Narodowe Centrum Badań i Rozwoju

ZAPYTANIE O SZACUNKOWĄ WARTOŚĆ ZAMÓWIENIA NA ZAKUP SYSTEMU KLASY „SIEM", WRAZ Z KOMPLETEM NIEZBĘDNYCH LICENCJI ORAZ USŁUG

Narodowe Centrum Badań i Rozwoju (NCBR), z siedzibą w Warszawie (00-695) przy ul. Nowogrodzkiej 47a (NIP: 701-007-37-77, REGON: 141032404) (zwane dalej: „Zamawiającym") planuje wszczęcie postępowania o udzielenie zamówienia publicznego, którego przedmiotem będzie zakup zintegrowanego ZAKUP SYSTEMU KLASY „SIEM", WRAZ Z KOMPLETEM NIEZBĘDNYCH LICENCJI ORAZ USŁUG (zwanego dalej: „Rozwiązaniem", „Systemem SIEM" lub „Systemem"). W związku z powyższym, w celu oszacowania wartości zamówienia Zamawiający zwraca się z prośbą o udzielenie informacji na temat ceny netto oraz brutto całkowitego kosztu realizacji zamówienia.

I. Przedmiot zamówienia:

Zakup systemu klasy „SIEM", wraz z kompletem niezbędnych licencji oraz usług, w zależności od wybranej opcji: w modelu SaaS, w modelu tradycyjnym z wykorzystaniem infrastruktury Zamawiającego lub w modelu tradycyjnym z dostawą infrastruktury pod oferowane Rozwiązanie.

II. Kod CPV:

48000000-8: Pakiety oprogramowania i systemy informatyczne

48730000-4: Pakiet oprogramowania zabezpieczającego

III. Opis przedmiotu zamówienia:

1. Przedmiot zamówienia obejmuje:

1.1 Sprzedaż i dostawę licencji dla **oprogramowania klasy „SIEM"** oraz wsparcia producenta przez okres obowiązywania umowy, tj. 18, 24 lub 36 miesięcy, w zależności od wybranej opcji: w modelu SaaS, w modelu tradycyjnym z dostawą infrastruktury lub w modelu tradycyjnym na istniejącej infrastrukturze Zamawiającego.

1.2 W przypadku modelu tradycyjnego w załączeniu należy wyspecyfikować wycenianą infrastrukturę.

1.3 Przeprowadzenie przez Wykonawcę autorskiego warsztatowego przekazania wiedzy dla 2 (dwóch) osób, którego zakres obejmuje;

a. Architekturę i konfigurację oprogramowania klasy SIEM,
b. Administrowanie systemem klasy SIEM,
c. Użytkowanie systemu klasy SIEM.

1.4 Świadczenie serwisu i wsparcia technicznego Wykonawcy dla oprogramowania przez okres 18, 24 lub 36 miesięcy od dnia podpisania umowy.

1.5 Przeprowadzenie przez Wykonawcę wdrożenia oferowanego rozwiązania.

2. Wymagania dotyczące dostawy sprzętu (w przypadku jego zaoferowania), oprogramowania oraz licencji:

2.1 Dostawa musi zostać zrealizowana w terminie do 10 dni kalendarzowych od dnia podpisania Umowy.

2.2 Koszty dostawy (w tym koszty opakowania, ubezpieczenia, transportu) ponosi Wykonawca.

2.3 Wykonawca zobowiązuje się dostarczyć wymagany sprzęt (w przypadku jego zaoferowania), oprogramowanie oraz licencje pochodzące z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych świadczonych przez sieć serwisową producenta na terenie Polski.

2.4 Dostawa, instalacja, konfiguracja oprogramowania, aplikacji, modułów wymaganych do zbudowania zaoferowanego Systemu, musi być zgodna z wymaganymi funkcjonalnościami oraz oczekiwaniami Zamawiającego.

2.5 Dostawa, instalacja, licencji wymaganych do poprawnej pracy Systemu, musi być zgodna z wymaganymi funkcjonalnościami, przy minimalnym zapewnieniu wielkości gromadzonych logów/danych na poziomie 50 GB dziennie.

2.6 Zamówione licencje muszą być dostarczone do Zamawiającego w postaci wygenerowanych na stronie producenta plików licencyjnych lub w formie plików wygenerowanych i przesłanych przez Wykonawcę na wskazany przez Zamawiającego adres e-mail.

3. Wymagania dot. zakresu usług

3.1 W przypadku modelu tradycyjnego, z wykorzystaniem infrastruktury Zamawiającego lub dostawą infrastruktury pod oferowane Rozwiązanie, wdrożenie zaoferowanego Systemu zgodnie z zakładanymi funkcjonalnościami jak i specyfikacją techniczną Zamawiającego. Niezbędne zasoby dla wdrożenia Systemu na posiadanej platformie VMware zapewni Zamawiający.

3.2 Opracowanie dokumentacji powykonawczej będącej częścią wdrożenia Systemu.

3.3 Warsztatowe przekazanie wiedzy zgodnie ze specyfikacją Zamawiającego.

3.4 Świadczenie serwisu i wsparcia technicznego Wykonawcy, świadczona przez okres 18, 24 lub 36 miesięcy, od dnia podpisania umowy, w zależności od wybranej opcji .

3.5 Usługa wsparcia technicznego producenta świadczona przez okres 18, 24 lub 36 miesięcy, od dnia podpisania umowy, w zależności od wybranej opcji.

`

4. Wymagana funkcjonalność systemu

4.1 System nie może posiadać ograniczeń w postaci ilości urządzeń, z których pobierane są logi, jak również liczby źródeł generowanych logów.

4.2 System musi zapewniać wydajność parsowania logów, których wielkość dochodzi do 50 GB oraz dla których częstość zdarzeń na sekundę (EPS) może dochodzić do 30000 EPS.

4.3 Zaoferowany System nie może blokować/odrzucać logów/danych w przypadku przekroczenia dziennego limitu danych (w odniesieniu do wykorzystywanych w danym momencie licencji), jak również otrzymywanych zdarzeń na sekundę (EPS).

4.4 System musi umożliwiać co najmniej półroczne przechowywanie gromadzonych logów oraz ich wydajną analizę na co najmniej 12TB danych.

4.5 System musi zapewnić mechanizm identyfikacji zapisywanych danych, który pozwoli na unikanie duplikacji danych

4.6 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.

4.7 Wyszukiwanie danych musi być możliwe z wykorzystaniem filtrów opartych o dane znormalizowane np. zapytanie o konkretny adres IP występujący jako adres źródłowy połączeń. System musi również pozwalać na wyszukiwanie danych w oparciu o wyrażenia regularne zastosowane wobec całego logu jak również pojedynczych pól.

4.8 System musi analizować zdarzenia w oparciu o znaczniki czasu zawarte w oryginalnych logach jeśli tylko są dostępne.

4.9 System musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności, związanych z analizą danych obejmującą:

a. mechanizmy pobierania danych,
b. raporty, dashboardy i formularze,
c. nowe funkcje analityczne,
d. nowe sposoby wizualizacji,
e. mechanizmy powiadamiania, w tym dwukierunkowe inne niż przewidział producent.

Realizacja tych funkcjonalności nie może wymagać konieczności angażowania producenta

4.10 Musi istnieć możliwość tworzenie interaktywnych dashboardów zawierających elementy interfejsu użytkownika takie, jak np. pola tekstowe, listy wyboru, checkbox itp. pozwalające na parametryzacje wyświetlanych informacji. Musi istnieć możliwość tworzenie ich bez konieczności programowania (z wykorzystaniem narzędzi graficznych).

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

4.12 Komunikacja użytkownika z Systemem musi odbywać się przy użyciu przeglądarki internetowej (wsparcie dla co najmniej: Microsoft Edge, Firefox, Chrome). Nie jest dopuszczalne wymaganie instalacji jakiegokolwiek dedykowanego oprogramowania klienckiego na stacjach roboczych użytkowników, w tym wtyczek i środowisk uruchomieniowych w rodzaju Adobe Flash, Java lub Microsoft Silverlight.

4.13 Do celów administracyjnych dopuszczalne jest wymaganie zdalnego dostępu do konsoli systemu operacyjnego serwera przy użyciu standardowych narzędzi, takich klient SSH lub RDP.

4.14 System powinien wspierać Role Based Access Control (RBAC), umożliwiając precyzyjne nadawanie uprawnień dla administratorów, w zakresie monitorowanego obszaru systemu informatycznego oraz dostępnych operacji w systemie zarządzania. Tożsamość administratorów musi być weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania co najmniej LDAP lub Active Directory

4.15 System musi umożliwiać pobieranie logów z co najmniej następującymi protokołami:

a. syslog UDP/TCP,
b. trap SNMP,
c. logi i informacje przechowywane w bazach danych. Nie mniej niż Oracle, MS SQL, MySQL, PostgreSQL. Musi istnieć możliwość instalacji sterowników do innych typów baz danych w standardzie JDBC lub ODBC (alternatywnie),
d. pliki tekstowe,
e. WMI,
f. NetFlow v5 i v9, sFlow, jFlow, IPFIX.

Pobieranie danych z ww. protokołów musi być możliwe bez wykorzystania agenta dla monitorowanych urządzeń i serwerów.

4.16 System musi umożliwiać stosowanie agentów na monitorowanych serwerach i stacjach roboczych. Agent musi również umożliwiać pobieranie informacji zarówno z systemu, na którym został zainstalowany, jak również z zewnętrznych systemów (np. w celu obsłużenia logów w strefach DMZ lub lokalizacjach zdalnych). Konfiguracja agenta, po podłączeniu do serwera zarządzającego musi odbywać się centralnie. Agent musi zapewniać możliwość szyfrowania i uwierzytelniania komunikacji z serwerem centralnym. Agent musi mieć możliwość równoważenia obciążenia (wysyłanych danych) pomiędzy kilka serwerów centralnych rozwiązań działających w klastrze lub niezależnie.

4.17 System musi posiadać interfejs programowania aplikacji (API) w postaci bibliotek programistycznych dla języków: Java, Python, JavaScript, PHP, Ruby oraz C#.

4.18 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:

a. DHCP,
b. DNS,
c. HTTP,
d. IMAP,
e. SIP,
f. SMB,
g. SMTP.

Prowadzenie nasłuchu musi być możliwe z dedykowanego serwera, jak również musi być możliwe z agenta zainstalowanego na stacji roboczej lub serwerze.

4.19 System musi posiadać udokumentowany interfejs REST (Representational State Transfer) umożliwiający integrację z zewnętrznymi systemami teleinformatycznymi.

4.20 Mechanizm przechowywania logów/danych/zdarzeń wdrożonego rozwiązania musi uniemożliwiać nieupoważnione usunięcie całości lub części logów, danych, raportów i innych informacji oraz zapewniać dostęp do nich tylko dla uprawnionych, uwierzytelnionych użytkowników.

4.21 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.

4.22 Zaoferowany System musi umożliwiać Zamawiającemu skalowalność/rozbudowę architektury/infrastruktury w przypadku wzrostu wymagań wydajnościowych i

pojemnościowych wynikających z przekazywania, gromadzenia oraz zwiększania szczegółowości poziomu logowanych zdarzeń (logów/danych).

4.23 Licencja Systemu nie może ograniczać liczby elementów gromadzących oraz analizujących logi.

4.24 Musi istnieć możliwość określenia szczegółowości zbieranych danych w zakresie wybranych protokołów, określonych pól protokołów (np. http_user_agent) oraz opcjonalnie agregacji danych.

4.25 System musi zapewnić nieprzerwaną kontynuację pracy w przypadku awarii jednego z centrum przetwarzania danych lub dowolnego elementu infrastruktury tego Systemu.

4.26 System musi posiadać oraz umożliwiać akceleracją 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.

4.27 Tabele i wykresy prezentowane na bazie dostarczonych logów/danych muszą posiadać funkcję drill-down, tzn. po zaznaczeniu danej pozycji w tabeli lub wykresie interfejs powinien pokazywać odpowiadające im logi/dane.

4.28 Musi istnieć możliwość definiowania akcji typu drill down powiązanych z różnymi typami zdarzeń oraz pól. Dostępne akcje powinny obejmować zewnętrzny URL lub raport/dashboard w samym Systemie. Dla zewnętrznych URL musi istnieć możliwość przekazania parametru lub parametrów na podstawie wartości pól, których dotyczy akcja drilldown.

4.29 Rozwiązanie musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie, w jakiej ten log został przesłany do Rozwiązania.

4.30 System musi automatycznie (tj. bez uprzedniego definiowania schematu danych wejściowych) analizować dane zdarzanie (dzienniki systemowe w formie Syslog, Netflow, itp.) pod kątem zawartości i struktury danych. Wynikiem analizy powinny być informacje mapowane w formacie łatwym do późniejszego wyszukiwania i analizy, np. w strukturach klucz-wartość.

4.31 Rozwiązanie powinno wspierać geolokalizację zdarzeń na bazie adresów IP. Dane geolokalizacyjne (np. kraj) dla zdarzeń mają służyć w narzędziu do prezentacji na mapie, jak również umożliwiać ich wykorzystanie w wyszukiwaniu wartości pól oraz w regułach korelacyjnych

4.32 Rozwiązanie 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.

4.33 Mechanizm pobierania logów/danych ze źródeł, powinien umożliwiać wstępną selekcję logów/danych przed wysłaniem ich do Systemu oraz/lub rozpoczęciem parsowania (bez konieczności rekonfiguracji poziomu logowania zdarzeń w źródle), w celu analizy tylko istotnych zdarzeń, jak również oszczędności wynikających z ograniczeń licencyjnych i wydajnościowych.

4.34 Rozwiązanie 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.

4.35 System musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu (np. dodanie nowych pól, zmianę znaczenia lub nazwy istniejących itp.).

4.36 System musi umożliwiać obsługę logów w formacie XML bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą XML. System musi umożliwiać obsługę logów w formacje JSON bez konieczności tworzenie parserów. Nazwy pól powinny być określone strukturą JSON.

4.37 System musi umożliwiać obsługę logów w formacje CSV bez konieczności tworzenie parserów. Nazwy pól powinny być wierszem nagłówkowym CSV. Musi istnieć możliwość obsługi różnych delimiterów (przecinek, kropka, średnik, tabulator itp.) oraz wartości pól w cudzysłowach.

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

4.39 System musi umożliwiać rozwiązywanie adresów IP do nazw hostów i na odwrót.

4.40 Zaoferowany System musi umożliwiać wydajną pracę użytkownika przeglądającego zdarzenia i generującego raporty oraz samego Systemu, w szczególność parsowania danych których wielkość dochodzi do 50 GB dziennie.

4.41 Zaoferowany System musi umożliwiać parsowanie logów o długości co najmniej 10000 znaków oraz zawierających więcej niż jedna linię.

4.42 Zaoferowany System musi umożliwiać tworzenie bazy definicji formatów logów.

4.43 Proces odpowiedzialny za parsowania logów musi analizować poszczególne logi/dane, i wyszukiwać w nich istotne informacje o logowanym zdarzeniu, między innymi: data i czas zdarzenia, nazwa użytkownika, nazwa systemu logującego, nazwa/adres IP systemu, źródła logów, rodzaj zdarzenia (np. zalogowanie/wylogowanie/ zablokowanie użytkownika, przepuszczenie/zablokowanie ruchu sieciowego, wykrycie szkodliwego kodu itp.).

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

4.45 System musi wyszukiwać czas zdarzenia (timestamp) z analizowanego logu i wykorzystywać go do reguł korelacyjnych.

4.46 System musi umożliwiać definiowanie pól za pomocą wyrażeń regularnych (REGEX).

4.47 System musi umożliwiać w czasie rzeczywistym wyszukiwanie zdarzeń w logach/danych o zadanych wartościach pól, w oparciu o wyrażenia regularne (REGEX).

4.48 System musi umożliwiać przeglądanie (w jednej konsoli systemu) w czasie rzeczywistym, logów pobieranych/dostarczanych do Systemu w celu uniknięcia konieczności logowania się do każdego monitorowanego systemu osobno, w celu sprawdzenia statusu połączenia (przepuszczone, zablokowane). Filtrowanie w czasie rzeczywistym musi dopuszczać wyszukiwanie informacji za pomocą wyrażeń regularnych (REGEX).

4.49 System musi umożliwiać tworzenie alertów/powiadomień po wykryciu zdarzenia wynikającego z korelacji danych, wykonanych przez regułę korelacyjną.

4.50 System musi umożliwiać tworzenie reguł korelacyjnych na bazie parsowanych logów/danych z różnych źródeł.

4.51 System musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI, jak języka zapytań charakterystycznego dla danej Systemu.

4.52 System musi umożliwiać tworzenie reguł korelacyjnych o długim okresie działania (czas pomiędzy najstarszym, a najnowszym zdarzeniem w ramach grupy zdarzeń powiązanych ze sobą). Okres ten nie może być ograniczany żadnymi innymi limitami, poza dostępnością danych w Systemie.

4.53 Musi istnieć możliwość zastosowania bez modyfikacji reguł korelacyjnych dla danych historycznych, w celu wykrycia podobnych zdarzeń w przeszłości.

4.54 Rozwiązanie musi umożliwiać wykrywanie sytuacji niestandardowej (anomalii) niezgodnej z poprzednio zarejestrowanym wzorcem (np. w celu wykrycia ataku DOS, wykrycia wewnętrznego ruchu sieciowego który wcześniej nie występował, uruchomienia nowej niewystępującej wcześniej aplikacji, pojawienia się nowego użytkownika itp).

4.55 W zaoferowanym Systemie musi istnieć możliwość tworzenia własnych raportów, zarówno w formie tekstowej jak i reprezentacji graficznej, a także automatycznego, cyklicznego wysyłania raportów wiadomością e-mail, w postaci PDF.

4.56 System musi wspierać pracę użytkowników o różnych rolach i w następujących obszarach:
   a. Analiza zdarzeń w obszarze bezpieczeństwa teleinformatycznego,
   b. Analiza pracy systemów informatycznych w zakresie wydajności i awarii systemów/urządzeń teleinformatycznych,
   c. Analiza pracy aplikacji wdrażanych/tworzonych przez pracowników NCBR.

4.57 System musi zapewnić rozliczność działań użytkowników, w szczególności rejestrowanie dostępu do przetwarzanych logów/danych.

4.58 Rozwiązanie musi umożliwiać jednoczesną pracę analityczną co najmniej dla 20-u użytkowników.

4.59 Licencja Rozwiązania musi umożliwiać utworzenie kont i pracę dla co najmniej 20-u użytkowników.

4.60 System musi umożliwiać odseparowanie środowiska pracy użytkowników o różnych rolach.

4.61 Wdrożony System musi być odporny na ataki sieciowe.

4.62 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.

4.63 System musi zawierać mechanizmy zarządzania incydentami obejmujące co najmniej:
   a. Możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych,
   b. Możliwość przypisania incydentu do osoby,
   c. Możliwość zmiany statusu i priorytetu incydentu,
   d. Możliwość tworzenia komentarzy,
   e. Możliwość automatycznego i ręcznego modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy.
   f. Możliwość tworzenia wyjątków stałych i czasowych dla reguł i zdarzeń spełniających określone warunki.
   g. Możliwość raportowania wydajności obsługi incydentów.

4.64 Możliwość zintegrowania z systemami monitoringu np. Zabbix, Solarwinds, w celu monitorowania liczników wydajnościowych oraz dostępności serwisów w kontekście użytkownika/systemu końcowego.

4.65 W przypadku zaoferowania Zamawiającemu Systemu budowanego w oparciu o sprzęt typu appliance, musi zostać zapewniona wydajność niezbędna do parsowania logów/danych, których wielkość dochodzi do 50 GB dziennie oraz dla

których częstość zdarzeń na sekundę (EPS) może dochodzić do 30000 EPS – nie może wtedy dochodzić do utraty (dropowania) logów/danych. Zdarzenia muszą być przechowywane w systemie przez co najmniej pół roku.

4.66 System zbudowany w oparciu o sprzęt musi zapewniać wysoką dostępność (konfiguracja klastra HA) w zakresie kolekcji logów i bazy danych. Awaria pojedynczego elementu nie może wpływać na możliwość pobierania i rejestrowania logów. Musi istnieć możliwość dodania kolejnych węzłów klastra w trakcie używania Systemu, w celu zwiększenia wymagań dotyczących wydajności lub dostępności.

4.67 Sprzęt, w przypadku jego zaoferowania, do budowy Systemu musi posiadać 18, 24 lub 36 miesięczną gwarancję producenta w zależności od wybranej opcji.

4.68 Rozwiązanie w modelu SaaS musi uwzględniać poniższe wymagania:

a. Wszystkie wymagane środowiska muszą zostać wdrożone, uruchomione i użytkowane w Centrach Danych znajdujących się wyłącznie na terenie państw EOG.
b. Zamawiający wymaga SLA na poziomie nie mniejszym niż 99,999% tj. nie więcej niż 6 minut przestoju w pracy Systemu rocznie,
c. Komunikacja powinna odbywać się w sposób bezpieczny i szyfrowany. W przypadku integracji z systemami wewnętrznymi Zamawiającego, Wykonawca jest odpowiedzialny za zestawienie bezpiecznego i szyfrowanego połączenia z infrastrukturą Centrum. Połączenie to musi być kompatybilne z infrastrukturą Zamawiającego, a zakres uzgodniony z Zamawiającym.
d. Wykonawca będzie wykonywał przynajmniej raz dziennie kopie zapasowe danych systemu i udostępniał je Zamawiającemu na życzenie.
e. Wykonawca jest odpowiedzialny za zapewnienie, że wszystkie dane są szyfrowane na źródle (przed opuszczeniem firmowej sieci) oraz podczas ich transferu i przechowywania. Musi się to odbywać bez negatywnego wpływu na współczynnik redukcji danych.
f. Wykonawca jest odpowiedzialny za zapewnienie ochrony przed atakami DDoS, niezbędnych zapór ogniowych i innych środków bezpieczeństwa teleinformatycznego.
g. Wykonawca jest odpowiedzialny za zapewnienie odpowiednio wydajnego środowiska wymaganego do optymalnej pracy Systemu, zgodnie z wymaganiami Zamawiającego.
h. Rozwiązanie musi być zgodne z międzynarodowymi standardami i wytycznymi dotyczącymi bezpieczeństwa, takimi jak ISO 27001, w celu utrzymania działania infrastruktury obliczeniowej i zapewnienia prywatności danych.

i. Wykonawca musi zapewnić ścisłe procedury uwierzytelniania użytkowników i administratorów.
j. Wykonawca musi zapewnić procedury i środki umożliwiające monitorowanie wszystkich operacji przeprowadzanych w systemie informacyjnym oraz raportowanie, zgodnie z obowiązującymi przepisami, w przypadku wystąpienia incydentów dotyczących danych klienta.
k. Wykonawca musi zapewnić, że konfiguracja zasobów współdzielonych uniemożliwia wzajemny dostęp do danych na nich ulokowanych poprzez różne podmioty.
l. Wykonawca musi niezwłocznie powiadomić Zamawiającego o każdym przypadku naruszenia zasad bezpieczeństwa, wtargnięcia lub prośby agencji rządowych o dostęp do danych, aby umożliwić Zamawiającemu zarządzanie tymi wydarzeniami proaktywnie.
m. Wykonawca musi zapewnić, że w przypadku zwolnienia zasobów wszystkie bloki pamięci i wszelkie kopie danych, jeśli takie istnieją, zostaną tak usunięte bądź wyzerowane przez Wykonawcę, aby dane nie mogły zostać odzyskane.
n. Wykonawca nie może przetwarzać ani przechowywać danych Zamawiającego poza EOG.
o. Wykonawca jest zobowiązany do przetwarzania danych osobowych klienta wyłącznie do celów związanych z właściwą realizacją usług i wyłącznie zgodnie z jego instrukcjami.
p. Dane przechowywane na infrastrukturze Wykonawcy pozostają własnością Zamawiającego.
q. Wykonawca musi posiadać system zarządzania uprawnieniami ograniczający dostęp do pomieszczeń oraz danych tylko do osób, które muszą go mieć ze względu na pełnione funkcje i zakres obowiązków.
r. Wykonawca musi określić wspólnie z Zamawiającym zasady przeszukiwania, retencji i usuwania danych dostarczonych przez Zamawiającego.
s. Wykonawca musi raportować wszystkie incydenty bezpieczeństwa danych, ze szczególnym uwzględnieniem tych, które dotyczyć mogą danych osobowych przetwarzanych przez Zamawiającego w chmurze oraz udzielić Zamawiającemu wszelkiej możliwej pomocy przy zwalczaniu skutków takich incydentów bezpieczeństwa.
t. Rozwiązanie musi mieć zdolność korzystania z zewnętrznego systemu autoryzacji (potencjalnie dostarczonego w przyszłości przez Zamawiającego) wraz z funkcjonalnością SSO na podstawie standardów wymienionych w pozostałych wymaganiach.

u. Rozwiązanie powinno mieć możliwość autoryzowania użytkowników w zewnętrznym repozytorium LDAP i AD. Komunikacja z zewnętrznymi repozytoriami winna odbywać się w sposób bezpieczny.
v. Rozwiązanie musi wspierać połączenie z systemem SSO przynajmniej przy użyciu jednego z następujących standardów: SAML, Oauth, OpenID.
w. System musi umożliwiać dodawanie, usuwanie i modyfikację użytkowników i grup.
x. Delegowani użytkownicy powinni móc zarządzać całością uprawnień dla grup i użytkowników.
y. Delegowani użytkownicy powinni móc tworzyć grupy i nowych użytkowników.
z. System musi umożliwiać czasowe blokowanie kont przez administratorów oraz ich odblokowywanie.
aa. System musi przechowywać logi pełnej historii zdarzeń takich jak (ale nie ograniczonych do): logowanie i próby logowania, operacje na zasobach, modyfikacje uprawnień użytkowników, dodawanie grup i użytkowników, kasowanie obiektów.
bb. System rejestruje aktywności Użytkowników (login, adres IP, nazwa komputera, czas).
cc. System weryfikuje ważność hasła. Ważność hasła powinna wygaszać po upływie określonej w konfiguracji liczbie dni. System wymusza zmianę hasła. Hasła nie mogą się powtarzać w okresie określonej w konfiguracji liczbie miesięcy.
dd. Zamawiający wymaga aby dokumentacja API była publicznie dostępna i nie stanowiła tajemnicy firmy.
ee. W przypadku zastosowania gotowego oprogramowania dokumentacja producenta tego oprogramowania musi zostać dołączona do dokumentacji technicznej całego Systemu.

5. Wymagania odnośnie warsztatowego przekazania wiedzy:

5.1 Zamawiający wymaga przeprowadzenie przez Wykonawcę autorskiego warsztatowego przekazania wiedzy, o którym mowa w pkt 1.2. dla 2 (dwóch) osób, w siedzibie Zamawiającego w Warszawie przy ul. Nowogrodzkiej 47a lub w postaci szkolenia on-line, w terminie 3 miesięcy od dnia podpisania umowy.

**6. Zakres wsparcia technicznego i serwisu Rozwiązania **

6.1. Zakres wsparcia producenta oprogramowania klasy SIEM:

6.1.1. Dostęp do pomocy technicznej oprogramowania;

6.1.2. Dostęp do poprawek i nowych wersji Systemu;

6.1.3. Dostęp do dokumentacji technicznej;

6.1.4. Dostęp do konta wsparcia oprogramowania SIEM, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta oprogramowania.

6.2. Zakres serwisu i wsparcia technicznego dostawcy Systemu:

6.2.1. Zapewnienie systemu zgłoszeń, dostępnego dla upoważnionych pracowników Zamawiającego, w dni robocze (poniedziałek-piątek) od 8:00 do 16:00 z wyjątkiem dni świątecznych i ustawowo wolnych od pracy, spełniającego poniższe wymagania:

- System zgłoszeń musi obejmować następujące kanały zgłoszeń: serwis WWW, poczta elektroniczna, telefon.
- W ramach systemu zgłoszeń zapewnienie kanału WWW do śledzenia i aktualizacji zarejestrowanych zgłoszeń oraz zapewnienie możliwości automatycznego dodawania wpisów w systemie poprzez e-mail.

6.2.2. Usuwanie usterek i błędów z zachowaniem poniższych zasad:

- Usunięcie błędu krytycznego lub wykonanie obejścia błędu krytycznego (umożliwiającego korzystanie z Systemu SIEM) nastąpi w czasie 48h od przekazania zgłoszenia przez Zamawiającego. Jeżeli jednak bezpośrednią przyczyną powstania błędu krytycznego Systemu SIEM jest wada w oprogramowaniu, usunięcie błędu krytycznego nastąpi poprzez współpracę Wykonawcy z producentem Rozwiązania w terminie możliwie najszybszym z punktu widzenia producenta, nie dłuższym niż 10 dni roboczych od przyjęcia zgłoszenia.
- Usunięcie innych błędów nastąpi w ciągu 5 dni roboczych od przekazania zgłoszenia przez Zamawiającego.
- Usunięcie usterek nastąpi w ciągu 10 dni roboczych od przekazania zgłoszenia przez Zamawiającego.
- W przypadku braku możliwości usunięcia usterek i błędów w podanych wyżej terminach, Wykonawca niezwłocznie dostarczy i wdroży czasowo równoważne rozwiązanie zastępcze (workaround). Rozwiązanie zastępcze musi zostać każdorazowo uzgodnione i zaakceptowane przez Zamawiającego.
- Rozwiązanie zastępcze może funkcjonować nie dłużej niż 30 dni od daty jego wdrożenia.

6.2.3. Utrzymanie i aktualizacje zaimplementowanych dashboardów, raportów i alertów stworzonych na potrzeby Zamawiającego.

6.2.4. Świadczenie usług konsultacyjnych w zakresie funkcjonowania Systemu SIEM:

- Wymiar: do 4 godz. miesięcznie; niewykorzystane godziny w danym miesiącu przechodzą do wykorzystania na kolejny miesiąc;
- Dostępność: dni robocze od 8:00 do 16:00 z wyjątkiem dni świątecznych i ustawowo wolnych od pracy;
- Miejsce: zdalnie;
- Realizacja zadań wynikających z zakresu umowy;
- Wsparcie w pracach rozwojowych i zadaniach administracyjnych.

6.2.5. Wykonawca zapewni wsparcie techniczne przez okres obowiązywania umowy, tj. 18, 24 lub 36 miesięcy, w zależności od wybranej opcji. Objęcie usługami wsparcia technicznego i serwisu Systemu SIEM musi zapewnić Zamawiającemu pełną gotowość Wykonawcy do świadczenia opisanych w niniejszej specyfikacji usług od pierwszego dnia obowiązywania Umowy. Ponadto, świadczone usługi nie mogą negatywnie wpływać na zintegrowane z Systemem SIEM aplikacje biznesowe i inne systemy bezpieczeństwa informacji.

6.2.6. Wsparcie techniczne musi być świadczone przez zespół składający się, z co najmniej dwóch inżynierów Wykonawcy, posiadających stosowne kompetencje, potwierdzone certyfikatem ukończenia szkolenia z technologii wdrożonego Rozwiązania.

7. Opis posiadanych przez Zamawiającego licencji, wsparcia dla posiadanego Systemu SIEM oraz infrastruktury:

7.1. Licencja Splunk Enterprise 50GB/day, ze wsparciem producenta ważna do dnia 2020-03-13.

7.2. Licencja Splunk Enterprise Security 50GB/day, ze wsparciem producenta ważna do dnia 2020-03-13.

7.3. Zamawiający posiada uruchomione następujące maszyny wirtualne dla w/w rozwiązania:

a. Splunk MC,
b. Splunk DS Lic Srv,
c. Splunk HFW,
d. Splunk - Indexer 1,
e. Splunk - Indexer 2,
f. Splunk – SH.

8. **Rozliczenie umowy odbywać się będzie zgodnie z poniższym harmonogramem:**

8.1. Dostarczenie licencji – jednorazowo po potwierdzeniu przez Zamawiającego jej otrzymania;

8.2. Wdrożenie systemu – jednorazowo po potwierdzeniu przez Zamawiającego prawidłowego wykonania usługi – opcjonalnie, przy wyborze systemu wraz z infrastrukturą (model tradycyjny).

8.3. Usługa wsparcia technicznego Wykonawcy – w cyklach miesięcznych, po zakończeniu miesiąca, w którym świadczona była usługa;

8.4. Usługa konsultacyjna Wykonawcy – w cyklach miesięcznych na podstawie iloczynu liczby faktycznie wykorzystanych w okresie rozliczeniowym roboczogodzin i stawki godzinowej wskazanej w ofercie.

9. **Zamawiający zastrzega sobie możliwość naliczenia kar umownych, w tym co najmniej:**

30% w razie niewykonania przedmiotu zamówienia,

10% za każdy przypadek nienależytego wykonania przedmiotu zamówienia,

a także w przypadku przekroczenia terminów wskazanych w umowie.

IV. **Termin realizacji zamówienia**:

W zależności od wybranej opcji umowa zawarta zostanie na okres 18, 24 lub 36 miesięcy.

Dostawa licencji w terminie do 10 dni kalendarzowych od podpisania umowy.

Zamawiający na etapie szacowania wartości zamówienia zastrzega sobie możliwość negocjacji wskazanych terminów.

V. **Miejsce oraz termin przedłożenia informacji o koszcie usług:**

Drogą e-mailową na adres karolina.zych@ncbr.gov.pl i slawomir.ponikowski@ncbr.gov.pl do dnia **12 października 2020 r. do godz. 23.59.**

VI. **Wycena powinna być złożona na załączonym formularzu wyceny szacunkowej:**

FORMULARZ WYCENY SZACUNKOWEJ

PEŁNA NAZWA WYKONAWCY: .....

ADRES Z KODEM POCZTOWYM: .....

TELEFON: …….…….....

ADRES E-MAIL: .....

NUMER NIP:……..…….....

NUMER REGON: .....

Wycena

Nawiązując do zapytania o szacunkowy koszt wykonania zamówienia publicznego, którego przedmiotem będzie zakup systemu klasy „SIEM”, wraz z kompletem niezbędnych licencji oraz usług, w zależności od wybranej opcji: w modelu SaaS, w modelu tradycyjnym z wykorzystaniem infrastruktury Zamawiającego lub w modelu tradycyjnym z dostawą infrastruktury pod oferowane Rozwiązanie, wyceniamy wykonanie przedmiotu zamówienia, w pełnym rzeczowym zakresie ujętym w zapytaniu, za cenę:

W modelu SaaS						
Okres	18 miesięcy		24 miesięcy		36 miesięcy	
Netto zł:						
Brutto zł:						
w tym	netto zł	brutto zł	netto zł	brutto zł	netto zł	brutto zł
wartość licencji						
wartość wsparcia technicznego						
wartość usług konsultacyjnej	48 roboczogodzin		96 roboczogodzin		144 roboczogodziny	

W modelu tradycyjnym z oferowanym sprzętem (infrastrukturą) i usługą wdrożenia (w załączeniu specyfikacja wycenionego sprzętu)						
Okres	18 miesięcy		24 miesięcy		36 miesięcy	
Netto zł:						
Brutto zł:						
w tym	netto zł	brutto zł	netto zł	brutto zł	netto zł	brutto zł
wartość licencji						
wartość usługi wdrożenia						
wartość urządzeń i aplikacji systemowych						
wartość wsparcia technicznego						
wartość usług konsultacyjnej	48 roboczogodzin		96 roboczogodzin		144 roboczogodziny	

Na istniejącej infrastrukturze Zamawiającego						
Okres	18 miesięcy		24 miesięcy		36 miesięcy	
Netto zł:						
Brutto zł:						
w tym	netto zł	brutto zł	netto zł	brutto zł	netto zł	brutto zł
wartość licencji						
wartość usługi wdrożenia						

wartość wsparcia technicznego						
wartość usług konsultacyjnej	48 roboczogodzin		96 roboczogodzin		144 roboczogodziny	

Proponowane rozwiązanie (nazwa systemu): ……

Wdrożenie rozwiązania nastąpi w terminie …….. dni od dostarczenia licencji.

Oświadczamy, że:

1. Nie wnosimy żadnych zastrzeżeń do zapytania o szacunkowy koszt.
2. Przyjmujemy do wiadomości, że:
   2.1. złożenie wyceny na zapytanie o szacunkowy koszt, jak też otrzymanie w jego wyniku odpowiedzi nie jest równoznaczne z udzieleniem zamówienia przez Narodowe Centrum Badań i Rozwoju (nie rodzi skutków w postaci zawarcia umowy);
   2.2. powyższe zapytanie szacunkowe nie stanowi oferty w rozumieniu Kodeksu Cywilnego;
   2.3. Zamawiający dopuszcza możliwość doprecyzowania lub skorygowania zapisów i warunków niniejszego zapytania;
   2.4. Zamawiający zastrzega sobie prawo do unieważnienia zapytania szacunkowego bez podania przyczyny.
3. Oświadczam, że wypełniłem/-am obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO*) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu złożenia wyceny w niniejszym postępowaniu**.
   **rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).*
   *** W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).*
4. Oświadczam, że uzyskałem zgody osób biorących udział w przygotowaniu wyceny, a także wyrażam zgodę na przetwarzanie moich danych osobowych przez Narodowe Centrum

Badań i Rozwoju z siedzibą w Warszawa 00-695, Nowogrodzka 47a, i przyjmuję do wiadomości, że moje dane podane w wycenie będą przetwarzane w celu związanym z przygotowaniem postępowania.

…… …….

miejscowość, data

podpis, imię i nazwisko

lub podpis na pieczęci imiennej