***Załącznik nr 2 do SWZ***

**FORMULARZ OFERTY**

**dla Narodowego Centrum Badań i Rozwoju,**

**z siedzibą w Warszawie, ul. Chmielna 69, 00-801 Warszawa**

**Wykonawca:**

Ja/my[[1]](#footnote-1) niżej podpisani:

…………………………………………………………………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

działając w imieniu i na rzecz:

........................................................................................................................................

*(pełna nazwa Wykonawcy/Wykonawców w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia)*

Adres: ………………………………………………………………………………………………

Kraj …………………………………..

REGON ………………………………

NIP: …………………………………..

TEL. ………………………………….

adres e-mail:…………………………………… *(na który Zamawiający ma przesyłać korespondencję)*

Proszę określić rodzaj Wykonawcy.

  mikroprzedsiębiorstwo

  małe przedsiębiorstwo

  średnie przedsiębiorstwo

  jednoosobowa działalność gospodarcza

  osoba fizyczna nieprowadząca działalności gospodarczej

  inny rodzaj ……………………………………..

**Ubiegając się o udzielenie zamówienia publicznego na „Zakup odnowienia licencji oprogramowania SIEM - usługa serwisu, wsparcia technicznego i konsultacyjna”, nr postępowania 29/23/PN,** składamy ofertę na realizację przedmiotu zamówienia w zakresie określonym w Specyfikacji Warunków Zamówienia i jej załącznikach na następujących warunkach:

1. Oferowana łączna cena za realizację przedmiotu zamówienia wynosi ……………. złotych netto, powiększona o należny podatek od towarów i usług, tj. kwota ………….. złotych brutto, w tabeli poniżej:

Nazwa oferowanego systemu …………………………………………….………….

Nazwa oferowanych dodatkowych komponentów infrastruktury[[2]](#footnote-2) …………………………………………….………….

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | Produkt | Liczba | Cena jednostkowa (netto) PLN  | Wartośćnetto PLNkol. 4 x kol. 5 | **stawka VAT** % | **Wartość podatku VAT****kol. 6 x stawka VAT** **PLN** | Wartość (brutto) kol. 6 + kol. 8 **PLN** |
| 1 | 2 | 4 | 5 | 6 | 7 | 8 | 9 |
| **1** | Przedłużenie licencji dla posiadanego Systemu SIEM opartego na architekturze Splunk Enterprise wraz z usługą **Wsparcia technicznego producenta** na poziomie Standard lub produkt równoważny | 1  | ……….. zł | ……….. zł | ….. % VAT |  | ……….. zł |
| **2** | Usługa wdrożenia produktu równoważnego[[3]](#footnote-3)  |  | ……….. zł | ……….. zł | ….. % VAT |  | ……….. zł |
| **3** | Usługa wsparcia technicznego Wykonawcy[[4]](#footnote-4) |  | ……….. zł | ……….. zł | ….. % VAT |  | ……….. zł |
| **4** | **Prawo Opcji:**Usługi konsultacyjne[[5]](#footnote-5) | 350 roboczogodzin | ……….. zł | ……….. zł | ….. % VAT |  | ……….. zł |
| **5.**  | Dodatkowe komponenty infrastruktury[[6]](#footnote-6) |  | ……….. zł | ……….. zł | ….. % VAT |  | ……….. zł |

1. OŚWIADCZAMY, że zamówienie wykonamy w terminie wymaganym przez Zamawiającego, wskazanym w Specyfikacji Warunków Zamówienia i Projektowanymi Postanowieniami Umowy.
2. OŚWIADCZAMY, że zapoznaliśmy się ze Specyfikacją Warunków Zamówienia i akceptujemy ją oraz spełniamy wszystkie warunki w niej zawarte.
3. OŚWIADCZAMY, że jesteśmy związani niniejszą ofertą w terminie wskazanym w SWZ i Ogłoszeniu o zamówieniu.
4. OŚWIADCZAMY, że zapoznaliśmy się z Projektowanymi Postanowieniami Umowy, określonymi w Załączniku nr 3 do Specyfikacji Warunków Zamówienia i akceptujemy je bez zastrzeżeń oraz zobowiązujemy się - w przypadku wyboru naszej oferty - do zawarcia umowy na warunkach w nich określonych, w miejscu i terminie wyznaczonym przez Zamawiającego.
5. OŚWIADCZAMY, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[[7]](#footnote-7) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.[[8]](#footnote-8)
6. Wypełnimy, zgodnie z art. 13 lub art. 14 RODO2, obowiązki informacyjne wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskamy w celu ubiegania się o udzielenie zamówienia publicznego na dalszym etapie niniejszego postępowania bądź realizacji zamówienia (o ile nasza oferta zostanie wybrana jako najkorzystniejsza w niniejszym postępowaniu).
7. Jeśli realizacja przedmiotowego zamówienia związana będzie z powierzeniem nam przetwarzania danych osobowych, będziemy przetwarzać je zgodnie z obowiązującymi przepisami przez cały czas realizacji zamówienia, w szczególności spełnimy wszystkie obowiązki nałożone na podmiot przetwarzający przez przepisy RODO. Jednocześnie gwarantujemy wysoki poziom bezpieczeństwa powierzonych nam danych, przy zastosowaniu stosownych środków technicznych i organizacyjnych, zgodnie z art. 32 RODO. Zobowiązujemy się również do współpracy z NCBR przy realizacji jej obowiązków dotyczących ochrony danych osobowych, wynikających z obowiązujących przepisów prawa.
8. Wraz z ofertą SKŁADAMYnastępujące oświadczenia i dokumenty:
	1. ………………………..
	2. ……………………….

…………….……., dnia …………. r.

*……………………………….*

*Imię i nazwisko*

*/podpisano elektronicznie/*

**Informacja dla Wykonawcy:**

Formularz oferty musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania Wykonawcy kwalifikowanym podpisem elektronicznym i przekazany Zamawiającemu wraz z dokumentem/dokumentami potwierdzającymi prawo do reprezentacji Wykonawcy przez osobę podpisującą ofertę.

**Załącznik nr 2a do SWZ**

Wykaz spełniania kryteriów stosowanych w celu oceny równoważności oprogramowania, ***składany w przypadku zaoferowania rozwiązania równoważnego*** jako dowód na potwierdzenie, że rozwiązanie

równoważne spełnia kryteria stosowane w celu oceny równoważności (składany wraz z ofertą w celu potwierdzenia parametrów wymaganych w OPZ)

|  |  |  |  |
| --- | --- | --- | --- |
| **Opis wymagania** | **Oświadczenie Wykonawcy:****Spełnia/Nie spełna** | **Opis oferowanych wymagań lub sposobu spełnienia wymagania** | **Wskazanie miejsca w dokumentacji[[9]](#footnote-9) oprogramowania, w którym znajduje się potwierdzenie spełnienie danego wymagania (nazwa dokumentu, numer strony dokumentu, pkt, etc. oraz 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 na potwierdzenie spełnienia danego wymagania (np. zrzut ekranu konfiguracji/testu, karta katalogowa, specyfikacja techniczna, dokumentacja licencyjna, dokumentacja.** |
| 1.      Oferowany System musi być rozwiązaniem komercyjnym, posiadającym wsparcie techniczne producenta. Nie dopuszcza się rozwiązań open source. |  |  |  |
| 2.      Oferowany System musi funkcjonować w środowisku wirtualizacyjnym Vmware. |  |  |  |
| 3.      Zamawiający nie dopuszcza rozwiązań chmurowych. |  |  |  |
| 4.      Oferowane funkcjonalności muszą mieć pokrycie w oficjalnie dostępnej dokumentacji technicznej producenta, którą dostawca udostępni na żądanie Zamawiającego wraz ze wskazaniem punktów odnoszących się do danej funkcjonalności wymaganej w OPZ. |  |  |  |
| 5.      System musi cechować się uniwersalnością, tzn. oprócz funkcjonalności dedykowanych bezpieczeństwu powinno zapewniać możliwość wykorzystania wybranego rozwiązania do analityki biznesowej, raportowania, monitoringu infrastruktury teleinformatycznej oraz zarządzania i monitoringu logów systemowych i aplikacyjnych. |  |  |  |
| 6.      Rozwiązanie musi umożliwiać uwierzytelnianie i szyfrowanie połączenia między komponentami Systemu. |  |  |  |
| 7.      System musi samodzielnie zarządzać retencją danych. |  |  |  |
| 8.      System musi umożliwiać na konfigurację w wysokiej dostępności eliminującej wystąpienie pojedynczego punktu awarii. |  |  |  |
| 9.      Architektura Systemu musi umożliwiać na rozdzielenie na osobne komponenty (w domyśle maszyny wirtualne) funkcji związanych z pobieraniem danych, przechowywaniem, wyszukiwaniem i zarządzaniem zebranymi logami. |  |  |  |
| 10.  System nie może posiadać ograniczeń w postaci ilości urządzeń, z których pobierane są logi, jak również liczby źródeł generowanych logów; |  |  |  |
| 11.  System musi zapewniać wydajność parsowania logów, których wielkość dochodzi do 60/70/101 GB dziennie oraz dla których częstość zdarzeń na sekundę (EPS) może dochodzić do 36000 EPS; |  |  |  |
| 12.  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); |  |  |  |
| 13.  System musi umożliwiać co najmniej półroczne przechowywanie gromadzonych logów oraz ich wydajną analizę na co najmniej 15TB danych;  |  |  |  |
| 14.  System musi zapewnić mechanizm identyfikacji zapisywanych danych, który pozwoli na unikanie duplikacji danych; |  |  |  |
| 15.  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; |  |  |  |
| 16.  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; |  |  |  |
| 17.  System musi analizować zdarzenia w oparciu o znaczniki czasu zawarte w oryginalnych logach jeśli tylko są dostępne; |  |  |  |
| 18.  Zestaw funkcjonalności analitycznych musi uwzględniać co najmniej następujące funkcje: Statystyki typu suma, średnia, mediana, odchylenie standardowe, najstarszy, najnowszy dla zadanego klucza (np. średni godzinny wolumen danych dla adresu źródłowego); Funkcje wykrywania anomalii danych liczbowych. Rozwiązanie musi pozwalać na wykrywanie anomalii dla dowolnych parametrów zawartych w logach a nie tylko parametrów ruchu sieciowego; System musi wykrywać rzadkie wystąpienia wartości i zdarzeń w określonym podzbiorze; Budowanie korelacji w oparciu o zdarzenia zawierające jednakowe wartości danych pól; Badanie zmian wartości danego pola i alarmowanie lub raportowanie w oparciu o zmianę tej wartości (np. wzrost liczby niepoprawnych zalogowań o 50%). |  |  |  |
| 19.  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. |  |  |  |
| 20.  Musi istnieć możliwość tworzenia 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); |  |  |  |
| 21.  System musi posiadać możliwości wizualizacji danych na raportach i dashboardach z wykorzystaniem: tabel, wykresów (co najmniej: słupkowy, kołowy, liniowy, punktowy, bąbelkowy), map, map kolorowanych. Tworzenie wyżej wymienionych komponentów wizualizacji musi odbywać się bezpośrednio na poziomie zapytania. |  |  |  |
| 22.  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; |  |  |  |
| 23.  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;  |  |  |  |
| 24.  System musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości (ang. healtcheck). |  |  |  |
| 25.  System musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów – login/logoff, uruchamiane zapytania i zmiany konfiguracji Systemu. |  |  |  |
| 26.  Do celów administracyjnych dopuszczalne jest wymaganie zdalnego dostępu do konsoli systemu operacyjnego serwera przy użyciu standardowych narzędzi, takich klient SSH lub RDP; |  |  |  |
| 27.  System musi 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; |  |  |  |
| 28.  Zaoferowany System musi umożliwiać pobieranie logów / danych zapisanych w plikach (dziennikach systemowych / aplikacyjnych) jak również w postaci komunikatów przechwytywanych z portów TCP/UDP oraz z wykorzystaniem następujących mechanizmów: Wysyłanie logów / danych ze źródłowego systemu na wskazany port TCP/UDP serwera, będącego częścią wdrażanego rozwiązania (np. syslog); Rozwiązanie musi wspierać zbieranie danych w formacie CEF oraz przyjmowanie logów z Syslog Relay; Wskazanie w interfejsie użytkownika wdrażanego rozwiązania Systemu na znajdujący się lokalnie plik / katalog. Wykonywanie zapytań SQL w zewnętrznych bazach danych i pobieranie wyników zapytań. Alternatywnie musi istnieć możliwość komunikacji z bazami danych w standardzie JDBC lub ODBC; Windows Management Infrastructure (WMI). |  |  |  |
| 29.  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. |  |  |  |
| 30.  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; |  |  |  |
| 31.  System musi posiadać interfejs programowania aplikacji (API) w postaci bibliotek programistycznych dla języków: Java, Python, JavaScript, PHP, Ruby oraz C#; |  |  |  |
| 32.  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; |  |  |  |
| 33.  System musi posiadać udokumentowany interfejs REST (Representational State Transfer) umożliwiający integrację z zewnętrznymi systemami teleinformatycznymi; |  |  |  |
| 34.  Mechanizm przechowywania logów/danych/zdarzeń Systemu musi uniemożliwiać nieupoważnione usunięcie całości lub części logów, danych, raportów i innych informacji oraz zapewniać dostęp do nich tylko dla uprawnionych, uwierzytelnionych użytkowników; |  |  |  |
| 35.  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; |  |  |  |
| 36.  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); |  |  |  |
| 37.  System musi umożliwiać skalowalność poziomą poprzez dodawanie kolejnych węzłów klastra w celu spełnienia wymagań dot. wydajności lub dostępności. |  |  |  |
| 38.  Rozwiązanie musi wspierać mechanizm planowanego przenoszenia danych na pamięci masowe niższego poziomu na podstawie czasu lub okresu. |  |  |  |
| 39.  System musi pozwalać na podłączenie dodatkowej przestrzeni dyskowej CIFS/NFS w celu przechowywania danych archiwalnych. Dane archiwalne powinny być dostępne w systemie w ten sam sposób jak dane dostępne on-line. |  |  |  |
| 40.  Licencja Systemu nie może ograniczać liczby elementów gromadzących oraz analizujących logi; |  |  |  |
| 41.  Musi istnieć możliwość określenia szczegółowości zbieranych danych w zakresie wybranych protokołów, określonych pól protokołów (np. http\_user\_agent) oraz opcjonalnie agregacji danych;  |  |  |  |
| 42.  System musi zapewnić nieprzerwaną kontynuację pracy w przypadku awarii jednego z centrum przetwarzania danych lub dowolnego elementu infrastruktury tego Systemu; |  |  |  |
| 43.  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; |  |  |  |
| 44.  Tabele i wykresy prezentowane na bazie dostarczonych logów/danych muszą posiadać funkcję drill-down, tzn. po zaznaczeniu danej pozycji w tabeli lub wykresie interfejs musi pokazywać odpowiadające im logi/dane; |  |  |  |
| 45.  Musi istnieć możliwość definiowania akcji typu drill down powiązanych z różnymi typami zdarzeń oraz pól. Dostępne akcje muszą 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; |  |  |  |
| 46.  System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie, w jakiej ten log został przesłany do Systemu; |  |  |  |
| 47.  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;  |  |  |  |
| 48.  System musi 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; |  |  |  |
| 49.  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.; |  |  |  |
| 50.  Mechanizm pobierania logów/danych ze źródeł, musi 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; |  |  |  |
| 51.  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; |  |  |  |
| 52.  System musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu (np. dodanie nowych pól, zmianę znaczenia lub nazwy istniejących itp.); |  |  |  |
| 53.  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; |  |  |  |
| 54.  System musi umożliwiać obsługę logów w formacje CSV bez konieczności tworzenie parserów. Nazwy pól muszą być wierszem nagłówkowym CSV. Musi istnieć możliwość obsługi różnych delimiterów (przecinek, kropka, średnik, tabulator itp.) oraz wartości pól w cudzysłowach; |  |  |  |
| 55.  System musi umożliwiać automatyczną normalizację logów zawierających w treści pary zmienna i wartość, np. „user=jkowalski” musi tworzyć pole „user” o wartości „jkowalski”; |  |  |  |
| 56.  System musi umożliwiać obsługę logów w formacie CEF, JSON i CSV |  |  |  |
| 57.  Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zwarte w zewnętrznych repozytoriach: |  |  |  |
| a.       Katalogi LDAP, |  |  |  |
| b.      Bazy danych,  |  |  |  |
| c.       Bazy noSQL |  |  |  |
| d.      Dane geolokalizacyjne. |  |  |  |
| 58.  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. |  |  |  |
| 59.  System musi umożliwiać rozwiązywanie adresów IP do nazw hostów i na odwrót;  |  |  |  |
| 60.  System musi umożliwiać wydajną pracę użytkownika przeglądającego zdarzenia i generującego raporty oraz samego Systemu, w szczególność parsowania danych, których wielkość dochodzi do 60/70/101 GB dziennie; |  |  |  |
| 61.  System musi umożliwiać parsowanie logów o długości co najmniej 10000 znaków oraz zawierających więcej niż jedna linię; |  |  |  |
| 62.  System musi umożliwiać tworzenie bazy definicji formatów logów; |  |  |  |
| 63.  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.); |  |  |  |
| 64.  System musi automatycznie proponować definicje pól, dla poszczególnego typu logów wykorzystywanych do dalszej analizy oraz tworzyć statystyki występowania poszczególnych wartości tych pól; |  |  |  |
| 65.  System musi wyszukiwać czas zdarzenia (timestamp) z analizowanego logu i wykorzystywać go do reguł korelacyjnych; |  |  |  |
| 66.  System musi umożliwiać definiowanie pól za pomocą wyrażeń regularnych (REGEX); |  |  |  |
| 67.  System musi umożliwiać w czasie rzeczywistym wyszukiwanie zdarzeń w logach/danych o zadanych wartościach pól, w oparciu o wyrażenia regularne (REGEX); |  |  |  |
| 68.  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); |  |  |  |
| 69.  System musi umożliwiać tworzenie alertów/powiadomień po wykryciu zdarzenia wynikającego z korelacji danych, wykonanych przez regułę korelacyjną; |  |  |  |
| 70.  System musi umożliwiać tworzenie reguł korelacyjnych na bazie parsowanych logów/danych z różnych źródeł; |  |  |  |
| 71.  System musi umożliwiać tworzenie reguł korelacyjnych przy użyciu zarówno narzędzi graficznych GUI, jak języka zapytań charakterystycznego dla danej Systemu; Zamawiający nie dopuszcza Systemy, w którym do tworzenia reguł korelacyjnych przy użyciu dodatkowych narzędzi firm trzecich |  |  |  |
| 72.  Wynikiem działania reguły korelacyjnej powinno być utworzenie alarmu lub zwiększenie współczynnika ryzyka związanego z obiektem uczestniczącym w zdarzeniu (użytkownik, host, port itp.). |  |  |  |
| 73.  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; |  |  |  |
| 74.  Musi istnieć możliwość zastosowania bez modyfikacji reguł korelacyjnych dla danych historycznych, w celu wykrycia podobnych zdarzeń w przeszłości; |  |  |  |
| 75.  System 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); |  |  |  |
| 76.  W 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; |  |  |  |
| 77.  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.  |  |  |  |
| 78.  System musi zapewnić rozliczność działań użytkowników, w szczególności rejestrowanie dostępu do przetwarzanych logów/danych; |  |  |  |
| 79.  System musi umożliwiać jednoczesną pracę analityczną co najmniej dla 20 użytkowników; |  |  |  |
| 80.  Licencja Systemu musi umożliwiać utworzenie kont i pracę dla co najmniej 20 użytkowników; |  |  |  |
| 81.  System musi umożliwiać odseparowanie środowiska pracy użytkowników o różnych rolach; |  |  |  |
| 82.  System musi być odporny na ataki sieciowe; |  |  |  |
| 83.  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; |  |  |  |
| 84.  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. |  |  |  |

…………….……., dnia …………. r.

*……………………………….*

*Imię i nazwisko*

*/podpisano elektronicznie/*

***Załącznik nr 4 do SWZ***

**Zamawiający:**

………………………………………………………………………………

*(pełna nazwa/firma, adres)*

**Wykonawca:**

………………………………………………………………………………

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

………………………………………………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**Oświadczenia wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia**

**DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z ART. 5K ROZPORZĄDZENIA 833/2014 ORAZ ART. 7 UST. 1 USTAWY o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego**

**składane na podstawie art. 125 ust. 1 ustawy Pzp**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **zakup odnowienia licencji oprogramowania SIEM - usługa serwisu, wsparcia technicznego i konsultacyjna, nr postępowania 29/23/PN**,prowadzonego przez Narodowe Centrum Badań i Rozwojuoświadczam, co następuje:

**OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:**

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 5k rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1), dalej: rozporządzenie 833/2014, w brzmieniu nadanym rozporządzeniem Rady (UE) 2022/576 w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 111 z 8.4.2022, str. 1), dalej: rozporządzenie 2022/576.[[10]](#footnote-10)
2. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (t. j.: Dz. U. z 2023 poz. 129, 185)*.*[[11]](#footnote-11)

**INFORMACJA DOTYCZĄCA POLEGANIA NA ZDOLNOŚCIACH LUB SYTUACJI PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY W ZAKRESIE ODPOWIADAJĄCYM PONAD 10% WARTOŚCI ZAMÓWIENIA:**

[UWAGA*: wypełnić tylko w przypadku podmiotu udostępniającego zasoby, na którego zdolnościach lub sytuacji wykonawca polega w zakresie odpowiadającym ponad 10% wartości zamówienia. W przypadku więcej niż jednego podmiotu udostępniającego zasoby, na którego zdolnościach lub sytuacji wykonawca polega w zakresie odpowiadającym ponad 10% wartości zamówienia, należy zastosować tyle razy, ile jest to konieczne.*]

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego **w Rozdziale VI pkt 2 ppkt 4 SWZ***,* polegam na zdolnościach lub sytuacji następującego podmiotu udostępniającego zasoby: ………………………………………………………………………...…………………………………….… *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*,
w następującym zakresie: …………………………………………………………………………… *(określić odpowiedni zakres udostępnianych zasobów dla wskazanego podmiotu)*, co odpowiada ponad 10% wartości przedmiotowego zamówienia.

**OŚWIADCZENIE DOTYCZĄCE PODWYKONAWCY, NA KTÓREGO PRZYPADA PONAD 10% WARTOŚCI ZAMÓWIENIA:**

[UWAGA*: wypełnić tylko w przypadku podwykonawcy (niebędącego podmiotem udostępniającym zasoby), na którego przypada ponad 10% wartości zamówienia. W przypadku więcej niż jednego podwykonawcy, na którego zdolnościach lub sytuacji wykonawca nie polega, a na którego przypada ponad 10% wartości zamówienia, należy zastosować tyle razy, ile jest to konieczne.*]

Oświadczam, że w stosunku do następującego podmiotu, będącego podwykonawcą, na którego przypada ponad 10% wartości zamówienia: ……………………………………………………………………………………………….………..….…… *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*,
nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia przewidziane w  art.  5k rozporządzenia 833/2014 w brzmieniu nadanym rozporządzeniem 2022/576.

**OŚWIADCZENIE DOTYCZĄCE DOSTAWCY, NA KTÓREGO PRZYPADA PONAD 10% WARTOŚCI ZAMÓWIENIA:**

[UWAGA*: wypełnić tylko w przypadku dostawcy, na którego przypada ponad 10% wartości zamówienia. W przypadku więcej niż jednego dostawcy, na którego przypada ponad 10% wartości zamówienia, należy zastosować tyle razy, ile jest to konieczne.*]

Oświadczam, że w stosunku do następującego podmiotu, będącego dostawcą, na którego przypada ponad 10% wartości zamówienia: ……………………………………………………………………………………………….………..….…… *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*,
nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia przewidziane w art. 5k rozporządzenia 833/2014 w brzmieniu nadanym rozporządzeniem 2022/576.

**OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

**INFORMACJA DOTYCZĄCA DOSTĘPU DO PODMIOTOWYCH ŚRODKÓW DOWODOWYCH:**

Wskazuję następujące podmiotowe środki dowodowe, które można uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, oraz dane umożliwiające dostęp do tych środków:

1) ......................................................................................................................................................

*(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)*

2) .......................................................................................................................................................

*(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)*

 …………………………………….

  *Data;* *kwalifikowany podpis elektroniczny*

***Załącznik nr 5 do SWZ***

**Zamawiający**

………………………………………………………………

*(pełna nazwa/firma, adres)*

**Podmiot udostępniający zasoby:**

………………………………………………………………

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

………………………………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**Oświadczenia podmiotu udostępniającego zasoby**

**DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z ART. 5K ROZPORZĄDZENIA 833/2014 ORAZ ART. 7 UST. 1 USTAWY o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego**

**składane na podstawie art. 125 ust. 5 ustawy Pzp**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Zakup odnowienia licencji oprogramowania SIEM - usługa serwisu, wsparcia technicznego i konsultacyjna, nr postępowania 29/23/PN**,prowadzonego przez Narodowe Centrum Badań i Rozwoju*,* oświadczam, co następuje:

**OŚWIADCZENIA DOTYCZĄCE PODMIOTU UDOSTEPNIAJĄCEGO ZASOBY:**

1. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 5k rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1), dalej: rozporządzenie 833/2014, w brzmieniu nadanym rozporządzeniem Rady (UE) 2022/576 w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 111 z 8.4.2022, str. 1), dalej: rozporządzenie 2022/576.[[12]](#footnote-12)
2. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego* (t. j.: Dz. U. z 2023 poz. 129, 185)*.*[[13]](#footnote-13)

**OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

**INFORMACJA DOTYCZĄCA DOSTĘPU DO PODMIOTOWYCH ŚRODKÓW DOWODOWYCH:**

Wskazuję następujące podmiotowe środki dowodowe, które można uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, oraz dane umożliwiające dostęp do tych środków:

1) ......................................................................................................................................................

*(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)*

2) .......................................................................................................................................................

*(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji)*

 …………………………………….

  *Data; kwalifikowany podpis elektroniczny*

1. niepotrzebne skreślić [↑](#footnote-ref-1)
2. W przypadku oferty na produkt równoważny [↑](#footnote-ref-2)
3. W przypadku oferty na produkt równoważny [↑](#footnote-ref-3)
4. W przypadku oferty na produkt równoważny [↑](#footnote-ref-4)
5. W przypadku oferty na produkt równoważny [↑](#footnote-ref-5)
6. W przypadku oferty na produkt równoważny [↑](#footnote-ref-6)
7. 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). [↑](#footnote-ref-7)
8. 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 Wykonawca nie składa oświadczenia (usunięcie treści oświadczenia następuje np. przez jego wykreślenie). [↑](#footnote-ref-8)
9. publicznie i powszechnie dostępnej na stronach internetowych producenta oprogramowania [↑](#footnote-ref-9)
10. Zgodnie z treścią art. 5k ust. 1 rozporządzenia 833/2014 w brzmieniu nadanym rozporządzeniem 2022/576 zakazuje się udzielania lub dalszego wykonywania wszelkich zamówień publicznych lub koncesji objętych zakresem dyrektyw w sprawie zamówień publicznych, a także zakresem art. 10 ust. 1, 3, ust. 6 lit. a)–e), ust. 8, 9 i 10, art. 11, 12, 13 i 14 dyrektywy 2014/23/UE, art. 7 i 8, art. 10 lit. b)–f) i lit. h)–j) dyrektywy 2014/24/UE, art. 18, art. 21 lit. b)–e) i lit. g)–i), art. 29 i 30 dyrektywy 2014/25/UE oraz art. 13 lit. a)–d), lit. f)–h) i lit. j) dyrektywy 2009/81/WE na rzecz lub z udziałem:

obywateli rosyjskich lub osób fizycznych lub prawnych, podmiotów lub organów z siedzibą w Rosji;

osób prawnych, podmiotów lub organów, do których prawa własności bezpośrednio lub pośrednio w ponad 50 % należą do podmiotu, o którym mowa w lit. a) niniejszego ustępu; lub

osób fizycznych lub prawnych, podmiotów lub organów działających w imieniu lub pod kierunkiem podmiotu, o którym mowa w lit. a) lub b) niniejszego ustępu,

w tym podwykonawców, dostawców lub podmiotów, na których zdolności polega się w rozumieniu dyrektyw w sprawie zamówień publicznych, w przypadku gdy przypada na nich ponad 10 % wartości zamówienia. [↑](#footnote-ref-10)
11. Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego,* z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:

1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655 ze zm.) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy. [↑](#footnote-ref-11)
12. Zgodnie z treścią art. 5k ust. 1 rozporządzenia 833/2014 w brzmieniu nadanym rozporządzeniem 2022/576 zakazuje się udzielania lub dalszego wykonywania wszelkich zamówień publicznych lub koncesji objętych zakresem dyrektyw w sprawie zamówień publicznych, a także zakresem art. 10 ust. 1, 3, ust. 6 lit. a)–e), ust. 8, 9 i 10, art. 11, 12, 13 i 14 dyrektywy 2014/23/UE, art. 7 i 8, art. 10 lit. b)–f) i lit. h)–j) dyrektywy 2014/24/UE, art. 18, art. 21 lit. b)–e) i lit. g)–i), art. 29 i 30 dyrektywy 2014/25/UE oraz art. 13 lit. a)–d), lit. f)–h) i lit. j) dyrektywy 2009/81/WE na rzecz lub z udziałem:

obywateli rosyjskich lub osób fizycznych lub prawnych, podmiotów lub organów z siedzibą w Rosji;

osób prawnych, podmiotów lub organów, do których prawa własności bezpośrednio lub pośrednio w ponad 50 % należą do podmiotu, o którym mowa w lit. a) niniejszego ustępu; lub

osób fizycznych lub prawnych, podmiotów lub organów działających w imieniu lub pod kierunkiem podmiotu, o którym mowa w lit. a) lub b) niniejszego ustępu,

w tym podwykonawców, dostawców lub podmiotów, na których zdolności polega się w rozumieniu dyrektyw w sprawie zamówień publicznych, w przypadku gdy przypada na nich ponad 10 % wartości zamówienia. [↑](#footnote-ref-12)
13. Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. *o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego,* z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:

1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655 ze zm.) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy. [↑](#footnote-ref-13)