;
   ii. minimalna retencja danych wynosząca 100 dni dla logów przetwarzanych w podsystemie analizy i korelacji zdarzeń Systemu SIEM, danych dostępnych online,
   iii. komponent realizujący zadanie zbierania (przechowywania) i zarządzania logami musi być zaprojektowany w architekturze wysokiej dostępności (HA)
   iv. system będzie obsługiwał minimum 250GB dziennego przyrostu danych surowych przetwarzanych w komponencie zbierania i zarządzania logami,
   v. komponent SIEM musi zostać zaprojektowany na obsługę 10000 (dziesięć tysięcy) zdarzeń na sekundę (10000 EPS) oraz 200GB/dzień przyrostu danych filtrowanych.

Pytanie 6:

Treść:

6. w ramach przedmiotu zamówienia Wykonawca dostarczył komponent pozwalający na archiwizację (backup) i odtwarzanie po awarii komponentów dostarczonego systemu SIEM, w jednym z następujących wariantów:
   a) Wykonawca dostarczy i wdroży licencje klienckie do oprogramowania Veeam Backup&Replication w wersji 10.0., Zamawiający dysponuje oprogramowaniem serwerowym Veeam oraz przestrzenią do backupu i udostępni je na potrzeby realizacji tego przedmiotu zamówienia;

Czy zamawiający potwierdza, iż posiada wystarczającą przestrzeń dyskową do archiwizacji danych z systemu SIEM/LogManager i wymaganie 6 a) dotyczy tylko i wyłącznie licencji systemu Veeam?

Odpowiedź Zamawiającego:

Zamawiający potwierdza, iż posiada wystarczającą przestrzeń dyskową do archiwizacji danych z systemu SIEM/LogManager i wymaganie pkt II. 1. 6) a) dotyczy wyłącznie licencji systemu Veeam.

Pytanie 7:

Treść SIWZ:

8) wszystkie dostarczane systemy aplikacyjne zapewniały możliwość zarządzania lokalnego i zdalnego poprzez:
   a) graficzny interfejs użytkownika (GUI) dostępny przez standardową przeglądarkę z ochroną kryptograficzną (HTTPS),

b) dostęp do interfejsów administracyjnych musi być możliwy z wykorzystaniem zewnętrznych serwerów autoryzacyjnych (Active Directory, RADIUS lub LDAP) z obsługą zarządzania w oparciu o role,
c) możliwość synchronizacji czasu za pomocą protokołu NTP lub SNTP.

Prosimy o potwierdzenie iż wymaganie 8 a) dotyczy konsoli zarządzającej GUI pochodzącej od jednego producenta i zarządzającej wszystkimi komponentami systemu oraz działającej w protokole HTTPS.

Odpowiedź Zamawiającego:

Zamawiający nie potwierdza, iż wymaganie pkt II.1.8) a) Opisu przedmiotu zamówienia dotyczy konsoli zarządzającej GUI pochodzącej od jednego producenta i zarządzającej wszystkimi komponentami systemu, ponieważ w ocenie Zamawiającego taki zapis jest charakterystyczny dla konkretnego producenta, co mogłoby ograniczyć konkurencję.

Pytanie 8:

3. Wymagania funkcjonalne w zakresie pozyskiwanie danych
   1) System musi umożliwiać pobieranie logów/zdarzeń, z co najmniej z następujących systemów i aplikacji:
      a) Windows 2003/2008/2012/2016/2019 oraz 7/8/10,
      b) Systemów usług katalogowych Active Directory, LDAP,
      c) Systemu poczty elektronicznej Microsoft Exchange,
      d) Systemu bezpieczeństwa Mail Gateway TM IMSVA,
      e) Serwerów DNS,
      f) Serwerów DHCP,
      g) Serwerów http,
      h) Systemów Linux, w tym dystrybucji Debian, RedHat, Centos,
      i) VMware ESX 5.5 lub nowsze,
      j) urządzeń sieciowych Cisco, HP,
      k) urządzanie bezpieczeństwa Palo Alto, Check Point, F5, Cisco, Citrix ADC, Symantec Endpoint Protection,
      l) Netscout nGenius 5010 Packet Flow Switch (PFS), TruView 6300,
      m)

Czy zamawiający w punkcie 3 l) oczekuje podłączenia logów z systemu Netscout czy też odbioru kopii przepływów (flow) z tego systemu do log manager/SIEM?

Jeśli oczekiwaniem jest wysyłanie kopii przepływów to prosimy o specyfikację ilościową tej części – limit ilości przepływów w ciągu sekundy lub minuty.

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że poprzez wymóg określony w pkt II.3 1). l) Opisu przedmiotu zamówienia, oczekuje podłączenia logów z systemu Netscout. TruView 6300.

Pytanie 9:

Treść SIWZ:

n) źródeł danych geolokalizacyjnych,
o) porzez pozyskiwanie logów Zamawiający rozumie:
   i. pobranie logów oraz ich zapisanie w podsystemie serwera funkcji SRV-LM-1 a następnie przesłanie:
      – wstępnie przefiltrowanych logów, istotnych z punktu widzenia bezpieczeństwa, do podsystemu konsolidacji, analizy i korelacji zdarzeń SIEM (serwera funkcji SRV SIEM-1),
      – wszystkich pobranych logów (logów surowych) do podsystemu zarządzania logami (serwer funkcji SRV-LM-2),
p) klasyfikację zdarzeń wg typów (np. zalogowanie użytkownika, nawiązanie połączenia, itp.),
q) normalizację logów, czyli nadanie kontekstów znaczeniowych dla poszczególnych fragmentów logu np. username, source ip, itp.

Treść wymagania wskazuje strukturę fizyczną systemu dostosowaną do konkretnego systemu. Mając na uwadze optymalne przygotowanie oferty prosimy o odpowiedzi na pytania:

– Czy Zamawiający potwierdza iż dane geolokalizacyjne muszą być dostępne dla wszystkich zebranych logów w systemie niezależnie od funkcji log manager lub SIEM?
– Czy Zamawiający potwierdza iż wzbogacanie o dane geolokalizacyjne musi być realizowane w ten sam sposób dla wszystkich zebranych logów w systemie niezależnie od funkcji log manager lub SIEM? W naszej ocenie takie wymaganie pozwala na łatwe zarządzanie wyjątkami oraz wyniki spójne niezależnie od funkcji.

- Czy Zamawiający rezygnuje z bezpośredniego wskazania struktury systemu charakterystycznej dla konkretnego rozwiązania na rzecz wymagań funkcjonalnych? Szczegółowe wskazanie ilości serwerów oraz ich funkcji w naszej ocenie ogranicza konkurencyjność oraz możliwości optymalizacyjne oferty innych dostawców.
- Czy klasyfikacja zdarzeń z punktu o) musi być przeprowadzana jednokrotnie przy przyjęciu danych źródłowych i dostępna dla wszystkich funkcji systemu (log manager oraz SIEM)?
- Czy normalizacja logów musi być realizowana przez wszystkie funkcje systemu (log manager oraz SIEM)?
- Czy normalizacja logów musi być realizowana jeden raz i spójnie zarządzana dla wszystkich funkcji? Obsługa jednej bazy normalizatorów oraz wymaganie braku powielania operacji w naszej ocenie zdecydowanie poprawi zarządzalność systemem oraz stabilność rozwiązania.

Odpowiedź Zamawiającego:

1. Czy Zamawiający potwierdza iż dane geolokalizacyjne muszą być dostępne dla wszystkich zebranych logów w systemie niezależnie od funkcji log manager lub SIEM?

Ad. 1
Zamawiający wyjaśnia, że wymaga aby dane geolokalizacyjne były dostępne w podsystemie konsolidacji, analizy i korelacji zdarzeń SIEM.

2. Czy Zamawiający potwierdza iż wzbogacanie o dane geolokalizacyjne musi być realizowane w ten sam sposób dla wszystkich zebranych logów w systemie niezależnie od funkcji log manager lub SIEM? W naszej ocenie takie wymaganie pozwala na łatwe zarządzanie wyjątkami oraz wyniki spójne niezależnie od funkcji.

Ad. 2
Zamawiający potwierdza iż wzbogacanie o dane geolokalizacyjne może być realizowane w ten sam sposób dla wszystkich zebranych logów w systemie niezależnie od funkcji log manager lub SIEM.

3. Czy Zamawiający rezygnuje z bezpośredniego wskazania struktury systemu charakterystycznej dla konkretnego rozwiązania na rzecz wymagań funkcjonalnych? Szczegółowe wskazanie ilości serwerów oraz ich funkcji w naszej ocenie ogranicza konkurencyjność oraz możliwości optymalizacyjne oferty innych dostawców.

Ad. 3
W odpowiedzi na pytanie 5, Zamawiający dokonał modyfikacji zapisów pkt II.1.5) poprzez dodanie ppkt d). Wprowadzona modyfikacja umożliwi Wykonawcy zaprojektowanie systemu bez ograniczania ilości serwerów oraz ich funkcji.

4. Czy klasyfikacja zdarzeń z punktu o) musi być przeprowadzana jednokrotnie przy przyjęciu danych źródłowych i dostępna dla wszystkich funkcji systemu (log manager oraz SIEM)?

Ad. 4
Zamawiający dokonał modyfikacji pkt II.3.1) Opisu przedmiotu zamówienia poprzez usunięcie ppkt o).

5. Czy normalizacja logów musi być realizowana przez wszystkie funkcje systemu (log manager oraz SIEM)?

Ad. 5
Zamawiający wyjaśnia, że normalizacja logów nie musi być realizowana przez wszystkie funkcje systemu (log manager oraz SIEM).

6. Czy normalizacja logów musi być realizowana jeden raz i spójnie zarządzana dla wszystkich funkcji? Obsługa jednej bazy normalizatorów oraz wymaganie braku powielania operacji w naszej ocenie zdecydowanie poprawi zarządzalność systemem oraz stabilność rozwiązania.

Ad. 6.
Zamawiający wyjaśnia, że normalizacja logów nie musi być realizowana jeden raz i spójnie zarządzana dla wszystkich funkcji.

Pytanie 10:

Treść SIWZ

4) System SIEM musi umożliwiać pobieranie logów, co najmniej następującymi protokołami (metodami):
   a) syslog UDP/TCP,
   b) trap SNMP,
   c) logi i informacje przechowywane w bazach danych, dla co najmniej MS SQL, MySQL, PostgreSQL,
   d) pliki tekstowe,
   e) XML,

f) WMI,
g) NetFlow v5 i v9, sFlow, jFlow, IPFIX.

Prosimy Zamawiającego o doprecyzowanie wymagań wydajnościowych do realizowanie odbioru przepływów flow (zwłaszcza z ppkt g)). W części specyfikującej odbiór logów podano tylko dane dla logów: 5000 logów na sekundę.

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że nie jest w stanie doprecyzować wymagań wydajnościowych do realizowania odbioru przepływów flow.

Zamawiający wyjaśnia, że w ramach przedmiotowego postępowania nie wymaga dostarczenia licencji na realizowanie odbioru przepływów flow (opisanych w ppkt g).

Pytanie 11:

Treść SIWZ:

5) System SIEM musi umożliwiać pozyskiwanie danych z nasłuchu sieci. Zbierane informacje muszą obejmować wartości nagłówków połączeń do warstwy 4 ISO/OSI, oraz do warstwy 7 dla następujących protokołów:
   a) DHCP,
   b) DNS,
   c) HTTP,
   d) SMTP.

Prosimy o doprecyzowanie tego wymagania. Prosimy o specyfikację następujących parametrów, niezbędnych do prawidłowej wyceny systemu:

- Prędkości interfejsów nasłuchu
- Ilości interfejsów nasłuchu
- Zakres zbieranych informacji z nagłówków połączeń do warstwy 4, np. adresy, porty, protokoły, aplikacje, wielkości pakietów, protokół, flagi protokołu TCP
- Zakres zbieranych informacji (metadanych) warstwy 7 ISO/OSI dla DHCP.
- Zakres zbieranych informacji (metadanych) warstwy 7 ISO/OSI dla DNS.
- Zakres zbieranych informacji (metadanych) warstwy 7 ISO/OSI dla HTTP.
- Zakres zbieranych informacji (metadanych) warstwy 7 ISO/OSI dla SMTP.

Prosimy o potwierdzenie Zamawiającego iż powyższa funkcjonalność musi być realizowana przez system producenta SIEM i w jednej, spójnej konsoli GUI.

Odpowiedź Zamawiającego:

Zamawiający nie jest w stanie doprecyzować wymagania o wymienioną przez Wykonawcę specyfikację parametrów, ponieważ Zamawiający w tym zamówieniu nie wymaga dostarczenia licencji na realizowanie pozyskiwanie danych z nasłuchu sieci.

Zamawiający nie potwierdza, iż przytoczona przez Wykonawcę funkcjonalność musi być realizowana przez system producenta SIEM i w jednej, spójnej konsoli GUI, ponieważ w ocenie Zamawiającego taki zapis jest charakterystyczny dla konkretnego producenta, co mogłoby ograniczyć konkurencję.

Pytanie 12:

Treść SIWZ

4. Wymagania funkcjonalne – normalizacja danych
   1) System musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu (np. dodanie nowych pól, zmianę znaczenia lub nazwy istniejących itp.) bez konieczności przeprowadzania ponownego odbudowywania bazy danych Systemu SIEM.
      System SIEM musi pozwalać na równoległe używanie różnych sposobów normalizacji logów.
   2) System musi umożliwiać obsługę logów w formacie, co najmniej CEF, JSON, CSV.
   3) System musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość np. „user=jkowalski" powinno tworzyć pole „user" o wartości „jkowalski".
   4) System musi umożliwiać rozwiązywanie adresów IP do nazw hostów i na odwrót.
   5) System musi umożliwiać analizę logów, co najmniej w języku angielskim i polskim. Znaki w logach źródłowych kodowane przy użyciu różnych stron kodowych muszą być konwertowane do wspólnego kodowania (UTF8 lub UTF16).

Czy Zamawiający potwierdza iż wymaganie z powyższego punktu 4 dotyczy wszystkich danych źródłowych odbieranych przez cały system niezależnie od funkcji?

Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że wymaganie punktu II.4 Opisu przedmiotu zamówienia dotyczy co najmniej podsystemu konsolidacji, analizy i korelacji zdarzeń SIEM.

Pytanie 13:
Treść SIWZ:
5. Wymagania funkcjonalne – wyszukiwanie i przechowywanie danych
   1) System SIEM musi utrzymywać repozytorium logów z możliwością ich przeglądania w formie surowej (raw) oraz udostępniać użytkownikowi dane w formie znormalizowanej (z uwzględnieniem znaczenia poszczególnych zmiennych/pól logu).
   2) System SIEM musi umożliwiać skalowalność poprzez budowanie klastra, w celu spełnienia wymagań dotyczących wydajności lub dostępności.
   3) System musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej CIFS lub NFS lub iSCSI w celu przechowywania danych archiwalnych. Dopuszczalne jest by dane dostępne były z mniejszą wydajnością.
   4) System musi samodzielnie (automatycznie) zarządzać retencją danych.
   5) Przechowywane dane muszą być zabezpieczone przed modyfikacją z wykorzystaniem metod kryptograficznych.

Czy Zamawiający potwierdza iż zarządzane retencją danych powinno być realizowane centralnie z jednego miejsca (konsoli) niezależnie od funkcji (log manager lub SIEM)?
Czy Zamawiający potwierdza iż zabezpieczenie przed modyfikacją powinno być realizowane tym samym mechanizmem niezależnie od funkcji (log manager lub SIEM)?
Czy Zamawiający wymaga aby zarządzanie retencją było realizowane poprzez interfejs graficzny w sposób spójny dla wszystkich funkcji systemu (log manager lub SIEM)?
Odpowiedź Zamawiającego:
Zamawiający potwierdza iż zarządzane retencją danych może być realizowane centralnie z jednego miejsca (konsoli) niezależnie od funkcji (log manager lub SIEM).
Zamawiający potwierdza iż zabezpieczenie przed modyfikacją może być realizowane tym samym mechanizmem niezależnie od funkcji (log manager lub SIEM).
Zamawiający dopuszcza, aby zarządzanie retencją było realizowane poprzez interfejs graficzny w sposób spójny dla wszystkich funkcji systemu (log manager lub SIEM)

Pytanie 14:
Treść SIWZ:
6. Wymaganie funkcjonalne – narzędzia analityczne danych
Prosimy Zamawiającego o potwierdzenie iż wymagania punktu 6 dotyczą tylko części dla funkcji SIEM.
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że wymagania punktu II. 6 Opisu przedmiotu zamówienia dotyczą tylko części dla funkcji SIEM.

Pytanie 15:
Treść SIWZ:
6) System SIEM musi posiadać możliwości wizualizacji danych na raportach i dashboardach z wykorzystaniem:
   a) tabel,
   b) list zdarzeń,
   c) wykresów (co najmniej: słupkowy, kołowy, liniowy, punktowy, bąbelkowy),
   d) map.

W trosce o konkurencyjność składanych ofert prosimy o wykreślenie punktu d) map. Nie wszystkie systemy SIEM posiadają możliwość wizualizacji danych jednocześnie w raportach i dashboardach przez co wymaganie to ogranicza listę potencjalnych dostawców.
W trosce o konkurencyjność składanych ofert prosimy o zmianę brzmienia punktu c). Nie wszystkie systemy SIEM posiadają możliwość wizualizacji danych jednocześnie we wszystkich wskazanych formatach na raportach i dashboardach przez co wymaganie to ogranicza listę potencjalnych dostawców. Proponowane brzmienie: wykresów (co najmniej 3 z formatów: słupkowy, kołowy, liniowy, punktowy, bąbelkowy).
Odpowiedź Zamawiającego:

Zamawiający dokonuje modyfikacji zapisów Opisu przedmiotu zamówienia:
- w zakresie pkt II.6.6) c) w sposób następujący: „c) wykresów (co najmniej 3 z formatów:: słupkowy, kołowy, liniowy, punktowy, bąbelkowy)";
- w zakresie pkt II.6.6) d) poprzez wykreślenie punktu.

Pytanie 16:
Treść:
7) Musi istnieć 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.

Prosimy w wymaganiu z puntku 7) o zmianę treści na: "Musi istnieć możliwość umieszczania takich wizualizacji na dashboardach systemu." W naszej ocenie rozbudowa wizualizacji o zewnętrzne biblioteki powoduje automatycznie iż dashboard nie jest już standardowy.
Odpowiedź Zamawiającego:
Zamawiający dokonuje modyfikacji treści pkt II. 6.7), w brzmieniu zaproponowanym przez Wykonawcę, tj:
„7) Musi istnieć możliwość rozbudowy funkcjonalności o wizualizacje dostarczane przez zewnętrzne biblioteki komercyjne lub dostępne na zasadzie otwartego kodu. Musi istnieć możliwość umieszczania takich wizualizacji na dashboardach systemu.".

Pytanie 17:
Treść SIWZ
9) Musi istnieć 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 pól, których dotyczy akcja drilldown.

W trosce o konkurencyjność składanych ofert prosimy Zamawiającego o rezygnację z tego wymagania. Funkcja może być realizowana innymi metodami, charakterystycznymi dla danego systemu.
Odpowiedź Zamawiającego:
Zamawiający dokonuje modyfikacji treści pkt II.6.9) Opisu przedmiotu zamówienia, poprzez wykreślenie ww. punktu.

Pytanie 18:
Treść SIWZ
k) raporty dotyczące obsługi incydentów przez operatorów systemu,

Mając na uwadze potencjalną integrację systemu SIEM z zewnętrznym systemem obsługi zgłoszeń proponujemy rezygnację z tego wymagania gdyż będzie to powielenie funkcji dostępnej w zewnętrznym systemie.
Odpowiedź Zamawiającego:
Zamawiający podtrzymuje zapisy OPZ. Wymaganie pkt. II. 7. 14) k) jest powiązane z wymaganiami opisanymi w pkt. II. 7. 7) OPZ. Wskazane wymaganie ppkt. „k) raporty dotyczące obsługi incydentów przez operatorów systemu," nie dotyczy podsystemu korelacji zdarzeń (właściwego modułu SIEM).

Pytanie 19:
17) Mechanizm reguł korelacyjnych Systemu SIEM musi pozwalać na jednoczesną implementację, co najmniej 100 reguł korelacyjnych działających równocześnie na zdarzeniach w czasie rzeczywistym.

Prosimy o podanie minimalnej ilości reguł zaimplementowanych przez producenta w oferowanym systemie, spośród których Zamawiający może wybrać 100 aktywnych reguł.
Odpowiedź Zamawiającego:
Zamawiający nie podaje minimalnej ilości reguł zaimplementowanych przez producenta w oferowanym systemie, spośród których Zamawiający miałby wybrać 100 aktywnych reguł ponieważ w ocenie Zamawiającego takie wymaganie mogłoby w nieupoważniony sposób ograniczać konkurencję.

Pytanie 20:
Treść SIWZ
16) W dniu produkcyjnego uruchomienia System SIEM () musi zwierać, co najmniej 20 reguł korelacyjnych utworzonych na potrzeby Zamawiającego.

Prosimy o sprecyzowanie wymagania dotyczącego reguł: czy Zamawiający ma na myśli reguły, których wynikiem jest podniesienie alarmu w wypadku spełnienia warunków?
Czy reguły muszą mieś strukturę hierarchiczną i pozwalać na powtórne ich zastosowanie w innych regułach? Przykładem może być wyznaczanie poprzez jedną regułę standardowych godzin pracy i jej zastosowanie w innych regułach. Dzięki takiemu mechanizmowi możliwe jest dokonanie jednej zmiany reguły pierwotnej, a pozostałe reguły automatycznie będą działać według nowych kryteriów.

Odpowiedź Zamawiającego:

Tak, Zamawiający potwierdza, że reguły korelacyjne utworzone na potrzeby Zamawiającego, o których mowa w pkt II.7.16) Opisu przedmiotu zamówienia, to reguły, których wynikiem jest podniesienie alarmu w wypadku spełnienia warunków.
Zamawiający wyjaśnia, że reguły korelacyjne utworzone na potrzeby Zamawiającego, o których mowa w pkt II.7.16) Opisu przedmiotu zamówienia, mogą mieć strukturę hierarchiczną i pozwalać na powtórne ich zastosowanie w innych regułach.

Pytanie 21:

Treść SIWZ

11) System SIEM musi umożliwiać korzystanie z zewnętrznych subskrypcji tzw. wskaźników kompromitacji (ang. IOC Indicator of compromise).

Czy w ramach prowadzonego postępowania zamawiający oczekuje dostarczenia rozwiązania, które zawiera również własne bazy reputacyjne budowane w oparciu o usługi typu Threat Intelligence Feed udostępniane przez tego samego dostawcę i powszechnie rozpoznawane oraz wysoko oceniane przez takie organizacje jak Gartner?

Odpowiedź Zamawiającego:

W ramach prowadzonego postępowania Zamawiający nie wymaga dostarczenia rozwiązania, które zawiera również własne bazy reputacyjne budowane w oparciu o usługi typu Threat Intelligence Feed udostępniane przez tego samego dostawcę i powszechnie rozpoznawane oraz wysoko oceniane przez takie organizacje jak Gartner.
Opis przedmiotu zamówienia opisuje minimalne wymagania ilościowe i funkcjonalne i w żaden sposób nie ogranicza Wykonawcy w zakresie możliwości zaoferowania dodatkowych lub innych komponentów wzbogacających przedmiot zamówienia, Zamawiający oczekuje od Wykonawcy profesjonalnego rozwiązania technicznego.

Pytanie 22:

Dot. Zapis punkt 1, podpunkt 3d:
System SIEM realizował następujące zadania:[...] d. weryfikację funkcjonowania zasad bezpieczeństwa i stosowanych środków kontrolnych,
Czy Zamawiający pisząc to sformułowanie ma na myśli weryfikację spełnienia norm regulacyjnych np. PCI DSS, HIPPA itp? Jeśli nie, to prosimy o zobrazowanie na przykładzie.

Odpowiedź Zamawiającego:

Zamawiający oczekuje, że przedmiot zamówienia zaoferowany przez Wykonawcę będzie spełniał wymagania norm i przepisów obowiązujących w jednostkach administracji publicznej (np. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych).

Pytanie 23:

Dot. Zapis: punkt 1, podpunkt 5 a, od i. do iv.

1) architektura rozwiązania umożliwiała rozdzielenie, na co najmniej następujące osobne serwery funkcji rozumiane, jako rozwiązania zarówno sprzętowe, programowe jak i sprzętowo – programowe, w tym rozwiązania oparte o wirtualizację lub tzw. appliance:
   a) serwer funkcji SRV-LM-1 realizujący pierwszy poziom zbierania logów – danych źródłowych, stanowiący komponent zbierania i zarządzania logami (log manager) świadczący usługi przechowywania, wyszukiwania i zarządzania zebranymi logami surowymi (danymi źródłowymi), przy czym:
      i. gromadzi, wstępnie przetwarza i przesyła istotne logi – dane źródłowe, zdefiniowane w ramach projektu, do komponentu SIEM realizującego funkcję konsolidacji, analizy i korelacji zdarzeń,
      ii. gromadzi i przesyła wszystkie zebrane logi – dane źródłowe do serwera funkcji realizującego drugi poziom przetwarzania logów – tj. do serwera funkcji stanowiącego komponent zarządzania logami (log manager),

iii. wymagana minimalna retencja danych 7 dni;
iv. wymagane jest zastosowanie rozwiązania w trybie pracy klastra niezawodnościowego (HA);

Czy Zamawiający dopuszcza wykorzystanie dodatkowych agentów/mechanizmu connectorów, które będą wstępnie parsować i normalizować dane?

Odpowiedź Zamawiającego:

Zamawiający dopuszcza wykorzystania dodatkowych agentów/mechanizmu connectorów, które będą wstępnie parsować i normalizować dane.

Pytanie 24:

Według opisanych przez zamawiającego funkcji biznesowych systemu SRV-LM-1 służy wyłącznie do wstępnego gromadzenia oraz przesyłania logów do systemów przetwarzających dane pod kątem bezpieczeństwa – SRV-LM-2 oraz SRV-SIEM-1, a co za tym idzie jest elementem pośredniczącym.
Zamawiający wymaga wdrożenia mechanizmów HA dla tego elementu systemu, ale nie wymaga ich dla systemów przechowujących dane przez okres 2 lat, w wypadku SRV-LM-2, czy dla mechanizmu korelującego i wykrywającego incydenty bezpieczeństwa w czasie rzeczywistym – SRV-SIEM-1. Pytający sugeruje rozszerzenie objęcia mechanizmami HA właśnie te, bardziej, w przekonaniu Pytającego istotne, komponenty systemu, natomiast co do komponentu SRV-LM-1 sugeruje pominięcie tego wymagania, argumentując, że nawet w wyniku awarii tego komponentu dane nie ulegają utraceniu. Czy Zamawiający wyraża zgodę na sugerowane przez Pytającego zmiany?

Odpowiedź Zamawiającego:

W odpowiedzi na pytanie 5 Zamawiający dokonał modyfikacji zapisów modyfikacji zapisów pkt II.1.5) poprzez dodanie ppkt d), w brzmieniu:

d) Zamawiający uzna za równoważne zamodelowanie architektury Systemu SIEM, inne niż wskazane w pkt II.1.5) ppkt a) – c) pod warunkiem, że zostaną spełnione parametry pojemnościowe oraz niezawodnościowe (równoważne):
   i. minimalna retencja danych wynosząca 730 dni dla logów surowych;
   ii. minimalna retencja danych wynosząca 100 dni dla logów przetwarzanych w podsystemie analizy i korelacji zdarzeń Systemu SIEM, danych dostępnych online,
   iii. komponent realizujący zadanie zbierania (przechowywania) i zarządzania logami musi być zaprojektowany w architekturze wysokiej dostępności (HA)
   iv. system będzie obsługiwał minimum 250GB dziennego przyrostu danych surowych przetwarzanych w komponencie zbierania i zarządzania logami,
   v. komponent SIEM musi zostać zaprojektowany na obsługę 10000 (dziesięć tysięcy) zdarzeń na sekundę (10000 EPS) oraz 200GB/dzień przyrostu danych filtrowanych.

Wprowadzony zapis daje Wykonawcy możliwość równoważnego zamodelowanie architektury Systemu SIEM.

Pytanie 25:

Wzór umowy. § 11. Gwarancja i rękojmia za wady
W punkcie 5 Zamawiający zdefiniował oczekiwane parametry SLA, np dla „Awarii krytycznej" oczekiwany Czas Reakcji to 4 godziny, czas przywrócenia systemu to 24 godziny, czas usunięcia awarii 48 godzin od momentu dokonania zgłoszenia.
Dodatkowo w punkcie 9 ww paragrafu wprowadzono wymóg przyjmowania zgłoszeń w trybie 24/7/365.
Następnie w punkcie 10 pojawiają się zapisy:
„10. Podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nie może przekroczyć:
1) 4 godzin – w przypadku zgłoszenia Awarii Krytycznej,
2) 8 godzin – w przypadku zgłoszenia Błędu
od momentu dokonania przez Zamawiającego zgłoszenia Problemu funkcjonowania Systemu SIEM, jeżeli do zgłoszenia doszło do godziny 16:00 dnia roboczego; W przypadku jeżeli zgłoszenie Problemu nastąpi po godzinie 16:00 lub w dzień ustawowo wolny od pracy, podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nastąpi następnego dnia roboczego w godzinach od 8:15 do 12:15"
Prosimy o wyjaśnienie – czy zgłoszenia mają być obsługiwane w trybie 24/7/365 na co wskazują zapisy w punktach 5 oraz 9 czy też zgodnie z punktem 10 zgłoszenia są przyjmowane w trybie 24/7/365 natomiast obsługa zgłoszeń jest prowadzona tylko w dni w dni robocze?
Np. jaki będzie Czas Reakcji oraz Czas naprawy Awarii Krytycznej zgłoszonej w sobotę o godzinie 12:00?
Czy Wykonawca – zgodnie z zapisami w pkt 5 oraz 9 ma zapewnić Czas Reakcji do godziny 16 w tym samym dniu i Czas naprawy (48 godzin) do godziny 12:00 w poniedziałek, czy też zgodnie z zapisami w pkt 10 naliczanie Czasów Reakcji, przywrócenia systemu, usunięcia awarii startuje od poniedziałku od godziny 08:15?

Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że stosownie do zapisów § 11 projektu umowy, Zamawiający zastrzega sobie prawo do zgłaszania problemów funkcjonowania Systemu SIEM przez 7 dni tygodnia w godzinach 0:00-24:0, z zastrzeżeniem, że w przypadku jeżeli zgłoszenie Problemu nastąpi po godzinie 16:00 lub w dzień ustawowo wolny od pracy, podjęcie działań diagnostycznych przez Wykonawcę i kontakt ze zgłaszającym nastąpi następnego dnia roboczego w godzinach od 8:15 do 12:15, tj.:
1) zgłoszenia będą przyjmowane w trybie 24/7/365,
2) obsługa zgłoszeń będzie prowadzona tylko w dni w dni robocze,
naliczanie Czasu reakcji, Czasu przywrócenia systemu, Czasu naprawy, zgłoszonej po godzinie 16:00 lub w dzień ustawowo wolny od pracy, będzie realizowane od kolejnego dnia roboczego (np. poniedziałku) od godziny 08:15.

Pytanie 26:
OPZ Pkt II, ppkt 2:
Zamawiający wymaga aby System SIEM został tak zaplanowany i dostarczony, aby w przyszłości bez konieczności rozbudowy sprzętowej i aplikacyjnej, środowisko sprzętowo-programowe (nie dotyczy licencji na EPS lub licencji równoważnych) pozwalało na obsługę 10000 (dziesięć tysięcy) zdarzeń na sekundę (10000 EPS) oraz 200GB/dzień przyrostu danych filtrowanych w Systemie SIEM;
Zamawiający nie wymaga w tym zamówieniu, dostarczania stałej licencji dla Systemu SIEM o wartości 10000 EPS oraz 200GB/dzień lub równoważnej.
Czy Zamawiający dopuści system SIEM realizujący co najmniej 5000 (pięć tysięcy) zdarzeń na sekundę (EPS) wraz z obsługą minimum 100GB przyrostu dziennego danych filtrowanych w Systemie SIEM, który po rozbudowie sprzętowo-aplikacyjnej (w tym dostarczeniu odpowiednich licencji na EPS oraz wymaganego sprzętu) pozwoli na obsługę 10000 (dziesięć tysięcy) zdarzeń na sekundę (10000 EPS) oraz 200GB/s przyrostu danych filtrowanych w Systemie SIEM?
Odpowiedź Zamawiającego:
Zamawiający nie dopuszcza system SIEM realizującego co najmniej 5000 (pięć tysięcy) zdarzeń na sekundę (EPS) wraz z obsługą minimum 100GB przyrostu dziennego danych filtrowanych w Systemie SIEM, **który po rozbudowie sprzętowo-aplikacyjnej** (w tym dostarczeniu odpowiednich licencji na EPS oraz wymaganego sprzętu) pozwoli na obsługę 10000 (dziesięć tysięcy) zdarzeń na sekundę (10000 EPS**) oraz 200GB/s przyrostu danych filtrowanych w Systemie SIEM**.
Uzasadnienie.
Zamawiający podtrzymuje zapisy OPZ, ponieważ Zamawiający oczekuje od Wykonawcy zaprojektowania i dostarczenia systemu SIEM gotowego do obsługi 10000 (dziesięć tysięcy) zdarzeń na sekundę (10000 EPS) oraz 200GB/s przyrostu danych filtrowanych w Systemie SIEM.

Pytanie 27:
Dotyczy Załącznika nr 1 do SIWZ, Punkt IV. Zadanie II - Dostawa i wdrożenie Systemu SIEM, Punkt 1, Podpunkt 11:
„Zamawiający wymaga, aby dostarczane licencje były nieograniczone terytorialnie, bezterminowe, przenoszalne, uprawniające do korzystania z Oprogramowania Gotowego bez ograniczeń ilościowych innych niż określone w OPZ."
Podane wymagania są dyskryminujące dla rozwiązań licencjonowanych w określonych okresach czasu (np. 5 lat) oraz nieprzenaszalnych z uwagi na fakt że wielu z liczących się vendorów (pozycjonowanych jako liderzy w Raporcie Gartnera), stosuje ten model licencyjny. Tak przedstawione wymagania znacząco ograniczają konkurencję i stanowią naruszenie przepisów art. 29 ust. 2 PZP w związku z art. 7 ust. 1 i zasadę równego traktowania wykonawców i uczciwej konkurencji– stanowiącą fundamentalną zasady systemu zamówień publicznych.
W związku z powyższym wnosimy o zmianę wymagania na: Zamawiający wymaga, aby dostarczane licencje były nieograniczone terytorialnie, uprawniające do korzystania z Oprogramowania Gotowego bez ograniczeń ilościowych innych niż określone w OPZ."
Odpowiedź Zamawiającego:
Zamawiający wyraża zgodę na zmianę zaproponowaną przez Wykonawcę. Zamawiający modyfikuje treść zapisów pkt. IV.1.11) nadając mu brzmienie:
11) Zamawiający wymaga, aby dostarczane licencje były nieograniczone terytorialnie, uprawniające do korzystania z Oprogramowania Gotowego bez ograniczeń ilościowych innych niż określone w OPZ.

Pytanie 28:
Dotyczy Załącznika nr 1 do SIWZ, Punkt II. Zadanie II - Opis wymagań Systemu SIEM, Punkt 1, Podpunkt 5:

Czy Zamawiający dopuszcza inne niż podane w OPZ zamodelowanie architektury, o ile zostaną spełnione wszystkie parametry pojemnościowe oraz niezawodnościowe?
Uzasadnienie: W przypadku niektórych wiodących rozwiązań z obszaru Log Management / SIEM, funkcje poszczególnych komponentów nieco się różnią, względem opisu w pkt 5 (np. nie ma potrzeby przesyłania danych z komponentu opisanego jaki pierwszy poziom zbierania logów do komponentu SIEM) – w efekcie, pewne funkcje można np. połączyć a niektóre inaczej zamapować.

Odpowiedź Zamawiającego:

Zamawiający dokonał modyfikacji zapisów modyfikacji zapisów pkt II.1.5) poprzez dodanie ppkt d), w brzmieniu:

d) Zamawiający uzna za równoważne zamodelowanie architektury Systemu SIEM, inne niż wskazane w pkt II.1.5) ppkt a) – c) pod warunkiem, że zostaną spełnione parametry pojemnościowe oraz niezawodnościowe (równoważne):
   i. minimalna retencja danych wynosząca 730 dni dla logów surowych;
   ii. minimalna retencja danych wynosząca 100 dni dla logów przetwarzanych w podsystemie analizy i korelacji zdarzeń Systemu SIEM, danych dostępnych online,
   iii. komponent realizujący zadanie zbierania (przechowywania) i zarządzania logami musi być zaprojektowany w architekturze wysokiej dostępności (HA)
   iv. system będzie obsługiwał minimum 250GB dziennego przyrostu danych surowych przetwarzanych w komponencie zbierania i zarządzania logami,
   v. komponent SIEM musi zostać zaprojektowany na obsługę 10000 (dziesięć tysięcy) zdarzeń na sekundę (10000 EPS) oraz 200GB/dzień przyrostu danych filtrowanych.

Wprowadzony zapis daje Wykonawcy możliwość równoważnego zamodelowanie architektury Systemu SIEM.

Pytanie 29:

Dotyczy Załącznika nr 1 do SIWZ, Punkt II. Zadanie II - Opis wymagań Systemu SIEM, Punkt 2, Podpunkt 2 (Lista przepływów):
Czy Zamawiający dopuszcza zastosowania innych metod (protokołów lub API) do pozyskania logów z podanych systemów, przy założeniu co najmniej tego samego zakresu dostępnych danych?

Odpowiedź Zamawiającego:

Zamawiający w pkt II.2.2) Opisu przedmiotu zamówienia (Lista przepływów) wskazał, że: „(...) wymaga, aby w ramach realizacji przedmiotu zamówienia Wykonawca, dysponując profesjonalną wiedzą oraz korzystając z dobrych praktyk, dokonał analizy wskazanego w powyższych tabelach obszaru informacyjnego i stosownie do możliwości technicznych, funkcjonalnych oraz ograniczeń wynikających z liczby licencji Systemu SIEM zdefiniowanych przez Zamawiającego, zaplanował i wdrożył niezbędny do monitorowania zakres informacyjny.”. Zamawiający wyjaśnia, że w świetle powyższych zapisów Zamawiający dopuszcza zastosowania innych metod (protokołów lub API) do pozyskania logów z podanych systemów, przy założeniu co najmniej tego samego zakresu dostępnych danych.

Pytanie 30:

Dotyczy Załącznika nr 1 do SIWZ, Punkt IV. Zadanie II - Dostawa i wdrożenie Systemu SIEM, Punkt 1, Podpunkt 2 b)
Prosimy o wyjaśnienie co Zamawiający na myśli stawiając wymóg aby serwery były wyposażone w redundantne procesory. Czy Zamawiający oczekuje dostarczenia urządzenia z dwoma procesorami czy redundancji całego systemu?

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że stawiając wymóg, aby serwery były wyposażone w redundantne procesory miał na myśli dostarczenie urządzenia lub urządzeń z dwoma procesorami.
Opis przedmiotu zamówienia opisuje minimalne wymagania ilościowe i funkcjonalne i w żaden sposób nie ogranicza Wykonawcy w zakresie możliwości zaoferowania dodatkowych lub innych komponentów wzbogacających przedmiot zamówienia, Zamawiający oczekuje od Wykonawcy profesjonalnego rozwiązania technicznego.

Pytanie 31:

Czy biorąc pod uwagę aktualną sytuację epidemiologiczną Zamawiający dopuszcza możliwość realizowania prac projektowych w formie zdalnej (np. webex/zoom lub remote-access vpn)?

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że biorąc pod uwagę aktualną sytuację epidemiologiczną, dopuszcza możliwość realizowania prac projektowych, Zadanie I, w formie zdalnej (np. webex/zoom lub remote-access vpn). Środki komunikacji zdalnej zapewni Wykonawca.

Pytanie 32:
W punkcie 7.1. punkt A i B SIWZ Zamawiający zawarł wymóg, aby wymienione w tym punkcie osoby odpowiedzialne za wykonanie usług, w tym: Architekt ds. Systemów klasy SIEM lub analitycznych oraz Inżynier ds. Systemów klasy SIEM lub analitycznych, oprócz doświadczenia w zakresie projektowania i wdrażania systemów klasy SIEM, legitymowali się również:
- świadectwem dojrzałości wydanym przez szkołę działającą w systemie edukacji RP, lub
- urzędowym poświadczeniem znajomości języka polskiego na poziomie A1 stosownie do przepisów ustawy z dnia 7 października 1999r. O języku polskim.
Przedmiotowe postanowienie SIWZ w istotny sposób dyskryminuje osoby nie posługujące się językiem polskim, jak również istotnie narusza zasady otwartej konkurencji w ten sposób, że ogranicza dostęp do przetargu firmom zagranicznym, których pracownicy posiadają kwalifikacje zawodowe i doświadczenie określone w punktach 7.1. A a) i B a), ale nie posiadają wymienionych w punktach 7.1. A b) I B b) dokumentów potwierdzających znajomość języka polskiego.
Zauważyć trzeba również, że umowa o wykonanie usług objętych SIWZ dotyczy osób prawnych, a zatem Wykonawca zobowiązany jest wykonać przedmiot umowy zgodnie z warunkami umowy, a Zamawiający odebrać wykonane prace i zapłacić za wykonane usługi. Jest również oczywiste, że we wszystkich etapach realizacji umowy stosowany będzie język polski, jednakże w gestii Wykonawcy leży wybór sposobu w jaki komunikował się będzie z Zamawiającym. Istotne jest jedynie to, że Zamawiający nie ma żadnego obowiązku stosowania w kontaktach z wykonawcą na żadnym etapie realizacji umowy innego języka niż język polski.
Kwestionowane wyżej wymaganie SIWZ nie znajduje również podstawy prawnej w obowiązujących w tym zakresie przepisach, w tym w szczególności w ustawie z dnia 29 stycznia 2004r. Prawo zamówień publicznych (Dz.U. z 2015 poz. 2164 z późn.zm), a także przepisach wykonawczych tj. w Rozporządzeniu Ministra Rozwoju z dnia 27 lipca 2016r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz.U. poz. 1126 z późn.zm.).
Żaden z przepisów powołanych wyżej aktów prawnych nie przewiduje możliwości ograniczenia udziału wykonawców w publicznych przetargach na terenie UE ze względu na brak znajomości języka polskiego pracowników wykonawcy. Taki warunek, jak znajomość języka polskiego nie został tam po prostu wymieniony, i co więcej nie można tego warunku w żaden sposób wywieść w drodze interpretacji rozszerzonej z innych zawartych w tych aktach przepisów prawnych.
W związku z tym wnosimy o usunięcie kwestionowanego przez nas warunku dotyczącego kwalifikacji językowych pracowników wykonawcy, wymienionych w punkcie 7.1. A i B SIWZ (nr sprawy j.w.)
Odpowiedź Zamawiającego:
Zamawiający dokonał modyfikacji pkt 7.1.4) Specyfikacji Istotnych Warunków Zamówienia poprzez wykreślenie wymagań stawianych Architektowi ds. systemów klasy SIEM lub analitycznych oraz Inżynierowi ds. systemów klasy SIEM lub analitycznych odnoszących się do posługiwania się językiem polskim oraz posiadania świadectwa dojrzałości wydanego przez szkołę działającą w systemie edukacji Rzeczypospolitej Polskiej lub posiadania urzędowego poświadczenia znajomości języka polskiego, jako obcego na poziomie biegłości językowej A1 stosownie do przepisów ustawy z dnia 7 października 1999 r. o języku polskim (Dz.U. z 2019 r. poz. 1480, z późn. zm.);
Jednocześnie Zamawiający informuje, że dokonał modyfikacji zapisów pkt I Opisu przedmiotu zamówienia w sposób następujący poprzez dodanie zapisu: „(...) Zamawiający wymaga, aby w trakcie realizacji przedmiot zamówienia komunikacja pomiędzy stronami, w tym z osobami bezpośrednio uczestniczącymi w wykonywaniu zamówienia ze strony Wykonawcy odbywała się w języku polskim. Sposób zapewnienia komunikacji w języku polskim leży w gestii Wykonawcy.

Zamawiający dokonał następującej modyfikacji SIWZ:

SIWZ – pkt 7.1.4) – było

(...)
Określenie warunków:
Ponadto o udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy dysponują lub będą dysponować zespołem co najmniej 2 osób zdolnych do wykonywania zamówienia i spełniających poniższe wymagania:
A. Architekt ds. systemów klasy SIEM lub analitycznych – 1 osoba – która:

a) posiada doświadczenie w zakresie projektowania i wdrażania systemów klasy SIEM lub analitycznych, potwierdzone udziałem, w co najmniej jednym, w pełni zakończonym projekcie (umowie lub kontrakcie,) o wartości, co najmniej 246.000,00 zł brutto;
b) posługuje się językiem polskim oraz posiada świadectwo dojrzałości wydane przez szkołę działającą w systemie edukacji Rzeczypospolitej Polskiej lub posiada urzędowe poświadczenie znajomości języka polskiego, jako obcego na poziomie biegłości językowej A1 stosownie do przepisów ustawy z dnia 7 października 1999 r. o języku polskim (Dz.U. z 2019 r. poz. 1480, z późn. zm.);

B. Inżynier ds. systemów klasy SIEM lub analitycznych – 1 osoba – która:
a) posiada doświadczenie w zakresie wdrażania systemów klasy SIEM lub analitycznych, potwierdzoną udziałem, w co najmniej jednym, w pełni zakończonym projekcie (umowie lub kontrakcie), o wartości, co najmniej 246.000,00 zł brutto;
b) posługuje się językiem polskim oraz posiada świadectwo dojrzałości wydane przez szkołę działającą w systemie edukacji Rzeczypospolitej Polskiej lub posiada urzędowe poświadczenie znajomości języka polskiego, jako obcego na poziomie biegłości językowej A1 stosownie do przepisów ustawy z dnia 7 października 1999 r. o języku polskim (Dz.U. z 2019 r. poz. 1480, z późn. zm.);

SIWZ – pkt 7.1.4) – powinno być

(...)
Określenie warunków:
Ponadto o udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy dysponują lub będą dysponować zespołem co najmniej 2 osób zdolnych do wykonywania zamówienia i spełniających poniższe wymagania:

A. Architekt ds. systemów klasy SIEM lub analitycznych – 1 osoba – która:
posiada doświadczenie w zakresie projektowania i wdrażania systemów klasy SIEM lub analitycznych, potwierdzone udziałem, w co najmniej jednym, w pełni zakończonym projekcie (umowie lub kontrakcie,) o wartości, co najmniej 246.000,00 zł brutto;

B. Inżynier ds. systemów klasy SIEM lub analitycznych – 1 osoba – która:
posiada doświadczenie w zakresie wdrażania systemów klasy SIEM lub analitycznych, potwierdzoną udziałem, w co najmniej jednym, w pełni zakończonym projekcie (umowie lub kontrakcie), o wartości, co najmniej 246.000,00 zł brutto.

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt I – było

I. Przedmiot zamówienia obejmuje 5 zadań, w tym:
1. Zadanie I - Wykonanie projektu technicznego Systemu SIEM;
2. Zadanie II - Dostawa i wdrożenie Systemu SIEM;
3. Zadanie III - Optymalizacja działania Systemu SIEM;
4. Zadanie IV – Wykonanie instruktażu;
5. Zadanie V - Wykonanie Dokumentacji powykonawczej Systemu SIEM.

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt I – powinno być

II. Przedmiot zamówienia obejmuje 5 zadań, w tym:
6. Zadanie I - Wykonanie projektu technicznego Systemu SIEM;
7. Zadanie II - Dostawa i wdrożenie Systemu SIEM;
8. Zadanie III - Optymalizacja działania Systemu SIEM;
9. Zadanie IV – Wykonanie instruktażu;
10. Zadanie V - Wykonanie Dokumentacji powykonawczej Systemu SIEM.

Zamawiający wymaga, aby w trakcie realizacji przedmiot zamówienia komunikacja pomiędzy stronami, w tym z osobami bezpośrednio uczestniczącymi w wykonywaniu zamówienia ze strony Wykonawcy odbywała się w języku polskim. Sposób zapewnienia komunikacji w języku polskim leży w gestii Wykonawcy.

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt II.1.5) d) – było

Brak zapisów

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt II.1.5) d) – powinno być

d) Zamawiający uzna za równoważne zamodelowanie architektury Systemu SIEM, inne niż wskazane w pkt II.1.5) ppkt a) – c) pod warunkiem, że zostaną spełnione parametry pojemnościowe oraz niezawodnościowe (równoważne):

i. minimalna retencja danych wynosząca 730 dni dla logów surowych;
ii. minimalna retencja danych wynosząca 100 dni dla logów przetwarzanych w podsystemie analizy i korelacji zdarzeń Systemu SIEM, danych dostępnych online,
iii. komponent realizujący zadanie zbierania (przechowywania) i zarządzania logami musi być zaprojektowany w architekturze wysokiej dostępności (HA)
iv. system będzie obsługiwał minimum 250GB dziennego przyrostu danych surowych przetwarzanych w komponencie zbierania i zarządzania logami,
v. komponent SIEM musi zostać zaprojektowany na obsługę 10000 (dziesięć tysięcy) zdarzeń na sekundę (10000 EPS) oraz 200GB/dzień przyrostu danych filtrowanych.

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt II.3.1) o) - q) – było

o) porzez pozyskiwanie logów Zamawiający rozumie:
   i. pobranie logów oraz ich zapisanie w podsystemie serwera funkcji SRV-LM-1 a następnie przesłanie:
      – wstępnie przefiltrowanych logów, istotnych z punktu widzenia bezpieczeństwa, do podsystemu konsolidacji, analizy i korelacji zdarzeń SIEM (serwera funkcji SRV-SIEM-1),
      – wszystkich pobranych logów (logów surowych) do podsystemu zarządzania logami (serwer funkcji SRV-LM-2),
p) klasyfikację zdarzeń wg typów (np. zalogowanie użytkownika, nawiązanie połączenia, itp.),
q) normalizację logów, czyli nadanie kontekstów znaczeniowych dla poszczególnych fragmentów logu np. username, source ip, itp.

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt II.3.1) o) - q) – powinno być

o) klasyfikację zdarzeń wg typów (np. zalogowanie użytkownika, nawiązanie połączenia, itp.),
p) normalizację logów, czyli nadanie kontekstów znaczeniowych dla poszczególnych fragmentów logu np. username, source ip, itp.

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt II.6.6) c) - d) – było

c) wykresów (co najmniej: słupkowy, kołowy, liniowy, punktowy, bąbelkowy),
d) map.

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt II.6.6) c) - d) – powinno być

c) wykresów (co najmniej 3 z formatów: słupkowy, kołowy, liniowy, punktowy, bąbelkowy),

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt II.6.7) – było

7) Musi istnieć 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.

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt II.6.7) – powinno być

7) Musi istnieć możliwość rozbudowy funkcjonalności o wizualizacje dostarczane przez zewnętrzne biblioteki komercyjne lub dostępne na zasadzie otwartego kodu. Musi istnieć możliwość umieszczania takich wizualizacji na dashboardach systemu.

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt II.6.9) – było

9) Musi istnieć 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 pól, których dotyczy akcja drilldown.

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt II.6.9) – powinno być

Brak zapisów

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt IV.1.11) – było

11) Zamawiający wymaga, aby dostarczane licencje były nieograniczone terytorialnie, bezterminowe, przenoszalne, uprawniające do korzystania z Oprogramowania Gotowego bez ograniczeń ilościowych innych niż określone w OPZ.

Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia – pkt IV.1.11) – powinno być

11) Zamawiający wymaga, aby dostarczane licencje były nieograniczone terytorialnie, uprawniające do korzystania z Oprogramowania Gotowego bez ograniczeń ilościowych innych niż określone w OPZ

Załącznik nr 5 do SIWZ – Instrukcja wypełniania JEDZ – pozycja 158

Zmodyfikowana została treść wymagań określonych w pozycji 158 instrukcji JEDZ

Załącznik nr 6 do SIWZ – Oświadczenie JEDZ – pozycja 158

Zmodyfikowana została treść wymagań określonych w pozycji 158 Oświadczenia JEDZ

Modyfikacja stanowi integralną część Specyfikacji Istotnych Warunków Zamówienia.

Treść modyfikacji i wyjaśnień SIWZ oraz:

1) Sprostowanie ogłoszenia o zamówieniu;
2) SIWZ – zmieniony w dniu 11-09-2020 r.,
3) Załącznik nr 1 do SIWZ – Opis przedmiotu zamówienia– zmieniony w dniu 11-09-2020 r.,
4) Załącznik nr 5 do SIWZ – Instrukcja wypełniania JEDZ (wzór) – zmieniony w dniu 11-09-2020 r.,
5) Załącznik nr 6 do SIWZ – Oświadczenie w formie jednolitego dokumentu sporządzonego zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji Europejskiej wydanym na podstawie art. 59 ust. 2 dyrektywy 2014/24/UE – zmieniony w dniu 11-09-2020 r.,

zostały zamieszczone na stronie internetowej Zamawiającego: http://bip.stat.gov.pl/ogloszenia/zamowienia-publiczne/przetargi/ oraz na Platformie dostępnej pod adresem: http://gus.ezamawiajacy.pl.

Signed by / Podpisano przez:

Anna Monika Borowska

Date / Data: 2020-09-11 08:16