AGENCJA REZERW
MATERIAŁOWYCH

Warszawa, dnia 06.10.2020 r.

Biuro Zakupów

BZ.261.59.2020 /268

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. 1g**, załącznik nr 1 do IPU:

w wypadku awarii kolektora, kolektor zastępczy może być uruchomiony poprzez jego zarejestrowanie w warstwie przechowującej i korelującej. Konfiguracja (zarządzanie) kolektorów nie może odbywać się indywidualnie lecz za pomocą centralnego zarządzania. Nie mogą one posiadać żadnych parametrów konfiguracyjnych poza adresami IP, nazwą kolektora oraz, wymaganymi poświadczeniami, które byłyby wymagane w celu uruchomienia kolektora zastępczego.

Pytanie 1:

czy zapis należy rozumieć jako podanie adresu IP, nazwy kolektora i poświadczeń w momencie uruchomienia konektora zastępczego, a nie uruchamiania nowej instancji kolektora? Uruchomienie nowej instancji kolektora wymaga jego konfiguracji, jak również definicji źródeł danych, które będą monitorowane przez kolektor. Prosimy o uściślenie wymagania.

Odpowiedź:

Zgodnie z SIWZ sytuacja dotyczy awarii konektora i uruchomienia konektora zastępczego.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 2a**, załącznik nr 1 do IPU:

implementacja ma być zrealizowana w oparciu o maszyny wirtualne (VAVirtual Appliance).

Pytanie 2:

zakładamy, że zamawiający dopuści rozwiązanie typu software instalowane na systemie operacyjnym na wirtualnej maszynie?

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 2b**, załącznik nr 1 do IPU:

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 3:

zakładamy, że dopuszczalne jest rozwiązanie, w którym system jest zaprojektowany do działania w klastrze, który zapewnia ciągłość pracy w momencie awarii jednego lub kilku komponentów?

Odpowiedź:

Tak. Dopuszczalne jest rozwiązanie w którym system jest zaprojektowany do działania w klastrze.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 2e**, załącznik nr 1 do IPU:

klaster SIEM nie może posiadać ograniczeń licencyjnych związanych z ilością gromadzonych i przechowywanych zdarzeń i/lub danych. Jedynym ograniczeniem w tym zakresie może być rozmiar przestrzeni dyskowej.

Pytanie 4:

zapis jest sprzeczny z punktem 34. Systemy klasy SIEM są licencjonowane na liczbę przyjmowanych zdarzeń na sekundę lub też wolumen danych na dobę. Proponujemy usunięcie zapisu, gdyż znacząco ogranicza on zakres możliwych do zaoferowania systemów klasy SIEM. Sugerujemy usunięcie wymagania.

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ. Zamawiający nie jest w stanie określić potrzebnej przestrzeni na dobę.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 3b**, załącznik nr 1 do IPU:

zdolność do monitorowania statusu oraz dostępności usług takich jak: DNS, FTP/SCP, TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SSH, HTTP, HTTPS

Pytanie 5:

system SIEM służy do monitorowania zdarzeń bezpieczeństwa. Monitorowanie statusu oraz dostępności usług można zaimplementować wykorzystując przeznaczone do tego oprogramowanie np. Nagios. Ma to znaczący wpływ na licencję systemu SIEM, a co za tym idzie na koszt zakupu systemu. Czy w przypadku dostarczenia systemu SIEM wraz oprogramowaniem firm trzecich, jako kompletny i utrzymywany przez wykonawcę system, zamawiający dopuści takie rozwiązanie?

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 3c**, załącznik nr 1 do IPU:

wykryte urządzenie ma posiadać swoją reprezentację w bazie urządzeń (Configuration Management Database - CMDB) w ramach dostarczonego rozwiązania SIEM co jednocześnie ma umożliwiać prezentację następujących informacji (nie mniej niż): (...)

Pytanie 6:

rozwiązania klasy SIEM nie służą do zarządzania bazą danych urządzeń i serwerów. Funkcjonalność CMDB można uzyskać z pomocą rozwiązań firm trzecich. Czy w przypadku dostarczenia systemu SIEM wraz oprogramowaniem firm trzecich, jako kompletny i utrzymywany przez wykonawcę system, zamawiający dopuści takie rozwiązanie?

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 3b**, załącznik nr 1 do IPU:

zbieranie metryk wydajnościowych ma dotyczyć nie mniej niż: utylizacji interfejsów sieciowych, występujących tam błędów, ilości wysłanych i odebranych danych (np. bajtów), obciążenia CPU, wykorzystania pamięci, wykorzystania przestrzeni dyskowej, utylizacji poszczególnych procesów.

Pytanie 7:

monitorowanie statusu oraz dostępności usług można zaimplementować wykorzystując przeznaczone do tego oprogramowanie np. Nagios. Ma to znaczący wpływ na licencję systemu SIEM, a co za tym idzie na koszt zakupu systemu. Czy w przypadku dostarczenia systemu SIEM wraz oprogramowaniem firm trzecich, jako kompletny i utrzymywany przez wykonawcę system, zamawiający dopuści takie rozwiązanie?

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 14 d, e, f, g** załącznik nr 1 do IPU:

zdolność do monitorowania integralności plików, zdolność do monitorowania rejestru, zdolność do monitorowania urządzeń zewnętrznych (removable devices), zdolność do wykonywania poleceń PowerShell wraz z odsyłaniem wyniku ich działania w postaci logów.

Pytanie 8:

system SIEM nie posiada agentów, które monitorują systemy w sposób tak szczegółowy. Monitorowanie jest możliwe pod warunkiem posiadania odpowiedniego oprogramowania, które monitoruje wskazane zdarzenia np. EDR, DLP itp. Sugerujemy zmianę wymagania na zdolność monitorowania wymienionych zdarzeń za pomocą monitorowania rozwiązań, które są do tego przeznaczone, a które zamawiający posiada.

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 15 d, e** załącznik nr 1 do IPU:

zdolność do monitorowania integralności plików, zdolność do monitorowania procesu w oparciu o jego proces rodzimy oraz sumę kontrolną.

Pytanie 9:

system SIEM nie posiada agentów, które monitorują systemy w sposób tak szczegółowy. Monitorowanie jest możliwe pod warunkiem posiadania odpowiedniego oprogramowania, które monitoruje wskazane zdarzenia np. EDR, DLP itp. Sugerujemy zmianę wymagania na zdolność monitorowania wymienionych zdarzeń za pomocą monitorowania rozwiązań, które są do tego przeznaczone, a które Zamawiający posiada.

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 24** załącznik nr 1 do IPU:

system SIEM musi pozwalać na zbieranie konfiguracji urządzeń, identyfikowanie zmian w nich następujących wraz z możliwością porównywania poszczególnych wersji obok siebie.

AGENCJA REZERW
MATERIAŁOWYCH

Pytanie 10:

system SIEM służy do monitorowania zdarzeń bezpieczeństwa. Monitorowanie zarządzania konfiguracją urządzeń sieciowych można zaimplementować wykorzystując przeznaczone do tego oprogramowanie np. rConfig. Czy w przypadku dostarczenia systemu SIEM wraz oprogramowaniem firm trzecich, jako kompletny i utrzymywany przez wykonawcę system, zamawiający dopuści takie rozwiązanie?

Odpowiedź:

Nie. Zamawiający podtrzymuje zapisy zawarte w SIWZ.

Treść specyfikacji technicznej oprogramowania klasy SIEM **pkt. 29** załącznik nr 1 do IPU:

system SIEM musi pozwalać na przesłanie dowolnych zebranych zdarzeń z wykorzystaniem protokołu KAFKA.

Pytanie 11:

w jaki sposób rozumieć wymaganie? Czy wymaganie należy rozumieć jako możliwość przesłania zdarzeń w kolektorów do KAFKA, czy też pobrania zdarzeń z KAFKA do SIEM?

Odpowiedź:

Możliwość pobrania zdarzeń z KAFKA do SIEM.

DYREKTOR
Biura Zakupów
Hubert Burczyński