SAMODZIELNY PUBLICZNY
ZAKŁAD OPIEKI ZDROWOTNEJ MSWiA W RZESZOWIE
35-111 RZESZÓW, UL. KRAKOWSKA 16
TEL./17/86-43-312, FAX./17/850-70-53
NIP: 813-28-92-063, REGON: 690028840

Rzeszów, dnia 20.10.2022 r.

ZNAK SPRAWY Z/ZZP.2375.31.22

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

na dostawę i wdrożenie systemów SIEM (Security Information and Event Management) oraz SOAR (Security Orchestration, Automation and Response) dla SP ZOZ MSWiA w Rzeszowie

Postępowanie o udzielenie zamówienia publicznego prowadzone będzie w trybie podstawowym bez negocjacji o wartości powyżej 130.000,00 zł zgodnie z przepisami ustawy z 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 z późn. zm.)

Specyfikację zatwierdza: _____

Rozdział I NAZWA ORAZ ADRES ZAMAWIAJĄCEGO, NUMER TELEFONU, ADRES POCZTY ELEKTRONICZNEJ ORAZ STRONY INTERNETOWEJ PROWADZONEGO POSTĘPOWANIA.

Zamawiający: Samodzielny Publiczny Zakład Opieki Zdrowotnej MSWiA w Rzeszowie
Adres: ul. Krakowska 16, 35-111 Rzeszów
Numer tel.: 17/ 850-70-53
Adres poczty elektronicznej: zaopatrz@szpitalmsw.rzeszow.pl
Adres strony internetowej prowadzonego postępowania, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia (URL):
https://www.szpitalmsw.rzeszow.pl
Adres skrytki ePUAP: /SPZOZMSWRZESZOW/SkrytkaESP

Rozdział II TRYB UDZIELENIA ZAMÓWIENIA.

1. Postępowanie jest prowadzone w **trybie podstawowym bez przeprowadzenia negocjacji treści złożonych ofert** zgodnie z art. 275 pkt 1 ustawy Prawo zamówień publicznych. W związku z tym Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.

Rozdział III OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest dostawa i wdrożenie systemów SIEM (Security Information and Event Management) oraz SOAR (Security Orchestration, Automation and Response) dla Samodzielnego Publicznego Zakładu Opieki Zdrowotnej MSWiA w Rzeszowie, transportem na koszt i ryzyko Wykonawcy.

   1.1 Wykonawca nie dopuszcza składania ofert częściowych.
   1.2 Zamawiający nie przewiduje udzielania zamówień uzupełniających.
   1.3 Termin płatności wymagany przez Zamawiającego to 30 dni od daty dostarczenia faktury.
   1.4 Uwaga: Zamawiający pracuje od poniedziałku do piątku w godz. 7.00 – 14.35.

2. Okres, w którym realizowane będzie zamówienie: do 30.11.2022 r.
3. Główny kod CPV: **48730000-4 -** Pakiety oprogramowania zabezpieczającego

4. Zamawiający informuje, iż ilekroć w SWZ i jej załącznikach przedmiot zamówienia jest opisany:
   a) ze wskazaniem znaków towarowych, nazw własnych, patentów lub pochodzenia źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę to przyjmuje się, że wskazaniom takim towarzyszą wyrazy „lub równoważny”. Oznacza to, że dopuszcza się zaoferowanie wyrobów nie gorszych niż opisywanych, tj. spełniających wymagania techniczne, funkcjonalne i jakościowe, co najmniej takie jak wskazane w dokumentacji niniejszego postępowania,
   b) poprzez odniesienie się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy, to przyjmuje się, że dopuszcza się rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy „lub równoważne”.

5. **Przedmiot zamówienia**:

1. Zakres podstawowy przedmiotu zamówienia obejmuje w szczególności:

1) dostawę systemu typu Security Information and Event Management dalej zwanego jako SIEM lub oprogramowanie dedykowane, wraz z niezbędnymi licencjami oraz oprogramowaniem standardowym oraz jego wdrożenie i konfiguracja;

2) dostawę systemu typu Security Orchestration Automation & Response dalej zwanego jako SOAR lub oprogramowanie dedykowane, wraz z niezbędnymi licencjami oraz oprogramowaniem standardowym oraz jego wdrożenie i konfiguracja;

3) dostawę, wdrożenie i konfigurację skanera podatności opartego na licencji open source dalej zwanego jako Oprogramowanie dedykowane;

4) wykonanie i dostarczenie dokumentacji wdrożeniowej, w tym w szczególności:

a) projektu wdrożenia,
b) dokumentacji technicznej,
c) dokumentacji dla użytkownika.

5) wykonanie i dostarczenie dokumentacji powdrożeniowej

6) przeprowadzenie 3-dniowego, certyfikowanego szkolenia z obsługi SIEM i SOAR dla 4 pracowników Zamawiającego.

7) zapewnienie 12-miesięcznej gwarancji oraz wsparcia technicznego dla systemu SIEM, SOAR i skanera podatności, zgodnie z Projektem Umowy oraz Opisem Przedmiotu Zamówienia.

Rozdział IV TERMIN WYKONANIA ZAMÓWIENIA

Okres w którym będzie realizowane zamówienie: 30 dni od dnia zawarcia umowy.

Rozdział V WARUNKI UDZIAŁU W POSTĘPOWANIU,

O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:

1. Nie podlegają wykluczeniu na podstawie
   a)art. 108 ust.1 ustawy ;
2. Wykluczenie Wykonawcy następuje zgodnie z art. 111 p.z.p.
3. Spełniają następujące warunki dotyczące:
   3.1) zdolności do występowania w obrocie gospodarczym:
   Zamawiający nie precyzuje warunku w tym zakresie
   3.2) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:
   Zamawiający nie precyzuje warunku w tym zakresie
   3.3) sytuacja ekonomiczna lub finansowa:
   Zamawiający nie precyzuje warunku w tym zakresie,
   3.4) zdolność techniczna lub zawodowa:
   Zamawiający nie precyzuje warunku w tym zakresie.

Rozdział VI Informacja dla Wykonawców wspólnie ubiegających się o udzielenie zamówienia (Spółki cywilne/Konsorcja)

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku, Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty.
2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Rozdziale VIII ust. 1 SWZ, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w zakresie, w jakim każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
3. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które roboty budowlane/dostawy/usługi wykonają poszczególni wykonawcy.
4. Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.

Rozdział VII. Informacja dla Wykonawców polegających na zasobach innych podmiotów na zasadach określonych w art. 118 ustawy Pzp oraz dla Wykonawców zamierzających powierzyć wykonanie części zamówienia podwykonawcom

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają usługi, do realizacji których te zdolności są wymagane.
3. **Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z ofertą**, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
4. Zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w ust. 3 powyżej, potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
    1) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
    2) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
    3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.

5. Zamawiający ocenia, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez wykonawcę spełniania warunków udziału w postępowaniu oraz, jeżeli dotyczy, kryteriów selekcji, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.
6. Jeżeli zdolności techniczne lub zawodowe, sytuacja ekonomiczna lub finansowa podmiotu udostępniającego zasoby nie potwierdzają spełniania przez Wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, Zamawiający zażąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
7. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.

Rozdział VIII Wykaz dokumentów i oświadczeń, których złożenia Zamawiający wymaga od Wykonawcy w postępowaniu o udzielenie zamówienia

A. PODMIOTOWE ŚRODKI DOWODOWE

1. **Wraz z ofertą Wykonawca zobowiązany jest złożyć** oświadczenie, o którym mowa w art. 125ust. 1 ustawy Pzp, stanowiące wstępne potwierdzenie, że Wykonawca na dzień składania ofert:
   1) nie podlega wykluczeniu,
   2) spełnia warunki udziału w postępowaniu.
2. Wzór oświadczenia, o którym mowa w ust. 1 powyżej stanowi **Załącznik nr 2** do SWZ.
3. **Zamawiający wezwie Wykonawcę, którego oferta została najwyżej** oceniona, do złożenia w wyznaczonym terminie (nie krótszym niż 5 dni od dnia wezwania) następujących podmiotowych środków dowodowych (aktualnych na dzień złożenia):

4.1 aktualnego na dzień złożenia - odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;

4.1 oświadczenia wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, dotyczące przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076 i 1086), z innym wykonawcą, który złożył ofertę w postępowaniu **Załącznik nr 3**

6. Zamawiający nie będzie wzywał do złożenia podmiotowych środków dowodowych, jeżeli możeje uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile Wykonawca wskazał w oświadczeniu, o którym mowa w części A ust. 1 powyżej, dane umożliwiające dostęp do tych środków.

7. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.

8. Jeżeli Wykonawca nie złożył podmiotowych środków dowodowych lub są one niekompletne lub zawierają błędy, Zamawiający wezwie Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie, chyba że oferta Wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub zachodzą przesłanki unieważnienia postępowania.

a. Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych podmiotowych środków dowodowych.
b. Jeżeli złożone przez Wykonawcę podmiotowe środki dowodowe budzą wątpliwości Zamawiającego, może on zwrócić się bezpośrednio do podmiotu, który jest w posiadaniu informacji lub dokumentów istotnych w tym zakresie dla oceny spełniania przez Wykonawcę warunków udziału w postępowaniu, kryteriów selekcji lub braku podstaw wykluczenia, o przedstawienie takich informacji lub dokumentów.
c. Oświadczenie, o którym mowa w części A ust. 1 powyżej składa się pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.

B PRZEDMIOTOWE ŚRODKI DOWODOWE

Zamawiający nie wymaga złożenia przedmiotowych środków dowodowych.

C INNE DOKUMENTY SKŁADANE PRZEZ WYKONAWCĘ WRAZ Z OFERTĄ

1. Uzupełniony formularz ofertowy – zgodnie z **Załącznikiem nr 1** do SWZ.
2. Pełnomocnictwo upoważniające do złożenia oferty, jeżeli ofertę składa pełnomocnik.
3. Pełnomocnictwo do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia - dotyczy ofert składanych przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia;
4. Pełnomocnictwo do złożenia oferty musi być złożone w oryginale w takiej samej formie, jak składana oferta (t.j. w formie elektronicznej lub postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym).
5. Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego stosownie do art. 97 §2 ustawy z dnia 14 lutego 1991 r. Prawo o notariacie, które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie pisemnej kwalifikowanym podpisem, podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez upełnomocnionego.

Rozdział IX Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się drogą elektroniczną przy użyciu miniPortalu, który dostępny jest pod adresem:
   https://miniportal.uzp.gov.pl/, ePUAPu, dostępnego pod adresem: https://epuap.gov.pl/wps/portal oraz poczty elektronicznej email: zaopatrz@szpitalmsw.rzeszow.pl

2. Osoba uprawniona do kontaktu z Wykonawcami:
   - w sprawach proceduralnych:
     - Marek Pytel – Sekcja Zaopatrzenia i Zamówień Publicznych
       tel. /17/ 86-43-215 w godz. 10:00 – 12:00,
       e-mail: zaopatrz@szpitalmsw.rzeszow.pl
3. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do następujących formularzy: „Formularz do złożenia, zmiany, wycofania oferty lub wniosku" oraz do „Formularza do komunikacji".
4. Wymagania techniczne i organizacyjne wysyłania i odbierania korespondencji elektronicznej, przekazywanej przy ich użyciu, opisane zostały w Regulaminie korzystania z systemu miniPortal pod adresem https://miniportal.uzp.gov.pl/WarunkiUsługi.aspx oraz Regulaminie ePUAP. Zasady składania ofert oraz dokumentów składanych wraz z ofertą, oraz wymagania techniczne i organizacyjne ich wysyłania opisane zostały w Instrukcji użytkownika
5. Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z miniPortalu, określone w Regulaminie miniPortalu oraz zobowiązuje się przestrzegać postanowień tego regulaminu.
6. Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do: „złożenia, zmiany i wycofania oferty" oraz do komunikacji wynosi 150 MB.
7. Za datę przekazania oferty, oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp, podmiotowych środków dowodowych, przedmiotowych środków dowodowych oraz innych informacji, oświadczeń lub dokumentów, przekazywanych w postępowaniu, przyjmuje się datę ich przekazania na ePUAP.
8. W postępowaniu o udzielenie zamówienia korespondencja elektroniczna (inna niż oferta Wykonawcy i załączniki do oferty) odbywa się elektronicznie za pośrednictwem dedykowanego formularza dostępnego na ePUAP oraz udostępnionego przez miniPortal (Formularz do komunikacji). Korespondencja przesłana za pomocą tego formularza nie może być szyfrowana. We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem ogłoszenia (BZP)
9. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę za pośrednictwem Formularza do komunikacji jako załączniki. Zamawiający dopuszcza również możliwość składania dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów i oświadczeń za pomocą poczty elektronicznej, na adres e-mail: zaopatrz@szpitalmsw.rzeszow.pl.
10. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów i oświadczeń musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30.12.2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz.U. z 2020 r. poz. 2452) oraz Rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy (Dz.U. z 2020 r. poz. 2415).
11. Zamawiający przekazuje link do postępowania oraz ID postępowania jako **Załącznik nr 6** do SWZ. Identyfikator postępowania jest dostępny na liście wszystkich postępowań na miniPortalu

12. **Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SWZ**. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.
13. Jeżeli wniosek o wyjaśnienie treści SWZ wpłynął po upływie terminu składania wniosku, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpatrzenia. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
14. Jeżeli Zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 12 powyżej, przedłuży termin składania ofert o czas niezbędny do zapoznania się z wyjaśnieniami oraz przygotowania i złożenia oferty.
15. Treść zapytań wraz z wyjaśnieniami, bez ujawniania źródła zapytania, Zamawiający zamieści na stronie internetowej prowadzonego postępowania.
16. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert, zmienić treść SWZ. Dokonaną zmianę treści specyfikacji Zamawiający zamieści na stronie internetowej prowadzonego postępowania.
17. W przypadku, gdy zmiana treści SWZ będzie istotna dla sporządzenia oferty lub będzie wymagać dodatkowego czasu na zapoznanie się ze zmianą i przygotowanie oferty, Zamawiający przedłuży termin składania ofert o czas niezbędny na zapoznanie się ze zmianą SWZ i przygotowanie oferty.
18. Jeżeli zmiana treści SWZ prowadzi do zmiany treści ogłoszenia o zamówieniu, Zamawiający zamieszcza w Biuletynie Zamówień Publicznych ogłoszenie o zmianie ogłoszenia.

Rozdział X Opis sposobu przygotowania oferty

1. Ofertę należy sporządzić wg wzoru stanowiącego **Załącznik Nr 1** do SWZ.
2. **Każdy Wykonawca może złożyć tylko jedną ofertę.** Złożenie przez Wykonawcę więcej niż jednej oferty, spowoduje odrzucenie wszystkich ofert złożonych przez tego Wykonawcę.
3. W formularzu oferty Wykonawca zobowiązany jest podać adres skrzynki ePUAP i/lub poczty elektronicznej, poprzez który prowadzona będzie korespondencja związania z postępowaniem.
4. Oferta musi być sporządzona w języku polskim, w postaci elektronicznej w formacie danych: .pdf, .doc, .docx, .rtf, .xps, .odt i opatrzona kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
5. Sposób zaszyfrowania oferty opisany został w Instrukcji użytkownika dostępnej na miniPortalu.
6. Do przygotowania oferty konieczne jest posiadanie przez osobę upoważnioną do reprezentowaniaWykonawcy kwalifikowanego podpisu elektronicznego, podpisu osobistego lub podpisu zaufanego.
7. Wszystkie złożone przez Wykonawcę oświadczenia i dokumenty sporządzone w języku obcym, muszą być złożone wraz z tłumaczeniem na język polski.
8. **Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa** w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2019 r. poz. 1010), które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym opisaniem pliku „Załącznik stanowiący tajemnicę przedsiębiorstwa" a następnie wrazz plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum (ZIP). Zamawiający nie ujawni informacji stanowiących tajemnicę

przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert zastrzeże,że nie mogą być one udostępniane oraz wykaże, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji zgodnie z postanowieniami art. 18 ust. 3 ustawy Pzp. Wykonawca nie może zastrzec informacji, o których mowaw art. 222 ust. 5 ustawy Pzp.

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

Rozdział XI ZŁOŻENIE OFERTY

1. Wykonawca składa ofertę za pośrednictwem „***Formularza do złożenia, zmiany, wycofania oferty lub wniosku***" dostępnego na ePUAP i udostępnionego również na miniPortalu. Funkcjonalność do zaszyfrowania oferty przez wykonawcę jest dostępna dla wykonawców na miniPortalu, w szczegółach danego postępowania. W formularzu OFERTA wykonawca zobowiązany jest podać adres skrzynki ePUAP, na którym prowadzona będzie korespondencja związana z postępowaniem.
2. Ofertę należy sporządzić w języku polskim, w formie elektronicznej lub w postaci elektronicznej w formacie danych: .odt, .doc, .docx, .pdf.
3. Ofertę składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
   Ofertę należy złożyć w oryginale.
   Nazwa pliku z formularzem ofertowym powinna zawierać słowo OFERTA. W przeciwnym razie zamawiający nie ponosi odpowiedzialności za nieotwarcie nieprawidłowo opisanego pliku z formularzem ofertowym w trakcie sesji otwarcia ofert.
4. Sposób złożenia oferty, w tym zaszyfrowania oferty, opisany został w „Instrukcji użytkownika", dostępnej na stronie: https://miniportal.uzp.gov.pl/
5. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r., poz. 1913), wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa", a następnie wraz z plikami stanowiącymi jawną część należy ten plik zaszyfrować.
6. Do oferty należy dołączyć oświadczenie o niepodleganiu wykluczeniu, spełnianiu warunków udziału w postępowaniu, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym, a następnie zaszyfrować wraz z plikami stanowiącymi ofertę.
7. Oferta może być złożona tylko do upływu terminu składania ofert.
8. Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę za pośrednictwem „***Formularza do złożenia, zmiany, wycofania oferty lub wniosku***" dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób zmiany i wycofania oferty został opisany w „Instrukcji użytkownika" dostępnej na miniPortalu.
9. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.

Podpis zaufany – ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2019 r., poz. 700 ze zm.).
Podpis osobisty – ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (t.j. Dz. U. z 2019 r., poz. 653 ze zm.).

Rozdział XII TERMIN SKŁADANIA I OTWARCIA OFERT

1. **Ofertę należy złożyć w terminie do dnia 28.10.2022 r. do godz. 09:00.**
2. **Otwarcie ofert** nastąpi w dniu **28.10.2022 r. o godz. 09:30** , za pośrednictwem miniPortalu.
3. Najpóźniej przed otwarciem ofert, Zamawiający udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. Niezwłocznie po otwarciu ofert, Zamawiający udostępni na stronie internetowej prowadzonego postępowania informacje o:
   1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania Wykonawców, których oferty zostały otwarte;
   2) cenach zawartych w ofertach.
5. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.

Rozdział XIII WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający nie wymaga wniesienia wadium.

Rozdział XIV TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca jest związany ofertą przez okres 30 dni tj. do dnia 26.11.2022r. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2 powyżej, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
4. W przypadku braku zgody, o której mowa w ust. 3 powyżej, oferta podlega odrzuceniu, a Zamawiający zwraca się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba że zachodzą przesłanki do unieważnienia postępowania.

Rozdział XV OPIS SPOSOBU OBLICZENIA CENY

1. Cena podana w ofercie musi zawierać wszystkie koszty związane z terminową realizacją i prawidłowym wykonaniem przedmiotu zmówienia
2. Cena jednostkowa x ilość = wartość netto + podatek VAT = wartość brutto.
3. Ceny netto, brutto, wartość podatku VAT należy zaokrąglić do dwóch miejsc po przecinku.
4. Cenę ostateczną oferty należy podać w złotych polskich cyfrą i słownie.
5. Cena netto podana w formularzu nie ulegnie zmianie przez cały czas obowiązywania umowy.
6. Wykonawca, składając ofertę, informuje Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

Rozdział XVI OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM ZNACZENIA TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. **Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty**

   Wybór oferty dokonany zostanie na podstawie poniższych kryteriów (nazwa kryterium, waga, sposób punktowania):

Lp.	*Nazwa kryterium*	*Waga*	*Sposób punktowania*
1.	***Cena***	***60%***	***Cena oferty najniższej podzielona przez cenę oferty ocenianej x waga***
2.	***Okres gwarancji***	***40%***	***ilość punktów przyznana badanej ofercie za kryterium okres gwarancji podzielona przez maksymalną ilość punktów możliwą do uzyskania w kryterium okres gwarancji x waga***

Oferty nieodrzucone oceniane będą według wzoru:
(Cmin/Cb * 60%) * 100 + (Gb/60 * 40%) * 100 = liczba punktów

gdzie:
Cmin – najniższa cena spośród ofert nieodrzuconych;
Cb – cena oferty rozpatrywanej;
Gb – liczba miesięcy dodatkowej gwarancji powyżej wymaganego terminu podstawowego, tj. powyżej 12 miesięcy w ofercie rozpatrywanej

(Przykład: zaoferowano gwarancję 12 miesięcy, więc Gb=0; zaoferowano gwarancję 13 miesięcy, więc Gb=1; zaoferowano gwarancję 14 miesięcy, to Gb=2; zaoferowano gwarancję 24 miesięce, to Gb=12);

24 – maksymalna liczba miesięcy dodatkowej gwarancji powyżej wymaganego terminu podstawowego, tj. powyżej 12 miesięcy w ofercie o najdłuższej gwarancji;
Minimalny okres gwarancji wymagany przez zamawiającego wynosi 12 miesięcy.
Zamawiający dokona oceny tego kryterium w zakresie od 12 do 24 miesięcy.

Minimalny okres gwarancji wymagany przez zamawiającego wynosi 12 miesięcy.
Zamawiający dokona oceny tego kryterium w zakresie od 12 do 24 miesięcy.
Okres powyżej 25 miesięcy nie będzie dodatkowo punktowany.

12 miesięczny okres gwarancji otrzyma 0 punktów jako podstawowy, wymagany przez zamawiającego.
Brak wpisu dot. długości okresu gwarancji w FORMULARZU OFERTOWYM będzie traktowany przez zamawiającego jako 12 miesięczny okres gwarancji.
100 – stały wskaźnik.

UWAGA: Punkty w kryterium „Cena" oraz „Okres gwarancji" wyliczone będą do dwóch miejsc po przecinku.

Ostateczna liczba punktów będzie stanowić sumę punktów uzyskanych w poszczególnych kryteriach : Cena + Okres gwarancji

Rozdział XVII INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Umowa zostanie zawarta w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty - zawiadomienie to zostanie przesłane przez zamawiającego do wykonawców przy użyciu środków komunikacji elektronicznej.
2. Zamawiający zawrze umowę przed upływem wskazanego w pkt.1 terminu, jeżeli w postępowaniu zostanie złożona tylko jedna oferta
3. W przypadku, gdy zostanie wybrana jako najkorzystniejsza oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Wykonawca przed podpisaniem umowy na wezwanie Zamawiającego przedłoży umowę regulującą współpracę Wykonawców.
4. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postępowanie.

Rozdział XVIII WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

Rozdział XIX ISTOTNE POSTANOWIENIA UMOWY ORAZ MOZLIWOŚCI JEJ ZMIANY

1. Istotne postanowienia umowy zawiera wzór umowy stanowiący **Załącznik nr 4** do niniejszej SWZ. W jej treści podano wszelkie istotne dla Zamawiającego warunki realizacji zamówienia
2 Zamawiający przewiduje możliwość wprowadzenia zmian do zawartej umowy w sprawie zamówienia publicznego, na podstawie art. 455 ustawy Pzp, oraz na warunkach określonych we wzorze umowy.

Rozdział XX POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

W toku postępowania o udzielenie zamówienia Wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł, lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów uPzp, przysługują środki ochrony prawnej określone w Dziale IX uPzp.

Rozdział XXI OCHRONA DANYCH OSOBOWYCH

KLAUZULA INFORMACYJNA

INFORMACJA O ZASADACH PRZETWARZANIA DANYCH OSOBOWYCH W ZWIĄZKU Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO	
TOŻSAMOŚĆ ADMINISTRATORA	**Samodzielny Publiczny Zakład Opieki Zdrowotnej Ministerstwa Spraw Wewnętrznych i Administracji w Rzeszowie** ul. Krakowska 16, 35-111 Rzeszów, e-mail: sekretariat@szpitalmsw.rzeszow.pl, tel.: 17 86 43 313
INSPEKTOR OCHRONY DANYCH	Imię i nazwisko: **Przemysław Tuleja,** adres email: kancelaria.tuleja@gmail.com
CELE PRZETWARZANIA I PODSTAWY PRAWNE	Dane osobowe będą przetwarzane w celu przeprowadzenia postępowania o udzielenie zamówienia publicznego. Podstawę prawną przetwarzania stanowi art. 6 ust. 1 lit. c) Ogólnego rozporządzenia o ochronie danych oraz przepisy Ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (dalej: „p.z.p.")
ODBIORCY DANYCH	Dane osobowe mogą być przekazywane tylko takim podmiotom, które są do tego uprawnione na podstawie przepisów prawa i tylko w takim zakresie, jaki jest niezbędny do realizacji ich uprawnienia. Odbiorcami danych osobowych będą więc wszelkie osoby i podmioty, którym udostępniona zostanie dokumentacja postępowania na gruncie art. 8 oraz art. 96 ust. 3 p.z.p., z zachowaniem ograniczeń zasady jawności wskazanych w ww. przepisach. Każdy wniosek o udostępnienie danych podlega weryfikacji pod względem jego legalności oraz adekwatności żądanego zakresu danych.
OKRES PRZECHOWYWANIA DANYCH	Dane osobowe Wykonawcy, któremu udzielono zamówienia publicznego będą przechowywane przez **cztery lata,** a jeżeli umowa zawarta została na dłużej: **do czasu wygaśnięcia umowy -** po tym okresie zostaną wybrakowane. Zasada ta wynika z art. 97 Ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych. Dane osobowe pozostałych Wykonawców będą przechowywane przez **pięć lat -** po tym okresie zostaną wybrakowane. Zasada ta wynika z Ustawy z dnia z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.
PRAWA PODMIOTÓW DANYCH	Na warunkach Ogólnego rozporządzenia o ochronie danych podmiotom danych **przysługują** następujące prawa: • dostępu do treści swoich danych (art. 15 RODO); • do sprostowania danych (art. 16. RODO); • do ograniczenia przetwarzania danych (art. 18 RODO); • prawo do niepodlegania procesom zautomatyzowanego podejmowania decyzji, w tym profilowania (art. 22 RODO). W przypadku, gdy realizacja prawa dostępu do danych wymagałaby niewspółmiernie dużego wysiłku, zamawiający może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania

	o udzielenie zamówienia publicznego lub konkursu. Skorzystanie z prawa do sprostowania lub uzupełnienia danych osobowych nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego lub konkursu ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Prawo zamówień publicznych, zaś skorzystanie z prawa do ograniczenia przetwarzania nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego lub konkursu. Podmiotom danych **nie przysługują** następujące prawa: • 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.
PRAWO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO	Podmiotom danych przysługuje prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych w państwie członkowskim ich zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia. Polskim organem nadzoru jest **Prezes Urzędu Ochrony Danych Osobowych** z siedzibą pod adresem 00-193 Warszawa, ul. Stawki 2, adres email: **kancelaria@uodo.gov.pl.**
ŹRÓDŁO POCHODZENIA DANYCH OSOBOWYCH	Dane osobowe pochodzą z ofert złożonych w trakcie postępowania o udzielenie zamówienia publicznego oraz z przedłożonych, na żądanie zamawiającego, oświadczeń lub dokumentów niezbędnych do przeprowadzenia postępowania.
INFORMACJA O DOWOLNOŚCI LUB OBOWIĄZKU PODANIA DANYCH	Podanie treści danych osobowych jest warunkiem koniecznym do wzięcia udziału w postępowaniu o udzielenie zamówienia publicznego. Niepodanie treści danych osobowych może skutkować wezwaniem do złożenia oświadczeń lub dokumentów niezbędnych do przeprowadzenia postępowania lub brakiem możliwości wzięcia udziału w postępowaniu, odrzuceniem oferty.
INFORMACJA O ZAUTOMATYZOWANYM PODEJMOWANIU DECYZJI ORAZ PROFILOWANIU	Państwa dane osobowe nie będą przedmiotem zautomatyzowanego podejmowania decyzji, w tym profilowania.

Rozdział XXII ZAŁĄCZNIKI DO SWZ

Załącznik Nr 1 - Formularz ofertowy
Załącznik Nr 2 - Oświadczenie wykonawcy składane na podst. art. 125 ust. 1 ustawy Pzp
Załącznik Nr 3- Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej
Załącznik Nr 4- Wzór umowy
Załącznik Nr 5 -Wymagania funkcjonalne dla systemu
Załącznik Nr 6 – ID postępowania na miniPortalu

Załącznik nr 1
do SWZ

Zamawiający:
Samodzielny Publiczny Zakład Opieki Zdrowotnej MSWiA
w Rzeszowie, ul. Krakowska 16, 35-111 Rzeszów

FORMULARZ OFERTOWY

Wykonawca:

……

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

reprezentowany przez:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Adres poczty elektronicznej (e-mail) wykonawcy: .....
Adres skrzynki ePUAP wykonawcy: .....

Nazwa				
	Wartość netto w PLN	Stawka VAT	Kwota VAT	Wartość brutto w PLN
Dostawa i wdrożenie systemów SIEM (Security Information and Event Management) oraz SOAR (Security Orchestration, Automation and Response) dla SP ZOZ MSWiA w Rzeszowie				

Oświadczenia dotyczące postanowień zawartych w SWZ:

Termin płatności w dniach	**30 dni od dnia wystawienia faktury**

Oferowany okres gwarancji	**……..** **(min. 12 msc-y, max. 24 msc-e)** *Wypełnia Wykonawca
Termin realizacji zamówienia	**Do 30.11.2022r.**

1. zapoznałem się z treścią SWZ dot. przetargu w trybie podstawowym bez negocjacji na Dostawę i wdrożenie systemów SIEM (Security Information and Event Management) oraz SOAR (Security Orchestration, Automation and Response) oraz z załączonymi do niej projektami umów i akceptuję określone w nich warunki bez zastrzeżeń;

2. w razie wyboru mojej oferty zobowiązuję się do dostarczania przedmiotu zamówienia zgodnego z jego opisem zawartym w SWZ, za cenę podaną w Formularzu cenowym i w terminie podanym w SWZ i Projekcie umowy;

3. w cenie oferty zostały uwzględnione wszystkie koszty związane z realizacją przedmiotu zamówienia;
4. wartość lub procentowa część zamówienia jaka zostanie powierzona podwykonawcy lub podwykonawcom .....
5. zgodnie art. 225 ustawy Prawo zamówień publicznych oświadczamy, iż wybór naszej oferty ***będzie/*nie będzie** prowadził do powstaniu u Zamawiającego obowiązku podatkowego zgodnie z przepisami ustawy o podatku od towarów i usług.
   ** niepotrzebne skreślić*

   Wybór oferty Wykonawcy prowadzi do „powstania u Zamawiającego obowiązku podatkowego", kiedy zgodnie z przepisami ustawy o podatku od towarów i usług to nabywca (Zamawiający) będzie zobowiązany do rozliczenia (odprowadzenia) podatku VAT).

   W przypadku, gdy wybór oferty Wykonawcy będzie prowadził do powstania u Zamawiającego obowiązku podatkowego Wykonawca zobowiązany jest wskazać nazwę (rodzaj) towaru lub usług, wartość tego towaru lub usług bez kwoty podatku VAT. Nazwa towaru lub usług prowadzących do powstania u Zamawiającego obowiązku podatkowego …… oraz wartość tych towarów i usług bez podatku od towarów i usług: …….. PLN.

   - Wykonawca jest:
   - *mikroprzedsiębiorstwem,
   - *małym przedsiębiorstwem,
   - *średnim przedsiębiorstwem,
   - *jednoosobową działalnością gospodarczą,
   - *osobą fizyczną nieprowadzącą działalności gospodarczej,
   - *innym rodzajem

** niepotrzebne skreślić*

6. wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO* wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.**
7. wszystkie dane zawarte w mojej ofercie są zgodne z prawdą i aktualne w chwili składania oferty.
8. składamy ofertę na ____ stronach.
9. wraz z ofertą składamy następujące oświadczenia i dokumenty:

   12.1. ……

   12.2. ……

   12.3. ……..

10. Oświadczamy, że nie podlegamy wykluczeniu z przedmiotowego postępowania na podstawie art. 7 ust. 1 i 9 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 ze zm.).

.....
/ miejscowość, data/ Nazwa wykonawcy/

_____

** rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).*

*** W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie)/*

Załącznik nr 2 do SWZ

Dane Zamawiającego:
Samodzielny Publiczny Zakład Opieki Zdrowotnej
MSWiA w Rzeszowie
ul. Krakowska 16
35-111 Rzeszów

Dane Wykonawcy:
Nazwa:
……..…...
Siedziba/adres:
…….
NIP/PESEL, KRS/CEiDG *(w zależności od podmiotu)*
…….

OŚWIADCZENIE WYKONAWCY
składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.
Prawo zamówień publicznych

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„……”**
prowadzonego przez Samodzielny Publiczny Zespół Opieki Zdrowotnej MSWiA w Rzeszowie oświadczam/y, co następuje:

Oświadczenie dotyczące spełniania warunków udziału w postępowaniu

Oświadczam/y, że **spełniam warunki udziału w postępowaniu** określone przez Zamawiającego w Rozdziale V ust. 1 Specyfikacji Warunków Zamówienia

……..……., dnia……..…..…..……r.
(miejscowość)

Informacja w związku z poleganiem na zasobach innych podmiotów

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez Zamawiającego w Rozdziale V ust. 1 SWZ polegam na zasobach następującego/ych podmiotu/ów:
……
……
w następującym zakresie……
(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).

……., dnia…….r.
(*miejscowość*)

Informacja:

Dokument musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania firmy kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym i przekazany Zamawiającemu wraz z dokumentem (-ami) potwierdzającymi prawo do reprezentacji Podmiotu przez osobę podpisującą ofertę

Oświadczenie dotyczące braku podstaw wykluczenia

Oświadczam, że **nie występują** wobec mnie podstawy wykluczenia z postępowania o udzielenie zamówienia publicznego, o których mowa w art. 108 ust. 1 ustawy Pzp*
Oświadczam, **że zachodzą** w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. …….. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust 1).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze*:
……
* jeżeli nie dotyczy proszę przekreślić

……., dnia…….r.
(*miejscowość*)

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.

……., dnia…….r.
(*miejscowość*)

Informacja:
Dokument musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania firmy kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym i przekazany Zamawiającemu wraz z dokumentem (-ami) potwierdzającymi prawo do reprezentacji Podmiotu przez osobę podpisującą ofertę

Załącznik nr 3 do SWZ

OŚWIADCZENIE

o przynależności lub braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076)

Dotyczy postępowania o udzielenie zamówienia publicznego na:

……
……

Niniejszym oświadczam, **że należę / nie należę** *(niepotrzebne skreślić)* do tej samej grupy kapitałowej z innymi Wykonawcami, którzy złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w niniejszym postępowaniu.

Wykaz wykonawców należących do tej samej grupy kapitałowej, którzy złożyli oferty

Lp.	Wskazanie wykonawcy

W załączeniu dowody wskazujące, że istniejące między wykonawcami należącymi do tej samej grupy kapitałowej, powiązania nie prowadzą do zachwiania uczciwej konkurencji w postępowaniu o udzielenie zamówienia.

……
(data i podpis osoby uprawnionej do reprezentacji Wykonawcy)

Uwaga!
Oświadczenie należy złożyć na wezwanie Zamawiającego.
W przypadku gdy w postępowaniu o udzielenie zamówienia publicznego złożono tylko jedną ofertę (lub w ramach tej samej części zamówienia złożono tylko jedną ofertę częściową to oświadczenie o przynależności do grupy kapitałowej nie jest dokumentem niezbędnym do przeprowadzenia postępowania) - brak obowiązku składania w/w oświadczenia Zamawiającemu.
Oświadczenie dotyczące grupy kapitałowej składane jest po złożeniu oferty i dotyczy jedynie powiązań z innymi Wykonawcami, którzy złożyli oferty w tym postępowaniu.

WZÓR UMOWY

zawarta w dniu … r. pomiędzy:

Samodzielnym Publicznym Zakładem Opieki Zdrowotnej MSWiA w Rzeszowie, wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji i samodzielnych publicznych zakładów opieki zdrowotnej KRS, prowadzonym przez Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy KRS pod numerem KRS 0000020148 adres: ul. Krakowska 16, 35-111 Rzeszów, NIP: 813 28 92 063 zwanym dalej „**Zamawiającym”** reprezentowanym przez:

.....
a

.....

zwanym w treści umowy „**Wykonawcą”** reprezentowanym przez:
.....
w rezultacie dokonania przez Zamawiającego wyboru oferty Wykonawcy w drodze postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie podstawowym bez negocjacji o wartości powyżej 130.000,00 zł zgodnie z przepisami ustawy z 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 z późn. zm.) została zawarta umowa o następującej treści:

§ 1

1. Przedmiotem umowy jest **Dostawa i wdrożenie systemów SIEM (Security Information and Event Management) oraz SOAR (Security Orchestration, Automation and Response)** dla SP ZOZ MSWiA w Rzeszowie.
2. Wykonawca zobowiązuje się zrealizować Przedmiot Umowy zgodnie z Umową, SWZ oraz złożoną przez Wykonawcę Ofertą. Wykonawca oświadcza, iż znane mu są wszystkie warunki wykonania Umowy.
3. Wykonawca oświadcza, iż zrealizuje Przedmiot Umowy z należytą starannością, według najwyższych profesjonalnych standardów, zgodnie ze wskazówkami Zamawiającego.
4. Wykonawca oświadcza, że spełnia wszelkie określone odrębnymi przepisami warunki niezbędne do wykonania Przedmiotu Umowy oraz, że jego doświadczenie i kompetencje umożliwiają należyte wykonanie Umowy.
5. W ramach realizacji Przedmiotu Umowy Wykonawca zobowiązany jest do dostawy i wdrożenia systemów SIEM (Security Information and Event Management) oraz SOAR (Security Orchestration, Automation and Response) a także uruchomienia, wszystko w ramach wynagrodzenia wynikającego z niniejszej umowy.
6. W ramach realizacji Przedmiotu umowy Wykonawca zobowiązuje się ponadto do przeszkolenia personelu Zamawiającego w zakresie korzystania z systemów.
7. Urządzenie wraz z wyposażeniem dodatkowym, jeżeli jest wymagane, zostanie dostarczone w oryginalnych opakowaniach, na koszt i ryzyko Wykonawcy.
8. Wykonawca oświadcza, że posiada doświadczenie, kwalifikacje i uprawnienia wymagane

do prawidłowego wykonania przedmiotu niniejszej umowy oraz dysponuje osobami i środkami finansowymi pozwalającymi na prawidłową i terminową realizację przedmiotu niniejszej umowy.

§ 2

1. Dostawa i wdrożenie nastąpi w terminie 5 dni od wezwania przez Zamawiającego. Całość umowy zostanie wykonana w terminie do 30 dni od podpisania Umowy.
2. Zmiana terminu wykonania przedmiotu umowy jest dopuszczalna w przypadku wystąpienia okoliczności niezawinionych przez Wykonawcę, których pomimo dołożenia należytej staranności nie można było przewidzieć w chwili zawarcia umowy, w szczególności będących następstwem siły wyższej.
3. Zmiana terminu realizacji przedmiotu umowy z przyczyn wskazanych w ust. 2 może nastąpić wyłącznie za zgodą Zamawiającego, na pisemny wniosek Wykonawcy, zawierający uzasadnienie zmiany terminu.
4. Zmiana terminu realizacji przedmiotu umowy jest również dopuszczalna w przypadku, gdy zmiana ta będzie wynikała z potrzeb organizacyjnych Zamawiającego.
5. Wykonawca odpowiada za naruszenie terminu wykonania przedmiotu umowy w przypadku, gdy opóźnienie będzie wynikało z opóźnień dostawców Wykonawcy lub jego podwykonawców.

§ 3

1. Z tytułu realizacji przedmiotu umowy Wykonawcy przysługuje całkowite wynagrodzenie w wysokości **… zł** (słownie: …100) brutto, w … zł netto (słownie: …/100) plus podatek VAT w wysokości …%, tj. … zł.
2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszystkie koszty związane z realizacją przedmiotu umowy, w tym w szczególności cenę sprzedaży, dostawy, wdrożenia, a także koszty testów i próbnych uruchomień, a także koszty przeszkolenia personelu Zamawiającego.

§ 4

1. Zapłata wynagrodzenia nastąpi w terminie do 30 dni od daty dostarczenia Zamawiającemu faktury VAT przez Wykonawcę.
2. Płatność zostanie dokonana w PLN przelewem na rachunek bankowy Wykonawcy wskazany w treści faktury VAT.
3. W przypadku przekroczenia terminu płatności Zamawiający zastrzega sobie prawo negocjowania odroczenia terminu płatności i wysokości naliczonych odsetek.
4. Dniem zapłaty jest dzień, w którym Zamawiający dokonuje obciążenia swojego rachunku bankowego na rzecz Wykonawcy.

§ 5

1. Wykonawca udziela Zamawiającemu 12 miesięcznej gwarancji oraz wsparcia technicznego dla systemu SIEM, SOAR i skanera podatności, począwszy od dnia dostawy i wdrożenia systemów.
2. Gwarancja obejmuje wady Urządzenia lub jego elementów powstałe z przyczyn tkwiących w nim samym lub jego elementach, a także wady będące efektem wad

projektu, użytych materiałów, bądź też nieprawidłowego wykonania lub montażu Urządzenia przez Wykonawcę.

3. W przypadku zgłoszenia wady, usterki lub awarii systemów , Wykonawca zobowiązany jest przystąpić do usunięcia wady, usterki lub awarii w terminie **72 godzin** od momentu otrzymania zawiadomienia o wykryciu wady.
4. W przypadku zgłoszenia wady, usterki lub awarii systemów, Wykonawca zobowiązany jest do usunięcia wady w terminie 5 dni roboczych od daty zgłoszenia.
5. W celu usunięcia wady Wykonawca winien:
   1) naprawić wadliwą rzecz w siedzibie Zamawiającego lub Wykonawcy,
   Wszelkie koszty związane z wymianą lub naprawą systemów obciążają Wykonawcę.
6. W przypadku uchybienia przez Wykonawcę obowiązkowi naprawy lub wymiany w terminie, o którym mowa w ust. 5, Zamawiającemu przysługuje prawo do odstąpienia od umowy.
7. Wszelkie koszty związane z postępowaniem reklamacyjnym ponosi Wykonawca.
8. W okresie gwarancji Wykonawca zapewnia bezpłatny przegląd serwisowy w okresie gwarancji (zgodnie z zaleceniami producenta Urządzenia), z wymianą elementów eksploatacyjnych na koszt i ryzyko Wykonawcy.
9. Wykonawca zapewnia pełny, bezpłatny przegląd okresowy na 1 miesiąc przed upływem terminu gwarancji.
10. Uprawnienia Zamawiającego z tytułu gwarancji nie wyłączają uprawnień Zamawiającego z tytułu rękojmi. Okres rękojmi równy jest okresowi gwarancji i rozpoczyna bieg wraz z gwarancją.

§ 6

1. Strony postanawiają, że naprawienie szkody wynikłej z niewykonania lub nienależytego wykonania umowy nastąpi przez zapłatę kar umownych lub przez zapłatę odszkodowania.
2. Zamawiający uprawniony jest do naliczenia i wyegzekwowania od Wykonawcy następujących kar umownych:
   1) w wysokości 10% wynagrodzenia brutto, o którym mowa w §4 ust. 1 umowy – jeżeli którakolwiek ze stron odstąpi od umowy z przyczyn, za które odpowiada Wykonawca,
   2) w wysokości 10% wynagrodzenia brutto, o którym mowa w §4 ust. 1 umowy – jeżeli Wykonawca odstąpi od wykonywania umowy z powodu przyczyn, za które Zamawiający nie ponosi winy lub za które nie odpowiada Zamawiający,
   3) w wysokości 0,2% wynagrodzenia brutto, o którym mowa w §4 ust. 1 umowy - za każdy dzień zwłoki w stosunku do terminu wykonania umowy określonego w § 2 ust. 1.
   4) w wysokości 0,2% wynagrodzenia brutto, o którym mowa w §4 ust. 1 umowy – za każdy dzień zwłoki w usunięciu wad lub usterek w okresie rękojmi lub gwarancji.
3. Łączna maksymalna wysokość kar umownych, których mogą dochodzić strony wynosi 20% wartości brutto przedmiotu umowy.
4. W przypadku gdy kary umowne przewidziane w ust. 2 nie pokrywają szkody Zamawiającemu przysługuje prawo żądania odszkodowania na zasadach ogólnych.

§ 7

1. Oprócz przypadków wymienionych w przepisach Kodeksu cywilnego, Zamawiającemu przysługuje prawo odstąpienia od umowy w trybie natychmiastowym w przypadku:
   1) w terminie 30 dni od dnia powzięcia wiadomości o zaistnieniu istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie

umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu;
   2) jeżeli zachodzi co najmniej jedna z następujących okoliczności:
      a) dokonano zmiany umowy z naruszeniem art. 454 p.z.p. i art. 455 p.z.p.,
      b) Wykonawca w chwili zawarcia umowy podlegał wykluczeniu na podstawie art. 108 p.z.p.,
      c) Trybunał Sprawiedliwości Unii Europejskiej stwierdził, w ramach procedury przewidzianej w art. 258 Traktatu o funkcjonowaniu Unii Europejskiej, że Rzeczpospolita Polska uchybiła zobowiązaniom, które ciążą na niej na mocy Traktatów, dyrektywy 2014/24/UE, dyrektywy 2014/25/UE i dyrektywy 2009/81/WE, z uwagi na to, że Zamawiający udzielił zamówienia z naruszeniem prawa Unii Europejskiej.
2. W przypadku odstąpienia z powodu dokonania zmiany umowy z naruszeniem art. 454 p.z.p. i art. 455 p.z.p., Zamawiający odstępuje od umowy w części, której zmiana dotyczy.
3. W przypadku odstąpienia przez Zamawiającego od umowy Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.

§ 8

1. Zmiana niniejszej umowy jest możliwa:
   1) wycofania z dystrybucji przedmiotu umowy i zastąpienia go produktem o parametrach nie gorszych niż oferowany, za cenę taką jaka została ustalona w niniejszej umowie,
   2) zmiany terminu dostawy z przyczyn niezależnych od Wykonawcy,
   3) ustawowej zmiany stawki podatku VAT.
2. Zmiana niniejszej umowy jest możliwa:
   1) gdy ulegnie zmianie stan prawny w zakresie dotyczącym realizowanej umowy, który spowoduje konieczność zmiany sposobu wykonania zamówienia przez Wykonawcę;
   2) wystąpią przeszkody o charakterze obiektywnym (zdarzenia nadzwyczajne, zewnętrzne i niemożliwe do zapobieżenia, w tym mieszczące się w zakresie pojęciowym tzw. „siły wyższej") np. pogoda uniemożliwiająca wykonanie umowy, inne zdarzenia niezawinione przez żadną ze stron umowy. Strony mają prawo do skorygowania uzgodnionych zobowiązań i przesunąć termin realizacji maksymalnie o czas trwania przeszkody. Strony zobowiązują się do natychmiastowego poinformowania się nawzajem o wystąpieniu ww. przeszkód;
   3) w innych przypadkach, uzasadnionych interesem Zamawiającego, przy czym zmiana wymaga zgody Zamawiającego.
3. Zmiana niniejszej umowy jest możliwa jeżeli łączna wartość zmian jest mniejsza niż progi unijne oraz jest niższa niż 10% wartości pierwotnej umowy.
4. Zmiana niniejszej umowy wymaga formy pisemnej pod rygorem nieważności.

§ 9

1. Wszelkie różnice poglądów lub spory, strony zobowiązują się załatwić w drodze polubownych negocjacji.
2. Jeśli próba pojednania stron nie powiedzie się, spór zostaje ostatecznie rozstrzygnięty przez sąd właściwy dla siedziby Zamawiającego.

§ 10

W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy Kodeksu cywilnego oraz Ustawy z dnia 11.09.2019 r. - Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019).

§ 11

1. Strony potwierdzają, że Wykonawca zapoznał się ze Specyfikacją Warunków Zamówienia, zawierających m.in. istotne dla Zamawiającego postanowienia i zobowiązania.
2. Integralną częścią niniejszej umowy jest Oferta Wykonawcy oraz Specyfikacja Warunków Zamówienia.

§ 12

1.Adres Wykonawcy do doręczeń wszelkiej korespondencji związanej z niniejszą umową jest adresem wskazanym powyżej w umowie. O każdej jego zmianie Wykonawca jest zobowiązany powiadomić Zamawiającego. W przypadku zaniechania tego obowiązku, korespondencja wysyłana do Wykonawcy na ostatni jego adres znany Zamawiającemu, uważana jest za skutecznie doręczoną.

2.Wykonawca jest zobowiązany do informowania Zamawiającego o zmianie formy prawnej prowadzonej działalności, o wszczęciu postępowania układowego lub upadłościowego oraz zmianie jego sytuacji ekonomicznej mogącej mieć wpływ na realizację umowy oraz o zmianie siedziby firmy pod rygorem skutków prawnych wynikających z zaniechania, w tym do uznania za doręczoną korespondencję skierowaną na ostatni adres podany przez Wykonawcę

3. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach po jednym egzemplarzu dla każdej ze stron.

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 5 do SWZ

Wymagania funkcjonalne dla systemu	
Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi.	
NR	Wymaganie
1	System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.
2	Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach.
3	System musi posiadać wbudowane mechanizmy zapewniające możliwość pobierania zdarzeń poprzez wykorzystanie RestFull-API, sterownika ODBC, agenta do czytania plików płaskich, protokołów IMAPS, POP3S, MAPI do pobierania wiadomości ze skrzynek poczty elektronicznej oraz obsługi zapytań WQL w ramach protokołu WMI;
4	System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.
5	System musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych zdarzeń umożliwiający ich podział na poszczególne pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie ich w systemie.
6	System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, obejmującą zmianie wartości tych pól lub dodanie nowych w oparciu o ich wartości lub wzorzec wyszukiwania. Cały proces musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
7	Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.
8	Normalizacja musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.
9	Normalizacja logów musi posiadać mechanizm geolokalizacyjny, pozwalający na wzbogacenie pól o nazwę lub kod kraju korzystając z wbudowanej w produkt bazy.
10	System musi posiadać predefiniowany zestaw parserów oraz umożliwiać ich wersjonowanie, aby po wgraniu nowej wersji parsera, w razie przypadku gdy będzie to konieczne przywrócić jedną z poprzednich wersji.
11	System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg" znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.
12	Proces normalizacji musi posiadać możliwość optymalizacji, poprzez automatyczny dobór odpowiedniego parsera dla źródła logów w zależności od składni w której te logi są przesyłane. Przykładowo jeżeli logi są przesyłane w standrdzie CEF system dobierze odpowiedni parser, w przypadku gdy źródło zmieni format generowania zdarzeń na LEEF system musi automatycznie zmienić parser bez ingerencji operatora.
13	System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej.
14	System musi być wyposażony w graficzny interfejs umożliwiający określenie miejsca składowania logów (wskazania właściwego repozytorium logów) w zależności od zwartości tych logów, gdzie reguły przekierowania muszą umożliwiać definiowanie warunków po wszystkich sparsowanych polach. Przykładowo jeżeli w zdarzeniu znajduje się informacja o danych poufnych to zdarzenie to zostanie przekierowane do repozytorium A, natomiast w przypadku gdy tej informacji nie będzie to zdarzenie zostanie przekierowane do repozytorium B.
15	Każde z repozytorium logów musi mieć możliwość definiowania własnych zasad retencji uwzględniających

	zdefiniowanie okresu przechowywania lub ilości miejsca przeznaczonego na dane repozytorium. Dla każdego z repozytorium w przypadku jego zapełnienia musi być możliwa konfiguracja, która zapewni automatyczne przeniesienie logów do archiwum lub umożliwi ich nadpisanie.
16	System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu, w tym m.in. odseparowanie zdarzeń korelacyjnych na oddzielne repozytoria danych składowane na osobnych serwerach i dedykowanych do tego celu zasobów dyskowych od wszelkich repozytoriów logów.
17	Ze względu na możliwość wygenerowania dużej ilości danych przez algorytmy uczenia maszynowego system musi mieć możliwość rozdzielenia ich składowania na osobny serwer i dedykowane zasoby dyskowe.
18	System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.
19	System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.
20	System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.
21	System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie znormalizowanej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne.
22	System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.
23	Elektroniczna dokumentacja musi posiadać możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. „Kliknięcie" na dowolny z obiektów na pierwszym planie musi pozwolić na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi być możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów.
24	System musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji również w formie tabelarycznej.
25	System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci, np.: poziom krytyczności systemów oraz usług.
26	System musi umożliwiać generowanie elektronicznej dokumentacji sieci i systemów w sposób automatyczny na podstawie dostarczonych przez producenta reguł wykrywania oraz edytora graficznego pozwalającego utworzyć dodatkowe reguły.
27	System musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Ma umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewnić wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.
28	Definiowanie reguł wykrywania musi bazować na sparsowanych polach oraz wyszukanych zależnościach między różnymi zdarzeniami z wielu źródeł oraz po aktywacji automatycznie uzupełnić elektroniczną dokumentację o następujące informacje: a. nowe zasoby wykryte w sieci, b. typy wykrytych zasobów (np.: serwer lub stacja robocza), c. zastosowane na nich zabezpieczenia,

	d. usługi z którymi się komunikują, e. nowe usługi wykryte na zasobie, f. komunikacje do usług wykrytych na zasobie.
29	System musi umożliwiać uwiarygodnianie uzyskiwanych informacji na bazie wartości progowych osiągniętych w zadanej jednostce czasu i dopiero po ich uwiarygodnieniu uzupełniać automatycznie elektroniczną dokumentację.
30	System powinien posiadać zestaw predefiniowanych reguł do automatycznego uzupełniania elektronicznej dokumentacji, których uruchomienie będzie automatycznie aktualizować elektroniczną dokumentację bez ingerencji operatora.
31	Interfejs interaktywnej mapy sieci musi posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT który został zdefiniowany w elektronicznej dokumentacji oraz nazwę usługi której ta komunikacja dotyczy.
33	System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów. Baza powinna obsługiwać protokół TLP w wersji 2.0 oraz obsługiwać następujące typy wskaźników: a. fqdn, b. e-mail, c. nazwa pliku, d. ścieżka do pliku, e. hash, f. adres IP, g. klucz rejestru, h. cmd.
34	System musi umożliwiać synchronizację wskaźników kompromitacji (IOC) z platformami dostępnymi publicznie. Wymagane jest aby produkt posiadał gotowy mechanizm pobierania wskaźników z platformy MISP (https://www.misp-project.org/).
35	System musi umożliwiać definiowanie list referencyjnych zarówno z jedną wartością jak i łączących unikalne wartości w pojedynczym wierszu (np: obraz pliku, hash, nazwa procesu).
36	Listy referencyjne muszą mieć możliwość synchronizacji z listami publikowanymi publicznie (np.: „Malicious IPs”, „Malicious domain” czy „Tor Exit Nodes”).
37	System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie, minimum to: nazwa komputera wraz z systemem operacyjnym, nazwa użytkownika, login, e-mail, przynależność do grup, przełożonego, jednostkę organizacyjną oraz listę kont uprzywilejowanych.
38	System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.
39	System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. Oczekiwanym wynikiem analizy jest lista niezgodności, (np: czy na zasobie jest ustawione wymuszanie zmiany haseł w zadanym okresie czasu).
40	System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.
41	System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.
42	Rozwiązanie musi zawierać mechanizm pasywnej analizy podatności, obejmującej systemy IT uzupełnione o informację zgodne z słownikiem CPE (ang. Common Platform Enumeration) umożliwiającą import wykrytych podatności zasobu do systemu z publicznie dostępnej bazy CVE (ang. Common Vulnerabilities and Exposures) i dalszą obsługę tych podatności w systemie.
43	System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy Mitre ATT&CK oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach oraz wyświetlania szczegółów związanych z daną techniką, w szczególności: i. id techniki,

	j. taktykę, k. platformy których dotyczy, l. potencjalne źródła, m. opis zagrożenia, n. mityzację, o. sposób detekcji, p. referencje.
44	System w swoim działaniu musi korzystać z wbudowanych algorytmów uczenia maszynowego dla celów zbudowania i utrzymywania modelu danych użytkowników i komputerów.
45	Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych ze skonfigurowanego (wskazanego) okresu lub zdefiniowanej ilości zdarzeń wymaganych do ukończenia procesu nauczania. Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania oraz umożliwić odrębne uczenie w ramach zdefiniowanych zakresów czasowych (np.: rozdzielenie zdarzeń do nauczania w godzinach pracy od zdarzeń po godzinach pracy).
46	System musi posiadać zestaw predefiniowanych i konfigurowalnych reguł do automatycznego przyporządkowania użytkowników i zasobów do właściwych profili nauczania, reguły te muszą zapewnić minimum: a. rozdzielenie procesu nauczania zachowania się użytkowników uprzywilejowanych od użytkowników nieuprzywilejowanych, b. rozdzielenie procesu nauczania zachowania się stacji roboczych od serwerów, c. rozdzielenie serwerów świadczących usługi w sieci Internet od serwerów świadczących usługi lokalnie w organizacji, d. rozdzielenie procesu nauczania serwerów należących do domeny od pozostałych serwerów.
47	System uczenia maszynowego musi posiadać wbudowane mechanizmy nie wymagające żadnej dodatkowej konfiguracji, które po zakończeniu procesu nauki umożliwią detekcję anomalii zachowania użytkowników oraz zasobów (UEBA).
48	Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować zdarzenia, zawierające minimum informację o użytkowniku lub adresie IP na którym została wykryta anomalia oraz wykorzystany algorytm. System musi umożliwiać wykorzystanie tych zdarzeń w celu dalszej korelacji.
49	System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej (np: utrata wizerunku, związana z zagrożeniem przełamania zabezpieczeń serwera webowego organizacji dostępnego z sieci Internet).
50	System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.
51	Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.
52	System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać: a. sparsowane pola oraz ich wartości, b. listy referencyjne, c. atrybuty użytkowników z Active Directory, d. atrybuty komputerów z Active Directory, e. bazę wskaźników kompromitacji (IOC), f. informacje z elektronicznej dokumentacji, g. anomalie w zachowaniu użytkowników (UBA), h. anomalie w zachowaniu zasobów (EBA), i. podatności na zasobach, j. wyniki analizy konfiguracji, k. techniki MITRE ATT&CK®,
53	Reguły koralacjne bazujące na sparasowanych polach i ich wartościach muszą umożliwić:

	g. wykrycie dowolnej treści w logach, h. wykrycie zmiany jednego z kilku pól, i. wykrycie zaniku wiadomości, j. wykrycie nowej wartości pola w zadanym okresie czasu, k. wykrycie incydentu będącego pochodną zdarzeń występujących w określonej kolejności, l. wykrycie zdefiniowanej ilości przesłanych danych w zadanym okresie czasu, m. wykrycie chwilowego wzrostu ilości przesłanych danych (tzw. Peek) w stosunku do całkowitej ilości przesłanych danych w zadanym okresie czasu, n. wykrycie sumarycznego wzrostu przesłanych danych w zdefiniowanej strefie bezpieczeństwa, o. wykrycie zdefiniowanej ilości przesyłanych pakietów w zadanym okresie czasu, p. wykrycie chwilowego wzrostu (tzw. Peek) w stosunku do ilości przesyłanych pakietów w zadanym okresie czasu, q. wykrycie sumarycznego wzrostu ilości pakietów przesyłanych w zdefiniowanej strefie bezpieczeństwa, r. wykrycie ilości uruchomionych procesów w zadanym okresie czasu, s. wykrycie skanowania portów.
54	Reguły korelacyjne bazujące na listach referencyjnych muszą umożliwić: a. wykrycie wystąpienia wartości pola na wybranej liście, b. wykrycie niewystępowania wartości pola na wybranej liście, c. wykrycie wystąpienia pary wartości na wybranej liście (np.: proces i obraz pliku z którego został uruchomiony), d. wykrycie niewystąpienia pary wartości na wybranej liście (np.: nazwa użytkownika wraz aplikacją z którą się wcześniej nie łączył).
55	Reguły korelacyjne wykorzystujące atrybuty użytkowników z Active Directory muszą umożliwić: a. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego konto w Active Directory, b. wykrycie czy zdarzenie pochodzi od użytkownika posiadającego uprzywilejowane konto w Active Directory, c. wykrycie czy zdarzenie pochodzi od użytkownika podszywającego się pod konto użytkownika Active Directory (np.: którego e-mail zdefiniowany w Active Directory różni się od e-maila ze zdarzenia mimo, zgodności pozostałych atrybutów konta). d. wykrycie czy zdarzenie pochodzi od użytkownika należącego do wybranej grupy w Active Directory (np.: Domain Admins), e. wykrycie czy zdarzenie pochodzi od użytkownika nie należącego do wybranej jednostki organizacyjnej.
56	Reguły korelacyjne wykorzystujące atrybuty komputerów z Active Directory muszą umożliwić: a. wykrycia czy zdarzenie pochodzi z komputera należącego do domeny Active Directory, b. wykrycia czy zdarzenie pochodzi z komputera z systemem operacyjnym zdefiniowanym w Active Directory, c. wykrycia czy zdarzenie pochodzi z komputera z wybranej jednostki organizacyjnej.
57	Reguły korelacyjne wykorzystujące bazę wskaźników kompromitacji (IOC) muszą umożliwić: a. wykrycie czy źródłowy adres IP nie jest oznaczony w systemie jako wskaźnik kompromitacji; b. wykrycie czy HASH występujący w zdarzeniu nie jest oznaczony w systemie jako wskaźnik kompromitacji; c. wykrycie czy docelowa nazwa hosta (FQDN) nie jest oznaczona w systemie jako wskaźnik kompromitacji;
58	Reguły korelacyjne wykorzystujące informacje z elektronicznej dokumentacji muszą umożliwić: a. wykrycie połączenia z serwera do stacji roboczej w przypadku braku informacji o rodzajach zasobu w korelowanym zdarzeniu, b. wykrycie połączenia do usługi przez nieautoryzowanego użytkownika, c. wykrycie nieautoryzowanej usługi na serwerze, d. wykrycie nieautoryzowanego połączenia do usługi na serwerze, e. wykrycie nieautoryzowanego połączenia z serwera usług, f. wykrycie nieautoryzowanego połączenia do sieci Internet.
59	Reguły korelacyjne wykorzystujące anomalie w zachowaniu użytkowników (UBA) muszą umożliwić: a. wykrycie anomalii ilościowej związanej z kontem użytkownika wskazującej na potencjalny atak

	(D)DoS lub próbę propagacji złośliwego oprogramowania, b. wykrycie anomalii związanej ze zmianą zachowania na koncie użytkownika, wskazującej na potencjalny atak APT/Ransomware, c. wykrycie różnych typów anomalii na koncie użytkownika wskazujących na możliwe przejecie konta użytkownika przez cyberprzestępcę lub złośliwe oprogramowanie, d. wykrycie anomalii związanych z logowaniami użytkowników w ramach sesji VPN.
60	Reguły korelacyjne wykorzystujące anomalie w zachowaniu zasobów (EBA) muszą umożliwić: a. wykrycie anomalii ilościowej związanej z komputerem wskazującej na potencjalny atak (D)DoS lub próbę propagacji złośliwego oprogramowania, b. wykrycie anomalii związanej ze zmianą zachowania komputera, wskazującej na potencjalny atak APT/Ransomware, c. wykrycie różnych typów anomalii na komputerze, wskazujących na możliwe przejecie komputera przez cyberprzestępcę lub złośliwe oprogramowanie, d. wykrycie anomalii związanych z procesami uruchamianymi na serwerach.
61	Reguły korelacyjne wykorzystujące podatności na zasobach muszą umożliwić: a. wykrycie skanowania portów z zasobu posiadającego krytyczne podatności, b. wykrycie wielokrotnych prób połączeń do zasobu posiadającego krytyczne podatności, c. wykrycie zdarzeń o wysokim „severity" na zasobach posiadającego krytyczne podatności, d. wykrycie zdarzeń o wysokim „severity" do zasobów posiadających krytyczne podatności.
62	Reguły korelacyjne wykorzystujące wyniki analizy konfiguracji muszą umożliwić: a. wykrycie wielokrotnych prób nieudanego logowania do komputera, umożliwiającego ustawienie hasła zawierającego mniej niż 14 znaków, b. wykrycie wielokrotnych prób nieudanego logowania do komputera, który umożliwia tworzenie haseł nie spełniających następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.
63	Reguły korelacyjne wykorzystujące technikach MITRE ATT&CK® muszą umożliwić: a. wykrycie zdefiniowanej ilości technik w zdarzeniach dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, b. wykrycie zdefiniowanej ilości zdarzeń w ramach jednej techniki dotyczących wybranego hosta identyfikowanego po nazwie lub adresie IP, c. wykrycie incydentu będącego pochodną zdarzeń z technik występujących w określonej kolejności na wybranym adresie IP lub zasobie identyfikowanym po nazwie.
65	Pojedyncza reguła korelacyjna musi mieć możliwość wzajemnej korelacji wszystkich powyższych mechanizmów umożliwiając, m.in.: a. wykrycie anomalii na koncie uprzywilejowanym użytkownika, b. wykrycie ruchu z serwera domenowego do skompromitowanej domeny wykazanej w liście referencyjnej, c. wykrycie wielu typów anomalii na komputerze z krytyczną podatnością, d. Wykrycie złośliwego oprogramowania na bazie wskaźnika kompromitacji stanowiącego HASH procesu, z którego następuje nieautoryzowana próba dostępu do usługi, e. wykrycie wielokrotnych prób nieudanego logowania na konto uprzywilejowane, którego hasło nie spełnia następujących kryteriów złożoności: duża litera, mała litera, liczba, znak specjalny.
66	System przy wykorzystaniu reguł kwalifikacyjnych musi automatycznie selekcjonować zdarzenia wygenerowane przez reguły korelacyjne, wybierając do obsługi tylko zdarzenia spełniające zdefiniowane warunki (tzw. zdarzenia w obsłudze). Pozostałe zdarzenia powinny być wykluczone z obsługi, ale równocześnie pozostać w systemie, zachowując możliwość ich obsługi na żądanie operatora. Zastosowane reguły selekcji zdarzeń do obsługi muszą równocześnie umożliwiać wyliczenie właściwego dla nich priorytetu. Reguły selekcji i priorytetyzacji zdarzeń w obsłudze muszą uwzględniać: a. sparsowane pola oraz ich wartości, b. atrybuty użytkowników z Active Directory, c. atrybuty komputerów z Active Directory, d. informacje z elektronicznej dokumentacji.
67	Zdarzenia w obsłudze, muszą obsługiwać opcje grupowania polegającą na tym, że każde kolejne zdarzenie

	wynikające z reguł korelacyjnych spełniających tą samą regułę w zdefiniowanym okresie czasu będzie automatycznie dodawane do tego samego zdarzenia w obsłudze. Grupowanie musi odbywać się po: a. adresie IP, b. koncie domenowym użytkownika, c. strefie bezpieczeństwa, d. zakresie adresów IP.
68	Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. Playbook) oraz pozwalać na tworzenie własnych scenariuszy obsługi oraz ich edycję z poziomu interfejsu graficznego. System musi wspierać funkcję „Drag and Drop" umożliwiającą m.in. na zamianę kolejności realizacji poszczególnych kroków poprzez ich przenoszenie za pomocą myszki komputerowej.
69	System musi potrafić wczytywać informacje z innych systemów bezpieczeństwa i traktować je, jako elementy/dowody dla zdarzeń w obsłudze.
70	Zdarzenia w obsłudze muszą umożliwiać gromadzenie dodatkowych informacji wygenerowanych podczas ich obsługi oraz umożliwiać do nich dostęp bezpośrednio z poziomu tych zdarzeń, obejmujących m.in. a. wszystkie skorelowane zdarzenia, b. korespondencja pocztowa, c. załączniki z próbkami lub dowodami, d. wskaźniki kompromitacji (IOC), e. informacje pozyskane z innych systemów.
71	System powinien posiadać możliwość rejestracji zgłoszeń przez stronę webową udostępnianą przez system dla użytkowników z innych jednostek organizacyjnych oraz umożliwić ich przekształcenie w zdarzenia w obsłudze z możliwością rozdzielenia uprawnień dla obu tych czynności. System musi umożliwiać scenariusz, gdzie użytkownik zgłasza incydent, który zanim zostanie zakwalifikowany do dalszej obsługi musi zostać autoryzowany przez uprawnionego do tego celu operatora.
72	Dla obsługiwanych zdarzeń system powinien umożliwiać automatyczne pozyskanie informacji z innych systemów oraz bazując na uzyskanej od nich odpowiedzi automatycznie zmieniać ich status, np.; na podstawie pozyskanego wskaźnika kompromitacji (IOC) zmienić status zdarzenia na incydent bezpieczeństwa.
73	Dla zdarzeń w obsłudze dotyczących ruchu sieciowego pomiędzy źródłem a celem transmisji system musi automatycznie wyznaczyć wektor zagrożenia i zaprezentować go w formie graficznej, na której będą zwizualizowane następujące dane: a. identyfikację celu i źródła zagrożenia, b. nazwę oraz adres IP źródła zagrożenia, c. rodzaj zasobu będący źródłem zagrożenia np.: urządzenie mobilne, stacja robocza, d. lokalizację z które pochodzi zagrożenie np.: Internet, e. strefę bezpieczeństwa z której pochodzi zagrożenie, f. prawdopodobieństwo zagrożenia ze strefy stanowiącej jego źródło, g. wszystkie urządzenia sieciowe chroniące cel zagrożenia i zastosowane na nich mechanizmy zabezpieczeń (np.: Application Control, Network Firewall, User Identification), h. nazwę oraz adres IP celu zagrożenia, i. zabezpieczenia lokalne chroniące cel zagrożenia, j. strefę bezpieczeństwa w której znajduje się cel zagrożenia.
74	Dla każdego wektora zagrożenia system musi automatycznie wyliczać efektywność zastosowanych mechanizmów zabezpieczeń, pozwalającą w ramach wbudowanych w system edytowalnych reguł ocenić prawdopodobieństwo materializacji się cyberzagrożeń. Przykładowo dla serwera webowego dostępnego ze strefy Internet zagrożenie przełamania zabezpieczeń ma niskie prawdopodobieństwo w przypadku gdy jest on zabezpieczony przez rozwiązanie klasy Web Application Firewall.
75	Dla wyznaczonych w czasie obsługi wektorów zagrożeń przedstawiane wyniki szacowania prawdopodobieństwa muszą być zwizualizowane operatorowi w formie listy zagrożeń z oszacowanymi dla nich poziomami, przykładowe wartości z listy to: wysoki poziom prawdopodobieństwa włamania na serwer oraz średni poziom prawdopodobieństwa infekcji złośliwym oprogramowaniem.
76	Dla zdarzeń w obsłudze zarówno w odniesieniu do adresów źródłowych jak i docelowych system musi umożliwiać operatorowi uzupełnianie pozyskanych informacji, dotyczących zarówno źródła i celu zagrożenia w następującym zakresie:

	a. nazwy zasobu, b. rodzaju zasobu, c. ważności zasobu dla organizacji, d. rodzaj przetwarzanych informacji, e. usług, które ten zasób świadczy, f. lokalizację użytkowników, którzy z niego korzystają, g. Usługi z których zasób korzysta.
77	System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać minimum dostępność operatora, jego obciążenia oraz parametry zasobu którego dotyczy zdarzenie, minimum typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Przykładowo zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych.
78	Zdarzenia w obsłudze muszą obejmować statusy właściwe dla procesu obsługi zdarzeń, minimum to: a. nowe zdarzenie – jako zdarzenie zarejestrowane w systemie, b. segregacja – segregacja i kwalifikacja zdarzeń, c. incydent bezpieczeństwa – zdarzenie zakwalifikowane jako incydent bezpieczeństwa, d. fałszywy alarm – zdarzenie zakwalifikowane jako fałszywy alarm, e. zdarzanie obsłużone – zdarzenie, które zostało obsłużone w systemie. System musi także zapewniać możliwość ich edycji w zakresie dodawania (np.: wydzielenie z segregacji statusu kwalifikacji) lub usuwania statusów oraz konfiguracji przejść pomiędzy nimi. Przykładowo umożliwić przejście ze statusu „incydent bezpieczeństwa" do statusu „zdarzenie zamknięte", ale zablokować zmianę ze statusu „incydent bezpieczeństwa" na status „fałszywy alarm".
79	System powinien umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi zdarzeń oraz dokonywać automatycznego pomiaru tych czasów i ich weryfikacji względem zdefiniowanych wartości. Wyniki pomiarów czasów SLA powinny być stale aktualizowane i prezentowane na liście zdarzeń zakwalifikowanych do obsługi.
80	System musi umożliwiać grupowanie manualne dla zdarzeń w obsłudze, których powiązanie zostanie wykryte przez operatorów w trakcie obsługi i umożliwiać zgrupowanie ich do jednego zdarzenia. Zgrupowane zdarzenia muszą być podrzędne w stosunku do zdarzenia z którym są grupowane oraz synchronizować z nim statusy. Zarówno dla zdarzeń przetwarzanych przez operatora jaki i automatycznie przetwarzanych przez system (w ramach playbooka) zmiana statusu głównego zdarzenia musi wymusić zmianę statusu pozostałych, przykładowo zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne. Na liście zdarzeń oraz w podglądzie każdego zdarzenia powinna się pojawić informacja o zdarzeniach do niego powiązanych.
81	Obsługiwane zdarzenia muszą zapewniać historyczność obejmującą wszystkie aktywności realizowane w ramach poszczególnych statusów. Aktywności muszą uwzględniać zarówno akcje realizowana w ramach samego systemu (m.in. zmiana priorytetu czy przekazanie zdarzenia innemu operatorowi) jak i akcje związane z interakcją z innymi systemami. Dodatkowo historia musi też zawierać wszelkie komentarze wpisywane przez operatorów.
82	Dla każdego obsługiwanego zdarzenia system powinien udostępniać automatyczny raport obejmujący wszystkie podjęte działania wraz z komentarzami operatorów.
83	W ramach obsługi zdarzeń system musi automatycznie porównywać wskaźniki kompromitacji zidentyfikowane w bieżącym zdarzeniu względem wszystkich wskaźników pozyskanych do tej pory w ramach dotychczasowej obsługi. Przykładowo jeżeli w obsługiwanym zdarzeniu znajduje się FQDN oraz HASH to system musi automatycznie je porównać z wszystkimi wskaźnikami typu FQDN oraz HASH zebranymi do tej pory w obsługiwanych zdarzeniach bez względu na to czy wskaźniki te zostały wpisane ręcznie czy zostały pozyskane automatycznie z innych systemów.
84	System powinien pozwalać, przy użyciu języków skryptowych ogólnie dostępnych (np. Python lub PowerShell), na skonfigurowanie nowych integracji z zewnętrznymi systemami oraz zapewnić dla tych systemów mechanizmy bezpiecznego zarządzania i przechowywania danych związanych z tymi integracjami, m.in. loginy, hasła oraz klucze API.
85	W ramach obsługi zdarzenia dla operatora powinien być dostępny dedykowany panel analityczny

	pozwalający mu na: a. podgląd aktywności zagrożonego zasobu na linii czasu, b. w przypadku zagrożenia sieciowego podgląd aktywności zarówno ofiary jak i celu ataku, c. w przypadku identyfikacji użytkownika podgląd jego aktywności na linii czasu, d. podgląd reguły korelacyjnej, która wygenerowała zdarzenie, e. w przypadku wykrytej techniki Mitre ATT@CK jej szczegółowy opis, f. listowanie podpiętych zdarzeń wraz z mechanizmami filtrowania po nich, g. gotowe i proste w użyciu filtry rozszerzajcie analizę zdarzeń o: • listę wszystkich zdarzeń pomiędzy celem a źródłem ataku w zadanym okresie czasowym, np.: godzinę przed oraz 2 godziny po, • listę wszystkich zdarzeń dotyczących źródła lub celu ataku w zadanym okresie czasowym, h. gotowe i proste w użyciu filtry rozszerzajcie analizę logów o: • listę wszystkich logów pomiędzy celem a źródłem ataku w zadanym okresie czasowym, • listę wszystkich logów dotyczących źródła lub celu ataku w zadanym okresie czasowym.
86	Dla zdarzeń w obsłudze system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: a. warunki powiadomień, o zdarzeń o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, o zdarzeń o przekroczonych czasach SLA o definiowalny okres, o zdarzeń ze zbliżającym się i definiowalnym terminem przekroczenia SLA, o zdarzeń, których priorytet osiągnął określoną wartość, o zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, o zdarzeń na których doszło do naruszenia bezpieczeństwa, o zdarzeń powstałych poprzez zdefiniowaną regułę korelacyjną, o zdarzeń realizujących zdefiniowaną usługę, o zdarzeń przetwarzających sklasyfikowane informację, o zdarzeń przetwarzanych na krytycznych zasobach, b. odbiorców powiadomień, w tym: o operatora, któremu zostało przydzielone zdarzenie, o właściciela zasobu na którym wystąpiło zdarzenie, o zespół obsługi, który odpowiada za obsługę zdarzeń, o właściciela usługi która jest realizowana na zasobie na którym wystąpiło zdarzenie, o podmiot zewnętrzny, jeżeli zdarzenie dotyczy zasobu obsługiwanego przez firmę zewnętrzną. c. kanały powiadomień, m.in. e-mail, sms, komunikator, d. zastosowanie mechanizmów grupowania: o grupowanie wielu powiadomień w jednej wiadomości, o ograniczenie liczby wierszy powiadomienia do określonej wartości.
87	System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im zdarzenia do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: a. utworzenia nowego zdarzenia z określonym priorytetem, b. utworzenia nowego zdarzenia na zasobie krytycznym, c. utworzenia nowego zdarzenia na zasobie realizującym zdefiniowaną usługę, d. utworzenie nowego zdarzenia na zasobie przetwarzającym dane osobowe, e. utworzenie nowego zdarzenia na podstawie zdefiniowanej reguły korelacyjnej, f. modyfikacji przydzielonego operatorowi zdarzania przez innego operatora, g. zamknięcia przydzielonego operatorowi zdarzania przez innego operatora, h. przejęcia przydzielonego operatorowi zdarzania przez innego operatora.
88	Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego: a. wybór raportu który ma zostać wysłany, b. zdefiniowanie jego tytułu, c. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny,

	d. możliwość ograniczenia cyklu do dni powszednich, e. określenie daty przesłania pierwszego raportu, f. możliwości ograniczenia okresu przez jaki raport będzie przesyłany, do: o zdefiniowanej daty końcowej, o określnej liczby raportów, g. określenie odbiorców raportu.
89	System musi umożliwiać obsługę podatności w ramach scenariuszy obsługi (playbook).
90	Importowane do systemu podatności muszą być przeanalizowane pod względem ryzyka jakie mogą wygenerować dla organizacji. W tym celu musi być dostępny mechanizm ich automatycznej priorytetyzacji bazujący na regułach, które wyznaczą dla podatności wymagających obsługi priorytet w oparciu o następujące parametry: a. strefę bezpieczeństwa w której została wykryta podatność, b. prawdopodobieństwo obecności intruza lub złośliwego oprogramowania w tej strefie, c. rodzaj zasobu którego dotyczy ta podatność, d. ważność tego zasobu dla organizacji, e. przetwarzane na tym zasobie informacje, np.: dane osobowe, f. usługi realizowane przez ten zasób, np.: DNS, g. wartość parametrów CVSS dla podatności, np.: „Confidentiality Impact" = High, h. poprawność konfiguracji zasobu na którym została wykryta podatność, np.: brak reguł wymuszenia złożoności haseł, a. szacowane prawdopodobieństwo przełamania zabezpieczeń ze zdefiniowanej strefy, która jest autoryzowana do dostępu do tego zasobu, np.: wysokie prawdopodobieństwa zagrożenia ze strefy Internet dla zasobu z wykrytą podatnością, który świadczy usługę w strefie Internet.
91	W systemie musi być dostępny predefiniowany zestaw reguł automatycznej priorytetyzacji wszystkich importowanych podatności oraz interfejs umożliwiający definiowanie własnych reguł umożliwiających zarówno zakwalifikowanie podatności do obsługi jaki i możliwość ich wyłączenia z obsługi w przypadku znikomego zagrożenia dla organizacji.
92	Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach: b. wyliczonym priorytecie podatności, c. aktualnym statusie obsługi, d. ważności zasobu na którym została wykryta, e. adresie IP tego systemu, f. parametrów SLA związanych z tym statusem, g. przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe, h. parametrach CVSS, np.: lista podatności których „Access Complexity (AC)" = „low" oraz „Access Vector (AV) = „Network".
93	System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień dla kadry zarządzającej obejmujących eskalacje oraz monitorowanie SLA. Szablony powinny uwzględniać powiadomienie kierownikom jednostek organizacyjnych w następujących sytuacjach: a. przekroczenia czasu reakcji o określony czas np.; o godzinę, b. możliwości przekroczenia czasu reakcji, np.: została godzina aby rozpocząć obsługę zdarzenia i uchronić się przed przekroczeniem czasu reakcji, c. przekroczenia czasu reakcji dla zdarzenia na zasobie przetwarzającym dane osobowe, d. przekroczenia czasu reakcji dla zdarzenia na zasobie krytycznym, e. przekroczenia czasu reakcji dla zdarzenia na zasobie realizującym krytyczną usługę, f. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów przetwarzających dane osobowe, g. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów krytycznych, h. przekroczenia czasu obsługi zdarzeń zakwalifikowanych jako incydent bezpieczeństwa, dotyczących zasobów realizujących krytyczną usługę, i. przekroczenia czasu reakcji dla podatności na zasobie przetwarzającym dane osobowe, j. przekroczenia czasu reakcji dla podatności na zasobie krytycznym,

	k. przekroczenia czasu reakcji dla podatności na zasobie realizującym krytyczną usługę,
94	Dla obsługiwanych podatności system musi być wyposażony w graficzny interfejs umożliwiający definiowanie własnych powiadomień obejmujących: a. warunki powiadomień, o podatności o przekroczonych czasach SLA definiowalnych dla wszystkich statusów obsługi, o podatności o przekroczonych czasach SLA o definiowalny okres, o podatności ze zbliżającym się i definiowalnym terminem przekroczenia SLA, o podatności, których priorytet osiągnął określoną wartość, o zdarzeń realizujących zdefiniowaną usługę, o zdarzeń przetwarzających sklasyfikowane informację, o zdarzeń przetwarzanych na krytycznych zasobach, b. odbiorców powiadomień, w tym: o operatora, któremu została przydzielona podatność, o właściciela zasobu na którym wystąpiła podatność, o zespół obsługi, który odpowiada za obsługę podatności, o właściciela usługi na która jest realizowana na zasobie na którym wystąpiła podatność, o podmiot zewnętrzny, jeżeli zdarzenie dotyczy podatności na zasobie obsługiwanym przez firmę zewnętrzną. c. kanały powiadomień, m.in. e-mail, sms, komunikator, d. zastosowanie mechanizmów grupowania: o grupowanie wielu powiadomień w jednej wiadomości, o ograniczenie liczby wierszy powiadomienia do określonej wartości.
95	System powinien posiadać gotowe szablony powiadomień pozwalające na wysyłanie powiadomień jego operatorom w przypadku gdy system przydzieli im podatności do obsługi. Szablony powinny uwzględniać powiadomienie operatorów w następujących sytuacjach: a. przydzielenia nowej podatności do obsługi z określonym priorytetem, b. przydzielenia nowej podatności do obsługi na zasobie krytycznym, c. przydzielenia nowej podatności do obsługi na zasobie realizującym zdefiniowaną usługę, d. przydzielenia nowej podatności do obsługi na zasobie przetwarzającym dane osobowe, e. modyfikacji przydzielonej operatorowi podatności przez innego operatora, f. zamknięcia przydzielonej operatorowi podatności przez innego operatora, g. przejęcia przydzielonej operatorowi podatności przez innego operatora.
96	Dla kadry zarządzającej system musi umożliwiać automatyczną dystrybucję raportów poprzez pocztę elektroniczną. System musi umożliwiać dostęp do kreatora umożliwiającego: a. wybór raportu który ma zostać wysłany, b. zdefiniowanie jego tytułu, c. zdefiniowanie cyklu w jakim ma zostać wysyłany, np.: tygodniowy lub miesięczny, d. możliwość ograniczenia cyklu do dni powszednich, e. określenie daty przesłania pierwszego raportu, f. określenie okresu przez jaki będą one przesyłane, poprzez: o zdefiniowanie daty końcowej, o bez daty końcowej, o określenie liczby raportów, e. określenie odbiorców raportu.
95	System powinien w formie graficznej prezentować podsumowanie aktualnego stanu bezpieczeństwa organizacji w postaci tzw. „Dashboard”, tj. dostosuje zakres i prezentacje danych do potrzeb zalogowanego użytkownika.
	System musi pozwalać na tworzenie dedykowanych dashbord’ów obejmujących: a. zestaw wykresów dla bieżącego użytkownika, b. zestaw wykresów dla wybranego użytkownika, c. zestaw wykresów dla roli zdefiniowanej w systemie, np.: administratorzy systemu, d. zestaw wykresów dla wybranego zespołu obsługi, np.: operatorzy SOC.

96	System musi zapewniać zestaw predefiniowanych dashbord'ów obejmujących następujące wykresy: a. wykres przedstawiający status klasyfikacji zdarzeń, który obejmuje: • ilość zdarzeń nowych i niesklasyfikowanych, • ilość zdarzeń sklasyfikowanych jako incydenty bezpieczeństwa, • ilość zdarzeń sklasyfikowanych jako fałszywe alarmy, b. wykres przedstawiający skale zagrożeń, który obejmuje: • ilość zasobów krytycznych na których są obsługiwane zdarzenia, • ilość zasobów niekrytycznych na których są obsługiwane zdarzenia, c. wykres przedstawiający źródła zagrożeń, który obejmuje: • ilość nowych zdarzeń dotyczących użytkowników, • ilość podjętych zdarzeń dotyczących użytkowników, • ilość nowych zdarzeń dotyczących zasobów, • ilość podjętych zdarzeń dotyczących zasobów, d. wykres przedstawiający poziom zagrożeń, który obejmuje: • ilość nowych zdarzeń w podziale na priorytety, • ilość podjętych zdarzeń w podziale na priorytety, e. wykres przedstawiający czas obsługi zagrożeń, który obejmuje: • ilość zdarzeń zarejestrowanych w bieżącym dniu, • ilość zdarzeń zarejestrowanych w ostatnim tygodniu, • ilość zdarzeń zarejestrowanych w ostatnim miesiącu, • ilość zdarzeń zarejestrowanych wcześniej niż w ostatnim miesiącu, f. wykres przedstawiający zagrożone usługi, który obejmuje: • ilość usług krytycznych zagrożonych przez obsługiwane zdarzenia, • ilość pozostałych usług zagrożonych przez obsługiwane zdarzenia, g. wykres przedstawiający zagrożone dane, który obejmuje: • ilość nowych zdarzeń dotyczących zasobów krytycznych przetwarzających sklasyfikowane informacje, • ilość podjętych zdarzeń dotyczących zasobów krytycznych przetwarzających sklasyfikowane informacje, • ilość nowych zdarzeń dotyczących pozostałych zasobów przetwarzających sklasyfikowane informacje, • ilość podjętych zdarzeń dotyczących pozostałych zasobów przetwarzających sklasyfikowane informacje, h. wykres przedstawiający skale podatności, który obejmuje: • ilość zasobów krytycznych na których są obsługiwane podatności, • ilość zasobów niekrytycznych na których są obsługiwane podatności, i. wykres przedstawiający czas obsługi podatności, który obejmuje: • ilość podatności zarejestrowanych w bieżącym dniu, • ilość podatności zarejestrowanych w ostatnim tygodniu, • ilość podatności zarejestrowanych w ostatnim miesiącu, • ilość podatności zarejestrowanych wcześniej niż w ostatnim miesiącu, j. wykres przedstawiający wagę podatności, który obejmuje: • ilość nowych podatności w podziale na priorytety, • ilość podjętych podatności w podziale na priorytety,
97	Nawigacja w ramach „Dashbordu" musi wspierać opcję „Drill down" w następującym zakresie: a. „kliknięcie" wartości prezentowanej na wykresie dotyczącej zdarzeń w obsłudze musi przenieść operatora systemu do listy tych zdarzeń z ustawionym automatycznie filtrem pozwalającym pokazać te same wartości których dotyczy wykres, b. „kliknięcie" wartości prezentowanej na wykresie dotyczącej podatności musi przenieść operatora systemu do listy tych podatności z ustawionym automatycznie filtrem pozwalającym pokazać te same wartości których dotyczy wykres, c. „kliknięcie" wartości prezentowanej na wykresie dotyczącej użytkowników (UBA) musi przenieść operatora systemu do listy tych użytkowników z ustawionym automatycznie filtrem pozwalającym

	pokazać te same wartości których dotyczy wykres, d. „kliknięcie" wartości prezentowanej na wykresie dotyczącej zasobów (EBA) musi przenieść operatora systemu do listy tych zasobów z ustawionym automatycznie filtrem pozwalającym pokazać te same wartości których dotyczy wykres, e. „kliknięcie" wartości prezentowanej na wykresie dotyczącej wybranych zdarzeń korelacyjnych musi przenieść operatora systemu do listy prezentującej te zdarzenia z ustawionym automatycznie filtrem pozwalającym pokazać te same wartości których dotyczy wykres, f. „kliknięcie" wartości prezentowanej na wykresie dotyczącej wybranych logów musi przenieść operatora systemu do listy prezentującej te logi z ustawionym automatycznie filtrem pozwalającym pokazać te same wartości których dotyczy wykres.
98	Rozwiązania może być dostarczone w ramach odrębnych rozwiązań, jednakże muszą być one zintegrowane w sposób umożliwiający spełnienie wszystkich wymagań z poziomu jednej konsoli.
99	Dostarczone rozwiązanie nie może działać w oparciu o oprogramowanie otwarte (ang: open source) w następującym zakresie funkcjonalnym: składowanie, parsowanie, korelacja logów, algorytmy uczenia maszynowego, analizę zachowania użytkowników i zasobów (UEBA), gdzie producent lub producenci oprogramowania muszą być wyłącznym właścicielem całości kodu oraz ten kod źródłowy musi być zamknięty.
100	W celach weryfikacji zgodności produktu z wymaganiami, musi być on dodatkowo oferowany przez autoryzowanego dystrybutora dostarczającego produkty z obszaru cyberbezpieczeństwa na rynku polskim, który w przypadku jakichkolwiek wątpliwości zamawiającego związanych z wymaganymi funkcjonalności będzie mógł je potwierdzić lub im zaprzeczyć.
101	W związku z tym, że obsługa systemu ma objąć także użytkowników nie posługujących się biegle językiem angielskim interfejs użytkownika musi umożliwiać obsługę w języku polskim lub posiadać możliwość wgrania plików językowych tłumaczących interfejs na język polski.
102	Zamawiający na tym etapie nie jest w stanie zmierzyć ilości danych przekazywanych do systemu, tj. EPS (Events Per Second) oraz nie zna wymagań związanych z architekturą proponowanego rozwiązania, dlatego oferowana licencje nie może nakładać limitów w tym zakresie.
103	Produkt musi umożliwiać równoczesną pracę co najmniej 4 operatorów oraz obsługiwać 500 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.
104	System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.
105	Funkcjonowanie rozwiązania musi umożliwiać konfigurację „on-premise", w której wszystkie funkcjonalności oraz przetwarzanie danych będzie się odbywać całkowicie w infrastrukturze zamawiającego, zapewniając tym samym możliwość konfiguracji systemu w strefie odseparowanej od sieci Internet.
106	System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), Redhat/Oracle Linux (minimum 7.x).
107	Dopuszczalne jest dostarczenie rozwiązania jako tzw. wirtualnego appliance pod warunkiem że obraz appliance jest udostępniany do pobrania przez producenta dostarczonego rozwiązania na jego oficjalnej stronie internetowej w postaci utwardzonego rozwiązania, łącznie z dedykowanym systemem operacyjnym, dla którego Producent regularnie dostarcza aktualizacje, w tym poprawki bezpieczeństwa.
108	Dostarczone rozwiązanie musi być objęte 12 miesięcznym wsparciem producenta lub producentów. 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).

Identyfikator postępowania na miniPortalu:

34870095-8b8c-4538-99a1-b5f330400d4c