AGENCJA REZERW
MATERIAŁOWYCH

Warszawa, dnia 27.10.2020 r.

Biuro Zakupów

BZ.261.59.2020/...277

Do Wykonawców

Dotyczy: postępowania o udzielenie zamówienia publicznego na dostawę, wdrożenie i uruchomienie oprogramowania klasy SIEM oraz świadczenie usług wsparcia technicznego na potrzeby Agencji Rezerw Materiałowych – znak sprawy: BZ.261.59.2020.

Działając na podstawie art. 38 ust. 2 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843, z późn. zm.), Zamawiający przekazuje wyjaśnienia treści SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 2. ppkt 2)**, załącznik nr 1 do SIWZ:

ma być możliwe stworzenie architektury redundantnej w której podstawowa instalacja rozwiązania SIEM podczas regularnej pracy wykonuje wszystkie operacje produkcyjne, zaś instalacja backupowa synchronizuje wszystkie dane i w razie awarii jest w stanie przejąć funkcjonowanie środowiska SIEM,

Pytanie 1:

W punkcie nr 2 podpunkt 2) Szczegółowego Opisu Przedmiotu Zamówienia - Załącznik nr 1 do SIWZ Zamawiający wymienia pięć typów środowisk witalizacyjnych, które rozwiązanie ma wspierać. Wymaganie to w dużym stopniu

ogranicza liczbę systemów klasy SIEM spełniających kryteria postępowania. Czy Zamawiający uzna to kryterium za spełnione jeżeli rozwiązanie będzie wspierać cztery spośród pięciu wymienionych środowisk witalizacyjnych w tym Hyper-V, VMware, Azure i AWS?

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 2. ppkt 11)**, załącznik nr 1 do SIWZ:

System musi mieć możliwość anonimizacji zebranych danych w zakresie nie mniejszym niż: adresy IP, nazwy hostów, adres MAC, adresy email, nazwy użytkowników. Proces ten ma być możliwy w oparciu o role/profile użytkowników administracyjnych. Ujawnienie danych (deanonimizacja) ma się odbywać z wykorzystaniem użytkownika udzielającego lub zabraniającego jej wykonania. W przypadku zatwierdzenia wspomnianego żądania, dane są ujawniane na określony czas, po którym powtórnie ulegają anonimizacji.

Pytanie 2:

W punkcie nr 2 podpunkt 11) Szczegółowego Opisu Przedmiotu Zamówienia - Załącznik nr 1 do SIWZ Zamawiający wymaga funkcjonalności pozwalającej na anonimizację danych. Czy Zamawiający uzna wymaganie za spełnione jeżeli deanonimizacja będzie się odbywać z wykorzystaniem użytkownika udzielającego lub zabraniającego wglądu do konkretnych typów danych jednak dane będą ujawniane lub anonimizowane poprzez akcje wykonywane manualnie przez użytkownika nadzorującego?

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 3. ppkt 2), 3), 4), 5), 6), 7), 8)** załącznik nr 1 do SIWZ:

Rozwiązanie SIEM musi mieć możliwość zbierania danych z monitorowanych urządzeń, również innych niż logi, co ma być osiągalne poprzez nie mniej niż: (...)

Pytanie 3:

W punkcie nr 3 Szczegółowego Opisu Przedmiotu Zamówienia - Załącznik nr 1 do SIWZ Zamawiający wymienia szereg podpunktów (szczególnie podpunkty 2), 3), 4), 5), 6), 7) ,8)) opisujących szczegółowe wymagania dodatkowe bezpośrednio nie związane z funkcjonalnością systemów klasy SIEM. Każdy z podpunktów ogranicza liczbę systemów klasy SIEM spełniających kryteria postępowania, a łącznie podpunkty 2), 3), 4), 5), 6), 7) ,8) dla punkt nr 3 mogą wskazywać na jedno rozwiązanie. Czy zamawiający dopuszcza zmianę zapisu punkt nr 3 z "3. Rozwiązanie SIEM musi mieć możliwość zbierania danych z monitorowanych urządzeń, również innych niż logi, co ma być osiągalne poprzez nie mniej niż:" na "3. Rozwiązanie SIEM może mieć możliwość zbierania danych z monitorowanych urządzeń, również innych niż logi, co może być osiągalne poprzez:"

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 19.**, załącznik nr 1 do SIWZ:

Muszą być wspierane zewnętrzne metody uwierzytelniania, nie mniej niż: Active Directory, LDAP, RADIUS.

Pytanie 4:

W punkcie nr 19 Szczegółowego Opisu Przedmiotu Zamówienia - Załącznik nr 1 do SIWZ Zamawiający wymienia wspierane zewnętrzne metody uwierzytelniania m.in. protokół RADIUS. Usługa uwierzytelniania RADIUS jest obecnie rzadko wykorzystywanym standardem w organizacjach, a wymaganie to ogranicza liczbę systemów klasy SIEM spełniających kryteria postępowania. Czy Zamawiający uzna to kryterium za spełnione jeżeli weryfikacja tożsamości operatorów będzie możliwa poprzez lokalne konto oraz zewnętrzne systemy uwierzytelnienia LDAP/ Active Directory?

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 21.**, załącznik nr 1 do SIWZ:

System SIEM musi mieć możliwość analizowania i odpytywania o zdarzenia w widoku analitycznym w trybie strumieniowym (streaming mode), w taki sposób że raport docelowy dotyczący analizowanych zdarzeń wykonywany jest przed ich zapisaniem na dysk twardy

Pytanie 5:

W punkcie nr 21 Szczegółowego Opisu Przedmiotu Zamówienia - Załącznik nr 1 do SIWZ Zamawiający wymagany aby System SIEM miał możliwość analizowania i odpytywania o zdarzenia w widoku analitycznym w trybie strumieniowym (streaming mode), w taki sposób że raport docelowy dotyczący analizowanych zdarzeń wykonywany jest przed ich zapisaniem na dysk twardy. Możliwość wyświetlania zdarzeń w automatycznym streaming mode nie jest podstawową

funkcją systemów klasy SIEM i ogranicza liczbę systemów klasy SIEM spełniających kryteria postępowania. Czy zamawiający uzna kryterium za spełnione, jeżeli dostarczony system SIEM będzie posiadał konsolę pozwalającą na wykonywanie wyszukiwań na podstawie zdefiniowanego wcześniej filtra pozwalających na przeprowadzenie inwestygacji/śledztwa wybranych zdarzeń?

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

DYREKTOR
Biura Zakupów
Hubert Burczyński