NCBR
Narodowe Centrum Badań i Rozwoju

DAZ.262.29.2023 Warszawa, 9 listopada 2023 r.

DO WSZYSTKICH ZAINTERESOWANYCH

INFORMACJA O DOKONANIU PONOWNEJ CZYNNOŚCI BADANIA I OCENY OFERT, INFORMACJA O WYBORZE NAJKORZYSTNIEJSZEJ OFERTY

Działając na podstawie art. 253 ust. 1 pkt 2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. 2023 poz. 1605 ze zm.) zwanej dalej „ustawą Pzp", Narodowe Centrum Badań i Rozwoju, zwane dalej „Zamawiającym", informuje, że w postępowaniu o udzielenie zamówienia publicznego, którego przedmiotem jest ***„Zakup odnowienia licencji oprogramowania SIEM - usługa serwisu, wsparcia technicznego i konsultacyjna", nr postępowania 29/23/PN*** po ponownej ocenie i badaniu ofert została:

- **<u>wybrana oferta złożona przez:</u>**

Apius Technologies S.A.
ul. Moniuszki 50
31-523 Kraków
Cena oferty: 760 878,00 złotych brutto

<u>Uzasadnienie faktyczne:</u>
Oferta jest ważna, odpowiadająca treści SWZ, uzyskała najwyższą liczbę punktów 100,00 zgodnie z przyjętym kryterium oceny ofert.

<u>Uzasadnienie prawne:</u>
art. 239 ust. 1 Pzp.

- **<u>odrzucona oferta złożona przez:</u>**

Network Experts sp. z o. o., sp. k.
ul. Chojnowska 8
03-583 Warszawa
Cena oferty: 727 299,00 złotych brutto

<u>Uzasadnienie faktyczne:</u>
Wykonawca Network Experts sp. z o. o., sp. k. – zaoferował produkt równoważny Elasticsearch i przedłożył wykaz spełniania kryteriów stosowanych w celu oceny równoważności oprogramowania.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

Zamawiający ponownie przeanalizował złożony przez Network Experts sp. z o. o., sp. k. wykaz i podtrzymał decyzję stwierdzającą niezgodność oferowanego systemu Elasticsearch z wymaganiami określonymi w części III.A Szczegółowego Opisu Przedmiotu Zamówienia.
Poniżej enumeratywnie wyliczone nieprawidłowości w odniesieniu do pozycji wskazanych w wykazie spełniania kryteriów stosowanych w celu oceny równoważności oprogramowania:
poz. 13 Wykazu: System musi umożliwiać co najmniej półroczne przechowywanie gromadzonych logów oraz ich wydajną analizę na co najmniej 15TB danych.

Wykonawca zamieścił w kolumnie 3 zrzut ekranu, nie podając źródła jego pochodzenia ani nie opisując czego konkretnie dotyczy. Wykonawca wskazał, że *System oferuje wydajną analizę co najmniej 55 TB danych co widać na powyższym zrzucie ekranu*. Wobec braku jakichkolwiek szczegółowych informacji nie ma możliwości stwierdzenia, że przedstawione dane potwierdzają, że system Elasticsearch umożliwia wydajną analizę. Nie można tego rodzaju niejasnej informacji uznać za potwierdzającą postawione wymaganie, wobec czego należy stwierdzić, że Wykonawca nie potwierdził spełnienia wymagania z pkt 13.

poz. 14 Wykazu: System musi zapewnić mechanizm identyfikacji zapisywanych danych, który pozwoli na unikanie duplikacji danych.

Data Streams nie gwarantuje uniknięcia duplikacji danych. Jest to rozwiązanie typu Append-only, które nie oferuje mechanizmu deduplikacji danych. Wskazane przez Wykonawcę miejsce w dokumentacji nie potwierdza spełnienie danego wymagania.

poz. 15 Wykazu: System musi utrzymywać repozytorium logów z możliwością ich przeglądania w formie rzeczywistej (surowej - raw) oraz udostępniać użytkownikowi dane w formie znormalizowanej (z uwzględnieniem znaczenia poszczególnych zmiennych/pól logu). Dostęp do danych w formie rzeczywistej jak i znormalizowanej musi być możliwe w oparciu o te same narzędzia.

Nawet jeśli wymusimy, aby event w formacie RAW znalazł się w evencie w Elasticsearchu, to traci on już formę źródłową -> Elasticsearch opiera się na eventach w formacie JSON. Nawet podczas stosowania ECS event znajduje się w jednym z kluczy w JSON. https://www.elastic.co/guide/en/ecs/current/ecs-event.html Wskazane przez Wykonawcę miejsce w dokumentacji nie potwierdza spełnienie danego wymagania.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

poz. 19 Wykazu: System musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności, związanych z analizą danych obejmującą:
d) nowe sposoby wizualizacji

Kibana posiada zamkniętą ilość typów/sposobów wizualizacji:
https://www.elastic.co/guide/en/kibana/current/create-a-dashboard-ofpanels-with-web-server-data.html#view-the-number-of-website-visitors

e) mechanizmy powiadamiania, w tym dwukierunkowe inne niż przewidział producent:
system posiada ograniczoną ilość mechanizmów powiadamiania:
https://www.elastic.co/guide/en/elasticsearch/reference/current/actions.html .Brak dwukierunkowych mechanizmów powiadamiania

Realizacja tych funkcjonalności nie może wymagać konieczności angażowania producenta:
z informacji podanych na przytoczonych stronach dokumentacji nie wynika spełnienie tego wymogu.

poz. 22 Wykazu: System musi umożliwiać integrację danych gromadzonych z różnych źródeł: aplikacji, baz użytkowników, w tym katalogu Active Directory. Dane muszą być dostępne jako spójna informacja na poziomie interfejsu analitycznego systemu.

Wg podanego linku oferowany system nie spełnia wymogu – Link z oferty prowadzi do AAD tj. do innego produktu/oprogramowania jakim jest Azure Active Directory: https://docs.elastic.co/en/integrations/azure/adlogs

poz. 25 Wykazu: System musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów – login/logoff, uruchamiane zapytania i zmiany konfiguracji Systemu.

Wg dokumentacji Elasticsearch domyślnie nie posiada w logach informacji o wykonanych zapytaniach na klastrze:
https://www.elastic.co/guide/en/elasticsearch/reference/current/auditingsearch-queries.html.
Ponadto linki z oferty prowadzą do metod integracji oferowanego systemu z innymi systemami, hostami, z których maja być zbierane dane. Jednakże wymóg ten dotyczył wprost oferowanego Systemu – tj. to oferowany System musi utrzymywać log audytowy czynności administratorów wykonywanych w oferowanym Systemie. Wykonawca nie wykazał zatem spełnienia tej funkcjonalności.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

Poz. 32 Wykazu: System musi umożliwiać pozyskiwanie danych z nasłuchu sieci. Zbierane informacje muszą obejmować wartości wszystkich nagłówków połączeń do warstwy 4 ISO/OSI, oraz do warstwy 7, dla następujących protokołów: DHCP, DNS, HTTP, IMAP, SIP, SMB, SMTP.

Jak wynika z podanego w ofercie linku do dokumentacji oferowanego rozwiązania, system Elasticsearch nie obsługuje protokołów: IMAP, SIP (tylko w tzw. beta), SMB, SMTP.

Wersje beta oprogramowania to etap w cyklu oprogramowania, który jest pośredni między fazą testów alfa, a pełnym stabilnym finalnym wydaniem. Wersje beta są udostępniane użytkownikom lub testerom w celu przetestowania oprogramowania. Ryzyka związane z korzystaniem z wersji beta obejmują w szczególności błędy w funkcjonowaniu oraz niestabilność pracy, braki w funkcjonalności, ryzyko utraty danych ze względu na potencjalne błędy oraz często brak wsparcia technicznego producenta. Zważywszy że oprogramowanie SIEM jest rozwiązaniem krytycznym z punktu widzenia bezpieczeństwa dla Zamawiającego nie dopuszczalne jest korzystanie z oprogramowania lub części funkcjonalności będących w fazie beta z racji na wskazane wcześniej ryzyka.

Poz. 35 Wykazu: Przechowywane dane muszą być zabezpieczone przed modyfikacją przy wykorzystaniu metod kryptograficznych. Musi być możliwe przechowywanie danych zabezpieczających (skróty/podpisy) poza systemem. Musi być możliwe znakowanie danych czasem.

Podany w formularzu ofertowym link nie opisuje kwestii przechowywania danych - dotyczy tylko komunikacji pomiędzy elementami środowiska Elasticsearch.

Poz. 40 Wykazu: Licencja Systemu nie może ograniczać liczby elementów gromadzących oraz analizujących logi.

Licencja ogranicza ilość liczby elementów gromadzących i analizujących logi poprzez licencjonowanie ilości RAM wykorzystywanej łącznie przez klaster. Licencjonowanie Enterprise jest teraz oparte na jednostkach zasobów Enterprise (ERU), co oznacza, w odniesieniu do subskrypcji Enterprise, liczbę równą całkowitej ilości GB pamięci RAM adresowanej przez całe podlegające rozliczeniu oprogramowanie Enterprise wdrożone przez Klienta w związku z subskrypcją Enterprise, podzieloną przez 64. Oto kilka przykładowych scenariuszy dla klastrów Enterprise Self-Managed:

3 hosty z uruchomionymi węzłami danych Elasticsearch z 128 GB na każdym hoście. ROUNDUP(128*3/64)= 6 to liczba ERU, które będą używane.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

6 hostów z uruchomionymi węzłami danych Elasticsearch z 64 GB na każdym hoście, 3 hosty z uruchomionymi węzłami nadrzędnymi Elasticsearch z 16 GB na każdym hoście, 1 host z uruchomioną Kibaną i innymi aplikacjami z 64 GB na hoście. Całkowita pamięć komponentów wynosi (64 GB6) + (16 GB3) + (1,4 GB - dla Kibany tylko maksymalna sterta). Jest to równe 433,4 GB. ROUNDUP(433.4/64) = 7 to liczba ERU, które będą używane.

Wykonawca nie wskazał ile jednostek ERU jest oferowane.

Poz. 43 Wykazu: System musi posiadać oraz umożliwiać akcelerację często wykonywanych zapytań i raportów, tak aby automatycznie przyśpieszać wykonanie raportu obejmującego długie okresy czasu (np. 6 miesięcy). Akceleracja musi być dostępna zarówno dla raportów wbudowanych, jak i własnych definiowanych przez użytkownika.

Podany w formularzu ofertowym link nie potwierdza wymogu. Elasticsearch nie posiada takiego mechanizmu wg dokumentacji producenta.

Poz. 47 Wykazu: System musi automatycznie (tj. bez uprzedniego definiowania schematu danych wejściowych) analizować dane zdarzenie (dzienniki systemowe, w szczególności w formie Syslog, Netflow) pod kątem zawartości i struktury danych. Wynikiem analizy muszą być informacje mapowane w formacie łatwym do późniejszego wyszukiwania i analizy, np. w strukturach klucz-wartość.

Rozwiązanie to w Elasticsearch jest niedojrzałe i w fazie testów – Technical Preview. W podanym linku widnieje zastrzeżenie: *This functionality is in technical preview and may be changed or removed in a future release*. (https://www.elastic.co/guide/en/fleet/current/syslog-processor.html

W kwestii użycia https://www.elastic.co/guide/en/logstash/current/pluginsinputs-syslog.html należy poprawnie zdefiniować postać wiadomości syslog za pomocą języka grok.

Warto nadmienić iż zgodnie z przyjętymi standardami dot. rozwoju oprogramowania technical preview jest bardzo wczesną wersją, występująca **przed** fazą beta. Oznacza to, iż nie posiada w pełni zaimplementowanych zakładanych przez producenta funkcjonalności, a funkcjonalności udostępnione w tej wersji nie zostały przetestowane pod kątem poprawności ich funkcjonowania, w związku z czym nie można tutaj mówić o w pełni działającej funkcjonalności.

poz. 49 Wykazu: System musi umożliwiać analizę standardowych logów infrastrukturalnych generowanych przez systemy operacyjne, dostęp webowy, firewalle, urządzenia sieciowe

(switche, routery, loadbalancery itd.), systemy bezpieczeństwa IPS/IDS/ Application & URL Filtering/Anti-Bot, WAF, IDM, DAM, itd.

Analogicznie jak w pkt 47 - Rozwiązanie to w Elasticsearch jest niedojrzałe i w fazie testów - Technical Preview: https://www.elastic.co/guide/en/fleet/current/syslog-processor.html

W kwestii użycia https://www.elastic.co/guide/en/logstash/current/pluginsinputs-

syslog.html należy poprawnie zdefiniować postać wiadomości syslog za pomocą języka grok.

Poz. 51 Wykazu: System musi pozwalać na modyfikację mechanizmów klasyfikacji zdarzeń i normalizacji logów dostarczonych razem z produktem (otwarty kod dostarczonych mechanizmów normalizacji). Aktualizacje oprogramowania nie mogą nadpisywać ww. modyfikacji.

W podanych w formularzu ofertowym linkach brak jest informacji o normalizacji logów.

Poz. 53 Wykazu: System musi umożliwiać obsługę logów w formacie XML bez konieczności tworzenie parserów. Nazwy pól muszą być określone strukturą XML. System musi umożliwiać obsługę logów w formacje JSON bez konieczności tworzenie parserów. Nazwy pól muszą być określone strukturą JSON.

Oferowany przez wykonawcę system nie spełnia wymogu - bez dodatkowego parsowania logów Elasticsearch nie jest w stanie przetworzyć poprawnie XML. Ponadto w podanym w formularzu ofertowym linku jest mowa o parserze logów XML. Nie wskazano miejsca w dokumentacji obsługi logów w formacie JSON.

Poz. 55 Wykazu: System musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość, np. „user=jkowalski” musi tworzyć pole „user” o wartości „jkowalski”.

Oferowany przez wykonawcę system nie spełnia wymogu - bez przygotowania parsera typu GROK nie jest możliwe otrzymanie takiej normalizacji.

Poz. 57 Wykazu: Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zwarte w zewnętrznych repozytoriach.

System nie spełnia tego wymogu

a. Katalogi LDAP – wskazany przez Wykonawcę link zawiera opis funkcjonalności aktualnie niedostępnej – w podanym linku widnieje zastrzeżenie: *You are looking at preliminary documentation for a future release.*

b. Bazy danych – brak informacji - Wykonawca nie wykazał spełnienia tej funkcjonalności.

c. Bazy noSQL – brak informacji - Wykonawca nie wykazał zatem spełnienia tej funkcjonalności.

Poz. 58 Wykazu: W celu ograniczenia zajętości przestrzeni dyskowej dane wzbogacające nie mogą być przechowywane razem z logami a wzbogacanie musi odbywać w locie w trakcie odczytu danych ze źródeł zewnętrznych.

Oferowany przez wykonawcę system nie spełnia wymogu – wg. dokumentacji jedyna możliwość wzbogacenia danych istnieje dla danych wejściowych na etapie zapisu ich na dysku. W późniejszym etapie nie ma możliwości wzbogacania już posiadanych zdarzeń.

poz. 62 Wykazu: System musi umożliwiać tworzenie bazy definicji formatów logów.

Podany link w formularzu ofertowym nie opisuje ww. zagadnienia. Wykonawca nie wykazał zatem spełnienia tej funkcjonalności.

poz. 64 Wykazu: System musi automatycznie proponować definicje pól, dla poszczególnego typu logów wykorzystywanych do dalszej analizy oraz tworzyć statystyki występowania poszczególnych wartości tych pól.

Na potwierdzenie spełnienia tego wymogu Wykonawca przedstawił link z dyskusji użytkowników na stronie discuss.elastic.co. Zgodnie z opisem kolumny nr 4 w załączniku nr 2a do SWZ, Wykonawca miał potwierdzić spełnienie parametru przez wskazanie miejsca w dokumentacji oprogramowania, w którym znajduje się potwierdzenie spełnienie danego wymagania (adres strony WWW pod którym dokument jest opublikowany, a także publicznie i powszechnie dostępny bez konieczności logowania). W przypadku jeśli wskazanie opisanego wyżej miejsca nie jest możliwe lub nie jest wystarczające, wykonawca powinien opisać sposób spełnienia danego wymagania dołączając inne przedmiotowe środki dowodowe. Podanie linku do dyskusji użytkowników nie stanowi przedmiotowego środka dowodowego, zawiera bowiem wyłącznie opinie prywatne użytkowników systemu. Wykonawca nie wykazał zatem spełnienia tej funkcjonalności.

poz. 66 Wykazu: System musi umożliwiać definiowanie pól za pomocą wyrażeń regularnych (REGEX).

Elasticsearch nie umożliwia definiowania pól za pomocą regexów. Możliwe jest tylko zastosowania GROK na etapie zasilania Elasticsearch danymi. Możliwe jest wyszukiwanie z wyrażeniami regularnymi.

Poz. 83 Wykazu: System musi posiadać możliwość automatycznego reagowania na zdarzenie oraz powiadamiania administratorów. Musi istnieć możliwość wysłania email oraz możliwość konfigurowania innych akcji w postaci skryptów, do których może być przekazywana dowolna liczba argumentów na podstawie treści Alarmu.

Oferowany przez wykonawcę system nie spełnia wymogu - brak możliwości konfigurowania akcji w postaci skryptów (ograniczona lista) https://www.elastic.co/guide/en/kibana/current/action-types.html

Po ponownym badaniu i ocenie ofert Zamawiający podtrzymuje decyzję wyrażoną w pierwszym rozstrzygnięciu postępowania, iż w przypadku ww. pozycji Wykazu załączonego przez Network Experts Sp. z o.o. Sp.k., informacje podane na stronach internetowych wskazanych przez Wykonawcę nie potwierdzają spełnienia wymagań Zamawiającego zawartych w SOPZ. Oferując rozwiązanie równoważne, tj. oprogramowanie Elasticsearch, Wykonawca nie wykazał, że system ten spełnia wszystkie wymagania techniczne. Niezgodności nie mogą być naprawione ani usunięte w drodze wyjaśnień treści oferty. Czynność ta powodowałaby niedozwoloną zmianę oferty i poprawienie błędów w jej treści. Zgodnie w wyrokiem KIO 338/22 w sytuacji, w której złożony Wykaz swoją treścią nie potwierdził zgodności oferowanego systemu z wymaganiami, cechami określonymi w szczegółowym opisie przedmiotu zamówienia to ofertę taką należy uznać za niezgodną z warunkami zamówienia, tym samym, odrzucić w oparciu o art. 226 ust. 1 pkt 5 ustawy PZP. Za niedopuszczalną, należałoby uznać procedurę polegającą na wezwaniu Wykonawcy do uzupełnienia Wykazu lub wezwania Wykonawcy do złożenia wyjaśnień. Nie ulega bowiem wątpliwości, że oferowany System nie potwierdził zgodności oferowanego produktu z wymaganiami, cechami określonymi w opisie przedmiotu zamówienia przez Zamawiającego.

Uzasadnienie prawne:

Art. 226 ust. 1 pkt 5 ustawy Pzp, zgodnie z którym Zamawiający odrzuca ofertę, jeżeli jej treść jest niezgodna z warunkami zamówienia.

Poniżej Zamawiający przedstawia nazwę i adres Wykonawców, którzy złożyli oferty wraz z punktacją przyznaną ofertom w każdym z kryteriów oceny ofert oraz punktację łączną:

Nr oferty	Nazwa wykonawcy	Cena brutto (zł)	Liczba punktów w kryterium „cena”	RAZEM
1	Apius Technologies S.A. ul. Moniuszki 50 31-523 Kraków	760 878,00	100	100
2	Network Experts sp. z o. o., sp. k. ul. Chojnowska 8 03-583 Warszawa	727 299,00	Oferta odrzucona	

W dniu 6.11.2023 r. do Zamawiającego wpłynęło odwołanie do KIO. Zamawiający informuje, że zgodnie z art. 577 ustawy Pzp w przypadku wniesienia odwołania, Zamawiający nie może zawrzeć umowy do czasu ogłoszenia przez Izbę wyroku lub postanowienia kończącego postępowanie odwoławcze.

Michał Zawadzki

Kierownik Projektu

Dział Systemów Informatycznych

/podpisano elektronicznie/