Olsztyn, 18 września 2020 roku

Znak sprawy: CIUWO.232.8.2020

Wykonawcy ubiegający się
o udzielenie zamówienia

Dotyczy: *postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na* ***zakup systemu kolekcji i korelacji logów - SIEM (Ogłoszenie nr 584745-N-2020 z 14 września 2020 r.)***

Uprzejmie informuję, że do Zamawiającego wpłynęły zapytania dotyczące wyjaśnienia treści Specyfikacji Istotnych Warunków Zamówienia w postępowaniu o udzielenie zamówienia publicznego jw. Działając na podstawie art. 38 ust. 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U. z 2018r. poz. 1986 ze zm.), Zamawiający informuje, że udziela następujących odpowiedzi na zadane poniżej pytania:

Pytanie 1:
2.1.16. System musi mieć możliwość identyfikacji aplikacji w oparciu o przepływy oraz poprzez zasilenie danymi z systemów analizy ruchu sieciowego do warstwy 7. Identyfikacja aplikacji nie może zachodzić wyłącznie w oparciu o port komunikacyjny TCP/UDP, ale musi uwzględniać faktyczną zawartość ruchu
Czy Zamawiający ma na myśli funkcjonalność rozwiązania (SIEM) polegająca na możliwości korzystania z informacji z zewnętrznych systemów analizy ruchu takich jak np. FlowMon , analogicznie jak w przypadku korzystania z analizy wykonywanych przez skanery podatności ?
Odpowiedź:
Zamawiający wyjaśnia, że chodzi o funkcjonalność rozwiązania (SIEM) polegającą na możliwości korzystania z informacji z zewnętrznych systemów analizy ruchu takich jak np. FlowMon, analogicznie jak w przypadku korzystania z analizy wykonywanych przez skanery podatności. Jednocześnie Zamawiający informuje, że działając na podstawie art. 38 ust. 4 ustawy Pzp dokonuje modyfikacji treści SIWZ tj. w załączniku nr 1 do wzoru umowy stanowiącej załącznik nr 5 do SWIZ (SOPZ) zmienia brzmienie punktu 2.1.16 na następujący:
„System musi mieć możliwość identyfikacji aplikacji poprzez zasilenie danymi z systemów analizy ruchu sieciowego do warstwy 7 (w tym przepływy). Identyfikacja aplikacji nie może zachodzić wyłącznie w oparciu o port komunikacyjny TCP/UDP, ale musi uwzględniać faktyczną zawartość ruchu,”

Pytanie 2:

2.1.26. System musi obsługiwać powszechnie dostępne na rynku metody do zbierania logów (Syslog TCP/UDP/TLS, WMI, ODBC/JDBC, SNMP, OPSEC LEA)

Rozwiązanie OPSEC LEA stosowany jest w rozwiązaniach firmy CheckPoint, które równocześnie obsługują protokół SysLog. Czy zamawiający pozwala na usuniecie tego wymagania tj. OPSEC LEA?

Odpowiedź:

Zamawiający informuje, że wyraża zgodę na usunięcie protokołu OPSEC LEA jako jednej z metod zbierania logów. Jednocześnie Zamawiający informuje, że działając na podstawie art. 38 ust. 4 ustawy Pzp dokonuje modyfikacji treści SIWZ tj. w załączniku nr 1 do wzoru umowy stanowiącej załącznik nr 5 do SWIZ (SOPZ) zmienia brzmienie punktu 2.1.26 na następujący:

„System musi obsługiwać powszechnie dostępne na rynku metody do zbierania logów (Syslog TCP/UDP/TLS, WMI, ODBC/JDBC, SNMP),"

Pytanie 3:

2.1.37. System musi zapewniać scentralizowane zarządzanie wszystkimi elementami i dostęp do funkcji administracyjnych z poziomu jednego interfejsu użytkownika wykorzystującego przeglądarkę sieci Web. Panel zarządczy umożliwiający szybką wizualizację informacji o sieci i zabezpieczeniach

Czy Zamawiający dopuszcza wykorzystanie klienta aplikacji jako głównego interfejsu pracy operatora oraz webowych interfejsów pomocniczych?

Odpowiedź:

Zamawiający informuje, że wyraża zgodę na wykorzystanie klienta aplikacji jako głównego interfejsu pracy operatora oraz webowych interfejsów pomocniczych. Jednocześnie Zamawiający informuje, że działając na podstawie art. 38 ust. 4 ustawy Pzp dokonuje modyfikacji treści SIWZ tj. w załączniku nr 1 do wzoru umowy stanowiącej załącznik nr 5 do SWIZ (SOPZ) zmienia brzmienie punktu 2.1.37 SOPZ na następujący:

„System musi zapewniać scentralizowane zarządzanie wszystkimi elementami i dostęp do funkcji administracyjnych z poziomu jednego interfejsu użytkownika wykorzystującego przeglądarkę sieci Web lub dedykowaną aplikację. Panel zarządczy umożliwiający szybką wizualizację informacji o sieci i zabezpieczeniach,"

Pytanie 4:

2.1.52. System musi umożliwiać analizę minimum 1500 zdarzeń na sekundę (EPS) i minimum 75000 przepływów na minutę (FPM), z możliwością rozbudowy licencyjnej do minimum 5000 zdarzeń na sekundę i 200000 przepływów na minutę,

Czy Zamawiający w celu doboru odpowiedniej licencji dla rozwiązań które nie bazują na ilości EPS i FPM dopuszcza model licencjonowania oparty na liczbę analizowanych adresów IP? Jeżeli tak to proszę o podanie liczby komputów oraz serwerów (fizycznych i wirtualnych) objętych działaniem rozwiązania.

Odpowiedź:

Zamawiający informuje, że dopuszcza model licencjonowania oparty na liczbie analizowanych adresów IP z zastrzeżeniem, że System oparty na takim sposobie licencjonowania powinien posiadać wydajność nie niższą niż System oparty na licencjonowaniu poprzez parametry EPS/FPM oraz obsługiwać minimum 150 źródeł logów (analizowanych IP).

Zamawiający informuje jednocześnie, że udzielone odpowiedzi będą wiążące dla wszystkich Wykonawców ubiegających się o udzielenie przedmiotowego zamówienia i zostały zamieszczone na stronie internetowej Zamawiającego.

Z UP. DYREKTORA CIUWO
GŁÓWNY SPECJALISTA
-//-
Maciej Maścianica