Ministerstwo Nauki
i Szkolnictwa Wyższego

Biuro Dyrektora Generalnego

Sprawa: BDG-WII.072.3.2024

Warszawa, dnia 23 kwietnia 2024 r.

Wykonawcy

ZAPYTANIE W CELU OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo Nauki i Szkolnictwa Wyższego (MNiSW), ul. Wspólna 1/3, 00-529 Warszawa (NIP 7011181865, REGON 527332079) zwraca się z prośbą o przedstawienie propozycji cenowej dla przedmiotu zamówienia pn. **Zakup systemu klasy SIEM**, opisanego w *Załączniku nr 1 do zapytania*.

Oszacowanie wartości zamówienia należy przedstawić w *Formularzu wyceny*, stanowiącym *Załącznik nr 2 do zapytania* oraz przesłać **do dnia 8 maja 2024 r.** na adres ofertyIT@nauka.gov.pl.

Ewentualne pytania/uwagi, mające wpływ na przedmiotową wycenę, proszę kierować na powyższy adres.

Niniejsze zapytanie ma na celu rozeznanie rynku oraz uzyskanie wiedzy na temat kosztów związanych z planowanym zamówieniem publicznym. Zapytanie nie stanowi oferty w myśl art. 66 Kodeksu cywilnego, jak również nie jest ogłoszeniem w rozumieniu ustawy Prawo zamówień publicznych.

Załączniki:

1) Opis zamówienia;
2) Formularz wyceny;
3) Klauzula informacyjna.

Łukasz Teterycz
Zastępca Dyrektora
/ – podpisano cyfrowo/

tel. (22) 52 92 725
sekretariat.bdg@mnisw.gov.pl
www.mnisw.gov.pl

ul. Wspólna 1/3
00-529 Warszawa

OPIS ZAMÓWIENIA

Zakup systemu klasy SIEM

Lp.	Wymaganie
1.	**Wymagana licencja wieczysta z 60-miesięcznym okresem wsparcia producenta + utrzymanie Wykonawcy przez 12 miesięcy.**
2.	Wszystkie opisane poniżej wymagania muszą być dostarczone jako wbudowana funkcjonalność produktu lub jako dodatkowe moduły oficjalnie dostarczane przez producenta w repozytorium aplikacji, a nie jako funkcjonalność dodana w ramach dodatkowych prac konfiguracyjnych i integracyjnych
3.	System musi być dostarczony w konfiguracji wysokodostępnej (cluster HA)
4.	System musi zbierać dane z przynajmniej następujących źródeł: Microsoft Windows Server 2016/2019/2022, Windows 10/Windows 11, Microsoft Exchange, Symantec Messaging Gateway, Vmware vSphere, Vmware Horizon, Fortinet Authenticator, KEMP, Checkpoint Firewall, Checkpoint Endpoint Security, Linux, Unix, ESET Mail Protect.
5.	System musi umożliwiać pobieranie logów z innych systemów za pomocą wielu metod. Minimalny wymagany zakres to: Syslog, CEF, LEEF, SNMP, Kafka, JDBC, flat file, OPSEC/LEA,
6.	System musi umożliwiać analizowanie logów wielolinijkowych
7.	System musi udostępniać mechanizmy pozwalające na integracje urządzeń i źródeł nie znajdujących się w powyższej liście, z wykorzystaniem graficznego kreatora reguł parsowania.
8.	Graficzny kreator reguł parsowania musi obsługiwać co najmniej formaty: JSON, CEF, LEEF, lista, lista par "klucz-wartość", XML.
9.	Graficzny kreator reguł parsowania musi umożliwiać tworzenie reguł z wykorzystaniem wyrażeń regularnych.
10.	Graficzny kreator reguł parsowania musi mieć możliwość podpowiadania użytkownikowi wzorca wyrażenia regularnego dla wskazanego łańcucha w payloadzie.
11.	Mechanizmy integracji źródeł, zarówno tych wskazanych przy wdrożeniu, jak i integrowanych w przyszłości przez Zamawiającego, nie mogą być w żaden sposób ograniczane licencyjnie przez producenta ani wymagać dodatkowych opłat ze strony Zamawiającego.
12.	System musi umożliwiać zmianę sposobu normalizacji danych w trakcie używania systemu i pozwalać na równoległe używanie różnych sposobów normalizacji logów.
13.	System musi posiadać możliwość automatycznego rozpoznawania źródeł logów, które są przekierowane do SIEM (zakładając, że posiada parser dla technologii tego źródła danych). Musi automatycznie rozpoznać typ logu i dobrać odpowiedni parser, tak aby nie była wymagana żadna aktywność ze strony administratora systemu.
14.	System musi umożliwiać pobieranie i analizę przepływów co najmniej w formatach: Netflow w wersji 1, 5, 7 i 9, IPFIX, sFLow w wersji 2, 4 i 5, J-Flow i Packeteer.
15.	System musi posiadać możliwość zainstalowania natywnego komponentu generującego dane o przepływach na podstawie analizy ruchu sieciowego.
16.	System musi mieć możliwość przeprowadzenia bezagentowej akwizycji danych. W uzasadnionych przypadkach dopuszczamy stosowanie agentów. W przypadku stosowania agentów, system nie może ograniczać licencyjnie ilości wykorzystywanych agentów.

17.	Zbierane informacje muszą być poddane w systemie korelacji, na podstawie których administratorzy systemu będą informowani o stanie bezpieczeństwa infrastruktury Zamawiającego oraz ostrzegani o ewentualnych incydentach bezpieczeństwa.
18.	System musi zawierać bazę co najmniej 100 predefiniowanych reguł korelacyjnych, których wykorzystanie przez Zamawiającego nie wymaga ponoszenia dodatkowych nakładów z tym związanych.
19.	System musi umożliwiać budowanie reguł korelacyjnych bazujących na zdarzeniach, przepływach, jednocześnie zdarzeniach i przepływach, a także na innych korelacjach.
20.	System umożliwia wykorzystanie reguł korelacyjnych jako bloków do wykorzystania w nadrzędnych regułach korelacyjnych.
21.	System, oprócz prezentowania informacji o alertach w tablicach, musi posiadać możliwość powiadamiania o zdarzeniach co najmniej przez: powiadomienie ekranowe, e-mail, syslog, SNMP, wywołanie skryptu.
22.	System musi umożliwiać zastosowanie w regułach korelacyjnych testów logicznych na wartościach pól bazy danych zdarzeń i przepływów.
23.	System musi umożliwiać zastosowanie w regułach języka zapytań bazy danych zdarzeń i przepływów.
24.	System musi umożliwiać zastosowanie w regułach testów zawartości payloadu zdarzenia.
25.	Rozwiązanie musi posiadać wbudowane mechanizmy śledzące wydajność reguł korelacyjnych.
26.	System musi umożliwiać oznaczanie reguł taktykami i technikami frameworku MITTRE ATT&CK.
27.	System nie może wykorzystywać bazy danych ogólnego zastosowania do przechowywania zdarzeń i przepływów.
28.	Baza danych musi umożliwiać wydawanie poleceń w języku zapytań bazy danych.
29.	Ze względu na zachowanie integralności danych, język bazy danych zdarzeń i przepływów może pozwalać na wykonanie jedynie polecenia SELECT. Baza danych nie może pozwalać na wykonywanie poleceń UPDATE, INSERT i DELETE.
30.	Dane pochodzące z logów zapisywane są w domyślnie dostępnych polach bazy danych przynajmniej takich jak: nazwa zdarzenia, kategoria zdarzenia, adres IP źródłowy, źródłowy port TCP/IP, adres IP źródłowy przed translacją, adres IP źródłowy po translacji, czas urządzenia, z którego wysłany był log, nazwa protokołu, nazwa użytkownika, nazwa hosta, nazwa grupy, nazwa NetBIOS (o ile zawartość tych pól jest zawarta w logu).
31.	Dane pochodzące z przepływów sieciowych muszą zostać domyślnie zapisane w dostępnych polach bazy danych przynajmniej takich jak: adres IP źródłowy, port źródłowy, adres IP docelowy, port docelowy, ilość wysłanych/odebranych.
32.	System musi umożliwiać dodanie własnych pól w bazie, które można przywoływać jako kryteria wyszukiwania, określane przy pomocy nowych wzorców.
33.	System musi przechowywać w bazie danych również payloady zdarzeń i przepływów.
34.	System musi umożliwiać wskazanie które pola mają być zapisywane w bazie danych bezpośrednio po otrzymaniu zdarzenia, a które nie. W tym drugim przypadku wartość pola jest każdorazowo wyznaczana z payloadu na podstawie reguł parsera w momencie użycia tego pola (np. przy wyświetleniu lub wykonaniu testu logicznego na polu).
35.	System musi umożliwić zapisanie wzorca wyszukiwania, a także związanych z nim szablonów prezentacji oraz wyników w celu późniejszego przywołania lub też udostępnienia wyszukiwania innym użytkownikom.
36.	System musi umożliwiać umieszczenie zapisanego wzorca w ramach utworzonej grupy wzorców, na tablicach (dashboard) oraz w miejscu umożliwiającym szybki dostęp.

37.	System musi być w stanie przyjąć i przetworzyć minimum 8000 zdarzeń na sekundę (EPS) i być gotowym na przyjęcie chwilowych gwałtownych przyrostów ilości zdarzeń bez ich utraty.
38.	System musi być w stanie przyjąć i przetworzyć minimum 200 000 przepływów sieciowych na minutę (FPM) i być gotowym na przyjęcie chwilowych gwałtownych przyrostów zdarzeń bez ich utraty.
39.	System musi być w stanie monitorować środowisko 120 serwerów, 700 stacji roboczych i 150 urządzeń sieciowych.
40.	System musi mieć możliwość budowania profilu stanu i zachowania środowiska IT oraz identyfikowania odchyleń i wykrywania anomalii na podstawie analizy behawioralnej.
41.	System musi mieć możliwość wykrywania anomalii na podstawie odchyłki wartości w ostatnim okresie od wartości w okresie historycznym.
42.	System musi mieć możliwość wykrywania anomalii na podstawie przekroczenia wartości progowej.
43.	System musi mieć możliwość wykrywania anomalii na podstawie odchyłki wartości od zarejestrowanego trendu.
44.	System musi umożliwiać tworzenie szablonów raportów.
45.	Wymagane formaty raportów: co najmniej PDF, HTML, XML, XLS, CSV.
46.	System musi mieć możliwość generowania raportów zgodnie z ustalonym harmonogramem czasowym.
47.	System musi mieć możliwość wysyłania mailem raportów na wskazane adresy.
48.	System musi mieć możliwość weryfikowania tożsamości użytkowników poprzez wykorzystanie kont lokalnych oraz zewnętrzne systemy uwierzytelnienia – MS Active Directory oraz RADIUS i LDAP.
49.	System musi zawierać funkcjonalność precyzyjnego nadawania uprawnień użytkownikom i administratorom.
50.	System musi posiadać zaimplementowane mechanizmy automatycznej kontroli własnego stanu oraz alarmowania w przypadku wykrytych nieprawidłowości.
51.	System musi posiadać zaimplementowany dedykowany dashboard prezentujący dokładne statystyki związane z wydajnością systemu, co najmniej utylizacja CPU, utylizacja pamięci RAM, heap usage, disk IO throughtput, disk IOPS, statystyki połączeń sieciowych, ilość wykonywanych zapytań, statystyki dotyczące wywołań API itp.
52.	System musi zapewniać centralne gromadzenie wszystkich logów i zapewniać ich bezpieczne przechowywanie oraz dostępność przez okres 30 dni.
53.	System musi samodzielnie zarządzać retencją danych.
54.	System musi umożliwiać wyspecyfikowanie różnego czasu retencji danych dla różnych zdarzeń i przepływów - na podstawie zawartości pól bazy danych.
55.	System musi posiadać mechanizm automatycznego archiwizowania danych i konfiguracji systemu do katalogu w lokalnym systemie plików i określenia retencji dla przechowywanych w ten sposób danych.
56.	System musi posiadać mechanizm wyszukiwania danych w zarchiwizowanych logach.
57.	System musi umożliwiać włączenie lub wyłączenie indeksacji pola bazy danych z interfejsu graficznego.
58.	Zdarzenia i przepływy muszą być przechowywane w postaci skompresowanej.
59.	System musi zapewniać możliwość obsługi poprzez przeglądarkę.

60.	System musi udostępniać możliwość prezentacji statystyk i wyników działania w postaci tablic (dashboard), których wygląd i rozkład poszczególnych składowych daje się dostosować do potrzeb administratora i użytkownika. Widoczność stworzonych i domyślnie dostępnych tablic można przełączać przy pomocy łatwo dostępnej listy rozwijanych pozycji.
61.	Informacje prezentowane w poszczególnych tablicach są wynikiem stworzonych przez producenta predefiniowanych korelacji, a także wyników wyszukiwania stworzonych przez użytkownika lub udostępnionych mu przez innych użytkowników i administratorów.
62.	System nie może wymagać instalacji dedykowanego oprogramowania klienckiego do jego obsługi.
63.	System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtrów tworzonych przy pomocy pól wyboru.
64.	System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtru wyspecyfikowanego w języku bazy danych.
65.	System musi umożliwiać prezentację zdarzeń i przepływów na podstawie filtru specyfikującego słowo występujące w payloadzie.
66.	System musi mieć możliwość tworzenia clustra wysokodostępnego dla każdego z komponentów (za wyjątkiem agenta instalowanego na innym serwerze/stacji oraz analizatora ruchu sieciowego). Awaria pojedynczego komponentu nie może spowodować utraty funkcjonalności i wydajności systemu.
67.	System musi posiadać architekturę skalowalną horyzontalnie poprzez dodawanie serwerów przechowujących część rozproszonej bazy danych i przetwarzających zdarzenia.
68.	Każda z reguł korelacyjnych musi mieć możliwość korelowania zdarzeń i przepływów z wszystkich serwerów przetwarzających dane, bądź z jednego serwera - zależnie od decyzji projektanta reguły.
69.	System musi umożliwiać prezentację zdarzeń i przepływów w postaci tabelarycznej, z możliwością wyboru okresu lub w czasie rzeczywistym.
70.	System musi posiadać dashboard prezentujący mapę, na której w czasie rzeczywistym są prezentowane incydenty lub dowolnie zdefiniowane zdarzenia.
71.	System musi umożliwiać automatyczne łączenie wielu incydentów w jeden.
72.	System musi posiadać aplikację monitorującą charakterystykę zachowań użytkowników (user behavior analysis), która pozwala na ocenę ryzykownych czynności podejmowanych przez wewnętrznych użytkowników na infrastrukturze.
73.	Aplikacja analizująca zachowania użytkowników musi przypisywać użytkownikom tzw. punkty ryzyka i generować alarm po przekroczeniu wartości progowej sumarycznych punktów ryzyka. Wartość progowa może być ustalana statycznie (bezwzględna wartość liczbowa) lub dynamicznie (na podstawie rozkładu wartości punktów ryzyka dla całej populacji użytkowników).
74.	Aplikacja musi wyświetlać kształtowanie się poziomu ryzyka dla użytkownika w czasie.
75.	System analizy zachowań użytkowników musi mieć możliwość wykorzystania uczenia maszynowego.
76.	Wbudowane modele uczenia maszynowego mają analizować trendy zachowań w czasie oraz porównywać zachowanie użytkownika z grupą innych użytkowników o podobnych parametrach charakteryzujących danego użytkownika - przykładowo ulokowanie w konkretnym kontenerze Active Directory lub posiadających konkretny atrybut (np. nazwa stanowiska).
77.	Użytkownik musi mieć możliwość tworzenia własnych modeli uczenia maszynowego analizujących trendy zmian wartości w czasie.
78.	W przypadku braku zdefiniowanych grup użytkowników, system sam wykonuje grupowanie użytkowników na podstawie podobnych wzorców zachowań.

79.	System ma możliwość wyspecyfikowania grup użytkowników, dla których punkty ryzyka są modyfikowane o wyspecyfikowany mnożnik.
80.	System musi umożliwić automatyczną geolokalizację źródła zagrożeń.
81.	System musi mieć możliwość tworzenia szczegółowego logu audytowego zawierającego informacje przynajmniej o logowaniu do systemu i zmianach w jego konfiguracji.
82.	Licencja systemu SIEM oraz system SIEM nie mogą ograniczać liczby równocześnie zalogowanych użytkowników.
83.	System musi posiadać możliwość automatycznego wykrywania nowych elementów infrastruktury poprzez analizę zdarzeń i/lub ruchu sieciowego. SIEM musi wykryć pojawienie się nowego adresu IP, adresu MAC i opcjonalnie zgłosić to operatorowi.
84.	System musi posiadać możliwość automatycznego grupowania elementów infrastruktury poprzez ich cechy charakterystyczne. Przykładowo, system SIEM powinien być w stanie dokonać klasyfikacji elementów posiadających otwarte porty charakterystyczne dla baz danych jako "serwery bazodanowe".
85.	System musi umożliwiać tworzenie własnego schematu opisu i oznaczania (tzw. tagowania) assetów.
86.	System musi umożliwiać filtrowanie assetów w oparciu o dowolne pole charakteryzujące dany element infastruktury.
87.	System musi zapewniać automatyczny mechanizm aplikacji poprawek do systemu.
88.	System musi umożliwiać utworzenie struktury adresacji IP używanej w poszczególnych miejscach sieci i w ten sposób określić adresacje obce. Ta struktura używana jest następnie do określenia kierunków rejestrowanych zdarzeń komunikacji i przepływów.
89.	System musi umożliwić konfigurację serwera poczty, przez który wysyłane są wiadomości pocztowe. Musi być możliwość konfiguracji innych serwerów poczty dla różnych serwerów przetwarzających zdarzenia i przepływy.
90.	System pozwala na integrację z systemami zarządzania podatnościami w celu uzupełnienia informacji o zasobach o bardziej szczegółowe dane.
91.	System pozwala na integrację z co najmniej tymi systemami zarządzania podatnościami: eEye, BigFix, Juniper NSM, Qualys, Rapid7, Tenable.
92.	System musi posiadać własną bazę reputacji IP.
93.	System musi posiadać możliwość przeprowadzenia korelacji historycznej, czyli symulacji działania reguły dla zdarzeń historycznych.
94.	System musi posiadać udokumentowany interfejs API.
95.	System musi posiadać narzędzie graficzne umożliwiające testowanie różnych zapytań API i weryfikację otrzymywanych danych.
96.	System musi umożliwiać rozdzielenie plików bazy danych na wiele "domen", z możliwością tworzenia oddzielnych reguł korelacyjnych dla domen.
97.	Licencja nie może ograniczać wielkości przetwarzanych danych w bajtach.
98.	System musi umożliwiać obfuskację (ukrywanie) danych wrażliwych zdarzeń i przepływów przed operatorem.
99.	System musi umożliwiać kontrolę integralności bazy danych przez zastosowanie hashowania.
100.	Producent systemu musi udostępniać zestawy dodatkowych reguł, ponad podstawowy zbiór reguł dostępny w produkcie po instalacji.
101.	System musi tworzyć indeks słów znajdujących się w payloadzie, w celu szybszego wyszukiwania zdarzeń.

102.	System musi umożliwiać detekcję nadużycia protokołu DNS typu: DGA, squatting, tunelowanie.
103.	System musi umożliwiać tworzenie aplikacji osadzanych w interfejsie graficznym systemu.
104.	System musi mieć możliwość uniemożliwienia użytkownikom wykonywanie zapytań, które mogą trwać zbyt długo lub wyszukiwani, które będą zwracały dużą ilość danych co może mieć negatywny wpływ na wydajność systemu. Takie polityki muszą mieć możliwość definiowania na poziomie użytkownika, roli lub tenantów.
105.	System oprócz podstawowego interfejsu przeglądania danych z funkcjonalnością administracyjną musi mieć dodatkowo odseparowany interfejs przeznaczony do pracy dla operatorów SOC. Interfejs ten musi być pozbawiony funkcjonalności administracyjnych i powinien w pełni być skoncentrowany na analizie incydentów bezpieczeństwa.
106.	System musi zawierać funkcjonalność wsparcia przy tuningu reguł. System powinien raportować reguły, które najczęściej inicjują incydenty bezpieczeństwa oraz reguły, które są najmniej efektywne.
107.	System musi automatycznie informować o nowych dodatkowych funkcjonalnościach dostępnych do ściągnięcia z dedykowanego repozytorium aplikacji.
108.	System musi zawierać dedykowany dashboard, który prezentuje przydatne artykuły, wiadomości, przypadki użycia, podcasty oraz odnośniki do szkoleń. Zawartość musi być dostosowana automatycznie do charakterystyki obsługiwanej infrastruktury.
109.	System musi umożliwiać wykorzystanie tzw. zapytań federacyjnych do różnych niezależnych instancji systemów SIEM w oparciu o format STIX.
110.	System musi umożliwiać prostą integrację z systemem klasy SOAR bez konieczności prowadzenia prac integracyjnych - przykładowo za pomocą gotowej aplikacji.
111.	Dodanie do systemu kolejnego komponentu analizującego/przechowującego zdarzenia/przepływy nie może wymagać dokupienia dodatkowej licencji.
112.	Utworzenie clustra HA komponentu poprzez dodanie serwera zapasowego nie może wymagać dokupienia dodatkowej licencji.
113.	System musi znajdować się w "ćwiartce liderów" w najnowszym opracowaniu tzw. magicznego kwadratu systemów SIEM wg. Gartnera.
114.	Zwiększenie strumienia EPS (zdarzeń na sekundę) monitorowanego przez SIEM nie może wymagać dokupienia dodatkowej licencji.
115.	Zwiększenie strumienia FPM (przepływów na minutę) monitorowanego przez SIEM nie może wymagać dokupienia dodatkowej licencji.
Wdrożenie:	
116.	Wdrożenie musi być realizowane przez producenta zaoferowanego systemu.
117.	Weryfikacja wymagań klienta (dokument wstępnej koncepcji wdrożenia).
118.	Opracowanie architektury logicznej i fizycznej komponentów SIEM (log i flow, kolektory, log i flow procesory, konsola).
119.	Specyfikacja i określenie wielkości maszyn wirtualnych na których będą zainstalowane komponenty SIEM.
120.	Źródła logów.
121.	Reguły korelacji – min. 200 reguł korelacyjnych

Szkolenie nr 1	
122.	5-dniowe szkolnie, realizowane przez producenta zaoferowanego rozwiązania bądź poprzez autoryzowane centrum kompetencyjne, z zarządzania dostarczonym rozwiązaniem SIEM dla 4 administratorów. W ramach szkolenia wymagane jest omówienie minimum poniższych zagadnień:
123.	Tworzenie własnego parsera
124.	Tworzenie reguł korelacyjnych
125.	Instalacja i konfiguracja aplikacji User Behaviour Analytics
126.	Tworzenie własnego interfejsu dashboardów
127.	Analiza przepływów sieciowych
128.	Szkolenie musi być przeprowadzone w j. polskim z jednym posiłkiem ciepłym i dwoma przerwami na kawę
Szkolenie nr 2	
129.	5-dniowe szkolnie, realizowane przez producenta zaoferowanego rozwiązania bądź poprzez autoryzowane centrum kompetencyjne, z zaawansowanego zarządzania dostarczonym rozwiązaniem SIEM dla 4 administratorów. W ramach szkolenia wymagane jest omówienie minimum poniższych zagadnień:
130.	Program szkolenia uzgodniony zostanie po 6-miesięcznym użytkowaniu systemu.
131.	Szkolenie musi być przeprowadzone w j. polskim, z jednym posiłkiem ciepłym i dwoma przerwami na kawę

Załącznik nr 2 do zapytania o wycenę

FORMULARZ WYCENY

Wykonawca …… *(pełna nazwa albo imię i nazwisko, siedziba/miejsce zamieszkania i adres jeżeli jest miejscem wykonywania działalności Wykonawcy)*	
NIP/REGON	……
Osoba do kontaktów z Zamawiającym	……
telefon	……
e-mail	……

Ministerstwo Nauki i Szkolnictwa Wyższego
ul. Wspólna 1/3
00-529 Warszawa

WYCENA NA PODSTAWIE OPISU PRZEDMIOTU ZAMÓWIENIA PRZEDSTAWIONEGO W ZAPYTANIU DOTYCZĄCYM OSZACOWANIA WARTOŚCI ZAMÓWIENIA (Sprawa: BDG-WII.072.3.2024)

Lp.	*Przedmiot zamówienia*	*Wartość netto PLN*	*Podatek VAT*	*Wartość brutto PLN*
1	*2*	*3*	*4*	*5 (kol. 3 + kol. 4)*
1	**Zakup systemu klasy SIEM - wymagana licencja wieczysta**	……	……%	……
2	**Wsparcie producenta na zakupiony System przez okres 60 miesięcy**	……	……%	……
3	**Utrzymanie Systemu przez Wykonawcę przez 12 miesięcy**	……	……%	……
4	**Szkolenie nr 1**	……	……%	……
5	**Szkolenie nr 2**	……	……%	……
	RAZEM CENA OPFERTY	……		……
Wartość brutto (słownie złotych) ……				

Cena brutto obejmuje wszystkie koszty i składniki związane z wykonaniem zamówienia opisanym przez Zamawiającego w zapytaniu o wycenę.

Załączniki *(jeśli dotyczy)*

……

data …… ……

podpis osoby/osób uprawnionej/uprawnionych do reprezentowania Wykonawcy

Informacja dla Wykonawcy
Formularz wyceny musi być podpisany przez osobę lub osoby uprawnione do reprezentowania Wykonawcy podpisem własnoręcznym – wówczas wycena składana jest w formie skanu, lub podpisem w formie elektronicznej (kwalifikowany podpis elektroniczny).

Klauzula informacyjna dot. przetwarzania danych osobowych przez Zamawiającego

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia 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 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2), dalej „RODO", informuję, że:

1) administratorem Pani/Pana danych osobowych jest Ministerstwo Nauki i Szkolnictwa Wyższego;
2) dane kontaktowe do inspektora ochrony danych w Ministerstwie Nauki i Szkolnictwa Wyższego: Ministerstwo Nauki i Szkolnictwa Wyższego, ul. Wspólna 1/3, 00-529 Warszawa, adres e-mail: inspektor@mnisw.gov.pl;
3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przeprowadzeniem postępowania o udzielenie zamówienia publicznego jak również zawarcia umowy w sprawie zamówienia oraz jej realizacji, a także udokumentowania postępowania o udzielenie zamówienia i jego archiwizacji;
4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym dokumentacja postępowania zostanie udostępniona /osoby lub podmioty zapewniające obsługę informatyczną Ministerstwa Nauki i Szkolnictwa Wyższego / wszystkie osoby, które zapoznają się z informacjami zamieszczonymi na stronie internetowej MNiSW;
5) Pani/Pana dane osobowe będą przechowywane do czasu ustania celu jakim jest przeprowadzenie postępowania o udzielenie zamówienia, zawarcie i wykonanie umowy, a następnie, jeśli chodzi o materiały archiwalne, zgodnie z Instrukcją Kancelaryjną Ministerstwa Nauki i Szkolnictwa Wyższego oraz przepisami o archiwizacji dokumentów – przez okres co najmniej 5 lat od dnia przekazania ich do archiwum Ministerstwa Nauki i Szkolnictwa Wyższego;
6) obowiązek podania przez Panią/Pana danych osobowych jest wymogiem związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego;
7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
8) posiada Pani/Pan:
   - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących,
   - na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia Pani/Pana danych osobowych,
   - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych,
   - prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.