Znak sprawy: SzP.ZP.271.46.23

Zapytanie ofertowe dotyczące zamówienia publicznego
o wartości poniżej kwoty 130.000,00 zł na

ZAKUP I WDROŻENIE SYSTEMU TYPU SIEM W CELU ZWIĘKSZENIA CYBERBEZPIECZEŃSTWA ORAZ WYKONANIE AUDYTU BEZPIECZEŃSTWA W SZPITALU SPECJALISTYCZNYM IM. EDMUNDA BIERNACKIEGO W MIELCU

Zamówienie jest finansowane ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 działań w celu podniesienia poziomu bezpieczeństwa teleinformatycznego u świadczeniodawców

Podstawa prawna: Zarządzenie nr 118/2022 Dyrektora Szpitala Specjalistycznego im. Edmunda Biernackiego w Mielcu z dnia 22 lipca 2022 r. w sprawie przyjęcia regulaminu udzielania zamówień publicznych o wartości poniżej kwoty 130.000,00 zł

ZAMAWIAJĄCY:

Nazwa i adres:

Szpital Specjalistyczny im. Edmunda Biernackiego
ul. Żeromskiego 22
39-300 Mielec

tel/fax (17)780-01-46

e-mail: przetargi@szpital.mielec.pl

NIP: 817-175-08-93, REGON: 000308637

Szpital Specjalistyczny im. Edmunda Biernackiego w Mielcu zaprasza do złożenia oferty cenowej na poniżej opisany przedmiot zamówienia:

Zakup i wdrożenie systemu typu SIEM w celu zwiększenia cyberbezpieczeństwa oraz wykonanie audytu bezpieczeństwa w Szpitalu Specjalistycznym im. Edmunda Biernackiego w Mielcu

1. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA:

Przedmiotem zamówienia jest zakup i wdrożenie systemu typu SIEM (Security Information and Event Management) w celu zwiększenia cyberbezpieczeństwa oraz wykonanie audytu bezpieczeństwa w Szpitalu Specjalistycznym im. Edmunda Biernackiego w Mielcu

I. WYMAGANIA FUNKCJONALNE:

Lp.	Parametr	Wymagane
1.	Dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), do którego głównych funkcji należą gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł, agregację i wzbogacanie danych. Korelacja odbywa się na podstawie zdefiniowanych reguł określających te zależności.	TAK
2.	Zamawiający na potrzeby wdrożenia udostępni infrastrukturę w postaci serwerów wirtualnych według specyfikacji uzgodnionych z wykonawcą.	TAK
3.	Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na zakupiony System.	TAK
4.	System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows Server, Redhat/Oracle, Linux.	TAK (podać)
5.	W ramach zamówienia dostawca zapewnia licencje na wymagany system operacyjny.	TAK
6.	Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.	TAK
7.	Interfejs użytkownika Systemu musi być w języku polskim lub angielskim opcjonalnie możliwość wgrania plików językowych tłumaczących interfejs na język polski.	TAK

8.	System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.	TAK
9.	Rozwiązanie musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20 GB danych dziennie.	TAK (podać)
10.	System musi być tak wyskalowany, aby zapewniać możliwość obsługi co najmniej 100 aktualnych źródeł danych znajdujących się w sieci.	TAK (podać)
11.	System musi zapewniać retencję danych w okresie minimum 365 dni.	TAK (podać)
12.	System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu.	TAK
13.	Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.	TAK
14.	Autoryzacja do systemu musi być zintegrowana co najmniej z usługą katalogową Microsoft AD (Active Directory).	TAK
15.	System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.	TAK
16.	System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.	TAK
17.	System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.	TAK
18.	System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.	TAK
19.	Komunikacja pomiędzy poszczególnymi elementami Systemu, jak i komunikacja administratora do poszczególnych elementów musi być szyfrowana.	TAK
20.	System musi zapewniać normalizację (parsowanie) spływających do niego wiadomości w formatach: Syslog, WEF, Flat file, XML, JSON, JDBC/ODBC, Email, jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.	TAK
21.	System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.	TAK
22.	System może do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.	TAK
23.	System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.	TAK

24.	Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.	TAK
25.	System musi posiadać predefiniowany zestaw parserów zdarzeń.	TAK
26.	Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.	TAK
27.	System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.	TAK
28.	System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.	TAK
29.	Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS).	TAK
30.	System musi umożliwić korelację zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi w przepływach sieciowych oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności.	TAK
31.	System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.	TAK
32.	System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.	TAK
33.	System musi umożliwiać wykorzystanie baz reputacyjnych w regułach korelacyjnych.	TAK
34.	System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook.	TAK
35.	System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.	TAK
36.	System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.	TAK
37.	W systemie musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.	TAK
38.	System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.	TAK
39.	Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.	TAK
40.	System musi generować raporty do formatów co najmniej PDF.	TAK

41.	System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu.	TAK
42.	Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.	TAK
43.	System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym: • Wykrycia dowolnej treści w logach, • Wykrycia wystąpienia wartości pola na wybranej liście, • Wykrycia niewystępowania wartości pola na wybranej liście, • Wykrycia zmiany jednego z kilku pól, • Wykrycia zdarzeń występujących z zadaną częstotliwością, • Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego, • Wykrycia zaniku Wiadomości, • Wykrycia nowej wartości pola w zadanym okresie czasu, • Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności . System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów	TAK
44.	Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.	TAK
45.	Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.	TAK
46.	System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.	TAK (podać)
47.	System musi umożliwiać integrację z Mitre ATT@CK.	TAK
48.	System musi posiadać bazę minimum 100 predefiniowanych reguł korelacyjnych.	TAK (podać)
49.	System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.	TAK
50.	System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.	TAK
51.	System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.	TAK
52.	System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów.	TAK
53.	System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows.	TAK

54.	System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP.	TAK

II. WDROŻENIE SYSTEMU:

1. Wykonawca, w terminie **maksymalnie 14 dni** od zawarcia umowy, będzie odpowiedzialny za dostarczenie, instalację i konfigurację oraz optymalizację środowiska Systemu w infrastrukturze Zamawiającego.
2. Po wdrożeniu systemu wykonawca w ramach zamówienia przeprowadzi audyt bezpieczeństwa zgodnie z wymaganiami opisanymi w załączniku nr 2 do Zarządzenia nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców.
3. Wykonawca przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji (tj. szczegółową dokumentację powdrożeniową oraz instrukcję/instrukcje obsługi).
4. Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w n/w zakresie:
   a) Przedstawienie architektury Systemu
   b) Omówienie procedur obsługi administracyjnej Systemu
   c) Omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń Systemu
   d) Przekazanie informacji na temat konfiguracji i zarządzania Systemem
   e) Instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną
5. Zasady realizacji instruktażu stanowiskowego:
   a) dla minimum 6 osób wskazanych przez Zamawiającego
   b) łączny wymiar instruktażu stanowiskowego: nie mniejszy niż 1 dzień, możliwość przeprowadzenia szkolenia w formie zdalnej.
   c) instruktaż stanowiskowy będzie realizowany minimum w oparciu o zakres wykonywanych prac wdrożeniowych Systemu,
   d) Osoby prowadzące instruktaż stanowiskowy muszą posiadać wiedzę oraz odpowiednie przygotowanie merytoryczne w zakresie wdrażanego Systemu, a także brać bezpośredni udział we wdrożeniu.
6. W ramach realizacji instruktażu stanowiskowego Wykonawca zapewni uczestnikom materiały dydaktyczne w języku polskim (w formie elektronicznej), co najmniej:
   a) podręcznik administratora i użytkownika w formie elektronicznej,
   b) opis możliwych do zastosowania rozwiązań: przypadków omawianych w czasie prowadzenia instruktażu oraz najczęściej występujących przypadków przy eksploatacji systemu.

III. INNE WARUNKI REALIZACJI ZAMÓWIENIA I GWARANCJA:

Lp.	Parametr	Wymagane
1.	Wykonawca udziela **gwarancji** na wykonane przez Wykonawcę w ramach umowy prace, przez okres **36 miesięcy** od dnia podpisania bez zastrzeżeń protokołu odbioru tych prac.	TAK (podać)
2.	Dostarczone rozwiązanie musi być objęte **min. 36 miesięcznym wsparciem**. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania oraz reagowanie na zgłaszane błędy systemowe. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego).	TAK (podać)

IV. Wykonując obowiązki określone w trybie art. 28 ogólnego Rozporządzenia Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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) zwanego „RODO", w przypadku umów których wykonanie związane jest z koniecznością powierzenie i przetwarzania danych osobowych gromadzonych przez Zamawiającego, strony zawrą porozumienie powierzenia przetwarzania danych osobowych. Obowiązkiem Wykonawcy jest wykazanie zdolności do przetwarzania danych zgodnie z art. 28.Wzór umowy powierzenia przetwarzania danych oraz arkusz weryfikacyjny i inne wymagania w zakresie ochronnych danych osobowych są opublikowane na stronie internetowej Zamawiającego www.szpital.mielec.pl.

V. Przedstawiona oferta nie może stanowić zbiorczych cenników, lecz winna zostać sporządzona wyłącznie z ukierunkowaniem na prowadzone postępowanie i odpowiadać wymaganiom Zamawiającego określonym w niniejszym Zapytaniu.

2. TERMIN I MIEJSCE REALIZACJI ZAMÓWIENIA:

2.1 Termin realizacji zamówienia obejmuje okres: **14 dni od daty zawarcia umowy**
2.2 Miejsce realizacji zamówienia: Szpital Specjalistycznego im. Edmunda Biernackiego w Mielcu, ul. Żeromskiego 22, 39-300 Mielec.

3. OPIS WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ DOKUMENTY WYMAGANE W OFERCIE:

3.1. Warunki udziału w postępowaniu:
Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie Wykonawca zobowiązany jest wykazać w sposób szczególny.

3.2. Wykonawca powinien przedstawić następujące oświadczenia i dokumenty:
a) Wypełniony formularz oferty zgodnie z załączonym do Zapytania wzorem (zaleca się złożyć ofertę na załączonym wzorze - Załącznik nr 1 do Zapytania),
b) Zaakceptowany wzór umowy – Załącznik nr 2 do Zapytania
c) W celu wykazania braku podstaw do wykluczenia z postępowania:
   – Odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru, chyba że Zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych a Wykonawca np. w Formularzu ofertowym wskazał dane umożliwiające dostęp do tych dokumentów w odniesieniu do Wykonawcy jak również w odniesieniu do podmiotów udostępniających zasoby.
d) W celu potwierdzenia, że oferowane dostawy odpowiadają wymaganiom Zamawiającego:
   – Oświadczenie, że oferowany asortyment jest zgodny z opisem przedmiotu zamówienia i posiada dokumenty wymagane przez obowiązujące prawo dla tego typu asortymentu (Załącznik nr 3 do Zapytania).

4. OPIS SPOSOBU PRZYGOTOWANIA OFERTY:

4.1. Ofertę należy sporządzić w postaci elektronicznej zgodnie z Formularzem ofertowym stanowiącym Załącznik nr 1 do Zapytania ofertowego.

4.2. Oferta oraz wszystkie załączniki muszą być sporządzone w języku polskim, podpisane przez osobę upoważnioną do reprezentowania Wykonawcy, zgodnie z wpisem w stosownym dokumencie uprawniającym do występowania w obrocie prawnym. **Dokumenty składa się pod rygorem nieważności w formie elektronicznej (tj. opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.**

4.3. Jeżeli uprawnienie do podpisania oferty nie wynika z właściwego rejestru lub centralnej ewidencji i informacji o działalności gospodarczej do oferty winno być dołączone stosowne pełnomocnictwo. Pełnomocnictwo winno być dołączone w oryginale lub kopii potwierdzonej za zgodność z oryginałem notarialnie.

4.4. Do oferty Wykonawca winien załączyć wszystkie wymagane dokumenty i oświadczenia.

4.5. W przypadku gdy Wykonawca jako załącznik do oferty, dołącza kopię jakiegoś dokumentu, kopia ta powinna być potwierdzona „za zgodność z oryginałem".

4.6. Każdy Wykonawca może złożyć tylko jedną ofertę.

4.7. Zamawiający nie dopuszcza możliwości składania ofert częściowych.

4.8. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

4.9. Oferty złożone po terminie nie będą rozpatrywane.

5. KOMUNIKACJA W POSTĘPOWANIU:

5.1. Komunikacja w postępowaniu o udzielenie zamówienia, w tym składanie ofert, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń między Zamawiającym a Wykonawcą, odbywa się przy użyciu środków komunikacji elektronicznej – poczta elektroniczna.

5.2. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści Zapytania Ofertowego na adres: **przetargi@szpital.mielec.pl**.

5.3. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem że wniosek o wyjaśnienie treści Zapytania Ofertowego wpłynie do Zamawiającego nie później niż na 4 dni przed upływem wyznaczonego terminu składania ofert. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści Zapytania Ofertowego.

5.4. Zawiadomienia, oświadczenia, dokumenty, wnioski lub informacje Wykonawcy przekazują drogą elektroniczną na adres: **przetargi@szpital.mielec.pl.**

5.5. Maksymalny rozmiar plików przesyłanych za pośrednictwem poczty elektronicznej wynosi 50 MB.

6. CENA OFERTY:

6.1. Wykonawca w przedstawionej ofercie winien zaoferować cenę kompletną, jednoznaczną i ostateczną.
Cena oferty – jest to wartość wyrażona w jednostkach pieniężnych, którą Zamawiający jest obowiązany zapłacić Wykonawcy za realizację przedmiotu zamówienia.

6.2. Cena powinna być skalkulowana w sposób jednoznaczny i powinna uwzględniać wszystkie koszty związane z realizacją zamówienia, m.in.:

a) sprzedaż i dostawę transportem własnym, na swój koszt i ryzyko przedmiotu zamówienia do siedziby Zamawiającego,
b) wniesienie towaru i jego rozładunek w miejscu wskazanym przez pracownika upoważnionego przez Zamawiającego
c) dostarczenie, instalację i konfigurację oraz optymalizację środowiska Systemu w infrastrukturze Zamawiającego
d) instruktaż stanowiskowy
e) licencje
f) gwarancje, wsparcie techniczne
g) audyt bezpieczeństwa po wdrożeniu systemu
h) marże, rabaty – jeżeli Wykonawca stosuje upusty cenowe
i) ubezpieczenie
j) podatek VAT (jeśli dotyczy)
k) cło (jeśli dotyczy),
l) podatek akcyzowy (jeśli dotyczy)

oraz wszystkie inne koszty nie wymienione wyżej, niezbędne do realizacji przedmiotu zamówienia.

6.3. Cena oferty to **iloczyn ceny jednostkowej towaru i ilości** asortymentu wskazanego w Zapytaniu powiększona o wartość VAT.
Cena jednostkowa towaru – jest to cena ustalona za jednostkę określonego towaru, którego ilość jest określona w jednostkach miar.

6.4. Cena oferty winna być wyrażona w walucie polskiej, z dokładnością do dwóch miejsc po przecinku. Zamawiający nie wyraża zgody na rozliczenia w walutach obcych.

6.5. Jeżeli zostanie złożona oferta, której wybór będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami.
Wykonawca, składając ofertę, poinformuje Zamawiającego, czy wybór oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego, wskazuje nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego, wskazuje wartość towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku, wskazuje stawkę podatku od towarów i usług, która z zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

7. KRYTERIA OCENY OFERT:

7.1. Zamawiający dokona oceny ważnych ofert na podstawie następujących kryteriów:

- **najniższa cena - 100 %**

7.2. Sposób oceny ofert:

kryterium „najniższa cena" jako kryterium wymierne obliczane zostanie wg wzoru:

$$Wpc = \frac{Cn}{Cof} \; x \; Rc$$

gdzie:

Wpc *– Wartość punktowa badanej oferty w kryterium „najniższa cena"*
Cn *– najniższa oferowana cena brutto spośród ofert, które zostały złożone*
Cof *– cena brutto oferty badanej*
Rc – *ranga kryterium „najniższa cena" (100)*

W kryterium „najniższa cena" Wykonawca może otrzymać maksymalnie 100 punktów.

8. MIEJSCE I TERMIN SKŁADANIA OFERT:

8.1. Ofertę sporządza się w postaci elektronicznej, w ogólnie dostępnych formatach danych w szczególności w formatach .pdf, .doc, .docx, .odt, .txt, .rtf. **Przesyłany plik należy spakować do formatu zip z ustawionym hasłem**.

Spakowany plik oraz hasło do niego składa się na adres:

oferty@szpital.mielec.pl

wiadomość należy oznakować napisem:

„Postępowanie, znak SzP.ZP.271.46.23"

8.2. W przypadku przesłania pliku bez hasła Wykonawca ponosi odpowiedzialność za ujawnienie treści oferty przed terminem otwarcia ofert i nie będzie z tego tytułu wnosił roszczeń względem Zamawiającego.

8.3. Nieprzekraczalny termin złożenia oferty **30.06.2023r.** godz. **9^{00}.**

8.4. O terminie wpływu decyduje termin ostatecznego wpływu oferty na adres: **oferty@szpital.mielec.pl.**

8.5. Złożone oferty zostaną otwarte w dniu **30.06.2023 r.** o godz. **10^{00}** w siedzibie Zamawiającego.

8.6. Wykonawca może wprowadzić zmiany lub wycofać złożoną przez siebie ofertę pod warunkiem, że Zamawiający otrzyma powiadomienie przed upływem terminu składania ofert. Powiadomienie musi być złożone według takich samych zasad jak składana oferta z dopiskiem: „ZMIANA / WYCOFANIE".

8.7. Wykonawca składający ofertę pozostaje nią związany przez okres **30 dni**. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

8.8. W toku badania i oceny ofert Zamawiający może wezwać Wykonawcę do złożenia wyjaśnień lub uzupełnień złożonej oferty.

9. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI UMOWY:

9.1. Z wyłonionym Wykonawcą zostanie zawarta pisemna umowa.

9.2. Wzór umowy zawierający wszystkie wymagane przez Zamawiającego warunki załączony jest do Zapytania ofertowego (Załącznik nr 2 do Zapytania ofertowego).

10. OGŁOSZENIE WYNIKÓW POSTĘPOWANIA:

Zamawiający jednocześnie poinformuje wszystkich Wykonawców o:

a) wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania i adres, jeżeli jest miejscem wykonywania działalności Wykonawcy, którego ofertę wybrano oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania i adresy, jeżeli są miejscami wykonywania działalności Wykonawców, którzy złożyli oferty, a także punktację przyznaną oferentom w każdym kryterium oceny ofert i łączną punktację,
b) Wykonawcach, których oferty zostały odrzucone,
c) unieważnieniu postępowania.

oraz zamieści informację na stronie internetowej Zamawiającego.

11. INFORMACJE DODATKOWE:

11.1. Zamawiający unieważni postępowanie o udzielenie zamówienia publicznego w przypadku, gdy:

a) nie złożono żadnej oferty spełniającej wymagania Zamawiającego,
b) cena najkorzystniejszej oferty przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia, chyba że Zamawiający może zwiększyć kwotę do ceny najkorzystniejszej oferty,
c) wystąpiła zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie Zamawiającego, czego nie można było wcześniej przewidzieć.

11.2. W przypadku, gdy Wykonawca odstąpi od podpisania umowy, Zamawiający może podpisać umowę z kolejnym Wykonawcą, który w toku prowadzonego badania ofert otrzymał najwyższą liczbę punktów.

12. OSOBY UPOWAŻNIONE DO KONTAKTU Z WYKONAWCAMI:

- Grzegorz Krupa - w sprawach merytorycznych
- Małgorzata Hajduga, Arkadiusz Brach - w sprawach formalno-prawnych

13. KLAUZULA INFORMACYJNA Z ART. 13 RODO:

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), zwane dalej „RODO", Zamawiający informuje, iż:

a) Administratorem Pani/Pana danych osobowych jest Szpital Specjalistyczny im. Edmunda Biernackiego z siedzibą przy ul. Żeromskiego 22, 39-300 Mielec. Dane kontaktowe:
   - poczta elektroniczna: sekretariat@szpital.mielec.pl
   - telefon: 17 780-01-39
b) Administrator wyznaczył Inspektora Danych Osobowych, z którym można się kontaktować pod adresem e-mail

iod@szpital.mielec.pl

c) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego na zakup i wdrożenie systemu typu SIEM w celu zwiększenia cyberbezpieczeństwa oraz wykonanie audytu bezpieczeństwa w Szpitalu Specjalistycznym im. Edmunda Biernackiego w Mielcu, znak SzP.ZP.271.46.23 prowadzonym w trybie postepowania o wartości poniżej kwoty 130.000,00 zł (Zarządzenie nr 118/2022 Dyrektora Szpitala Specjalistycznego im. E. Biernackiego w Mielcu z dnia 22.07.2022r. w sprawie przyjęcia regulaminu udzielania zamówień publicznych o wartości poniżej kwoty 130.000,00 zł).

d) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania na podstawie Ustawy z dnia 6 września 2001r. o dostępie do informacji publicznej (t.j. Dz.U. z 2020r. poz. 2176),

e) Pani/Pana dane osobowe będą przechowywane przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

f) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego;

g) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;

h) posiada Pani/Pan:
   - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych *(skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy oraz nie może naruszać integralności protokołu oraz jego załączników)*;
   - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem okresu trwania postępowania o udzielenie zamówienia publicznego oraz przypadków, o których mowa w art. 18 ust. 2 RODO *(prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego*;
   - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

i) nie przysługuje Pani/Panu:
   - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

j) przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez Administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

14. ZAŁĄCZNIKI DO ZAPYTANIA OFERTOWEGO:

Załącznik nr 1 - Formularz ofertowy

Załącznik nr 2 - Projekt umowy

Załącznik nr 3 – Oświadczenie, że oferowany asortyment jest zgodny z opisem przedmiotu zamówienia i posiada dokumenty wymagane przez obowiązujące prawo dla tego typu asortymentu

……
Podpis Dyrektora szpitala lub osoby upoważnionej

Załącznik nr 1 do Zapytania ofertowego

....., dnia .....
(miejscowość)

(pieczęć firmowa Wykonawcy)

FORMULARZ OFERTY

Dane Wykonawcy: .....

Adres (siedziba) Wykonawcy: .....

Tel. ..... E-mail……..

NIP: ..... REGON: ..... .

Nawiązując do zapytania ofertowego na:

Zakup i wdrożenie systemu typu SIEM w celu zwiększenia cyberbezpieczeństwa oraz wykonanie audytu bezpieczeństwa w Szpitalu Specjalistycznym im. Edmunda Biernackiego w Mielcu, znak SzP.ZP.271.46.23

oferujemy realizację w/w Przedmiotu Zamówienia:

I. Cena oferty:

L.p. Asortyment	Nazwa handlowa, wymiar jedn. wielkość opakowania (jeżeli dotyczy)	Numer katalogowy	Producent	J.m.	Ilość	Cena jednostkowa			Wartość		
						netto	VAT %	brutto	netto (kol. 5x6)	VAT zł	brutto (kol. 9+10)
1	2	3		4	5	6	7	8	9	10	11
Całkowita wartość zamówienia									suma kolumna 9	suma kolumna 10	suma kolumna 11

WYMAGANIA FUNKCJONALNE

Lp.	**Parametr**	**Parametr wymagany**	**Parametr oferowany**
1.	Dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), do którego głównych funkcji należą gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł, agregację i wzbogacanie danych. Korelacja odbywa się na podstawie zdefiniowanych reguł określających te zależności.	TAK	

2.	Zamawiający na potrzeby wdrożenia udostępni infrastrukturę w postaci serwerów wirtualnych według specyfikacji uzgodnionych z wykonawcą.	TAK	
3.	Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na zakupiony System.	TAK	
4.	System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows Server, Redhat/Oracle, Linux.	TAK (podać)	
5.	W ramach zamówienia dostawca zapewnia licencje na wymagany system operacyjny.	TAK	
6.	Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.	TAK	
7.	Interfejs użytkownika Systemu musi być w języku polskim lub angielskim opcjonalnie możliwość wgrania plików językowych tłumaczących interfejs na język polski.	TAK	
8.	System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.	TAK	
9.	Rozwiązanie musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20 GB danych dziennie.	TAK (podać)	
10.	System musi być tak wyskalowany, aby zapewniać możliwość obsługi co najmniej 100 aktualnych źródeł danych znajdujących się w sieci.	TAK (podać)	
11.	System musi zapewniać retencję danych w okresie minimum 365 dni.	TAK (podać)	
12.	System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu.	TAK	
13.	Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.	TAK	
14.	Autoryzacja do systemu musi być zintegrowana co najmniej z usługą katalogową Microsoft AD (Active Directory).	TAK	
15.	System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.	TAK	
16.	System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.	TAK	
17.	System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych	TAK	

	obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.		
18.	System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.	TAK	
19.	Komunikacja pomiędzy poszczególnymi elementami Systemu, jak i komunikacja administratora do poszczególnych elementów musi być szyfrowana.	TAK	
20.	System musi zapewniać normalizację (parsowanie) spływających do niego wiadomości w formatach: Syslog, WEF, Flat file, XML, JSON, JDBC/ODBC, Email, jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.	TAK	
21.	System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.	TAK	
22.	System może do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.	TAK	
23.	System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.	TAK	
24.	Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.	TAK	
25.	System musi posiadać predefiniowany zestaw parserów zdarzeń.	TAK	
26.	Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.	TAK	
27.	System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.	TAK	
28.	System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.	TAK	
29.	Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS).	TAK	

30.	System musi umożliwić korelację zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi w przepływach sieciowych oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności.	TAK	
31.	System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.	TAK	
32.	System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.	TAK	
33.	System musi umożliwiać wykorzystanie baz reputacyjnych w regułach korelacyjnych.	TAK	
34.	System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook.	TAK	
35.	System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.	TAK	
36.	System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.	TAK	
37.	W systemie musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.	TAK	
38.	System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.	TAK	
39.	Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.	TAK	
40.	System musi generować raporty do formatów co najmniej PDF.	TAK	
41.	System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu.	TAK	
42.	Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.	TAK	
43.	System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym: • Wykrycia dowolnej treści w logach, • Wykrycia wystąpienia wartości pola na wybranej liście, • Wykrycia niewystępowania wartości pola na wybranej liście, • Wykrycia zmiany jednego z kilku pól,	TAK	

	• Wykrycia zdarzeń występujących z zadaną częstotliwością, • Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego, • Wykrycia zaniku Wiadomości, • Wykrycia nowej wartości pola w zadanym okresie czasu, • Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności . System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów		
44.	Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.	TAK	
45.	Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.	TAK	
46.	System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.	TAK (podać)	
47.	System musi umożliwiać integrację z Mitre ATT@CK.	TAK	
48.	System musi posiadać bazę minimum 100 predefiniowanych reguł korelacyjnych.	TAK (podać)	
49.	System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.	TAK	
50.	System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.	TAK	
51.	System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.	TAK	
52.	System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów.	TAK	
53.	System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows.	TAK	
54.	System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP.	TAK	

INNE WARUNKI REALIZACJI ZAMÓWIENIA I GWARANCJA:

Lp.	Parametr	Parametr wymagany	Parametr oferowany
1.	Wykonawca udziela **gwarancji** na wykonane przez Wykonawcę w ramach umowy prace, przez okres **36 miesięcy** od dnia podpisania bez zastrzeżeń protokołu odbioru tych prac.	TAK (podać)	
2.	Dostarczone rozwiązanie musi być objęte **min. 36 miesięcznym wsparciem**. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania oraz reagowanie na zgłaszane błędy systemowe. Przez błąd systemowy Zamawiający rozumie błędy krytyczne (zakłócenie uniemożliwiające działanie rozwiązania), błędy poważne (zakłócenie uniemożliwiające działanie części rozwiązania), błędy zwykłe (inne zakłócenia nie stanowiące błędu krytycznego lub poważnego).	TAK (podać)	

II. Oświadczamy, że:

* zapoznaliśmy się z Zapytaniem ofertowym i nie wnosimy zastrzeżeń,,
* wzór Umowy załączony do Zapytania (Załącznik nr 2) akceptujemy bez zastrzeżeń i zobowiązujemy się w przypadku wyboru naszej oferty do jej podpisania w miejscu i terminie wyznaczonym przez Zamawiającego,
* dostawy objęte przedmiotem zamówienia zrealizujemy w ciągu **14 dni od daty zawarcia umowy**,
* termin płatności za dostarczony przedmiot zamówienia wynosił będzie 60 dni od dnia doręczenia Zamawiającemu prawidłowo i zgodnie z umową wystawionej faktury, na rachunek bankowy Wykonawcy, prowadzony przez …… o numerze ……,
* wyszczególnione w złożonej ofercie ceny **pozostaną niezmienne przez okres trwania umowy**, z zastrzeżeniem przypadków wskazanych w umowie,
* uważamy się za związanych niniejszą ofertą przez okres **30 dni** od terminu składania ofert,
* zamówienie **zrealizujemy sami**/**zamierzamy powierzyć** wykonanie następujących części zamówienia (*niepotrzebne skreślić*) ……..…… **podwykonawcom** ……. (*o ile jest to wiadome, podać firmy podwykonawców*),
* wybór naszej oferty nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego na podstawie ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. U. z 2018, poz. 2174, z późn. zm.).
  Uwaga: jeżeli wybór oferty będzie prowadził na podstawie ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług do powstania u Zamawiającego obowiązku podatkowego Wykonawca zobowiązany jest dołączyć do oferty wykaz zawierający nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, ich wartość bez kwoty podatku oraz stawki podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy będzie miała zastosowanie.
* wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO (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)) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
  Uwaga: 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 (treść oświadczenia należy usunąć np. poprzez jego wykreślenie).

* 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 (Dz. U. 2022 poz. 835)

……..
(pieczątka i podpis Wykonawcy
lub jego uprawnionego przedstawiciela)

Data: ……

Załącznik nr 2 do Zapytania ofertowego

W Z Ó R U M O W Y

W dniu ..... pomiędzy **Szpitalem Specjalistycznym im. Edmunda Biernackiego w Mielcu**, **ul. Żeromskiego 22, 39-300 Mielec**, wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w Rzeszowie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000002538, REGON: 000308637, NIP: 8171750893, zwanym w dalszej części Umowy **„Zamawiającym”** reprezentowanym przez:

……

a ..... KRS ……NIP ..... REGON ..... zwanym w dalszej części Umowy **„Wykonawcą”** reprezentowanym przez:

……

……

stosownie do dokonanego przez Zamawiającego wyboru oferty Wykonawcy przeprowadzonego na podstawie *Zarządzenie nr 118/2022 Dyrektora Szpitala Specjalistycznego im. E. Biernackiego w Mielcu z dnia 22.07.2022r. w sprawie przyjęcia regulaminu udzielania zamówień publicznych o wartości poniżej kwoty 130.000,00 zł* udzielonego w trybie zapytania ofertowego dotyczące zamówienia publicznego o wartości poniżej 130.000,00 zł zostaje zawarta umowa następującej treści:

§ 1

1. Przedmiotem niniejszej umowy jest:
   a) sprzedaż, dostawa i wdrożenie systemu typu SIEM w celu zwiększenia cyberbezpieczeństwa - spełniającego wymagania określone w Zapytaniu ofertowym – na koszt i ryzyko Wykonawcy, o wymaganiach i parametrach określonych w Zapytaniu ofertowym, znak SzP.ZP.271.46.22 dalej: „Zapytanie”) oraz zgodnie z ofertą złożoną przez Wykonawcę z dnia ……
   b) zamontowanie, instalacja, podłączenie do istniejącej infrastruktury, konfiguracja, optymalizacja środowiska Systemu w infrastrukturze Zamawiającego, uruchomienie i oddanie przedmiotu zamówienia w stanie pełnej sprawności technicznej i użytkowej,
   c) dostawa i konfiguracja subskrypcji/licencji,
   d) przeszkolenie personelu Zamawiającego w zakresie obsługi oferowanego przedmiotu zamówienia, instruktaż stanowiskowy,
   e) przeprowadzenie audytu bezpieczeństwa po wdrożeniu systemu.
2. Przedmiot umowy dofinansowany jest ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 działań w celu podniesienia poziomu bezpieczeństwa teleinformatycznego u świadczeniodawców.
3. Zapytanie ofertowe i oferta złożona przez Wykonawcę stanowią integralną część niniejszej umowy.

§ 2

1. Wykonawca zobowiązany jest do wykonania obowiązków objętych przedmiotem umowy, o których mowa w § 1 ust.1 niniejszej umowy, transportem własnym, na swój koszt i ryzyko – do miejsca wskazanego przez Zamawiającego w terminie do **14 od dnia zawarcia umowy**.
2. Wykonawca dostarczy przedmiot zamówienia od poniedziałku do piątku w godzinach od 7:00 do 14:15, po uprzednim uzgodnieniu konkretnego terminu z Zamawiającym.
3. Dowodem dokonania czynności wymienionych w ust.1 jest protokół zdawczo-odbiorczy - formularz stanowiący Załącznik do niniejszej umowy, podpisany przez strony umowy.
4. Podpisany bezusterkowy protokół zdawczo-odbiorczy będzie stanowił podstawę do wypłaty należnego Wykonawcy wynagrodzenia.
5. W przypadku wykonania zamówienia w części dotyczącej transportu przy użyciu Podwykonawcy, Wykonawca odpowiada za działania, uchybienia i zaniedbania Podwykonawcy tak jak za własne działania, uchybienia i zaniedbania.
6. Zamawiający zastrzega sobie prawo zwrotu towaru niezgodnego z zamówieniem, niekompletnego lub posiadającego ślady zewnętrznego uszkodzenia z jednoczesnym wyznaczeniem nowego terminu ponownej dostawy.
7. Wykonawca zobowiązany jest do zachowania przy wykonywaniu niniejszej umowy należytej staranności,

z uwzględnieniem profesjonalnego charakteru swojej działalności.

§ 3

1. Strony uzgodniły wartość dostawy (netto) określoną w ofercie Wykonawcy na kwotę ..... (słownie: .....).
2. Wartość brutto zamówienia wynosi …… (słownie: ……).
3. Kwota, o której mowa w ust. 2 zaspokaja wszelkie roszczenia Wykonawcy wobec Zamawiającego z tytułu wykonania przedmiotu umowy i obejmuje wszelkie koszty związane z realizacją umowy, a w szczególności:
   a) sprzedaż i dostawę transportem własnym, na swój koszt i ryzyko przedmiotu zamówienia do siedziby Zamawiającego,
   b) wniesienie towaru i jego rozładunek w miejscu wskazanym przez pracownika upoważnionego przez Zamawiającego
   c) dostarczenie, instalację i konfigurację oraz optymalizację środowiska Systemu w infrastrukturze Zamawiającego
   d) instruktaż stanowiskowy
   e) licencje
   f) gwarancje, wsparcie techniczne
   g) audyt bezpieczeństwa po wdrożeniu systemu
   h) marże, rabaty – jeżeli Wykonawca stosuje upusty cenowe
   i) ubezpieczenie
   j) podatek VAT (jeśli dotyczy)
   k) cło (jeśli dotyczy),
   l) podatek akcyzowy (jeśli dotyczy)oraz wszystkie inne koszty nie wymienione wyżej, niezbędne do realizacji przedmiotu zamówienia.

§ 4

1. Wykonawca, po dostarczeniu, zamontowaniu, uruchomieniu i bezusterkowym przekazaniu protokołem zdawczo-odbiorczym przedmiotu umowy - wystawi fakturę VAT w języku polskim.
2. Zapłata za przedmiot umowy o którym mowa w § 1 płatna jest przelewem na rachunek bankowy Wykonawcy prowadzony przez …… o numerze …… w terminie 60 dni od dnia doręczenia Zamawiającemu prawidłowo i zgodnie z umową wystawionej faktury. W razie zmiany numeru rachunku bankowego, Wykonawca jest zobowiązany wskazać nowy rachunek bankowy. Wskazany numer rachunku/rachunków musi być zgłoszony do ewidencji tzw. „białej listy" tj. numerów rachunków rozliczeniowych, o których mowa w art. 49 ust. 1 pkt. 1 ustawy z dnia 29 sierpnia 1997r. - Prawo bankowe, lub imiennych rachunków w spółdzielczej kasie oszczędnościowo-kredytowej, której podmiot jest członkiem, otwartych w związku z prowadzoną przez członka działalnością gospodarczą – wskazanych w zgłoszeniu identyfikacyjnym lub zgłoszeniu aktualizacyjnym i potwierdzonych przy wykorzystaniu STIR w rozumieniu art. 119zg pkt 6 Ordynacji podatkowej.
3. Zamawiający oświadcza, że jest płatnikiem VAT uprawnionym do otrzymywania faktur VAT oraz, że posiada numer identyfikacyjny NIP 817-17-50-893.
4. Za termin dokonania zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.

§ 5

1. Wykonawca odpowiada za wady fizyczne dostarczonego przedmiotu zamówienia.
2. Przez wady fizyczne rozumie się w szczególności jakąkolwiek niezgodność dostarczonego przedmiotu zamówienia z opisem przedmiotu zamówienia zawartym w Zapytaniu ofertowym, oraz ze złożoną ofertą.
3. W razie stwierdzenia wad w dostarczonym asortymencie Zamawiający zobowiązuje się przesłać Wykonawcy pisemne zawiadomienie wraz z protokołem stwierdzającym wady.
4. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady prawne przedmiotu umowy (a także oprogramowania jeżeli dotyczy), w tym również za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej lub przemysłowej, w tym patentów, praw ochronnych na znaki towarowe oraz praw z rejestracji na wzory użytkowe i przemysłowe, pozostające w związku z wprowadzeniem do obrotu na terytorium Rzeczypospolitej Polskiej.
5. Zamawiający może wykonywać uprawnienia z tytułu rękojmi za wady przedmiotu umowy, niezależnie od uprawnień wynikających z gwarancji.

§ 6

1. Wykonawca na dostarczone ……. będące przedmiotem umowy udziela gwarancji na okres …… (przy czym okres gwarancji będzie się liczył od dnia zamontowania, uruchomienia i przekazania protokołem zdawczo-odbiorczym).

2. Okres gwarancji przerywany jest na okres dokonywania napraw gwarancyjnych przedmiotu umowy.
3. Wykonawca oświadcza, że:
    a. zobowiązuje się zapewnić w ramach przysługującego wynagrodzenia serwis gwarancyjny,
    b. zobowiązuje się zapewnić ……. -miesięczne wsparcie techniczne.
4. Wykonawca podejmie działania w celu usunięcia wady w czasie max. 48 godzin od chwili zgłoszenia (telefonicznie/mailem) awarii.
5. W przypadku wystąpienia wady w okresie gwarancji Wykonawca zobowiązuje się do jej usunięcia w terminie 3 dni roboczych od dnia zgłoszenia awarii.
6. Całość kosztów naprawy (w tym robocizna, części zamienne, podzespoły, dojazd serwisu, itp.) w okresie gwarancji ponosi Wykonawca.
7. Zamawiający może dochodzić roszczeń z tytułu gwarancji także po upływie terminu określonego w ust. 1 niniejszego paragrafu, o ile ujawnienie się wady nastąpiło przed upływem tego terminu.
8. Postanowienia ust. 4- 7 stosuje się odpowiednio do zgłoszenie wady na podstawie przepisów o rękojmi.

§ 7

1. Strony ustalają kary umowne mające zastosowanie w następujących przypadkach:
    a) za zwłokę w realizacji przedmiotu umowy Wykonawca zapłaci karę umowną w wysokości 0,1 % wartości brutto zamówienia za każdy dzień zwłoki ,
    b) z tytułu niedostarczenia przedmiotu umowy, odstąpienia od umowy lub jej wypowiedzenia z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10 % wartości brutto zamówienia,
    c) Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,2 % wartości brutto zamówienia za każdy dzień zwłoki liczony od upływu terminu określonego w § 6 ust. 5 umowy na usunięcie zgłoszonej wady w ramach udzielonej gwarancji.
2. Na Wykonawcy ciąży odpowiedzialność z tytułu uszkodzenia lub utraty przedmiotu umowy, aż do chwili potwierdzenia odbioru przez Zamawiającego. Z chwilą potwierdzenia odbioru przedmiotu umowy przechodzi na Zamawiającego ryzyko uszkodzenia lub utraty przedmiotu umowy.
3. Zamawiający zastrzega sobie możliwość potrącania kar umownych z wynagrodzenia przysługującego Wykonawcy po uprzednim wystawieniu noty obciążeniowej, na co Wykonawca wyraża zgodę.
4. Zamawiający zastrzega sobie możliwość dochodzenia odszkodowania przenoszącego wartość kar umownych ustalonych w niniejszej umowie ma zasadach ogólnych.
5. Wysokość kar umownych naliczonej z jednego lub kilku tytułów nie może przekroczyć 30% wartości brutto umowy określonej w § 3 ust. 1 umowy.
6. Zamawiający może odstąpić od umowy/wypowiedzieć umowę w przypadku nie zawarcia przez Wykonawcę umowy o przetwarzaniu danych osobowych zgodnie z art. 28 RODO z winy Wykonawcy, w tym w szczególności wskutek braku zdolności do zawarcia takiej umowy (niespełniania przesłanek z art. 28 RODO w terminie 30 dni od dnia zawarcia umowy nie później niż przed pierwszą czynnością Wykonawcy wymagającą przekazania danych osobowych, których administratorem jest Zamawiający (dotyczy umów, których wykonanie związane jest z koniecznością powierzenia i przetwarzania danych osobowych gromadzonych przez Zamawiającego).

§ 8

1. Czynność prawna mająca na celu zmianę wierzyciela Zamawiającego z tytułu wierzytelności wynikających z niniejszej umowy może zostać dokonana tylko w trybie określonym w art. 54 ust. 5 – 7 ustawy z 15 kwietnia 2011 roku o działalności leczniczej.
2. Zastrzeżenie o którym mowa w ust. 1 dotyczy w szczególności umów cesji wierzytelności, umów poręczenia, umów gwarancji, umów przekazu, umów zastrzegających świadczenie na rzecz osoby trzeciej umów skutkujących przystąpieniem osoby trzeciej do zobowiązań wynikających z niniejszej umowy, w tym umów skutkujących subrogacją generalną (art. 518 k.c.).
3. Zastrzeżenie o którym mowa w ust.1 dotyczy także umów na podstawie których wierzytelność względem Zamawiającego będzie stanowiła zabezpieczenie zobowiązań Wykonawcy (np. z tytułu umowy kredytu, pożyczki)
4. Wykonawca zobowiązuje się do nieudzielania pełnomocnictw szczególnych upoważniających pełnomocników do przyjmowania świadczeń pieniężnych wynikających z niniejszej umowy na swoje rachunki lub podmiotów innych niż Wykonawca.
5. Wykonawca zobowiązuje się do nie udzielania pełnomocnictw nieodwołalnych przez mocodawcę w zakresie dochodzenia roszczeń majątkowych wynikających z niniejszej umowy.
6. W razie wątpliwości przez czynność prawną mającą na celu zmianę wierzyciela w rozumieniu niniejszej umowy lub ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej Strony rozumieją każdą sytuację, w której Zamawiający byłby zobowiązany do zapłaty podmiotom innym niż Wykonawca lub na rachunek

bankowy innego podmiotu niż Wykonawca.

§ 9

1. Każda ze Stron niniejszej umowy zobowiązuje się do zachowania w poufności wszelkich, powziętych w ramach realizacji zamówienia, informacji dotyczących Zamawiającego i jego spraw, a w szczególności na temat prowadzonej przez nią działalności oraz metod działania, jej pracowników i współpracowników, klientów, oraz wszelkich innych informacji pozyskanych w związku z realizacją tej umowy, których ujawnienie mogłoby narazić tę stronę na szkodę, a także do nie przekazywania i nie udostępniania osobom trzecim dokumentów powierzonych przez Zamawiającego.
2. Obowiązek zachowania tajemnicy poufności, o którym mowa w ust. 1, nie dotyczy informacji, które:
   a) w czasie ich ujawnienia były publicznie znane,
   b) których obowiązek ujawnienia wynika z bezwzględnie obowiązującego przepisu prawa, orzeczenia sądu lub decyzji innego uprawnionego organu władzy, z zastrzeżeniem niezwłocznego powiadomienia strony, której informacje mają zostać ujawnione o takim obowiązku i zabezpieczeniu poufności tych informacji.

§ 10

1. Wszelkie zmiany treści niniejszej umowy, wymagają formy pisemnej (aneks) pod rygorem nieważności.
2. W sprawach nie uregulowanych umową stosuje się przepisy Kodeksu Cywilnego oraz ustawy z dnia 19 stycznia 2019 r. Prawo zamówień publicznych
3. Wszelkie spory wynikające z realizacji niniejszej umowy lub w związku z nią, będą rozstrzygane przez właściwy sąd powszechny, według siedziby Zamawiającego.
4. Niniejsza umowa została sporządzona w dwóch jednobrzmiących egzemplarzach – 1 egzemplarz dla Zamawiającego, 1 egzemplarz dla Wykonawcy.

Wykonawca ***Zamawiający***

Wzór umowy akceptuję bez zastrzeżeń:

…….

(pieczątka i podpis Wykonawcy
lub jego uprawnionego przedstawiciela)

Data: ……

….....
miejscowość data

PROTOKÓŁ ZDAWCZO – ODBIORCZY

Zamawiający :
Szpital Specjalistyczny im. Edmunda Biernackiego w Mielcu, ul. Żeromskiego 22

w imieniu którego odbioru, na podstawie oględzin zewnętrznych, dokonuje pracownik Sekcji Informatycznej:

…….
(Imię i Nazwisko, stanowisko)

niniejszym potwierdza przyjęcie od Wykonawcy :
……
……

w imieniu którego przekazuje:
…….
(Imię i Nazwisko, stanowisko)

Następujący przedmiot zamówienia:

Nazwa: …….
Typ: ……..
Nr seryjny: ……
Rok produkcji: …….
Ilość: …….

Stan dostawy : ……
……
……
……

Ewentualne zastrzeżenia :
……
……
……

Zamawiający: **Wykonawca:**

Załącznik nr 3 do Zapytania ofertowego

……
(Pieczęć firmowa)

OŚWIADCZENIE, ŻE OFEROWANE DOSTAWY ODPOWIADAJĄ WYMAGANIOM ZAMAWIAJĄCEGO

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego na **zakup i wdrożenie systemu typu SIEM w celu zwiększenia cyberbezpieczeństwa oraz wykonanie audytu bezpieczeństwa w Szpitalu Specjalistycznym im. Edmunda Biernackiego w Mielcu, znak SzP.ZP.271.46.23**, w imieniu reprezentowanej przeze mnie firmy oświadczam, że oferowany asortyment jest zgodny z opisem przedmiotu zamówienia i posiada dokumenty wymagane przez obowiązujące prawo dla tego typu asortymentu oraz spełnia wszystkie wymagania i parametry określone przez Zamawiającego w Zapytaniu ofertowym.

Na każde żądanie Zamawiającego niezwłocznie prześlemy wszystkie niezbędne kserokopie dokumentów potwierdzające Oświadczenie.

……..
(pieczątka i podpis Wykonawcy
lub jego uprawnionego przedstawiciela)

Data: ……