GUS
Dyrektor Generalny Głównego Urzędu Statystycznego
Anna Borowska

Warszawa, dnia 21.09.2020 r.

Modyfikacja i wyjaśnienia SIWZ

Działając na podstawie art. 38 ust. 1, 1a, 2, 4 i 4a ustawy Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843, z późn. zm.), zwanej dalej „stawą", 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.

Zamawiający zmienił termin składania ofert określając go na dzień 2 października 2020 r. godzina 10:00

Pytanie 46:
Treść SIWZ
W związku z zapisami z SIWZ punkt 3.6 Zatrudnienie na umowę o pracę oraz ze wzoru umowy § 8. Zatrudnienie na umowę o pracę prosimy o potwierdzenie naszego rozumienia, że osobami zatrudnionymi na umowę o pracę, o których mowa we wskazanych punktach, mają być specjaliści wskazani w SIWZ w punkcie 7.1 4) tj. Architekt ds. systemów klasy SIEM lub analitycznych i Inżynier ds. systemów klasy SIEM lub analitycznych?
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że zgodnie z art. 29 ust 3a ustawy Zamawiający określa w opisie przedmiotu zamówienia na usługi lub roboty budowlane wymagania zatrudnienia przez wykonawcę lub podwykonawcę na podstawie umowy o pracę osób wykonujących **wskazane przez zamawiającego czynności w zakresie realizacji zamówienia**, jeżeli wykonanie tych czynności polega na wykonywaniu pracy w sposób określony w art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2019 r. poz. 1040, 1043 i 1495).
W związku z powyższym, w § 8 ust 1 wzoru umowy, stanowiącego Załącznik nr 7 do SIWZ, Zamawiający wskazał czynności, w stosunku do których wymaga, aby osoby jej wykonujące zatrudnione były przez Wykonawcę lub podwykonawcę na podstawie umowy o pracę. W odniesieniu do każdej osoby, która wykonywać będzie wskazane w § 8 ust 1 wzoru umowy czynności, wymagane jest jej zatrudnienie na podstawie umowy o pracę.

Pytanie 47:
Wymaganie: a) obsługę, co najmniej 5000 (pięć tysięcy) zdarzeń na sekundę (ang. event per second, EPS),
Pytanie: Czy wymagania dotyczy serwer dla funkcji SRV-SIEM-1?
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że wymaganie dotyczy dostarczenia licencji dla serwera dla funkcji (podsystemu) analizy i korelacji zdarzeń Systemu SIEM np. SRV-SIEM-1 lub komponentu architektury równoważnej stosownie do wymagania zawartego w OPZ pkt II. 1. 5) d).

Pytanie 48:
Wymaganie: d) obsługę minimum 250GB dziennego przyrostu danych surowych przetwarzanych w podsystemie zbierania i zarządzania logami,
Pytanie: Czy wymagania dotyczy serwer dla funkcji SRV-LM-2?
Czy zapis należy rozumieć również jako równoważną obsługę strumienia danych o średnim natężeniu 12 500 EPS?
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że wymaganie dotyczy serwera dla funkcji (podsystemu) zbierania i zarządzania logami np. SRV LM 1 lub SRV LM-2 lub architektury równoważnej, stosownie do wymagania zawartego w OPZ pkt II. 1. 5) d) iv.

Zapis należy rozumieć również jako równoważną obsługę strumienia danych o średnim natężeniu 12 500 EPS.

Pytanie 49:
Wymaganie: e) obsługę minimum 730 dniowego (2 letniego) okresu retencji danych surowych w podsystemie zbierania i zarządzania logami,
Pytanie: Czy wymagania dotyczy serwer dla funkcji SRV-LM-2?
Jaka jest retencja (liczba dni) dla danych dostępnych w systemie w trybie online?
Jaka jest retencja (liczba dni) dla danych archiwalnych dostępnych w systemie w trybie offline?
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że wymaganie dotyczy serwera dla funkcji (podsystemu) zbierania i zarządzania logami np. SRV LM 2 lub równoważnego serwera funkcji, stosownie do wymagania zawartego w OPZ pkt II. 1. 5) d) i.
Zamawiający wyjaśnia, że retencja (liczba dni) dla danych dostępnych w systemie, (podsystemie) analizy i korelacji zdarzeń, w trybie online musi wynosić minimum 100 dni zgodnie z wymaganiami zawartymi w OPZ pkt II. 1. 1) c) oraz pkt II. 1. 5) d) ii.
Zamawiający wyjaśnia, że retencja (liczba dni) dla danych archiwalnych dostępnych w systemie, (podsystemie) zbierania (przechowywania) i zarządzania logami, w trybie offline musi wynosić minimum 730 dni zgodnie z wymaganiami zawartymi w OPZ pkt II. 1. 1) e) oraz pkt II. 1. 5) d) i.

Pytanie 50:
Wymaganie: 2) 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.
Pytanie:
Czy wymagania dotyczy serwer dla funkcji SRV-SIEM-1?
Jaka jest retencja (liczba dni) dla danych dostępnych w systemie w trybie online?
Jaka jest retencja (liczba dni) dla danych archiwalnych dostępnych w systemie w trybie offline?
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że wymaganie dotyczy serwera dla funkcji (podsystemu) analizy i korelacji zdarzeń Systemu SIEM np. SRV-SIEM-1 lub komponentu architektury równoważnej, stosownie do wymagania zawartego w OPZ pkt II. 1. 5) d) v.
Zamawiający wyjaśnia, że retencja (liczba dni) dla danych dostępnych w systemie, (podsystemie) analizy i korelacji zdarzeń, w trybie online musi wynosić minimum 100 dni zgodnie z wymaganiami zawartymi w OPZ pkt II. 1. 1) c) oraz pkt II. 1. 5) d) ii.
Zamawiający wyjaśnia, że retencja (liczba dni) dla danych archiwalnych dostępnych w systemie, (podsystemie) zbierania (przechowywania) i zarządzania logami, w trybie offline musi wynosić minimum 730 dni zgodnie z wymaganiami zawartymi w OPZ pkt II. 1. 1) e) oraz pkt II. 1. 5) d) i.

Pytanie 51:
Wymaganie: i. wymagana minimalna retencja danych 730 dni,
Pytanie
Jaka jest retencja (liczba dni) dla danych dostępnych w systemie w trybie online?
Jaka jest retencja (liczba dni) dla danych archiwalnych dostępnych w systemie w trybie offline?
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że retencja (liczba dni) dla danych dostępnych w systemie, (podsystemie) analizy i korelacji zdarzeń, w trybie online musi wynosić minimum 100 dni zgodnie z wymaganiami zawartymi w OPZ pkt II. 1. 1) c) oraz pkt II. 1. 5) d) ii.
Zamawiający wyjaśnia, że retencja (liczba dni) dla danych archiwalnych dostępnych w systemie, (podsystemie) zbierania (przechowywania) i zarządzania logami, w trybie offline musi wynosić minimum 730 dni zgodnie z wymaganiami zawartymi w OPZ pkt II. 1. 1) e) oraz pkt II. 1. 5) d) i.

Pytanie 52:
Wymaganie: i. wymagana jest minimalna retencja danych wynosząca 100 dni,
Pytanie:
Jaka jest retencja (liczba dni) dla danych dostępnych w systemie w trybie online?
Jaka jest retencja (liczba dni) dla danych archiwalnych dostępnych w systemie w trybie offline?
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że retencja (liczba dni) dla danych dostępnych w systemie, (podsystemie) analizy i korelacji zdarzeń, w trybie online musi wynosić minimum 100 dni zgodnie z wymaganiami zawartymi w OPZ pkt II. 1. 1) c) oraz pkt II. 1. 5) d) ii.
Zamawiający wyjaśnia, że retencja (liczba dni) dla danych archiwalnych dostępnych w systemie, (podsystemie) zbierania (przechowywania) i zarządzania logami, w trybie offline musi wynosić minimum 730 dni zgodnie z wymaganiami zawartymi w OPZ pkt II. 1. 1) e) oraz pkt II. 1. 5) d) i.

Pytanie 53:
Wymaganie: Tabela 2, Lista przepływów. Punkt 20 SCCM
Pytanie
Jaki jest dostępny standard protokołu API?
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że nie dysponuje informacją o standardzie protokołu API, jednocześnie Zamawiający informuje, że użytkowany jest SCCM - System Center Configuration Manager w wersji 2012 R2 SP1, Console version: 5.0.8239.1502, Site version: 5.00.8239.1000, a komunikacja do Systemu docelowego odbywa się w protokole TCP na porcie 1433.

Pytanie 54:
Wymaganie: 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:
Pytanie
Ile jest punktów nasłuchu sieci?
Jaki jest standard fizyczny punktu nasłuchu sieci?
Jaki jest wolumen ruchu w punkcie nasłuchu sieci?
Odpowiedź Zamawiającego:
Zamawiający nie jest w stanie przedstawić informacji w zakresie zadanych powyżej pytań, ponieważ Zamawiający w ramach przedmiotowego postępowania nie wymaga dostarczenia przez Wykonawcę licencji na realizowanie pozyskiwanie danych z nasłuchu sieci. Zamawiający wymaga, aby zaoferowany System SIEM miał możliwość rozbudowy o taką funkcjonalność.

Pytanie 55:
Wymaganie: h) wykryte podatności na podstawie raportów skanerów podatności, w tym z systemu Nessus,
Pytanie
Jaka jest liczba hostów (assets), które podlegają skanowaniu w systemie Nessus?
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że liczba hostów (assets), które podlegają skanowaniu w systemie Nessus wynosi ok. 850.

Zamawiający dokonał następującej modyfikacji SIWZ:

SIWZ – pkt 13.5 – było
Termin składania ofert upływa w dniu **25 września 2020 r. o godz. 10:00.**
SIWZ – pkt 13.5 – powinno być
Termin składania ofert upływa w dniu **2 października 2020 r. o godz. 10:00.**

Modyfikacja stanowi integralną część Specyfikacji Istotnych Warunków Zamówienia.
Treść modyfikacji i wyjaśnień SIWZ oraz:

1) Sprostowanie ogłoszenia o zamówieniu,
2) SIWZ – zmieniony w dniu 21-09-2020 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:

Małgorzata Jadwiga Sołtyszewska
Główny Urząd Statystyczny

Date / Data: 2020-09-21 15:14