



Cyberbezpieczny Samorząd

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

Nazwa zamówienia: Dostawa serwera oraz oprogramowania SIEM.

Numer referencyjny: ZF.272.1.21.2025

Załączniki do specyfikacji warunków zamówienia:

1. Szczegółowy opis przedmiotu zamówienia.
2. Widok interaktywnego formularza ofertowego.
3. Formularz rzeczowo – finansowy.
4. Oświadczenie o niepodleganiu wykluczeniu z postępowania.
5. Projektowane postanowienia umowy.

Rzeszów 31.12.2025



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

§ 1. Zamawiający

Powiat Rzeszowski
35-959 Rzeszów, ul. Grunwaldzka 15.

Postępowanie prowadzi:

Starostwo Powiatowe w Rzeszowie,
35-959 Rzeszów, ul. Grunwaldzka 15
telefon: 17 230 07 70;
e-mail: zampubliczne@powiat.rzeszowski.pl
dni i godziny pracy: poniedziałek - piątek, 7:30 – 15:30.

§ 2. Strona internetowa prowadzonego postępowania

1. Postępowanie prowadzone będzie przy użyciu **Platformy e-Zamówienia**, która jest dostępna pod adresem: <https://ezamowienia.gov.pl>.
2. Strona internetowa prowadzonego postępowania:
<https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-8cc4b64d-ee48-4914-a7ff-4b74f2f6bcab>
Identyfikator postępowania na platformie e-Zamówienia:
ocds-148610-8cc4b64d-ee48-4914-a7ff-4b74f2f6bcab
3. Zmiany i wyjaśnienia treści specyfikacji warunków zamówienia, zwanej dalej SWZ, oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem udostępniane będą na stronie internetowej prowadzonego postępowania wskazanej w ust. 2.

§ 3. Tryb udzielenia zamówienia

Zamówienie zostanie udzielone w trybie **podstawowym** zgodnie z **art. 275 pkt 1** ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2024 r. poz.1320 ze zm.), zwanej dalej ustawą pzp.

§ 4. Negocjacje

Najkorzystniejsza oferta zostanie wybrana bez przeprowadzenia negocjacji.

§ 5. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest dostawa, instalacja i wdrożenie oprogramowania SIEM (Security Information and Event Man) wraz z serwerem do SIEM (Security Information and Event Managment) w ramach projektu pn.: „Zwiększenie poziomu bezpieczeństwa cyfrowego Powiatu Rzeszowskiego oraz jego jednostek podległych” współfinansowanego przez Unię Europejską w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny samorząd” o numerze FERC.02.02-CS.01-001/23.
Oznaczenie wg Wspólnego Słownika Zamówień (CPV):
48821000-9 serwery sieciowe
48000000-8 pakiety oprogramowania i systemy informatyczne.
2. Zamawiający nie dopuszcza składania ofert częściowych. Przedmiot zamówienia obejmuje dostawę serwera wraz z oprogramowaniem do zarządzania informacjami i zdarzeniami bezpieczeństwa. Zamówienie nie jest podzielone na części, ponieważ elementy są ze sobą powiązane i zależą od siebie. Aby umożliwić spójne funkcjonowanie całego systemu, jego instalacje i wdrożenie niezbędne jest aby serwer oraz oprogramowanie dostarczył jeden wykonawca. Brak podziału zamówienia na części, biorąc pod uwagę jego wielkość i zakres, nie ogranicza konkurencji i nie ogranicza możliwości ubiegania się o zamówienie podmiotom z sektora MŚP.
3. Miejsce dostawy: Starostwo Powiatowe w Rzeszowie, 35-959 Rzeszów, ul. Grunwaldzka 15.
4. Wymagania techniczne oraz warunki realizacji przedmiotu zamówienia zostały określone w załącznikach: „Szczegółowy opis przedmiotu zamówienia” oraz „Projektowane postanowienia umowy”.



§ 6. Termin wykonania zamówienia

Zamówienie należy zrealizować w terminie **do 90 dni** od dnia podpisania umowy.

§ 7. Warunki udziału w postępowaniu

Zamawiający nie określa warunków udziału w postępowaniu.

§ 8. Podmiotowe środki dowodowe

Zamawiający nie wymaga złożenia podmiotowych środków dowodowych.

§ 9. Wymagania dotyczące wadium

Zamawiający nie wymaga od wykonawców wniesienia wadium.

§ 10. Komunikacja z wykonawcami

1. Komunikacja w postępowaniu między zamawiającym a wykonawcą odbywa się za pośrednictwem Platformy e-Zamówienia, która dostępna jest pod adresem: <https://ezamowienia.gov.pl> oraz poczty elektronicznej.
2. Korzystanie z Platformy e-Zamówienia jest bezwzględnie wymagane dla przekazywania oferty oraz załączników do oferty.
3. Wykonawca zamierzający wziąć udział w postępowaniu, musi posiadać konto podmiotu „Wykonawca” na Platformie e-Zamówienia. Korzystanie z Platformy e-Zamówienia jest bezpłatne. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa Regulamin Platformy e-Zamówienia, dostępny na stronie internetowej <https://ezamowienia.gov.pl> oraz informacje zamieszczone w zakładce „Centrum Pomocy”.
4. Komunikacja w postępowaniu, z wyłączeniem składania ofert, odbywa się za pośrednictwem poczty elektronicznej (adres zamawiającego: zampubliczne@powiat.rzeszowski.pl) lub za pośrednictwem „Formularzy do komunikacji” dostępnych w zakładce „Formularze”. Za pośrednictwem poczty elektronicznej lub „Formularzy do komunikacji”, odbywa się w szczególności przekazywanie oświadczeń, wezwań, zawiadomień a także zadawanie pytań. Składanie ofert odbywa się za pośrednictwem zakładki „Oferty/wnioski”, widocznej w podglądzie postępowania po zalogowaniu się na konto wykonawcy.
5. Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji” wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
6. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa Regulamin Platformy e-Zamówienia.
7. W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego pod numerem telefonu (22) 458 77 99 lub drogą elektroniczną poprzez formularz udostępniony na stronie internetowej <https://ezamowienia.gov.pl> w zakładce „Zgłoś problem”.
8. Jeżeli zamawiający lub wykonawca przekazują oświadczenia, wezwania oraz zawiadomienia lub zadają pytania za pośrednictwem poczty elektronicznej, każda ze stron na żądanie drugiej strony niezwłocznie potwierdza fakt ich otrzymania.
9. Osoby uprawnione do komunikowania się z wykonawcami:
Adam Janicki, Dorota Machej; e-mail: zampubliczne@powiat.rzeszowski.pl.
10. Interaktywna instrukcja obrazująca sposób komunikacji z wykorzystaniem Platformy e-Zamówienia dostępna jest na stronie internetowej <https://ezamowienia.gov.pl/pl/komponent-edukacyjny/> w zakładce „Komunikacja w postępowaniu”.



§ 11. Forma dokumentów i sposób podpisywania

1. Ofertę (formularz ofertowy i formularz rzeczowo - finansowy), oświadczenie, o którym mowa w art. 125 ust.1 ustawy pzp oraz pełnomocnictwo, należy sporządzić w formie elektronicznej lub postaci elektronicznej i podpisać kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
2. Dokumenty elektroniczne, o których mowa w ust.1 przekazuje się jako załączniki.
3. Informacje, oświadczenia lub dokumenty, inne niż wymienione w ust.1 przekazywane w postępowaniu, sporządza się w postaci elektronicznej i przekazuje się jako załącznik lub jako tekst wpisany bezpośrednio do wiadomości e-mail lub w treści „Formularza do komunikacji”.
4. Dokumenty elektroniczne powinny być sporządzone w formatach danych określonych w przepisach rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773). Rekomendowane formaty danych:
 - dla formularza ofertowego: .pdf,
 - dla oświadczeń i dokumentów składanych wraz z ofertą: .pdf, .odt, .doc, .docx, .jpg,
 - dla plików poddanych kompresji: .zip lub .7Z.
5. Sposób sporządzenia i przekazywania dokumentów elektronicznych musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 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) w szczególności z uwzględnieniem poniższych zasad:
 - 1) W przypadku gdy dokumenty potwierdzające umocowanie do reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego lub podwykonawcy, zwane dalej „dokumentami potwierdzającymi umocowanie do reprezentowania”, zostały wystawione przez upoważnione podmioty inne niż wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia lub podwykonawca, zwane dalej „upoważnionymi podmiotami”, jako dokument elektroniczny, przekazuje się ten dokument.
 - 2) W przypadku gdy dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej dokonuje odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia lub podwykonawca, w zakresie dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą.
 - 3) Pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
 - 4) W przypadku gdy pełnomocnictwo, zostało sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej dokonuje mocodawca.
 - 5) Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej może dokonać również notariusz.
 - 6) Przez cyfrowe odwzorowanie z dokumentem w postaci papierowej, należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.



Cyberbezpieczny Samorząd

6. W przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty, kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

§ 12. Opis sposobu przygotowania i składania oferty

1. Wykonawca może złożyć jedną ofertę.
2. Oferta musi być sporządzona pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej, i opatrzona kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
3. Ofertę podpisuje osoba uprawniona do reprezentacji wykonawcy zgodnie z formą reprezentacji wykonawcy określoną w rejestrze lub innym dokumencie, właściwym dla danej formy organizacyjnej lub upoważniony przedstawiciel wykonawcy.
4. Ofertę należy sporządzić w języku polskim wykorzystując interaktywny „Formularz ofertowy” udostępniony przez zamawiającego na Platformie e-Zamówienia i zamieszczony w podglądzie postępowania w zakładce „Informacje podstawowe”. Dokumenty sporządzone w języku obcym należy złożyć wraz z tłumaczeniem na język polski.
5. Zalogowany wykonawca używając przycisku „Wypełnij” widocznego pod „Formularzem ofertowym” zobowiązany jest do zweryfikowania poprawności danych automatycznie pobranych przez system z jego konta i uzupełnienia pozostałych informacji dotyczących wykonawcy/wykonawców wspólnie ubiegających się o udzielenie zamówienia.

6. Następnie wykonawca powinien pobrać „Formularz ofertowy”, zapisać go na dysku swojego komputera, uzupełnić pozostałymi danymi wymaganymi przez zamawiającego i ponownie zapisać na dysku swojego komputera oraz podpisać odpowiednim rodzajem podpisu elektronicznego, zgodnie z ust. 10.

UWAGA: Nie należy zmieniać nazwy pliku nadanej przez Platformę e-Zamówienia. Zapisany „Formularz oferty” należy otwierać i edytować w programie Adobe Acrobat Reader.

7. Wykonawca składa ofertę za pośrednictwem zakładki „Oferty/wnioski”, widocznej w podglądzie postępowania po zalogowaniu się na konto wykonawcy. Po wybraniu przycisku „Złóż ofertę” system prezentuje okno składania oferty umożliwiające przekazanie dokumentów elektronicznych, w którym znajdują się dwa pola „przeciągnij i upuść” służące do dodawania plików.
8. Wykonawca dodaje wybrany z dysku i uprzednio podpisany „Formularz ofertowy” w pierwszym polu „Wypełniony formularz ofertowy”. W kolejnym polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę” wykonawca dodaje pozostałe pliki stanowiące ofertę lub składane wraz z ofertą.
9. Jeżeli wraz z ofertą składane są dokumenty zawierające tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2022 r. poz.1233 ze zm.), wykonawca w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa”. Wykonawca zobowiązany jest, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji. Zaleca się, aby uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa było sformułowane w sposób umożliwiający jego udostępnienie. Zastrzeżenie przez wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane jako bezskuteczne ze względu na zaniechanie przez wykonawcę podjęcia niezbędnych działań w celu utrzymania poufności objętych klauzulą informacji, zgodnie z postanowieniami art. 18 ust. 3 ustawy pzp. Zarówno załącznik stanowiący tajemnicę przedsiębiorstwa jak i uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa należy dodać w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”.



Cyberbezpieczny Samorząd

10. „Formularz ofertowy” podpisuje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Rekomendowanym wariantem podpisu jest typ wewnętrzny. Podpis „Formularza ofertowego” wariantem podpisu w typie zewnętrznym również jest możliwy, ale wówczas powstały oddzielny plik podpisu dla tego formularza należy załączyć w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”.

UWAGA:

W związku ze zmianami po stronie Profilu Zaufanego obecnie nie ma możliwości podpisywania „podpisem zaufanym” interaktywnego formularza ofertowego, tak jak do tej pory. Aby podpisać formularz ofertowy pobrany z Platformy e-Zamówienia należy po pobraniu i wypełnieniu formularza zapisać go w wersji nieedytowalnej i następnie podpisać „podpisem zaufanym”.

W razie problemów z podpisem zaufanym pomoc można uzyskać telefonując pod numer: (42) 253 54 50 lub pisząc na adres e-mail: pz-pomoc@coi.gov.pl lub epuap-pomoc@coi.gov.pl.

W sprawach związanych z formularzem ofertowym pomoc można uzyskać kontaktując się z Infolinią Platformy e-Zamówienia pod numerem telefonu: (22) 458 77 99.

11. Pozostałe dokumenty wchodzące w skład oferty lub składane wraz z ofertą, podpisane kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być opatrzone podpisem typu zewnętrznego lub wewnętrznego.
12. Maksymalny łączny rozmiar plików stanowiących ofertę lub składanych wraz z ofertą to 250 MB.
13. Wykonawca może przed upływem terminu składania ofert wycofać ofertę. Wykonawca wycofuje ofertę w zakładce „Oferty/wnioski” używając przycisku „Wycofaj ofertę”.
14. Zamawiający nie przewiduje możliwości złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty.
15. Zamawiający nie dopuszcza składania ofert wariantowych.
16. Do oferty należy dołączyć:
- 1) **Formularz rzeczowo – finansowy** - wg wzoru stanowiącego załącznik do SWZ.
 - 2) **Oświadczenie o niepodleganiu wykluczeniu z postępowania**, o którym mowa w art. 125 ust. 1 ustawy pzp - wg wzoru stanowiącego załącznik do SWZ, odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia.
 - 3) **Odpis lub informację** z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru, w celu potwierdzenia, że osoba działająca w imieniu wykonawcy jest umocowana do jego reprezentowania.
Wykonawca nie jest zobowiązany do złożenia ww. dokumentów, jeżeli zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, **o ile wykonawca wskazał dane umożliwiające dostęp do tych dokumentów.**
 - 4) **Pełnomocnictwo** lub inny dokument potwierdzający umocowanie do reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia - **w przypadku reprezentowania wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia przez pełnomocnika.** Pełnomocnictwo musi być złożone w oryginale w takiej samej formie, jak składana oferta. Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego zgodnie z art. 97 § 2 ustawy z dnia 14 lutego 1991 r. - Prawo o notariacie (Dz.U. z 2024 r. poz.1001), które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie pisemnej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez pełnomocnika, któremu udzielono przedmiotowego pełnomocnictwa.
17. Interaktywna instrukcja obrazująca sposób składania oferty z wykorzystaniem Platformy e-Zamówienia dostępna jest na stronie internetowej https://ezamowienia.gov.pl/pl/komponent-edukacyjny/w_zakladce_oferty_wnioski_i_prace_konkursowe.





§ 12a. Oferta wspólna

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia.
2. W przypadku, o którym mowa w ust. 1, wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
3. Przepisy dotyczące wykonawcy stosuje się odpowiednio do wykonawców wspólnie ubiegających się o udzielenie zamówienia.
4. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenie, o którym mowa w art. 125 ust. 1 ustawy pzp, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia każdego z wykonawców oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
5. Jeżeli zostanie wybrana oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia, zamawiający może zażądać przed zawarciem umowy w sprawie zamówienia publicznego przedłożenia kopii umowy regulującej współpracę tych wykonawców.

§ 13. Termin składania ofert

Ofertę wraz z wymaganymi załącznikami należy złożyć w terminie **do 15.01.2026 r. do godz.9:00**.

§ 14. Termin otwarcia ofert

1. Otwarcie ofert nastąpi **15.01.2026 r. o godz.9:10**.
2. Otwarcie ofert nastąpi przy użyciu systemu **Platforma e-Zamówienia**, w przypadku awarii tego systemu, która spowoduje brak możliwości otwarcia ofert w terminie określonym w ust.1, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
3. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
4. Niezwłocznie po otwarciu ofert Zamawiający udostępni na stronie internetowej prowadzonego postępowania informacje, o których mowa w art. 222 ust. 5 ustawy pzp.

§ 15. Termin związania ofertą

Wykonawca jest związany ofertą do **13.02.2026 r.**

§ 16. Podstawy wykluczenia

1. Zamawiający, na podstawie art. 108 ust.1 ustawy pzp, wykluczy z postępowania, z zastrzeżeniem art. 110 ust.2 ustawy pzp, wykonawcę:
 - 1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
 - a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 2025 r., poz.383) zwanej dalej Kodeksem karnym,
 - b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
 - c) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz.U. z 2024 r. poz.1488 ze zm.) lub w art. 54 ust. 1-4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2025 r. poz.907 ze zm.),
 - d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
 - e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,



Cyberbezpieczny Samorząd

- f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz.U. z 2025 r. poz.1567),
 - g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
 - h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej
 - lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;
- 2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;
 - 3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
 - 4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
 - 5) jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2024 r. poz.1616 ze zm.), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;
 - 6) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 ustawy pzp, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.
2. Zamawiający, na podstawie art.109 ust.1 pkt 4 ustawy pzp, wykluczy z postępowania wykonawcę: w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.
 3. Zamawiający, na podstawie art.7 ust.1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2025 r. poz.514), zwanej dalej ustawą sankcyjną, wykluczy z postępowania wykonawcę:
 - 1) wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy sankcyjnej;
 - 2) którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2025 r. poz.644) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy sankcyjnej;

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

§ 17. Sposób obliczenia ceny

1. W cenie wykonawca zobowiązany jest uwzględnić wszystkie składniki i koszty mające wpływ na jej wysokość uwzględniając informacje i wymogi zawarte w szczegółowym opisie przedmiotu zamówienia.
2. Cenę oferty należy podać w złotych polskich z dokładnością do dwóch miejsc po przecinku.
3. Wykonawca podaje cenę oferty brutto, z uwzględnieniem kwoty podatku od towarów i usług VAT, w „Formularzu ofertowym” (pkt.VIII. Kryteria oceny ofert). Cenę oferty należy wyliczyć na podstawie „Formularza rzeczowo – finansowego”, który stanowi integralną część oferty. Wypełniony „Formularz rzeczowo – finansowy” należy złożyć wraz z „Formularzem ofertowym”. W przypadku rozbieżności pomiędzy kwotą wskazaną w „Formularzu ofertowym” a kwotą wskazaną w „Formularzu rzeczowo – finansowym”, jako poprawna zostanie przyjęta kwota wynikająca z „Formularza rzeczowo – finansowego”.
4. Jeżeli wybór oferty prowadził będzie do powstania u zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. z 2025 r. poz.775 ze zm.), wykonawca ma obowiązek w ofercie: poinformowania zamawiającego, że wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego; wskazania nazwy (rodzaju) towaru, którego dostawa będzie prowadziła do powstania obowiązku podatkowego; wskazania wartości towaru objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku; wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.
5. Wszelkie rozliczenia z zamawiającym będą odbywać się wyłącznie w złotych polskich.

§ 18. Opis kryteriów oceny ofert, wraz z podaniem wag tych kryteriów, i sposobu oceny ofert

1. Przy ocenie ofert i wyborze najkorzystniejszej oferty, zamawiający będzie się kierował kryterium ceny.
2. Za najkorzystniejszą zostanie uznana ta z ofert niepodlegających odrzuceniu, której cena będzie najniższa lub oferta, która będzie jedyną ofertą złożoną w postępowaniu niepodlegającą odrzuceniu.

§ 19. Projektowane postanowienia umowy

Projektowane postanowienia umowy określone zostały w załączniku „Projektowane postanowienia umowy”.

§ 20. Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

Zawarcie umowy nastąpi w trybie i terminie ustalonym między stronami.

§ 21. Informacje dotyczące zabezpieczenia należytego wykonania umowy

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

§ 22. Pouczenie o środkach ochrony prawnej przysługujących wykonawcy

1. Środki ochrony prawnej przysługują wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy pzp.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską





Cyberbezpieczny Samorząd

2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 ustawy pzp, oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Zasady wnoszenia środków ochrony prawnej określa Dział IX ustawy pzp (Art. 505 – 590) „Środki ochrony prawnej”.

§ 23. Informacje uzupełniające

1. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
2. Zamawiający nie przewiduje aukcji elektronicznej.

§ 24. Klauzula informacyjna

Na podstawie art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L z 2016 r. Nr 119, str. 1), dalej „RODO”, informuję, że:

- 1) Administratorem Pani/Pana danych osobowych jest Starostwo Powiatowe w Rzeszowie, ul. Grunwaldzka, 15, 35 – 959 Rzeszów, które realizuje zadania Starosty Rzeszowskiego oraz Zarządu Powiatu. Kontakt telefoniczny: 17 23 00 651, kontakt e-mail: starostwo@powiat.rzeszowski.pl.
- 2) W zakresie dotyczącym ochrony danych osobowych może Pani/Pan kontaktować się pisemnie z Inspektorem Ochrony Danych pod adresem: ul. Grunwaldzka 15, 35 – 959 Rzeszów, lub za pomocą adresu e-mail: rodo@powiat.rzeszowski.pl.
- 3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem;
- 4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy pzp;
- 5) Pani/Pana dane osobowe będą przechowywane, przez okres określony zgodnie z Rozporządzeniem 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 (Dz.U. z 2011 r. Nr 14 poz.67 ze zm.);
- 6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy pzp;
- 7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- 8) posiada Pani/Pan:
 - a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących,
 - b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (*Skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą pzp oraz nie może naruszać integralności protokołu oraz jego załączników.*),
 - c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO (*Prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.*),
 - d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
- 9) nie przysługuje Pani/Panu:



Cyberbezpieczny Samorząd

- a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,
- b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
- c) 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.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

A.1. Wymagania ogólne

Oferowany serwer i oprogramowanie muszą spełniać następujące warunki:

1. Oprogramowanie i serwer muszą pochodzić z legalnego kanału dystrybucji producenta, a korzystanie przez zamawiającego z dostarczonego serwera i oprogramowania nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, nigdy wcześniej nie instalowane i aktywowane na innym urządzeniu.
3. Wykonawca zobowiązany jest dostarczyć klucze licencyjne lub dokumenty potwierdzające prawo do korzystania z dostarczonego pakietu oprogramowania przez zamawiającego. Potwierdzeniem legalności systemu operacyjnego może być dokument pochodzący od producenta serwera lub wykonawcy (np. oświadczenie, certyfikat OEM, dokument licencyjny, faktura lub inny równoważny dokument), zgodny z obowiązującym modelem licencjonowania producenta oprogramowania.
4. Wszystkie licencje muszą być przeznaczone do użytku na terenie Rzeczypospolitej Polskiej.
5. Dostarczona licencja na oprogramowanie SIEM nie może wprowadzać dodatkowych, licencyjnych ograniczeń w zakresie wielkości przechowywanych danych ani funkcjonalności wyszukiwania informacji w zgromadzonych danych, poza ograniczeniami wynikającymi z parametrów technicznych infrastruktury Zamawiającego.
6. Wszystkie dostarczone licencje muszą być dostarczone w formie bezterminowej (wieczystej).
7. Wykonawca zobowiązany jest do przestrzegania ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2025 r. poz.24).
8. Serwer musi być:
 - 1) fabrycznie nowy, nieużywany przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu poprawnej pracy,
 - 2) wyprodukowany nie wcześniej niż w 2024 roku,
 - 3) dostarczony wraz z dokumentacją zawierającą: instrukcje obsługi, karty gwarancyjne (w przypadku gdy producent nie stosuje dokumentacji papierowej, wykonawca zobowiązany jest dostarczyć dokumentację w postaci elektronicznej lub wskazać adres strony internetowej do jej pobrania),
 - 4) oznakowany w taki sposób, aby możliwa była identyfikacja modelu i producenta oraz dostarczony w oryginalnym opakowaniu,
9. Serwer musi posiadać możliwość sprawdzenia konfiguracji po podaniu numeru seryjnego na stronie producenta lub dystrybutora.
10. Serwer musi posiadać oznakowanie CE zgodnie z wymogami określonymi w Rozporządzeniu Ministra Rozwoju z dnia 2 czerwca 2016 r. w sprawie wymagań dla sprzętu elektrycznego (Dz. U. z 2016 r. poz. 806).
11. Okres gwarancji dla serwera: 24 miesiące od daty odbioru przedmiotu umowy.
Jeżeli wykonawca oferuje gwarancję wynoszącą więcej niż 24 miesiące, w „Formularzu rzeczowo-finansowym” w wierszu „okres gwarancji”, należy wpisać oferowany okres gwarancji.
Wymagania w zakresie gwarancji: **Szczegółowe wymagania w zakresie gwarancji i wsparcia technicznego określone zostały w „projektowanych postanowieniach umowy”.**

A.2. Opis infrastruktury Zamawiającego wymagającej monitorowania:

System SIEM będący przedmiotem zamówienia, musi zbierać logi/dane z poniższych systemów Zamawiającego (źródła logów) udostępnionych przez Zamawiającego:

Rodzaj usługi lub urządzenia	Liczba urządzeń / nodów będących źródłami logów
Active Directory (liczba serwerów)	4
Windows Server (liczba serwerów)	86



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

FFLinux Server (liczba serwerów)	7
Stacje robocze (Windows/Linux)	208
DNS, DHCP	9 (dot. powiązań np. z AD)
Systemy bezpieczeństwa np.: serwer systemu antywirusowego, Web Application Firewall, NAC, DLP	2 (AIM / GPO)
Serwer poczty, system antyspamowy	https://poczta.powiat.rzeszowski.pl/roundcube/
Centralny Firewall / UTM	3 urządzenia logiczne, 6 urządzenia fizyczne
Pomocniczy Firewall / UTM	4 urządzenia fizyczne i logiczne
IPS / IDS	7
VPN	6 (site to site)
Przełączniki sieci LAN, punkty dostępowe WiFi	max. 42

B. Wymagania dla oprogramowania SIEM.

B.1. Wymagania systemowe:

- 1) Liczba obsługiwanych zdarzeń na sekundę (EPS): min. 5 000.
- 2) Przechowywanie, zarządzanie logami: min. 24 miesiące.
- 3) Liczba obsługiwanych urządzeń (adresów IP) min. 300.
- 4) Liczba zapisu zdarzeń na dobę: min. 10 000 MB.
- 5) System zbierania logów musi wspierać hiperwizory: min. Microsoft Hyper-V.
- 6) Zamawiający nie dopuszcza rozwiązań typu open source, które nie posiadają komercyjnego wsparcia producenta, gwarancji SLA, dedykowanego systemu aktualizacji oraz ważnej licencji komercyjnej. Wszystkie dostarczone komponenty systemu muszą być objęte wsparciem producenta.

B.2. Wymagania dla systemu SIEM dotyczące Systemu Zbierania i Analizy Logów.

- 1) W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
- 2) Ciągłe monitorowanie zasobów (CPU, RAM, dyski, ruch sieciowy) w odstępach co najmniej minutowych. Grupowanie hostów według kategorii (np. serwery, stacje robocze). Korelacja obciążeń między hostami z wykresami w czasie rzeczywistym. Konfigurowalne alerty (e-mail, SMS, przeglądarka) z informacjami o zdarzeniach (opis, priorytet, data).
- 3) Wizualizację statystyk zdarzeń i logów w czasie rzeczywistym (wykresy, dashboardy). Intuicyjną wyszukiwarkę z filtrowaniem po hostach, oprogramowaniu, kategoriach zagrożeń. Panel zarządzania regułami i „customowymi” logami z formularzami konfiguracyjnymi.
- 4) System powinien posiadać intuicyjny i przejrzysty interfejs, umożliwiający wizualizację danych pod kątem ich analizy. System musi umożliwiać wizualizację przy wykorzystaniu m.in. interaktywnych wykresów i grafik ponadto system musi posiadać wbudowaną zaawansowaną wyszukiwarkę umożliwiającą odfiltrowywanie danych i ich wizualizację wg. wybranych kategorii (np. poziom istotności).
- 5) System powinien umożliwiać konfigurację zaawansowanych scenariuszy powiadomień, które mogą być wysyłane poprzez e-mail, SMS. Użytkownicy powinni mieć możliwość ustawiania różnych poziomów priorytetów dla alertów, a także definiowania eskalacji dla poważniejszych problemów.
- 6) Rozwiązanie musi zostać dostarczone w postaci maszyn wirtualnej instalowanych w środowisku VMware lub Windows Hyper-V. Wymagane jest dostarczenie dedykowanego serwera fizycznego, na którym zostanie zainstalowane i uruchomione oprogramowanie SIEM w postaci maszyn wirtualnych.
- 7) Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską





Cyberbezpieczny Samorząd

- 8) System musi wykorzystywać agenta końcowego, który automatycznie uruchamia się wraz z systemem operacyjnym, działa w sposób niewidoczny dla użytkownika końcowego oraz jest chroniony przed usunięciem bez odpowiednich uprawnień. Agent musi umożliwiać zbieranie pełnej telemetrii z urządzeń końcowych, w tym: aktywności użytkownika, procesów, plików, zdarzeń systemowych oraz ruchu sieciowego. Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.
- 9) System musi używać różnych metod, takich jak skanowanie sieci, obsługa protokołów SNMP, IPMI i JMX, aby automatycznie wykrywać i konfigurować urządzenia w sieci.
- 10) System musi umożliwiać monitorowanie wydajności przy wykorzystaniu rozwiązań agentowych lub bez agentowych metodami monitorowania (np. przez SNMP, ICMP, IPMI), CSB musi efektywnie zbierać dane o wydajności i dostępności urządzeń. System powinien posiadać skalowalną architekturę dostosowaną do ilości urządzeń obsługiwanych w infrastrukturze Zamawiającego.
- 11) Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.
- 12) Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.
- 13) Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.
- 14) Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.
- 15) Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.
- 16) Rozwiązanie musi umożliwiać przysyłanie logów do innego serwera logów (funkcja syslog forwarder).
- 17) Integrację z MITRE ATT&CK z kategoryzacją zagrożeń (niski, średni, wysoki, krytyczny). Możliwość włączenia automatycznej ochrony (np. blokada IP, kwarantanna) w określonych godzinach/dniach. Wyszukiwarkę historii zagrożeń z filtrowaniem po hostach, IP, priorytetach i datach.
- 18) Generowanie raportów z wyborem hostów, grup hostów i modułów (np. podatności, zagrożenia). Filtrowanie raportów po priorytetach zdarzeń, przedziale czasowym i kategoriach. Eksport raportów w formatach CSV i PDF z opcją planowania automatycznego generowania.
- 19) Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.
- 20) Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.
- 21) Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).
- 22) Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.
- 23) System musi być kompatybilny z wieloma systemami operacyjnymi, co najmniej Linux, Windows, macOS.
- 24) Cały interfejs użytkownika powinien być dostosowany pod aktualne wymagania prawne związane z dostępnością serwisów użyteczności publicznej dla osób z niepełnosprawnościami.
- 25) System musi rejestrować zdarzenia akcje i reakcje użytkowników w CSB. Historia akcji poszczególnych użytkowników musi być raportowana i możliwa do odtworzenia w logach systemowych – chronologicznie.
- 26) Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).
- 27) Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów)
- 28) Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.
- 29) Rozwiązanie musi umożliwiać tworzenie statycznych raportów.
- 30) Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF.
- 31) Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.
- 32) Rozwiązanie musi umożliwiać tworzenie własnych raportów.
- 33) System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.



Cyberbezpieczny Samorząd

- 34) System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
- 35) Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.
- 36) Możliwość zgłaszania incydentów do CSIRT NASK w formacie zgodnym z formularzem NASK
- 37) Automatyczne generowanie zgłoszeń z poziomu interfejsu SIEM z polami (opis, priorytet, data).
- 38) Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.
- 39) System musi być zaprojektowany do przetwarzania wolumenu danych oraz liczby zdarzeń określonych w szczegółowym opisie przedmiotu zamówienia, bez degradacji funkcjonalności i dostępności systemu.
- 40) System musi gromadzić dane z różnych źródeł jednocześnie (co najmniej urządzenia sieciowe, serwery, urządzenia klienckie).
- 41) Zapisy, które pozwolą uprościć sposób przeszukiwania logów, żeby zaoferowane rozwiązanie nie wymagało zaawansowanej wiedzy związanej z przeszukiwaniem logów: Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości.
 - a) Interfejs wyszukiwania musi obsługiwać przeszukiwanie pełnotekstowe.
 - b) Interfejs wyszukiwania musi obsługiwać przeszukiwanie automatyczne w wielu repozytoriach niezależnie od ich lokalizacji bez potrzeby ich wskazywania.
 - c) Interfejs wyszukiwania powinien być dostępny z poziomu interaktywnej mapy sieci, umożliwiając wizualizację reguł korelacyjnych, ruchu sieciowego, aktywności procesów, modyfikacji rejestrów oraz wykonanych komend za pomocą menu kontekstowego dostępnego dla każdego obiektu na mapie.
- 42) System powinien posiadać wbudowanego asystenta AI, który wspiera operatora w obsłudze zdarzeń oraz zarządzaniu podatnościami.
- 43) Algorytmy sztucznej inteligencji musi umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
- 44) Asystent AI musi umożliwiać integrację z lokalnymi oraz publicznie dostępnymi modelami językowymi (LLM).
- 45) Asystent AI powinien działać kontekstowo, z możliwością przypisania odpowiednich promptów do każdego kontekstu.
- 46) System musi posiadać asystenta analizy AI (sztucznej inteligencji) ułatwiający analizę danych agregowanych w systemie. Asystent AI musi analizować dane pod kątem cyberbezpieczeństwa z naciskiem na określenie poziomu ryzyka oraz sposobu zabezpieczenia.
- 47) Asystent AI powinien oferować dedykowane tryby działania, obejmujące co najmniej obsługę incydentów, zarządzanie podatnościami, przeglądanie logów, analizę zdarzeń korelacyjnych oraz tworzenie nowych parserów
- 48) Asystent AI musi być wyposażony w edytor promptów, umożliwiający ich edycję oraz tworzenie nowych.
- 49) Prompty powinny być wersjonowane i możliwe do pobrania z portalu producenta.
- 50) Asystent AI musi być dostępny w trybie ciągłym oraz dynamicznie przełączać kontekst w zależności od wykorzystywanych funkcjonalności.
- 51) W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące incydenty na urządzeniach sieciowych Zamawiającego
- 52) System musi działać w architekturze hybrydowej:
 - a) Podstawowa funkcjonalność: w pełni lokalna (on-premises).
 - b) Kontrolowana komunikacja zewnętrzna z określonymi źródłami:
 - CSIRT NASK (obowiązek prawny)



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- MITRE ATT&CK, MISP (threat intelligence)
 - Wybrane źródła IoC (lista do uzgodnienia)
 - c) Możliwość pracy w trybie fully offline z lokalną bazą zagrożeń.
 - d) Wszystkie połączenia zewnętrzne przez proxy/firewall Zamawiającego.
- 53) Platforma sprzętowa dla SIEM musi obsługiwać szyfrowanie dysków.
- 54) Rozwiązanie musi wspierać implementację na środowisku wirtualnym takim jak m.in. VMWare, Hyper-V, Proxmox, KVM, OVM, OVF.
- 55) Musi posiadać moduły zabezpieczone połączeniem (HTTPS) w przeglądarce.
- 56) Konsola rozwiązania musi zawierać informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, sygnatury czasowe.
- 57) Konsola rozwiązania musi szacować poziom ryzyka dla każdego wykrytego zagrożenia oraz musi dawać możliwość tagowania zdarzeń i załączania opisu (notatek).
- 58) Konsola musi umożliwiać grupowanie takich samych zdarzeń w ramach jednego wpisu oraz podawać liczbę wystąpień identycznego zdarzenia.
- 59) Konsola musi umożliwiać utworzenie zgłoszenia z dowolnego zdarzenia.
- 60) Konsola musi posiadać dedykowany widok dla utworzonych zgłoszeń.
- 61) Z poziomu konsoli musi być dostępna opcja zmiany statusu zgłoszenia.
- 62) Rozwiązanie musi obsługiwać silniki detekcji takie jak Analiza Shellcode i Powershell, tj. detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wywoływania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach.
- 63) Rozwiązanie musi umożliwiać analizowanie całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń.
- 64) System musi być dostarczony z gwarancją oraz wsparciem technicznym obejmującym: dostęp do najnowszych wersji systemu SIEM, aktualizacji, poprawek; aktualizację silnika korelującego zbierane logi z regułami bezpieczeństwa systemu SIEM; aktualizację bazy scenariuszy postępowania dla rozpoznanych zagrożeń; kontakt z certyfikowanym inżynierem Wykonawcy lub producenta.
- 65) Dostarczone rozwiązanie musi umożliwiać korelacje zdarzeń przesyłanych lub pobieranych z innych systemów.
- 66) Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
- 67) System musi umożliwiać mapowanie zdarzeń bezpieczeństwa na poszczególne techniki z bazy wiedzy MITRE ATT&CK® oraz zapewniać mechanizmy filtrowania zdarzeń po tych technikach.
- 68) System powinien umożliwiać przeprowadzanie symulacji ataku w celu weryfikacji skuteczności mechanizmów wykrywania i reagowania na zagrożenia w infrastrukturze Zamawiającego. Funkcjonalność ta musi spełniać następujące wymagania:
- e) **scenariusze symulacji:** Administrator powinien mieć możliwość definiowania i dodawania nowych scenariuszy symulacji poprzez interfejs użytkownika systemu.
 - f) **konfiguracja szyfrowania:** Wybór algorytmu szyfrowania powinien być dostępny w panelu administracyjnym dla każdego scenariusza symulacji.

B.3. Raportowanie wyników symulacji:

- 1) System musi generować raporty z przebiegu symulacji ataku w formacie PDF, zawierające następujące informacje:
- a) Data i godzina przeprowadzenia symulacji.
 - b) Nazwa i opis scenariusza ataku.
 - c) Wykonane operacje (np. uruchomione skrypty, przesłane dane).
 - d) Status symulacji (np. powodzenie, niepowodzenie, wykrycie przez system SIEM).
 - e) Powiązanie z technikami MITRE ATT&CK, jeśli dotyczy.
- 2) Raporty muszą być dostępne do pobrania z poziomu interfejsu użytkownika oraz możliwe do automatycznego wysyłania na skonfigurowany adres e-mail Zamawiającego.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

B.4. Zarządzanie symulacjami:

- 1) System musi umożliwiać planowanie symulacji ataku w określonych godzinach lub dniach, z opcją harmonogramowania cyklicznego.
- 2) Interfejs użytkownika powinien zapewniać intuicyjne zarządzanie symulacjami, w tym:
 - a) Włączenie/wyłączenie scenariuszy.
 - b) Edycja parametrów symulacji (np. wybór hostów, algorytmów szyfrowania).
- 3) Możliwość ograniczenia symulacji do wybranych hostów lub grup hostów w infrastrukturze Zamawiającego.

B.5. Bezpieczeństwo symulacji:

- 1) Symulacje muszą być przeprowadzane w sposób bezpieczny, bez wpływu na działanie produkcyjnych systemów Zamawiającego.
- 2) Wszystkie dane generowane podczas symulacji muszą być szyfrowane zgodnie z wybranym algorytmem i usuwane po zakończeniu testu, z wyjątkiem danych zapisanych w raportach.
- 3) System musi zapewniać mechanizmy zapobiegające przypadkowemu uruchomieniu symulacji w środowisku produkcyjnym (np. wymaganie autoryzacji administratora).

B.6. Wymagania dodatkowe:

- 1) System musi posiadać interfejs graficzny do tworzenia własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie.
- 2) Reguły korelacyjne muszą uwzględniać dodatkowo parametry, które nie są zawarte bezpośrednio w samych zdarzeniach, przykładem jest reguła wykrywająca ruch z serwerów do sieci Internet na podstawie zdarzeń, w których nie ma informacji, że dotyczą one serwera.
- 3) Reguły korelacyjne muszą uwzględniać parametry obiektów w Active Directory umożliwiając odniesienie się do takiego obiektu w korelacji, na podstawie zdarzeń nie zawierających o nim informacji, przykładem będzie ruch sieciowy odwołujący się do konta użytkownika, na którym hasło nie jest wymagane.
- 4) Licencja na oferowany system nie może ograniczać liczby źródeł danych (urządzeń, systemów, aplikacji), z których pobierane są dane i zdarzenia.
- 5) System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL.
- 6) System musi posiadać wbudowaną funkcjonalność badania zachowania użytkowników oraz urządzeń (UEBA), która będzie oparta na danych pochodzących ze zgromadzonych logów oraz analizowanych za pomocą algorytmów sztucznej inteligencji.
- 7) Oferowana funkcjonalność UEBA musi zawierać wbudowane wizualizacje, kokpity oraz zestawy spredefiniowanych modeli analizy opartych na algorytmach sztucznej inteligencji.
- 8) System musi umożliwiać predykcję trendów bezpieczeństwa na podstawie danych historycznych, w tym przewidywanie prawdopodobieństwa ataków, prognozowanie obciążenia infrastruktury oraz identyfikację potencjalnych zagrożeń.
- 9) System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
- 10) System musi być wyposażony w zaawansowane metody analizy danych oparte na algorytmach sztucznej inteligencji.
- 11) Algorytmy sztucznej inteligencji muszą umożliwiać przewidywanie zachowań systemu poprzez zrozumienie liczby generowanych zdarzeń oraz wartości liczbowych w tych zdarzeniach, takich jak wysłane bajty (sent_bytes), rozmiar pliku (file_size) i czas trwania sesji (session_duration).
- 12) Algorytmy sztucznej inteligencji muszą umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
- 13) System musi umożliwiać tworzenie reguł detekcji na podstawie wzorców wykrytych anomalii, aby możliwa była automatyczna reakcja na podobne sytuacje w przyszłości.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- 14) System musi umożliwiać analizę ruchu sieciowego poprzez przechwytywanie i inspekcję pakietów w czasie rzeczywistym, w tym minimum protokołów HTTP DNS, FTP oraz SSH.
- 15) System na bazie gromadzonej kopii ruchu sieciowego musi identyfikować i klasyfikować ataki w oparciu o sygnatury oraz zachowanie użytkowników.
- 16) System musi umożliwiać zapisywanie pakietów ruchu sieciowego w formacie PCAP.
- 17) System musi umożliwiać analizę ruchu sieciowego pod kątem występowania opóźnień, retransmisji, Jitter, Server Response Time oraz Round Trip Time.
- 18) System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
 - a) wykrycia dowolnej treści w logach,
 - b) wykrycia wystąpienia wartości pola na wybranej liście,
 - c) wykrycia niewystępowania wartości pola na wybranej liście,
 - d) wykrycia zmiany jednego z kilku pól,
 - e) wykrycia zdarzeń występujących z zadaną częstotliwością,
 - f) wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
 - g) wykrycia zaniku wiadomości,
 - h) wykrycia nowej wartości pola w zadanym okresie czasu,
 - i) wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności.
- 19) System musi pozwalać na tworzenie parserów z poziomu GUI.
- 20) System musi posiadać predefiniowany zestaw parserów zdarzeń.
- 21) Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
- 22) System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
- 23) System musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.
- 24) System musi umożliwiać uruchomienie wysokiej dostępności na poziomie Agregacji, Retencji oraz Prezentacji.
- 25) System musi zapewniać mechanizmy niezawodnościowe, które zagwarantują ciągłość gromadzenia zdarzeń oraz ich uzupełnienie po przywróceniu sprawności systemu, bez ograniczeń w funkcjonalności interfejsu użytkownika. w przypadku awarii któregośkolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu.
- 26) System, w przypadku awarii któregośkolwiek z jego komponentów, powinien zapewnić mechanizmy niezawodnościowe gwarantujące ciągłość gromadzenia zdarzeń. Mechanizmy te nie mogą ograniczać możliwości wyszukiwania i analizy zdarzeń przez operatora, w szczególności z poziomu graficznego interfejsu użytkownika.
- 27) Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius.
- 28) System musi być projektowany, rozwijany i testowany z uwzględnieniem dobrych praktyk bezpieczeństwa aplikacji, zgodnie z zaleceniami OWASP, w szczególności OWASP Top 10. Interfejsy aplikacyjne oraz interfejs webowy Systemu powinny spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0, co najmniej na poziomie pierwszym (Level 1 – L1).

B.7. Wymagania dla systemu SIEM dotyczące funkcjonalności SOAR.

- 1) System musi być dostarczony wraz ze wsparciem producenta oprogramowania.
- 2) Licencja nie może ograniczać ilości założonych kont użytkowników systemu SOAR.
Licencja nie może ograniczać liczby jednocześnie zalogowanych operatorów systemu SOAR.
- 3) System musi wspomagać pracę zespołu reagowania na incydenty komputerowe (SOC, CERT, CSIRT, IRT itp.) tj. wspomagać procesy: monitorowania bezpieczeństwa teleinformatycznego, reagowania na



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

incydenty, zarządzania podatnościami, gdzie głównym celem jest standaryzacja i automatyzacja działań analityków cyberbezpieczeństwa.

- 4) System musi natywnie integrować się z systemem SIEM wykorzystywanym przez Zamawiającego tj. producent oprogramowania SOAR musi oficjalnie wspierać integrację z dostarczonym rozwiązaniem SIEM.
- 5) System musi umożliwiać automatyczne tworzenie incydentów wymagających obsłużenia na podstawie powiadomień z systemu SIEM, zgłoszeń przekazywanych przez użytkowników na dedykowany adres e-mail, zgłoszeń przypisanych w systemie typu helpdesk do odpowiedniej grupy, przez co najmniej system RTIR (Request Tracker Incident Response) lub Jira. Ponadto rozwiązanie musi umożliwiać automatyczne zamykanie obsłużonego zgłoszenia w systemie typu helpdesk, przynajmniej dla rozwiązania RTIR (Request Tracker Incident Response) lub Jira.
- 6) System musi umożliwiać ręczne utworzenie incydu.
- 7) System musi posiadać możliwość automatycznej oraz ręcznej klasyfikacji incydentów ze względu na ich krytyczność.
- 8) System musi umożliwiać tworzenie własnych definicji klasyfikacji incydentów i ich krytyczności. W ramach wdrożenia Wykonawca wraz z zamawiającym ustali oraz zaimplementuje właściwą klasyfikację incydentów w systemie.
- 9) System musi umożliwiać śledzenie czasu oraz podjętych działań w ramach utworzonego incydu oraz raportowanie czasów: Time-to-detect oraz czasów: Time-to-mitigate.
- 10) System musi umożliwiać łączenie utworzonych incydentów, w tym inteligentne łączenie automatyczne.
- 11) System musi umożliwiać automatyczne przydzielanie predefiniowanych zadań dla danych typów incydentów.
- 12) System musi umożliwiać tworzenie i edytowanie procedur reagowania na incydenty w postaci graficznej. System musi umożliwiać stosowanie podstawowych operatorów logicznych i matematycznych przy definicji procedur.
- 13) System musi umożliwiać automatyczne oraz ręczne przydzielanie incydentów wymagających obsłużenia do pracowników obsługujących system.
- 14) System musi umożliwiać automatyczną oraz ręczną weryfikację w wewnętrznych oraz zewnętrznych źródłach informacji, charakterystycznych dla danego incydu atrybutów.
- 15) System musi umożliwiać zaprojektowanie oraz wdrożenie automatycznych działań reagowania na dane typy incydentów.
- 16) System musi umożliwiać edycję kodu źródłowego automatycznych działań reagowania. Wymaga się stosowanie języka skryptowego uznanego za powszechny, w jego najnowszej wersji. Np. Python3.
- 17) System musi posiadać możliwość generowania dashboardów security z danych znajdujących się w SOAR, między innymi statystyk, w tym system musi posiadać możliwość tworzenia i konfiguracji widoków głównych na główny ekran dyspozycyjny w pomieszczeniu SOC.
- 18) System musi Umożliwiać dwustronną komunikację z użytkownikami systemu (np. w celu zebrania dodatkowych informacji od osób związanych z incydem) oraz operatorami systemu SOAR, na przykład poprzez zastosowanie interaktywnych formularzy.
- 19) System musi automatyzować proces analizy otrzymanych danych, realizować funkcje informacyjne, jak również podejmować funkcje naprawcze (np. automatyczna analiza pliku w chmurze sandbox wybranego producenta, wysłanie wiadomości e-mail do użytkownika zainfekowanej stacji końcowej, aby nie otwierał załącznika i blokada na urządzeniu sieciowym dostępu do wskazanych usług dla wybranego użytkownika).
- 20) System musi Posiadać wbudowaną bibliotekę minimum 5 typów incydentów, a także powinno dostarczać specjalizowane typy incydentów związane z integrowanymi systemami, pozwalając jednocześnie na ich edycję lub kopiowanie celem stworzenia własnej karty incydu.
- 21) System musi umożliwić wykorzystanie w skryptach własnych bibliotek zewnętrznych oraz programów (np. poprzez umożliwienie uruchomienia skryptów we własnym kontenerze, zawierającym pożądane oprogramowanie).



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- 22) System musi Pozwalać na kopiowanie oraz edycję już istniejących scenariuszy jak również dodawanie nowych.
- 23) System musi pozwalać na edycję i dodawanie nowych scenariuszy obsługi incydentu (tzw. playbook) za pomocą graficznego interfejsu użytkownika bez konieczności wykorzystania języków skryptowych lub znajomości języków programowania.
- 24) System musi pozwalać na tworzenie scenariuszy zagnieżdżonych, tzn. scenariusz nadrzędny może zawierać scenariusze podrzędne uruchamiane na zasadzie pod-scenariuszy. Edycja/zmiana pod-scenariusza wpływa automatycznie na wszystkie scenariusze, które go wykorzystują, co ułatwia administrację.
- 25) System musi pozwalać na tworzenie scenariuszy zawierających:
 - a) zadania ręczne,
 - b) zadania zautomatyzowane,
 - c) zadania warunkowe automatyczne,
 - d) zadania warunkowe ręczne,
 - e) akwizycję danych przy użyciu formularzy,
 - f) filtry danych,
 - g) pod-scenariusze.
- 26) System musi pozwalać na automatyczne i ręczne wykonywanie dostępnych scenariuszy.
- 27) System musi pozwalać na automatyczne dokumentowanie uruchomionych scenariuszy wraz z wynikami jego działania.
- 28) System musi umożliwiać wizualizację przebiegu wykonania scenariusza (wizualizację rezultatu wszystkich wykonanych oraz pominiętych zadań, operacji warunkowych, decyzji itp.).
- 29) System musi pozwalać na sterowanie wykonaniem scenariusza przez operatora (zadania warunkowe ręczne) drogą korespondencyjną (m.in. z poziomu wiadomości email oraz wiadomości w komunikatorze takim jak np. Microsoft Teams, Slack, Mattermost itp.).
- 30) System musi pozwalać na uruchomienie scenariusza w trybie krokowym w celu analizy jego poprawności i usunięcia ewentualnych błędów.
- 31) System musi pozwalać na zatrzymanie scenariusza w trakcie jego wykonania.
- 32) System musi pozwalać na doraźne wykonanie dowolnego zadania automatyzacyjnego przez operatora SOC, bez konieczności tworzenia nowych / modyfikacji istniejących scenariuszy (np. przy użyciu wiersza poleceń).
- 33) System musi pozwalać na proste monitorowanie stanu wykonania scenariuszy powiązanych z incydentami. Ponadto, w przypadku wystąpienia jakichkolwiek anomalii w trakcie wykonania scenariusza, osoby odpowiedzialne za incydent powinny zostać natychmiast o tym poinformowane.
- 34) System musi pozwalać na przydzielanie zadań pojedynczego scenariusza różnym członkom zespołu SOC.
- 35) System musi pozwalać na przekazywanie parametrów pomiędzy zadaniami pojedynczego scenariusza.
- 36) System musi pozwalać na odczytywanie wyników analizy i wykorzystaniu ich w kolejnych zadaniach uruchomionego scenariusza.
- 37) System musi pozwalać na sprawdzenie historycznych danych na temat uruchomionych scenariuszy/zadań.
- 38) System musi pozwalać na okresowe uruchamianie scenariuszy w zdefiniowanym czasie i wedle harmonogramu.
- 39) System musi pozwalać na sprawdzenie, które incydenty nie zostały obsłużone.
- 40) System musi pozwalać na tworzenie własnych:
 - a) typów incydentów,
 - b) pól/etykiet incydentów,
 - c) typów wskaźników (ang. indicator),
 - d) pól/etykiet wskaźników (ang. indicator),
 - e) raportów,



Cyberbezpieczny Samorząd

- f) dashboardów.
- 41) System musi pozwalać na automatyczne wypełnianie pól incydentu bazując na typie incydentu lub jego atrybutach.
 - 42) System musi pozwalać na delegowanie zadań innym członkom zespołu SOC w ramach oceny danego incydentu.
 - 43) System musi pozwalać na współpracę pomiędzy członkami zespołu SOC (np. rozmowa między członkami zespołu a temat incydentu).
 - 44) System musi pozwalać na zapisywanie historycznych incydentów wraz z pełną informacją na temat podjętych akcji obsługi/rozwiązania w celu szkolenia/transferu wiedzy pomiędzy członkami zespołu SOC (Na historię incydentu składają się wyniki działania automatycznych i ręcznych zadań określonych w playbooku, komentarze analityków pracujących nad incydemtem, indykatory zagrożenia IOC (IP, URL, domeny, itd.) wyciągane automatycznie i wskazywane ręcznie w czasie obsługi incydentu, elementy analizy oznaczone przez analityków jako dowód w sprawie (np. zrzuty ekranu z widokiem podejrzanych stron web), pliki dodawane do historii obsługi incydentu przez analityków, itp.).
 - 45) System powinien **musi** umożliwiać eksport wskaźników kompromitacji do serwerów MISP jako funkcjonalność opcjonalną, umożliwiającą przyszłą integrację z platformą Threat Intel.
 - 46) System powinien umożliwiać eksport incydentów w formatach STIX 1/2, CSV, DOCX, PDF jako funkcjonalność opcjonalną.
 - 47) System musi obsługiwać uwierzytelnianie w następującej hierarchii:
 - a) PRIORYTET: MFA + SSO (SAML, OAuth, OpenID Connect).
 - b) Service accounts: dla systemów nieobsługujących SSO - z rotacją haseł.
 - c) API keys: szyfrowane, z kontrolą dostępu i audytem.
 - d) Globalnych poświadczeń: tylko jako ostateczność, z dodatkowymi zabezpieczeniami:
 - Szyfrowanie w spoczynku,
 - Audit log wszystkich użyci,
 - Regularna rotacja,
 - Ograniczenia IP/czasowe.
 - 48) System musi pozwalać na proste wyszukiwanie incydentów na podstawie ich cech (np. przy użyciu dedykowanego języka zapytań) oraz podobieństwa do innych incydentów (related incidents).
 - 49) System musi Pozwalać na wizualizację zależności pomiędzy podobnymi incydentami na poziomie wystąpień identycznych metadanych.
 - 50) System powinien opcjonalnie umożliwiać działanie jako platforma SOAR dla wielu instytucji/klientów z całkowitą separacją zasobów i przetwarzanych danych (tzw. wsparcie dla trybu multi-tenant), z całkowitą separacją zasobów i przetwarzanych danych (tzw. wsparcie dla trybu multi-tenant).
 - 51) System musi posiadać repozytorium wskaźników (ang. indicators), które kolekcjonuje i koreluje wskaźniki w ramach wszystkich incydentów, alertów i feedów dostarczanych do rozwiązania.
 - 52) System musi umożliwiać wykonywanie scenariuszy na podstawie zestawu wskaźników (ang. indicators) określonych przez użytkownika.
 - 53) System musi obsługiwać formaty strukturalne, takie jak JSON, CSV, STIX 1.X i STIX 2.X itp. w ramach integracji ze źródłami wskaźników (ang. indicators).
 - 54) System musi wspierać minimum następujące typy wskaźników (ang. indicators):
 - a) numery kart płatniczych
 - b) IBAN
 - c) adres email
 - d) konto użytkownika
 - e) wyniki CVE
 - f) domena
 - g) FQDN
 - h) nazwy hosta



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- i) IP (v4 oraz v6)
 - j) klucz i ścieżka rejestru
 - k) URL
 - l) CIDR.
- 55) System musi umożliwiać własną definicję wskaźników, jego pól oraz skryptów reputacyjnych.
- 56) System musi zapewniać użytkownikom możliwość automatycznej weryfikacji wskaźników (tzw. enrichment), wykonując odpowiedni scenariusz lub uruchamiając sprawdzanie na podstawie typu wskaźnika (ang. indicator).
- 57) System musi posiadać natywną integrację z MITRE ATT&CK i przypisywać do incydentów odpowiednie techniki i taktyki.
- 58) Interfejs użytkownika musi być dostępny w polskiej oraz angielskiej wersji językowej.
- 59) System musi udostępniać funkcjonalność war-room w celu usprawnienia współpracy pomiędzy analitykami i zespołami.
- 60) System musi wspierać model uczenia nadzorowanego dla najbardziej popularnych i czasochłonnych w ocenie incydentów typu phishing. SOAR na podstawie incydentów typu phishing z przeszłości, które zostały już sklasyfikowane (i rozwiązane), powinien zbudować model do automatycznej oceny nowych przychodzących wiadomości celem ich klasyfikacji jako: 'Poprawna', 'Spam' lub 'Złośliwa'.
- 61) System musi umożliwiać łatwą integrację z pozostałymi systemami klasy threat intel/threat hunting/threat share za pomocą API.
- 62) Zapewniać zestaw co najmniej 250 gotowych integracji pozwalających na szybką, dwustronną komunikację z zewnętrznymi systemami.
- 63) System musi zapewniać możliwość wglądu w kod integracji oraz jego klonowanie pod kątem wprowadzania modyfikacji lub napisania własnej wersji integracji.
- 64) System musi pozwalać na tworzenie wielu instancji integracji tego samego typu do rozwiązań firm trzecich (przykładowo dwie integracje z serwerami IMAP lub zaczytujące dane threat intel z dwóch źródeł w formacie JSON).
- 65) System musi zapewnić integrację (np. przy pomocy wtyczek) z popularnymi programami klasy IDE (np. PyCharm lub VSCode) w celu ułatwienia edycji skryptów.
- 66) System musi umożliwiać tworzenie zbiorczych raportów z utworzonych oraz obsługiwanych incydentów.
- 67) System musi posiadać zestaw przygotowanych raportów takich jak:
- a) raport na temat incydentów: dzienny, 7- i 30-dniowy,
 - b) raport na temat średniego czasu rozwiązania incydentu.
- 68) System musi pozwalać na tworzenie własnych raportów oraz dashboardów za pomocą predefiniowanych komponentów umożliwiających wizualizację pożądaných danych (np. wykres kołowy, słupkowy, liniowy, tabela itp.).
- 69) System musi być skalowalny – zapewnić możliwość łatwej rozbudowy (możliwość rozbudowy architektury o dodatkowe serwery/ urządzenia bez konieczności zmian programistycznych). Konstrukcja systemu powinna pozwalać na elastyczne skalowanie.
- 70) W ramach Systemu należy stosować mechanizmy zapewniające wysoką dostępność w szczególności mechanizmy klastrowe z wykorzystaniem wirtualizacji.
- 71) Konstrukcja Systemu musi zapewniać redundancje poszczególnych elementów, tak aby awaria któregośkolwiek z nich nie powodowała braku dostępności całego Systemu.
- 72) W skład rozwiązania muszą wchodzić mechanizmy zapewniające wysoką wydajność dla wszystkich komponentów, w szczególności dla serwerów Systemu, web oraz baz danych.
- 73) Zamawiający wymaga aby rozwiązanie umożliwiało skalowanie wydajności poprzez dodanie kolejnych serwerów aplikacyjnych/web.
- 74) Aplikacje klienckie nie mogą komunikować się bezpośrednio z bazą danych.
- 75) Wszystkie komponenty, aplikacje i usługi serwerowe muszą być uruchamiane jako usługi systemowe.

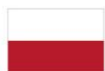


Cyberbezpieczny Samorząd

- 76) Zamawiający nie dopuszcza możliwości instalowania żadnych zabezpieczeń fizycznych w postaci kart, kluczy USB, fizycznych sieciowych serwerów licencyjnych.
- 77) System ma być w całości posadowiony w infrastrukturze Zamawiającego (ang. on-premises).
- 78) System musi działać w trybie hybrydowym:
- a) Podstawowa funkcjonalność: w pełni lokalna (on-premises),
 - b) Dozwolona komunikacja zewnętrzna wyłącznie z:
 - CSIRT NASK (obowiązek prawny),
 - Oficjalnymi bazami threat intelligence (MITRE ATT&CK, MISP),
 - Określonymi źródłami IoC (lista do uzgodnienia),
 - Możliwość wyłączenia wszystkich połączeń zewnętrznych (tryb fully offline),
 - Kontrola komunikacji przez proxy/firewall Zamawiającego.
- 79) Dostęp do Systemu musi być realizowany za pomocą przeglądarki internetowej, przy czym akceptowanym sposobem transmisji danych do przeglądarki WWW jest szyfrowanie przepływu danych, w szczególności należy wykorzystać szyfrowanie danych protokołem TLS. System musi być wyposażony w certyfikaty SSL (dostarczone przez Zamawiającego z wewnętrznego lub komercyjnego CA) dla serwerów WWW, a transmisja danych musi odbywać się z wykorzystaniem do tego celu protokołu HTTPS.
- 80) Wymagania odnośnie aplikacji klienckiej Systemu:
- a) Musi posiadać minimalne wymagania dla łącza przy pracy w sieci WAN lub Internet z przepustowością maksymalnie 1024 Kbps na jednego użytkownika;
 - b) Musi pracować w kontekście standardowego użytkownika Windows;
 - c) Aplikacja webowa:
 - nie może korzystać z komponentów ActiveX i wtyczek NPAPI;
 - nie może wykorzystywać Flasha, Silverlighta, apletów Java ani innej technologii klienckiej, która nie jest natywnie wspierana przez standardy W3C w przeglądarkach;
 - warstwę prezentacji należy tworzyć wyłącznie w formacie HTML5 i XHTML 1.1 lub z użyciem CSS3;
 - kod wynikowy strony musi poprawnie działać z każdą z niżej wymienionych przeglądarek w ich aktualnej wersji: Microsoft Edge na platformie MS Windows, Google Chrome na platformie MS Windows.
- 81) Ruch sieciowy pomiędzy wszystkimi elementami Systemu musi być szyfrowany za pomocą protokołów i algorytmów kryptograficznych uznanych powszechnie za bezpieczne. Wymagane jest stosowanie protokołów TLSv1.2, SSH 2 lub ich nowszych wersji z zastrzeżeniem, że do komunikacji z przeglądarką internetową użytkowników Systemu wymagane jest stosowanie TLSv1.3. Nie jest dopuszczalne stosowanie protokołu IPsec oraz protokołów SSL 2.0, SSL 3.0, TLS 1.0 i TLS 1.1 i starszych.
- 82) Wymagane jest stosowanie zaufanych certyfikatów X.509 dostarczonych przez Zamawiającego. Stosowane muszą być certyfikaty z wewnętrznej infrastruktury PKI Zamawiającego lub certyfikaty komercyjne zakupione przez Zamawiającego.
- 83) Autoryzacja administratorów Systemu musi bazować na rolach użytkowników. Rozwiązanie musi udostępniać mechanizm wielopoziomowego hierarchizowania uprawnień do jego zasobów z możliwością przydzielania i odbierania uprawnień przez administratora Systemu lub domeny Active Directory.
- 84) Rozwiązanie musi posiadać możliwość uwierzytelniania poprzez zewnętrzne serwery Active Directory.
- 85) Każdy Administrator rozwiązania musi posiadać indywidualne konto, pozwalające na jego jednoznaczną identyfikację. Identyfikator Administratora musi pokrywać się kontem Użytkownika w domenie Active Directory.
- 86) Wymaga się, aby skrót hasła przechowywany w projektowanej Systemu był wyliczany za pomocą bezpiecznej do zastosowań kryptograficznych funkcji mieszającej z wykorzystaniem tzw. mechanizmu soli (ang. Hashing with Salt).
- 87) Rozwiązanie musi posiadać wewnętrzny dziennik zdarzeń (audyt). Dziennik zdarzeń musi zawierać całą historię wszystkich operacji oraz składni realizowanych zapytań wykonywanych przez użytkowników



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Systemu. Rozwiązanie musi posiadać możliwość konfigurowalnego raportowania i automatycznego monitorowania i logowania aktywności Operatorów.

- 88) System musi posiadać logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora przypisanego do obsługi zdarzenia (co najmniej e-mail oraz SMS).
- 89) Kwalifikacja zdarzeń musi odbywać się na podstawie zestawu konfigurowalnych reguł, które automatycznie przypisują zdarzenie do obsługi lub je odrzucają
- 90) Obsługiwane zdarzenia muszą posiadać zestaw predefiniowanych scenariuszy obsługi (ang. playbook) oraz umożliwiać tworzenie, edycję i zarządzanie własnymi scenariuszami obsługi z poziomu interfejsu graficznego.
- 91) System musi być zdolny do pobierania informacji z innych systemów oraz wykorzystywać je do podejmowania decyzji dotyczących dalszego przebiegu playbooksa.
- 92) System musi być zintegrowany ze skanerem podatności oraz zapewnić obsługę tych podatności w ramach playbooków.
- 93) Kwalifikacja podatności musi odbywać się na podstawie zestawu konfigurowalnych reguł, które automatycznie przypisują podatności do obsługi lub je odrzucają.
- 94) System musi umożliwiać reagowanie na zagrożenia zarówno poprzez integrację z innymi systemami zabezpieczeń, jak i bezpośrednio na zaatakowanej stacji roboczej bądź serwerze.
- 95) W ramach dostępnych kroków zawartych w playbooku system musi umożliwiać przeszukiwanie logów historycznych, skorelowanych zdarzeń oraz bazy Threat Intel.
- 96) Dla obsługiwanych zdarzeń oraz podatności system musi umożliwiać zautomatyzowaną ocenę prawdopodobieństwa materializacji zagrożenia bazując na zestawie predefiniowanych reguł.
- 97) System musi umożliwiać definiowanie parametrów SLA dla wszystkich statusów obsługi oraz automatyczny pomiar tych czasów i ich weryfikację względem zdefiniowanych wartości, a także prezentację aktualnych wyników na liście zdarzeń zakwalifikowanych do obsługi.

B.8. Wymagania związane z aktualizacją i utrzymaniem produktu i zabezpieczeniem przed nieautoryzowaną modyfikacją:

- 1) Producent rozwiązania powinien zapewnić usługę umożliwiającą dostęp do aktualizacji oprogramowania oraz kontekstu systemu, w szczególności reguł korelacyjnych, playbooków, parserów, skryptów, promptów AI, list referencyjnych, profili użytkowników i komputerów oraz innych dostępnych aktualizacji, w formie online lub w sposób równoważny
- 2) Rozwiązanie powinno zapewnić dostęp do portalu, w którym automatycznie z poziomu interfejsu systemu będzie możliwe sprawdzenie dostępności nowych kontekstów oraz wersji. (przykład: nowa wersja zainstalowanej w systemie reguły korelacyjnej czy zupełnie nowy playbook, którego nie ma jeszcze zainstalowanego w systemie).
- 3) Rozwiązanie musi zapewnić mechanizm zabezpieczenia kontekstu przed nieautoryzowaną modyfikacją (np.: brak możliwości modyfikacji wersji reguły).

B.9. Wymagania dla systemu SIEM dotyczące funkcjonalności UEBA.

- 1) System musi analizować zachowania użytkowników i komputerów na bazie algorytmów uczenia maszynowego (ang. User and Entity Behaviour Analysis).
- 2) Modele zachowania użytkowników (UBA) i komputerów (EBA) muszą być tworzone automatycznie na bazie zdarzeń historycznych.
- 3) Algorytm nauczania musi mieć możliwość konfiguracji sposobu odrzucania wartości skrajnych mogących wpłynąć negatywnie na wyniki procesu nauczania.
- 4) Wykryte przez mechanizmy uczenia maszynowego anomalie muszą generować nowe zdarzenia i zapisywać je w repozytorium logów.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- 5) Algorytmy uczenia maszynowego muszą umożliwiać naukę danych statystycznych, w tym min. ilości generowanych typów zdarzeń oraz reguł przez hosta lub konto użytkownika.
- 6) Mechanizm uczenia maszynowego musi umożliwiać wskazanie wartości w zdarzeniach, które mają zostać objęte procesem nauczania oraz połączenia ich z warunkiem kwalifikującym.
- 7) System musi umożliwiać wykrywanie korelacji czasowych między zdarzeniami bezpieczeństwa w celu identyfikacji złożonych wzorców ataków wieloetapowych.
- 8) System musi posiadać wbudowaną bazę wskaźników kompromitacji, która umożliwi zbieranie, przechowywanie oraz przypisywanie wskaźników kompromitacji (IoC) do incydentów.
- 9) 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/>).
- 10) Listami wskaźników (malware, zagrożenia sieciowe, URL) z polami (czas, hash, źródło).
- 11) Integracją z zewnętrznymi źródłami (np. AbuseCH, VirusTotal).
- 12) Wyszukiwarką z filtrowaniem po kategoriach, datach i priorytetach.
- 13) Dane zgromadzone w bazie wskaźników kompromitacji powinny być możliwe do wykorzystania w regułach korelacyjnych.
- 14) Licencja na agentów musi obejmować wszystkie źródła logów liczonych jako komputery oraz serwery wykorzystywane w organizacji.
- 15) Pełen zakres funkcjonalności agenta musi być dostępny z poziomu centralnej konsoli zarządzania.
- 16) Agent powinien być w pełni kontrolowany za pośrednictwem playbooków, umożliwiając wykonywanie akcji izolacji oraz blokowania na podstawie warunków związanych z analizowanymi zdarzeniami.
- 17) Agent powinien umożliwiać blokowanie na poziomie jądra systemu (kernela).
- 18) Agent powinien obsługiwać tryb komunikacji jednostronnej, w którym nie otwiera żadnych portów, a jedynie sam inicjuje połączenia z konsolą zarządzającą.
- 19) Agent musi przysyłać do konsoli centralnej pełen zakres telemetrii, obejmujący m.in. połączenia sieciowe, modyfikacje rejestrów, uruchamianie procesów i komend oraz dostęp do plików, w celu korelacji danych.
- 20) Serwer administracyjny musi posiadać możliwość tworzenia grup komputerów.
- 21) Rozwiązanie musi zapewniać korzystanie z min. 100 szablonów raportów, przygotowanych przez producenta lub własnych raportów tworzonych przez administratora.
- 22) Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email oraz do dziennika syslog.
- 23) Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami.
- 24) System SIEM musi posiadać mechanizm monitorowania źródeł logów, gdzie w przypadku braku dostępności któregoś ze źródeł, system SIEM wygeneruje na konsoli alarm.

B.10. Wymagania dla systemu SIEM dotyczące funkcjonalności CMBD.

- 1) System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa.
- 2) System musi posiadać możliwość wizualizacji dokumentacji w formie interaktywnej mapy sieci, obejmującej strefy bezpieczeństwa, urządzenia sieciowe oraz punkty końcowe w tym serwery i komputery.
- 3) 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.
- 4) System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

C. Wymagania dla serwera systemu SIEM.

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1.	Obudowa	Obudowa o wysokości maks. 2U dedykowana do montażu w szafie rack 19", wraz z zestawem szyn montażowych. Możliwość instalacji minimum 12 dysków 3,5" Hot-Swap oraz możliwość opcjonalnego montażu dwóch dodatkowych dysków 2,5" Hot-Swap.
2.	Procesor	Zainstalowany minimum jeden procesor uzyskujący co najmniej 40200 punktów w teście wydajności wielowatkowej procesorów publikowanym na stronie www.cpubenchmark.net (w załączeniu obraz strony zawierający wyniki testu). Serwer musi umożliwiać rozbudowę do konfiguracji dwuprocesorowej.
3.	Pamięć RAM	Zainstalowane minimum 256 GB pamięci RAM ECC w nie więcej niż czterech modułach. Możliwość rozbudowy pamięci RAM do minimum 2 TB.
4.	Płyta główna	Płyta główna dedykowana do pracy w oferowanym serwerze, przystosowana do pracy ciągłej 24/7.
5.	Złącza PCIe	Wymagane minimum trzy wolne (nieobsadzone) złącza PCIe Gen4, w tym: – minimum jedno złącze PCIe Gen4 pracujące z prędkością x16, – minimum dwa złącza PCIe Gen4 pracujące z prędkością x8.
6.	Dysk twardy	Zainstalowane minimum 3 dyski SATA Hot-Swap o pojemności minimum 16 TB każdy, przeznaczone do pracy w serwerach i do pracy ciągłej (24/7). Zainstalowane minimum 3 dyski SSD o pojemności 1,94 TB każdy, klasy serwerowej.
7.	Karta sieciowa	Zainstalowane minimum dwie karty sieciowe, każda wyposażona w minimum 2 porty SFP+ 10 Gbit/s, wraz z modułami SFP+.
8.	Karta graficzna	Zintegrowana z układem zdalnego zarządzania serwerem karta graficzna.
9.	Porty	Minimum 1 port Ethernet RJ-45 dedykowany dla interfejsu zdalnego zarządzania. Minimum 4 porty USB, z czego nie mniej niż 2 w standardzie USB 3.1 lub nowszym. Możliwość instalacji portu szeregowego (COM) podłączonego bezpośrednio do płyty głównej, bez użycia adapterów do innych portów.
10.	Kontroler dyskowy	Minimum jeden sprzętowy kontroler SAS 12G, obsługujący poziomy RAID 0, 1, 5, 6, 10, 50, 60, wyposażony w minimum 4 GB pamięci cache. Kontroler wraz z okablowaniem i backplane (w tym ekspanderem SAS, jeżeli jest wymagany) musi zapewniać obsługę wszystkich zatok dyskowych oferowanej obudowy, tj. minimum 12 zatok 3,5" Hot-Swap.
11.	Zasilanie	Zainstalowane minimum dwa redundantne zasilacze Hot-Plug, każdy o mocy maksymalnej 1000 W, posiadające certyfikat efektywności energetycznej Platinum.
12.	Zarządzanie oraz obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej o serwera niezależnie od jego stanu (także podczas startu, restartu OS). Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja.
13.	Karta/moduł zarządzający i system zarządzania	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: <ul style="list-style-type: none">• monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe• praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP• dostęp do karty zarządzającej poprzez<ul style="list-style-type: none">- dedykowany port RJ45 z tyłu serwera lub- przez współdzielony port zintegrowanej karty sieciowej serwera





Cyberbezpieczny Samorząd

		<p>dostęp do karty możliwy</p> <ul style="list-style-type: none">- z poziomu przeglądarki webowej (GUI)- z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)- z poziomu skryptu (XML/Perl)- poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) <ul style="list-style-type: none">• wbudowane narzędzia diagnostyczne• zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego• obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przysyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie• wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników• przysyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)• obsługa zdalnego serwera logowania (remote syslog)• wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów• mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie• funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności• monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji• konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)• zdalna aktualizacja oprogramowania (firmware)• zarządzanie grupami serwerów, w tym:<ul style="list-style-type: none">- tworzenie i konfiguracja grup serwerów- sterowanie zasilaniem (wł/wył)- ograniczenie poboru mocy dla grupy (power capping)- aktualizacja oprogramowania (firmware)- wspólne wirtualne media dla grupy• możliwość równoczesnej obsługi przez 6 administratorów• autentykacja dwuskładnikowa (Kerberos)• wsparcie dla Microsoft Active Directory• obsługa SSL i SSH• enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli• wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API• wsparcie dla Integrated Remote Console for Windows clients <p>możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)</p>
14.	System operacyjny	<p>Microsoft Windows Server 2025 Standard – 16 Core License Pack lub równoważny</p> <ul style="list-style-type: none">• Zamawiający wymaga dostarczenia wraz z serwerem systemu operacyjnego klasy serwerowej.• Dostarczone licencje muszą zapewniać prawo do downgrade do niższych wersji, w tym do Windows Server 2019 Standard.• W przypadku dostarczenia licencji OEM dla oprogramowania Microsoft, Wykonawca zobowiązany jest dostarczyć nośniki instalacyjne oraz klucze licencyjne umożliwiające instalację i użytkowanie zarówno Windows Server 2025 Standard, jak i Windows Server 2019 Standard.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

		<ul style="list-style-type: none">W przypadku gdy oferowany serwer posiada więcej niż 16 rdzeni fizycznych, Wykonawca zobowiązany jest dostarczyć dodatkowe pakiety licencyjne typu Core License Pack w ilości zapewniającej licencjonowanie wszystkich rdzeni fizycznych serwera, zgodnie z zasadami licencjonowania producenta.Wszystkie oferowane i dostarczone licencje muszą być niewyłączne i bezterminowe. <p>Zamawiający dopuszcza zaoferowanie oprogramowania równoważnego względem Microsoft Windows Server 2025 Standard, pod warunkiem spełnienia łącznie poniższych wymagań:</p> <ul style="list-style-type: none">oprogramowanie równoważne musi:<ul style="list-style-type: none">być kompatybilne funkcjonalnie z oprogramowaniem referencyjnym,umożliwiać integrację z posiadaną przez Zamawiającego usługą Active Directory, w tym obsługę Zasad Grup (GPO) oraz WMI,być instalowane bezpośrednio na sprzęcie fizycznym serwera jako system operacyjny klasy serwerowej,posiadać możliwość aktualizacji w oparciu o poprawki bezpieczeństwa publikowane przez producenta oraz możliwość ich lokalnej dystrybucji bez dostępu do Internetu,znajdować się na liście systemów operacyjnych wspieranych przez producenta oferowanego serwera.Licencja musi być bezterminowa (wieczysta) i nie może być licencją czasową, subskrypcyjną ani opartą o rozwiązania chmurowe.Zamawiający nie dopuszcza licencji OEM dla rozwiązań równoważnych.Zastosowanie rozwiązania równoważnego nie może powodować konieczności wykonania dodatkowych prac integracyjnych, migracyjnych ani ponoszenia dodatkowych kosztów po stronie Zamawiającego.W przypadku zaoferowania rozwiązania równoważnego Wykonawca przeprowadzi na własny koszt instruktaż administratorów Zamawiającego w wymiarze co najmniej 16 godzin.
15.	Wsparcie dla systemów	<ul style="list-style-type: none">Microsoft Windows Server min. 2019, 2022.Red Hat Enterprise Linux (RHEL)SUSE Linux Enterprise Server (SLES)
16.	Gwarancja	24 miesiące gwarancji liczone od daty odbioru przedmiotu umowy.



Wydajność wielowątkowa, ranga od 1 do 801
Zaktualizowano 30 grudnia 2025 r.

Processor	Znak procesora	
AMD Ryzen Threadripper PRO 995WX	176 398	NA
AMD EPYC 9755	166 328	12 984.00 zł*
Procesor AMD EPYC Embedded 9755	164 010	NA
AMD EPYC 9965	160 542	14 813.00 zł*
AMD EPYC 9655P	160 490	10 811.00 zł*
Procesor AMD EPYC 9B45	158 790	13 564.00 zł*
AMD EPYC 9655	156 110	11 852.00 zł*
AMD Ryzen Threadripper PRO 9985WX	153 064	7999.00 USD
AMD EPYC 9845	152 985	13 564.00 zł*
AMD EPYC 9575F	147 606	7 687.00 zł*
AMD Ryzen Threadripper PRO 7995WX	143 785	9499.95 USD*
AMD Ryzen Threadripper 9980X	142 585	4599.99 USD
AMD Ryzen Threadripper 7980X	136 063	4743.28 dolarów
AMD EPYC 9555P	135 990	7983.00 zł*
AMD EPYC 9565	135 221	10 486.00 zł*
AMD Ryzen Threadripper PRO 7985WX	132 610	8 093.24 USD*
AMD EPYC 9745	130 698	12 141.00 zł*
Intel Xeon 6960P	130 659	9 625.00 USD*
Procesor AMD EPYC 9B14	126 288	NA
Procesor AMD EPYC 9J14	124 637	NA
AMD EPYC 9475F	122 476	7 592.00 zł*
AMD EPYC 9684X	122 017	7750.00 zł*
AMD EPYC 9654	119 246	5180.00 USD
Intel Xeon 6781P	117 946	8960.00 zł*
AMD EPYC 9V74	117 606	NA
AMD EPYC Embedded 9654P	116 927	NA
AMD EPYC 9455P	116 912	4819.00 zł*
AMD EPYC 9R14	116 475	NA
AMD EPYC 9654P	116 324	5345.00 USD
Procesor AMD EPYC 9D25	114 275	NA
AMD EPYC 9634	107 944	3949.99 USD*
AMD Ryzen Threadripper 9970X	107 237	2299.99 USD
AMD Ryzen Threadripper PRO 9975WX	106 464	4299.99 USD
AMD EPYC 9554P	104 920	4550.00 zł*
AMD EPYC 9554	103 544	3474.45 dolarów
AMD EPYC 9734	102 286	6 598.00 zł*
AMD EPYC 9474F	102 255	6203.66 zł*
Intel Xeon 6747P	101 685	6497.00 zł*
Intel Xeon 6741P	100 660	4421.00 zł*

Cena (USD)

AMD Ryzen Threadripper 7970X	99 203	2149.99 USD
Intel Xeon w9-3595X	98 602	5 889.00 zł*
AMD EPYC 9754	98 450	3499.95 USD
AMD EPYC 9355P	97 249	2998.00 zł*
AMD Ryzen Threadripper PRO 7975WX	95 891	3689.21 dolarów
AMD EPYC 9375F	95 768	5 306.00 zł*
AMD Ryzen Threadripper PRO 5995WX	94 959	3220.00 USD
AMD EPYC 9454P	94 708	3450.00 zł*
Intel Xeon Platinum 8570	93 722	9 595.00 USD*
AMD Ryzen Threadripper PRO 9965WX	93 124	2699.99 USD
AMD Ryzen Threadripper 9960X 24-rdzeniowy	92 657	NA
AMD EPYC 7773X	91 340	1 563.00 USD*
Intel Xeon 6740P	90 684	4650.00 zł*
Intel Xeon w9-3495X	90 418	5 889.00 zł*
Intel Xeon Platinum 8470 @2.00 GHz	89 850	9 359.00 zł*
AMD EPYC 9534	89 077	3649.95 USD
Intel Xeon Platinum 8488C	88 667	NA
AMD EPYC 9454	87 961	3250.00 dolarów
Intel Xeon 6780E	86 734	8 513.00 zł*
Intel Xeon w9-3575X	85 735	3 789.00 zł*
Procesor AMD EPYC 7J13	84 786	NA
AMD EPYC 9275F	84 620	3439.00 zł*
AMD EPYC 7763	84 440	1532.06 dolarów
Intel Xeon Platinum 8592+	84 013	11 600.00 USD*
AMD Ryzen Threadripper 7960X	83 584	1109.82 USD
AMD EPYC 7R43	83 535	NA
AMD Ryzen Threadripper PRO 3995WX	83 279	2900.99 USD*
AMD EPYC 7713	83 018	1299.95 USD
Intel Xeon Max 9480	82 913	920.40 zł*
AMD Ryzen Threadripper PRO 7965WX	82 250	2532.88 dolarów
AMD EPYC 9374F	82 009	5421.00 USD
Procesor AMD EPYC 7663	81 821	NA
Procesor AMD EPYC 7V13	81 764	NA
Procesor AMD EPYC 7T83	81 757	NA
AMD EPYC 7713P	81 582	2443.73 USD*
AMD EPYC 7K23	81 183	NA
AMD Ryzen Threadripper 3990X	79 705	2499.99 USD
Intel Xeon Platinum 8568Y+	79 683	6497.00 zł*
Intel Xeon 6737P	79 634	4995.00 zł*
Procesor AMD EPYC 7B13	79 390	NA
AMD EPYC 7R13	79 046	NA
AMD EPYC 7643P	77 307	2722.00 zł*
Procesor AMD EPYC 7C13	76 363	NA

AMD EPYC 7643	76 259	1 267.00 USD*
Intel Xeon 6740E	76 167	5 265.00 zł*
AMD EPYC 9255	75 809	NA
AMD Ryzen Threadripper PRO 5975WX	75 012	1840.00 USD
Intel Xeon Platinum 8461V	74 982	4491.00 zł*
Intel Xeon 6732P	74 849	5 295.00 zł*
AMD EPYC 9354P	74 626	2280.00 zł*
Intel Xeon 6730P	74 113	3726.00 zł*
AMD EPYC 9274F	73 982	2490.00 USD
AMD EPYC 9354	73 892	2819.00 USD
Intel Xeon Gold 6548Y+	73 387	3726.00 zł*
AMD EPYC 7662	72 298	4 579.00 zł*
Apple M3 Ultra 32 Core	72 171	NA
AMD EPYC 9384X	72 121	5 529.00 zł*
Ampere Altra Max	72 121	NA
AMD EPYC 8534P	71 900	8110.00 USD
AMD Ryzen 9 9950X3D2	71 585	NA
Intel Xeon w7-3565X	70 982	3025.16 dolarów*
AMD EPYC 7V12	70 622	NA
Intel Xeon Gold 6448H	70 280	3 658.00 zł*
AMD Ryzen 9 9950X3D	70 159	675.59 USD
AMD EPYC 7H12	69 633	1475.00 USD
AMD EPYC 7742	69 448	613.97 USD
AMD EPYC 7573X	69 432	5 250.00 USD*
AMD EPYC 7702	69 060	2570.04 dolarów
Apple M3 Ultra 28 Core	68 704	NA
AMD EPYC 4585PX	68 596	799.85 USD
Intel Xeon Platinum 8571N	68 385	NA
Intel Xeon W7-3555	67 754	2339.00 zł*
AMD Ryzen Threadripper PRO 9955WX	67 444	1499.99 USD
Intel Core Ultra 9 285K	67 426	516.00 zł
AMD Ryzen Threadripper PRO 5965WX	66 638	1499.00 USD
AMD EPYC 7543P	66 590	5104.00 zł*
AMD EPYC 8434P	66 490	5932.51 dolarów
Intel Xeon w7-2595X	66 049	2331.37 dolarów*
Procesor AMD EPYC 7B12	66 044	NA
AMD EPYC 9175F	65 894	4256.00 zł*
AMD Ryzen 9 9950X	65 860	559.98 USD
AMD EPYC 9334	65 568	2350.00 zł*
Intel Xeon w9-3475X	65 016	3859.99 USD*
Intel Xeon 6521P	64 761	1250.00 zł*
Intel Xeon Platinum 8469C	64 513	NA
AMD EPYC 75F3	64 505	1836.00 USD
AMD EPYC 4564P	64 443	670.15 zł

Intel Core Ultra 7 270K Plus	64 360	NA
AMD EPYC 4565P	64 068	589.00 zł*
Intel Xeon 6520P	64 010	1 295.00 USD*
AMD EPYC 7R32	63 969	NA
AMD EPYC 7702P	63 692	1547.00 USD
AMD EPYC 9254	63 540	1995.00 USD
AMD Ryzen Threadripper 3970X	62 918	1629.99 USD
Intel Xeon Gold 6438Y+	62 660	3141.00 zł*
Intel Xeon Platinum 8454H	62 347	6 540.00 USD*
AMD Ryzen 9 7950X3D	62 321	560.62 zł
Intel Xeon Platinum 8380 @ 2.30 GHz	62 318	7 301.00 zł*
AMD Ryzen Threadripper PRO 3975WX	62 275	1399.99 USD
AMD Ryzen 9 7950X	62 262	537.67 zł
AMD Ryzen 9 9955HX3D	62 071	NA
AMD EPYC 7543	61 909	3 761.00 zł*
Intel Xeon w7-3465X	61 600	3077.93 USD*
Intel Xeon 6710E	61 404	2 749.00 zł*
Intel Xeon 654	61 351	NA
Intel Xeon Gold 5520+	61 227	1849.99 USD*
AMD EPYC 74F3	60 666	2398.95 USD
Intel Core i9-13900KS	60 575	707.00 zł
Intel Core i9-14900KS	60 478	689.99 USD
Intel Xeon Gold 6448Y	60 449	3 583.00 zł*
Intel Xeon Gold 5512U	60 381	1 230.00 USD*
Intel Xeon Gold 6542Y	60 144	2878.00 zł*
AMD Ryzen Threadripper PRO 7955WX	60 053	NA
AMD EPYC 4584PX	59 990	1132.68 dolarów
AMD EPYC 7513	59 745	1587.79 USD
Procesor AMD EPYC 7K62	59 533	NA
AMD EPYC 7642	59 333	1482.45 dolarów
AMD EPYC 7473X	59 280	NA
Intel Xeon W-3375 @ 2.50 GHz	59 091	4499.00 zł*
Intel Xeon Gold 6421N	58 797	2368.00 zł*
Intel Core Ultra 7 265K	58 732	293.99 USD
Intel Core Ultra 7 265KF	58 671	269.99 USD
Intel Xeon Gold 6442Y	58 534	2878.00 zł*
Intel Core i9-14900K	58 517	448.95 USD
Intel Xeon W7-3545	58 453	2039.00 zł*
Intel Core i9-14900KF	58 382	442.99 USD
Intel Core i9-13900K	58 337	549.99 USD
Intel Xeon Gold 5420+	58 209	1 848.00 USD*
AMD Ryzen 9 7945HX3D	57 846	NA
AMD EPYC 9135	57 808	1 214.00 zł*
Intel Core Ultra 9 285HX	57 799	NA

Intel Core i9-13900KF	57 738	462.76 zł
Ampere ARM - 192 rdzenie 3200 MHz	57 444	NA
Intel Xeon Gold 6423N	57 434	2161.00 zł*
AMD EPYC 7552	57 414	1650.00 USD
Intel Core Ultra 9 285	57 377	534.00 zł
ARM Neoverse-V2 72 rdzeń 3465 MHz	57 369	NA
Intel Xeon W-3365 @ 2.70 GHz	57 312	3851.00 zł*
ARM Neoverse-V2 72 rdzeń 3447 MHz	57 299	NA
ARM Neoverse-V2 72 rdzeń 3519 MHz	57 240	NA
Intel Xeon Gold 6414U	57 200	2 296.00 zł*
Intel Xeon w7-2495X	57 168	2904.60 zł*
AMD EPYC 8324P	57 127	3890.00 USD
AMD EPYC 7443P	56 808	1045.00 USD
Intel Xeon Platinum 8362 @ 2.80 GHz	56 787	5 740.00 USD*
AMD EPYC 7443	56 743	2230.99 USD*
ARM Neoverse-V2 96 rdzeni 0 MHz	56 557	NA
AMD Ryzen Threadripper PRO 9945WX	56 471	NA
ARM Neoverse-V2 72 rdzeń 3411 MHz	56 432	NA
AMD Ryzen 9 9900X3D	56 273	569.00 zł
Intel Xeon Platinum 8375C @ 2.90 GHz	56 202	NA
Intel Core Ultra 9 275HX	56 098	NA
AMD Ryzen 9 9955HX	55 800	NA
AMD Ryzen AI Max+ 395	55 001	NA
Intel Xeon W7-3455	54 998	2489.00 zł*
AMD Ryzen Threadripper 3960X	54 763	870.99 USD
Intel Xeon w5-3535X	54 737	1960.94 USD*
AMD Ryzen 9 9900X	54 503	419.00 zł
Intel Xeon Platinum 8358 @ 2.60 GHz	54 416	4298.95 USD
AMD Ryzen 9 7945HX	54 323	NA
AMD EPYC 4545P	54 279	635.49 zł
Intel Xeon Platinum 8360Y @ 2.40 GHz	54 078	2799.97 USD*
AMD Ryzen 9 7940HX	53 584	NA
Intel Xeon w7-2475X	53 211	1906.93 USD*
AMD EPYC 9174F	53 067	2275.00 zł*
Intel Xeon Gold 6430	53 066	1868.81 dolarów
Intel Xeon w7-2575X	52 951	1 953.52 USD*
Procesor AMD EPYC 7F72	52 840	938.40 zł*
Intel Xeon Gold 6438N	52 789	3351.00 zł*
Intel Xeon w5-2565X	52 378	1 551.64 USD*
Intel Core i7-14700KF	52 237	433.99 USD
AMD EPYC 7502	52 198	825.00 zł
AMD Ryzen 9 8945HX	52 170	NA
Intel Core i7-14700K	52 169	363.88 USD

Intel Xeon Gold 6348 @ 2.60 GHz	51 843	2097.00 USD
AMD Ryzen AI Max+ Pro 395	51 788	NA
Intel Xeon Gold 6418H	51 711	2065.00 zł*
AMD Ryzen 9 9850HX	51 665	NA
Intel Xeon Gold 5412U	51 599	1 113.00 zł*
AMD Ryzen 9 7900X	51 318	314.00 zł
Intel Xeon 6511P	51 286	815.00 zł*
AMD EPYC 7502P	51 206	1298.95 USD
Intel Xeon Gold 6544Y	51 181	3 622.00 zł*
AMD Ryzen 9 8940HX	51 063	NA
Apple M2 Ultra 24 Core	50 828	NA
Intel Xeon Gold 6554S	50 777	3232.62 dolarów
AMD EPYC 7532	50 726	225.00 zł
AMD EPYC 7413	50 641	1375.00 USD
AMD EPYC 4484PX	50 547	NA
AMD Ryzen 9 7900X3D	50 222	529.80 zł
Intel Xeon Platinum 8562Y+	50 189	5945.00 zł*
AMD EPYC 4465P	50 189	420.19 zł
Intel Xeon 6736P	50 072	NA
AMD Ryzen Threadripper PRO 7945WX	49 756	NA
Intel Core Ultra 7 265	49 721	347.00 zł
Intel Core Ultra 7 255HX	49 608	NA
Intel Core Ultra 7 265F	49 427	276.77 zł
Intel Xeon Platinum 8347C @ 2.10 GHz	49 386	NA
Intel Xeon 6517P	49 099	1195.00 zł*
Montaż Jintide C5418Y	49 045	NA
Intel Xeon W7-3445	48 991	1 989.00 USD*
AMD EPYC 9224	48 967	1790.00 USD
AMD EPYC 7R12	48 934	NA
Intel Xeon Gold 6314U @ 2.30 GHz	48 916	2 782.00 zł*
AMD EPYC Embedded 8224P	48 869	NA
AMD Ryzen Threadripper PRO 5955WX	48 804	999.29 USD
Intel Core i9-13900F	48 717	529.95 USD
Intel Core Ultra 7 265HX	48 626	NA
AMD EPYC 9115	48 504	726.00 zł*
AMD EPYC 7453	48 453	1438.00 USD
AMD Ryzen 9 PRO 9945	48 288	NA
Intel Xeon W-3345 @ 3.00 GHz	48 140	2499.00 zł*
AMD Ryzen 9 7900	48 136	408.35 USD
AMD EPYC 9184X	48 058	3750.00 zł*
Intel Xeon w5-2555X	47 638	1 069.00 USD*
AMD EPYC 4464P	47 307	NA
ARM Ampere-1a 192 rdzenie 2600 MHz	47 202	NA
Intel Xeon Gold 6444Y	47 176	3 622.00 zł*
Intel Xeon Gold 6342 @ 2.80 GHz	47 076	3295.95 USD*

AMD Ryzen 9 PRO 7945	46 904	802.78 zł*
Intel Xeon Platinum 8368Q @ 2.60 GHz	46 681	NA
Intel Core i9-14900F	46 651	572.58 USD
Intel Xeon W-3175X @ 3.10 GHz	46 125	3039.28 USD*
AMD EPYC 73F3	46 103	2331.10 dolarów
AMD EPYC 7402	46 012	249.00 zł
Intel Xeon Gold 6530	45 989	2011.71 dolarów
Intel Core i9-13980HX	45 927	668.00 zł*
Intel Core i7-13700K	45 769	529.95 USD
AMD EPYC 7452	45 764	1298.95 USD
Intel Core i7-13700KF	45 724	423.47 zł
Intel Xeon Gold 5418Y	45 660	1 483.00 USD*
Intel Xeon Gold 6336Y @ 2.40 GHz	45 517	2500.00 dolarów
Intel Xeon w5-3525	45 498	1 339.00 USD*
AMD EPYC 8224P	45 421	1046.57 dolarów
AMD EPYC 7542	45 359	729.72 zł
AMD Ryzen 9 5950X	45 343	344.00 zł
Intel Core i9-14900	45 292	568.42 zł
Intel Xeon w5-2465X	45 257	1527.95 USD*
Intel Core i9-13900	45 167	449.99 USD
Intel Xeon w5-3435X	44 998	1 691.23 USD*
AMD Ryzen 9 7845HX	44 911	NA
Intel Xeon Gold 6538N	44 895	3351.00 zł*
Intel Core i9-14900HX	44 519	679.00 zł*
Intel Xeon Silver 4416+	44 140	1 176.00 zł*
AMD Ryzen 9 5900XT	44 078	349.00 zł
Apple M4 Max 16 rdzeni	44 017	NA
AMD EPYC 7402P	43 855	1090.00 USD
AMD EPYC 9124	43 646	1015.00 USD
AMD EPYC 7343	43 644	853.81 USD
Intel Core i9-12900KS	43 532	351.80 zł
Intel Core Ultra 5 245K	43 392	207.99 USD
Intel Core Ultra 5 245KF	43 357	209.99 USD
AMD Ryzen AI Max Pro 390	43 237	NA
ARM Neoverse-N1 128 rdzeń 2800 MHz	43 111	NA
Intel Xeon Gold 6526Y	43 018	1 517.00 USD*
AMD Ryzen 7 8840HX	42 922	NA
AMD Ryzen 7 7840HX	42 758	NA
Intel Core i9-13900T	42 514	549.00 zł*
Intel Xeon Gold 6312U @ 2.40 GHz	42 443	1809.59 USD*
Intel Core i9-13900HX	42 346	668.00 zł*
AMD EPYC 7D12	42 285	NA
Intel Core i7-13790F	42 202	322.04 zł
Intel Xeon Gold 6338N @ 2.20 GHz	42 086	4671.69 USD*

Intel Xeon Gold 6330 @ 2.00 GHz	42 072	1270.00 USD
AMD Ryzen AI Max 390	42 070	NA
Intel Core i7-14700F	41 470	302.97 USD
Procesor AMD EPYC 7F52	41 388	1895.30 zł*
Apple M1 Ultra 20 Core	41 359	NA
Apple M3 Max 16 rdzeni	41 267	NA
Intel Core i9-12900K	41 162	299.00 zł
Intel Core i9-13950HX	41 056	590.00 zł*
AMD EPYC 7313P	41 017	824.00 zł
Intel Core i7-14790F	40 904	NA
Intel Core i7-14700	40 892	429.00 zł
Intel Core i9-12900KF	40 828	279.97 USD
Intel Xeon Platinum 8275CL @ 3.00 GHz	40 794	NA
Intel Xeon w5-2545	40 782	889.00 zł*
Intel Xeon 6515P	40 720	740.00 zł*
Intel Xeon Gold 6416H	40 606	1 444.00 USD*
Intel Core Ultra 7 265T	40 438	NA
Intel Core i9-13900E	40 418	554.00 zł*
AMD EPYC 7352	40 370	725.00 zł
Intel Core Ultra 5 245HX	40 281	NA
Intel Xeon Gold 6338 @ 2.00 GHz	40 225	1604.29 USD
AMD Ryzen Threadripper PRO 5945WX	40 128	NA
Intel Core Ultra 5 235HX	40 122	NA
Intel Xeon W-3275M @ 2.50 GHz	40 012	7 453.00 zł*



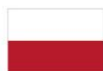
Cyberbezpieczny Samorząd

Widok interaktywnego formularza ofertowego.

UWAGA: Formularza nie należy wypełniać stanowi on jedynie obraz formularza udostępnionego na Platformie e-Zamówienia.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Dane identyfikacyjne formularza ofertowego

Numer wersji formularza
ofertowego: 1

Data udostępnienia formularza
ofertowego:

I. Dane podstawowe

Nazwa zamówienia/umowy
ramowej: Dostawa serwera oraz oprogramowania SIEM

Identyfikator postępowania: ocds-148610-8cc4b64d-ee48-4914-a7ff-4b74f2f6bcab

Numer referencyjny
postępowania: ZF.272.1.21.2025

Rodzaj oferty: Oferta

II. Zamawiający

Nazwa (firma) zamawiającego: POWIAT RZESZOWSKI

Krajowy numer identyfikacyjny: REGON 690581413

II.1 Zamawiający Adres

Ulica: ul. Grunwaldzka 15

Miejscowość: Rzeszów

Kod pocztowy: 35-959

Województwo: Podkarpackie

Kraj: Polska

III. Wykonawca

Nazwa (firma) wykonawcy:

Krajowy numer identyfikacyjny:

Status Wykonawcy:

III.1 Wykonawca Adres

Ulica:

Miejscowość:

Kod pocztowy:

Województwo:

Kraj:

Telefon:

Faks:

Adres poczty elektronicznej:

Adres strony internetowej
wykonawcy:

III.2 Wykonawca dane osoby reprezentującej

Czy wykonawca jest reprezentowany przez pełnomocnika: ☒ TAK ☐ NIE

Dane osoby reprezentującej (imię i nazwisko, podstawa reprezentacji - pełnomocnictwo, KRS, umowa spółki, inne):

III.3 Wykonawca Osoba do kontaktu

Dane osoby do kontaktu (imię i nazwisko, email, telefon):

IV. Oświadczenia

Wykonawca załącza do oferty oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy: ☒ TAK ☐ NIE

Adresy bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz. U. z 2024 r. poz. 1557 z późn. zm.), gdzie można uzyskać oświadczenia lub inne dokumenty dotyczące wykonawcy:

<https://ekrs.ms.gov.pl/web/wyszukiwarka-krs/strona-glowna/index.html> ☒ TAK ☐ NIE

Rodzaje dokumentów dostępne pod wskazanym adresem:

<https://prod.ceidg.gov.pl/CEIDG/CEIDG.Public.UI/Se arch.aspx>

☒ TAK ☐ NIE

Rodzaje dokumentów dostępne pod wskazanym adresem:

Inne bazy

☒ TAK ☐ NIE

Adres:

Rodzaje dokumentów dostępne pod wskazanym adresem:

Dokumenty i oświadczenia znajdujące się w posiadaniu zamawiającego (rodzaj dokumentu, nazwa i numer postępowania, w którym zostały złożone):

Oświadczenie wykonawcy o spełnieniu obowiązku informacyjnego z art. 13 lub 14 Rozporządzenia Parlamentu Europejskiego i Rady 2016/679. (Klauzula RODO):

☒ TAK ☐ NIE

Treść oświadczenia*:

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpodstawnie lub po podstawnie pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

Wykonawca załącza do oferty oświadczenie o braku podstaw wykluczenia: TAK

V. Zamówienie zastrzeżone

Nie dotyczy

VI. Tajemnica przedsiębiorstwa

Oferta zawiera tajemnicę przedsiębiorstwa: ☒ TAK ☐ NIE

Informacje stanowiące tajemnicę przedsiębiorstwa zawarte są w następujących dokumentach (załącznikach do oferty):

Uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa zawarte jest w następującym dokumencie (załączniku do oferty):

VII. Katalog elektroniczny

Wykonawca załącza do oferty katalog elektroniczny: ☒ TAK ☐ NIE

VIII. Kryteria oceny ofert

Kod waluty: PLN

Rodzaj kryterium: Cena

Cena:

Wartość słownie:

IX. Obowiązek podatkowy

Wybór ofert będzie prowadził do powstania u zamawiającego obowiązku podatkowego: ☒ TAK ☐ NIE

Nazwa i wartość towaru lub usługi, której dostawa lub świadczenie będzie prowadzić do powstania obowiązku podatkowego:

X. Sposób realizacji zamówienia

Wykonawca zamierza powierzyć wykonanie części zamówienia podwykonawcy: ☒ TAK ☐ NIE

Nazwa podwykonawcy, jeżeli jest znany:

Zakres zamówienia, który wykonawca zamierza
powierzyć do realizacji podwykonawcy:

XII. Lista załączników

Lista
załączników:

Wzór dokumentu, nie wypełniać



Cyberbezpieczny Samorząd

Formularz rzeczowo – finansowy

Lp.	Określenie urządzenia/oprogramowania	Ilość	Stawka podatku VAT (%)	Wartość brutto (zł)
1	Serwer do SIEM PRODUCENT, NAZWA : Numer produktu lub kod producenta: Zainstalowany system operacyjny: LICENCJA na system operacyjny bezterminowa (wieczysta). OKRES GWARANCJI: 24 miesiące.	1 szt.	23	
2	Oprogramowanie SIEM PRODUCENT, NAZWA : LICENCJA: bezterminowa (wieczysta).	1 szt.	23	
RAZEM WARTOŚĆ BRUTTO				

Oświadczam, że wszystkie oferowane urządzenia i oprogramowanie są zgodne z wymaganiami funkcjonalnymi i technicznymi określonymi w szczegółowym opisie przedmiotu zamówienia, a także posiadają parametry techniczne, nie gorsze niż parametry określone w szczegółowym opisie przedmiotu zamówienia.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

WYKONAWCA

.....

.....

(nazwa, adres)

OŚWIADCZENIE

o niepodleganiu wykluczeniu z postępowania

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych,
zwanej dalej „ustawą pzp” w postępowaniu o udzielenie zamówienia publicznego,
pn.: **Dostawa serwera oraz oprogramowania SIEM.**

W zakresie przesłanek wykluczenia z postępowania

- 1) Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art.108 ust.1 a także art.109 ust.1 pkt 4 ustawy pzp.
- 2) Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust.1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2025 r. poz.514).
- 3) 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 pkt 1,2,5 lub art.109 ust.1 pkt 4 ustawy pzp).
Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art.110 ust. 2 ustawy pzp podjąłem następujące środki naprawcze:

.....
.....

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.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

Projektowane postanowienia umowy

Umowa nr ZF.272.1.21.2025

zawarta w dniu /zawarta w dniu złożenia ostatniego kwalifikowanego podpisu elektronicznego w Rzeszowie pomiędzy:

Powiatem Rzeszowskim z siedzibą w Rzeszowie przy ul. Grunwaldzkiej 15, 35-959 Rzeszów,
REGON: 690581413, NIP: 8132919572, który reprezentują:

.....

.....

zwanym dalej w treści umowy **Zamawiającym**

a

.....

zwanym/zwaną dalej w treści umowy **Wykonawcą**

łącznie zwanymi dalej Stronami.

W wyniku przeprowadzenia postępowania o udzielenie zamówienia publicznego w trybie podstawowym zgodnie z art. 275 pkt.1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320 ze zm.), zwanej dalej ustawą pzp, strony zawarły umowę następującej treści:

PRZEDMIOT UMOWY

§1

1. Przedmiotem umowy jest dostawa, instalacja i wdrożenie oprogramowania SIEM (Security Information and Event Man) wraz z serwerem do SIEM (Security Information and Event Managment) w ramach projektu pn.: „Zwiększenie poziomu bezpieczeństwa cyfrowego Powiatu Rzeszowskiego oraz jego jednostek podległych” współfinansowanego przez Unię Europejską w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny samorząd” o numerze FERC.02.02-CS.01-001/23.
2. Serwer oraz oprogramowanie, o których mowa w ust. 1 wymienione są w „Wykazie rzeczowo-finansowym” stanowiącym załącznik do umowy.
3. Oprogramowanie i serwer musi pochodzić z legalnego kanału dystrybucji producenta, a korzystanie przez zamawiającego z dostarczonego serwera i oprogramowania nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.
4. Dostarczone oprogramowanie musi być fabrycznie nowe, nigdy wcześniej nie instalowane i aktywowane na innym urządzeniu.
5. Wykonawca zobowiązany jest dostarczyć klucze licencyjne lub dokumenty potwierdzające prawo do korzystania z dostarczonego pakietu oprogramowania przez zamawiającego. Potwierdzeniem legalności systemu operacyjnego może być dokument pochodzący od producenta serwera lub wykonawcy (np. oświadczenie, certyfikat OEM, dokument licencyjny, faktura lub inny równoważny dokument), zgodny z obowiązującym modelem licencjonowania producenta oprogramowania.
6. Wszystkie licencje muszą być przeznaczone do użytku na terenie Rzeczypospolitej Polskiej.
7. Dostarczona licencja na oprogramowanie SIEM nie może wprowadzać dodatkowych, licencyjnych ograniczeń w zakresie wielkości przechowywanych danych ani funkcjonalności wyszukiwania informacji w zgromadzonych danych, poza ograniczeniami wynikającymi z parametrów technicznych infrastruktury Zamawiającego.
8. Wszystkie dostarczone licencje muszą być dostarczone w formie bezterminowej (wieczystej).
9. Wykonawca zobowiązany jest do przestrzegania ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2025 r. poz.24).



Cyberbezpieczny Samorząd

10. Serwer musi być:

- 1) fabrycznie nowy, nieużywany przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu poprawnej pracy,
- 2) wyprodukowany nie wcześniej niż w 2024 roku,
- 3) dostarczony wraz z dokumentacją zawierającą: instrukcje obsługi, karty gwarancyjne (w przypadku gdy producent nie stosuje dokumentacji papierowej, wykonawca zobowiązany jest dostarczyć dokumentację w postaci elektronicznej lub wskazać adres strony internetowej do jej pobrania),
- 4) oznakowany w taki sposób, aby możliwa była identyfikacja modelu i producenta oraz dostarczony w oryginalnym opakowaniu,

11. Serwer musi posiadać możliwość sprawdzenia konfiguracji po podaniu numeru seryjnego na stronie producenta lub dystrybutora.

12. Serwer musi posiadać oznakowanie CE zgodnie z wymogami określonymi w Rozporządzeniu Ministra Rozwoju z dnia 2 czerwca 2016 r. w sprawie wymagań dla sprzętu elektrycznego (Dz. U. z 2016 r. poz. 806).

REALIZACJA UMOWY

§2

1. Przedmiot umowy zostanie wykonany w terminie **do 90 dni** od dnia zawarcia umowy.
2. Miejsce dostawy urządzeń: Starostwo Powiatowe w Rzeszowie, ul. Grunwaldzka 15, 35-959 Rzeszów.
3. Wykonawca zgłosi Zamawiającemu termin planowanej dostawy z co najmniej jednodniowym wyprzedzeniem.
4. W ramach realizacji umowy Wykonawca przeprowadzi minimum 32 godziny warsztatów dla grupy administratorów (grupa nie większa niż 5 osób). Zamawiający dopuszcza prowadzenie warsztatów w formie zdalnej. Szczegółowa agenda warsztatów oraz lista uczestników zostaną uzgodnione przez strony. Przez godzinę warsztatową rozumie się 60 minut. Z realizacji warsztatów zostanie sporządzony protokół podpisany przez przedstawicieli stron. Warsztaty swoim zakresem będą obejmować co najmniej:
 - 1) konsultacje administratorów Zamawiającego z certyfikowanym inżynierem Wykonawcy lub producenta w zakresie bieżącej obsługi systemu SIEM/SOAR,
 - 2) szkolenia z zakresu tworzenia nowych reguł w systemie SIEM/SOAR; tworzenia i obsługi zgłoszeń,
 - 3) omówienie nowych typów zagrożeń wykrywanych przez system SIEM/SOAR (tj.: wykrytych, zdiagnozowanych, opisanych, zaimplementowanych do systemu SIEM od czasu ostatnich warsztatów).
5. W ramach wdrożenia oprogramowania SIEM wraz z serwerem do SIEM wykonawca wykona poniższe czynności:
 - 1) dostawę, montaż, fizyczne podłączenie oraz uruchomienie serwera fizycznego przeznaczonego do pracy systemu SIEM, zgodnie z wymaganiami technicznymi określonymi w szczegółowym opisie przedmiotu zamówienia, w tym w zakresie zasilania, połączeń sieciowych oraz redundancji,
 - 2) w ramach podłączenia oraz uruchomienia serwera, Wykonawca zrealizuje następujące czynności:
 - a) dostarczy wszystkie potrzebne kable i elementy niezbędne do montażu i uruchomienia serwera w infrastrukturze IT Zamawiającego (montaż w szafie RACK 19”),
 - b) dostarczy, zamontuje w szafie RACK, uruchomi oraz podłączy serwer do infrastruktury LAN Zamawiającego,
 - c) przeprowadzi kompletną aktualizację oprogramowania układowego dostarczonego serwera do najnowszych obowiązujących wersji,
 - 3) instalację oraz konfigurację systemu operacyjnego serwera,
 - 4) instalację i konfigurację systemu SIEM wraz ze wszystkimi wymaganymi funkcjonalnościami, określonymi w szczegółowym opisie przedmiotu zamówienia, w tym mechanizmami SOAR oraz UEBA,
 - 5) konfigurację systemu SIEM umożliwiającą jego pełne uruchomienie oraz eksploatację w środowisku produkcyjnym Zamawiającego,
 - 6) integrację oraz uruchomienie mechanizmów zbierania, normalizacji, przetwarzania, korelacji oraz analizy zdarzeń bezpieczeństwa ze źródeł danych funkcjonujących w środowisku Zamawiającego,



Cyberbezpieczny Samorząd

niezbędnych do realizacji funkcjonalności systemu określonych w szczegółowym opisie przedmiotu zamówienia,

- 7) konfigurację reguł korelacyjnych, mechanizmów detekcji, klasyfikacji oraz obsługi zdarzeń, a także – jeżeli dotyczy – scenariuszy automatycznej reakcji (playbooków),
- 8) konfigurację mechanizmów obsługi incydentów bezpieczeństwa, w tym przypisywania zdarzeń do operatorów, statusów obsługi, parametrów SLA, rejestrowania działań operatorów oraz prowadzenia dzienników audytowych,
- 9) konfigurację funkcjonalności analitycznych, raportowych oraz audytowych systemu SIEM,
- 10) konfigurację ról, uprawnień oraz kont użytkowników systemu, w tym – jeżeli dotyczy – integrację z mechanizmami uwierzytelniania i autoryzacji stosowanymi przez Zamawiającego,
- 11) konfigurację mechanizmów aktualizacji, utrzymania oraz zabezpieczenia systemu przed nieautoryzowaną modyfikacją, w szczególności w zakresie reguł, playbooków oraz kontekstu systemowego,
- 12) przeprowadzenie testów funkcjonalnych, integracyjnych oraz odbiorowych potwierdzających spełnienie wymagań określonych w szczegółowym opisie przedmiotu zamówienia,
- 13) opracowanie i przekazanie Zamawiającemu kompletnej dokumentacji powdrożeniowej,
- 14) zapewnienie transferu wiedzy umożliwiającego samodzielną administrację, rozwój oraz utrzymanie systemu przez Zamawiającego,
- 15) zapewnienie wsparcia Zamawiającego przy uruchomieniu systemu do pracy produkcyjnej, w tym udział w czynnościach odbiorowych, okres stabilizacji systemu oraz usunięcie wszelkich nieprawidłowości stwierdzonych w trakcie odbioru lub początkowej eksploatacji,
- 16) dostosowanie konfiguracji systemu SIEM do istniejącej architektury teleinformatycznej Zamawiającego, w tym do stosowanych mechanizmów bezpieczeństwa, segmentacji sieci, polityk dostępu oraz obowiązujących procedur wewnętrznych,
- 17) weryfikację poprawności odbieranych danych, w tym ich kompletności, normalizacji, korelacji oraz prezentacji w systemie SIEM, wraz z potwierdzeniem poprawności znaczników czasu, identyfikacji źródeł oraz kompletności rejestrowanych zdarzeń,
- 18) konfigurację systemu SIEM w sposób zapewniający odporność na awarie pojedynczych komponentów oraz możliwość ciągłej pracy zgodnie z wymaganiami określonymi w szczegółowym opisie przedmiotu zamówienia,
- 19) realizację wdrożenia z uwzględnieniem obowiązujących przepisów prawa oraz norm i standardów wskazanych w szczegółowym opisie przedmiotu zamówienia, w szczególności w zakresie bezpieczeństwa informacji, audytu, rejestrowania zdarzeń oraz ochrony danych,
- 20) realizację wdrożenia w sposób niepowodujący uzależnienia Zamawiającego od Wykonawcy w zakresie bieżącej administracji, konfiguracji oraz rozwoju systemu,
- 21) realizację wdrożenia z uwzględnieniem zasad zarządzania zmianą, w tym uzgadniania z Zamawiającym istotnych zmian konfiguracyjnych, architektonicznych oraz integracyjnych,
- 22) zapewnienie bezpieczeństwa danych Zamawiającego przetwarzanych w trakcie wdrożenia, w tym ochrony danych logowych, konfiguracyjnych oraz uwierzytelniających przed nieuprawnionym dostępem, ujawnieniem lub utratą,
- 23) realizację czynności wdrożeniowych bezpośrednio w środowisku Zamawiającego, bez kopiowania danych produkcyjnych poza infrastrukturę Zamawiającego, o ile Zamawiający nie wyrazi na to odrębnej zgody,
- 24) przygotowanie systemu SIEM w sposób umożliwiający jego wykorzystanie na potrzeby audytów, kontroli oraz postępowań wyjaśniających prowadzonych przez Zamawiającego lub uprawnione organy,
- 25) zapewnienie realizacji wdrożenia przez osoby posiadające odpowiednie kwalifikacje oraz doświadczenie w zakresie wdrażania systemów klasy SIEM, SOAR i UEBA,



Cyberbezpieczny Samorząd

- 26) realizację wdrożenia w sposób umożliwiający dalszą rozbudowę systemu SIEM, w tym rozszerzanie zakresu integracji, funkcjonalności oraz wydajności bez konieczności ponownej instalacji systemu,
 - 27) konfigurację synchronizacji czasu systemu SIEM oraz wszystkich zintegrowanych komponentów z infrastrukturą czasu Zamawiającego (NTP), w sposób zapewniający spójność znaczników czasowych wszystkich rejestrowanych zdarzeń,
 - 28) konfigurację mechanizmów wykrywania, raportowania oraz obsługi błędów integracji źródeł danych, w tym informowania Zamawiającego o przerwach w zbieraniu zdarzeń lub nieprawidłowościach w ich przetwarzaniu,
 - 29) konfigurację mechanizmów zarządzania pojemnością, retencją oraz archiwizacją danych w systemie SIEM, zgodnie z wymaganiami Zamawiającego oraz obowiązującymi przepisami i politykami wewnętrznymi,
 - 30) konfigurację systemu SIEM w sposób umożliwiający obsługę zdarzeń masowych oraz gwałtownego wzrostu wolumenu logów bez utraty zdolności detekcji i analizy zdarzeń,
 - 31) konfigurację mechanizmów zabezpieczenia dostępu administracyjnego do systemu SIEM, w tym rejestrowania i audytowania działań administracyjnych oraz – jeżeli wymagane – stosowania uwierzytelniania wieloskładnikowego,
 - 32) konfigurację systemu SIEM w sposób umożliwiający logiczne rozdzielenie ról administracyjnych, operatorskich oraz audytowych, zgodnie z zasadą najmniejszych uprawnień,
 - 33) konfigurację mechanizmów umożliwiających odtworzenie systemu SIEM po awarii, w tym odtworzenie konfiguracji, danych oraz kontekstu systemowego,
 - 34) przekazanie Zamawiającemu pełnej odpowiedzialności operacyjnej nad systemem SIEM po zakończeniu wdrożenia, wraz z kompletem informacji, dostępów oraz dokumentacji niezbędnych do jego samodzielnej eksploatacji,
 - 35) formalne zakończenie wdrożenia poprzez przekazanie systemu do etapu utrzymania wraz z kompletem informacji niezbędnych do jego dalszej eksploatacji.
6. Wykonawca ponosi odpowiedzialność za prawidłowe wykonanie wdrożenia oraz zgodność jego efektów z wymaganiami określonymi w szczegółowym opisie przedmiotu zamówienia.
 7. Przedmiot umowy podlegał będzie odbiorowi. Z czynności odbioru zostanie spisany protokół odbioru z udziałem przedstawicieli Zamawiającego i Wykonawcy.
 8. Zamawiający zastrzega sobie możliwość ustanowienia inspektora, który działając z ramienia Zamawiającego będzie sprawował nadzór nad wdrożeniem oraz dokona kontroli przeprowadzonego wdrożenia. O fakcie powołania inspektora Wykonawca zostanie niezwłocznie poinformowany.

OSOBY DO KONTAKTU W SPRAWIE REALIZACJI UMOWY

§3

1. Strony umowy wskazują następujące osoby, które będą odpowiedzialne za realizację umowy:
 - 1) ze strony Zamawiającego:
 - 2) ze strony Wykonawcy:
(imię nazwisko; adres e-mail; nr telefonu)
2. Każda ze stron ma prawo zmienić osoby, o których mowa w ust. 1, niezwłocznie powiadamiając o tym drugą stronę na piśmie lub za pomocą poczty elektronicznej. Zmiana taka nie wymaga sporządzania aneksu do umowy.

WYNAGRODZENIE I ZASADY ROZLICZANIA

§4

1. Strony ustalają wynagrodzenie brutto za wykonanie przedmiotu umowy, zgodnie z ofertą Wykonawcy, na kwotę brutto: zł (słownie złotych:),
w tym:
wynagrodzenie netto: zł



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

kwota podatku VAT: zł.

2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszystkie koszty związane z właściwym i terminowym wykonaniem przedmiotu umowy.

§5

1. Rozliczenie za wykonanie przedmiotu umowy nastąpi jedną fakturą.
2. Podstawę do wystawienia faktury stanowił będzie protokół odbioru podpisany przez przedstawiciela Zamawiającego i Wykonawcy.
3. Należność za wykonanie przedmiotu umowy płatna będzie przelewem, w terminie do 30 dni od daty doręczenia Zamawiającemu faktury.
4. Wystawiana przez Wykonawcę faktura ma wskazywać:

jako nabywcę:	jako odbiorcę lub płatnika:
Powiat Rzeszowski 35-959 Rzeszów, ul. Grunwaldzka 15 NIP: 813-29-19-572	Starostwo Powiatowe w Rzeszowie 35-959 Rzeszów, ul. Grunwaldzka 15

5. Zamawiający nie udziela zaliczek.

KARY UMOWNE

§6

1. Wykonawca zapłaci Zamawiającemu kary umowne w następujących przypadkach i wysokościach:
 - 1) za zwłokę w wykonaniu przedmiotu umowy - w wysokości 0,2 % wynagrodzenia brutto określonego w § 4 ust. 1, za każdy dzień zwłoki,
 - 2) za zwłokę w wykonaniu naprawy gwarancyjnej w wysokości 0,05 % wynagrodzenia brutto określonego w § 4 ust. 1, za każdy dzień zwłoki liczonej od dnia wyznaczonego na usunięcie awarii,
 - 3) za odstąpienie od umowy z przyczyn leżących po stronie Wykonawcy - w wysokości 10 % wynagrodzenia brutto określonego w § 4 ust. 1.
2. łączna maksymalna wysokość kar umownych nie może przekroczyć 15 % wynagrodzenia brutto określonego w § 4 ust. 1.
3. Zamawiającemu przysługuje prawo dochodzenia odszkodowania przewyższającego wysokość zastrzeżonych kar umownych na zasadach ogólnych.
4. Zamawiający może dokonać potrącenia wymagalnych kar umownych z wynagrodzenia Wykonawcy.

ODSTĄPIENIE OD UMOWY

§7

1. Zamawiający, oprócz przyczyn wskazanych w kodeksie cywilnym, może odstąpić od umowy gdy:
 - 1) ujawnione zostaną okoliczności świadczące o tym, że Wykonawca złożył w postępowaniu prowadzonym w celu udzielenia zamówienia nieprawdziwe dokumenty, pełnomocnictwa lub oświadczenia,
 - 2) w stosunku do wykonawcy zostało wszczęte postępowanie upadłościowe, o ile będzie miało to wpływ na realizację Umowy,
 - 3) Wykonawca nie będzie wywiązywał się z postanowień niniejszej umowy, w tym zwłaszcza w przypadku zwłoki w terminie dostawy przedmiotu umowy, określonego w § 2 ust. 1.
2. Odstąpienie od umowy następuje poprzez złożenie przez Zamawiającego oświadczenia o odstąpieniu od umowy, w formie pisemnej, wraz z uzasadnieniem przyczyn odstąpienia. Oświadczenie to może zostać złożone w terminie 30 dni od dnia powzięcia wiadomości o wystąpieniu przesłanek wymienionych w ust. 1.
3. Odstąpienie od umowy nie ogranicza Zamawiającemu możliwości dochodzenia kar umownych, gwarancji, rękojmi oraz prawa żądania odszkodowania za niewykonanie lub nienależyte wykonanie przedmiotu umowy.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

GWARANCJA I WSPARCIE TECHNICZNE

§8

1. Wykonawca oświadcza, że dostarczony serwer objęty jest gwarancją na okres 24 miesięcy, począwszy od dnia odbioru przedmiotu umowy.
2. W okresie gwarancji Wykonawca zobowiązuje się zapewnić bezpłatne naprawy dostarczonego serwera lub jego bezpłatną wymianę na wolny od wad.
3. W przypadku wystąpienia awarii serwera wykonawca zobowiązuje się do zapewnienia naprawy zgodnie z następującymi zasadami:
 - 1) Naprawa urządzenia rozpoczęta zostanie w następnym dniu roboczym po otrzymaniu zgłoszenia awarii a czas naprawy nie powinien przekroczyć jednego dnia roboczego. Naprawa gwarancyjna dokonywana będzie w miejscu użytkowania urządzenia w godzinach 7:30-18:00. W przypadku zgłoszenia awarii po godz. 15:30 lub w dniu ustawowo wolnym od pracy, jako datę zgłoszenia przyjmuje się datę pierwszego dnia roboczego po dniu, w którym dokonano zgłoszenia. Naprawy nie mogą być realizowane w trybie wysyłkowym (door-to-door) bez wcześniejszego zapewnienia urządzenia zastępczego na zasadach określonych w pkt. 2.
 - 2) W przypadku gdy dokonanie naprawy nie będzie możliwe w miejscu użytkowania lub czas naprawy przekroczy jeden dzień roboczy, wykonawca zobowiązany jest dostarczyć oraz zainstalować, skonfigurować i uruchomić urządzenie zastępcze o parametrach nie gorszych od urządzenia uszkodzonego.
 - 3) W przypadku gdy naprawa urządzenia wykonywana będzie poza miejscem użytkowania, wykonawca transportuje uszkodzone urządzenie do serwisu, a po naprawie do miejsca użytkowania, na własny koszt i ryzyko a także dokonuje ponownej jego instalacji u zamawiającego, po czym nastąpi sprawdzenie poprawności działania naprawionego urządzenia.
 - 4) Na czas naprawy urządzenia poza miejscem użytkowania, niezależnie od rodzaju awarii, dysk twardy lub inny nośnik danych pozostaje u zamawiającego. Jeżeli awarii ulegnie sam dysk twardy lub inny nośnik danych, pozostaje on u zamawiającego i nie będzie oddawany do serwisu w celu naprawy, zaś wykonawca zobowiązany będzie do dostarczania nowego dysku twardego lub innego nośnika danych.
 - 5) W przypadku wystąpienia okoliczności, o których mowa w pkt.3 naprawa urządzenia poza miejscem użytkowania nie może trwać dłużej niż 30 dni roboczych od dnia uruchomienia urządzenia zastępczego, o którym mowa w pkt.2.
4. W przypadku trzykrotnej awarii tego samego urządzenia wykonawca dokona wymiany urządzenia na nowe wolne od wad.
5. W okresie gwarancji, jednak nie dłużej niż do 27 czerwca 2026 r. wykonawca zobowiązuje się zapewnić bezpłatne wsparcie techniczne przy rozwiązywaniu wszelkich problemów związanych z działaniem dostarczonego oprogramowania i serwera.
6. Wsparcie techniczne świadczone będzie w języku polskim, przez odpowiednio wyszkolony personel inżynierski, telefonicznie lub za pomocą środków komunikacji elektronicznej, w dni robocze w godzinach 7:30-18:00.
7. Wykonawca w okresie gwarancji zapewni bezpłatny dostęp do najnowszych wersji oprogramowania, bez konieczności wykupywania dodatkowych pakietów serwisowych.
8. Wykonawca w okresie gwarancji Wykonawca zobowiązany jest do nieodpłatnego usuwania wszelkich wad, błędów konfiguracyjnych oraz nieprawidłowości ujawnionych w trakcie eksploatacji systemu, wynikających z realizacji wdrożenia.
9. Korzystanie przez zamawiającego z uprawnień wynikających z gwarancji nie zwalnia wykonawcy od odpowiedzialności z tytułu wad lub nienależytej jakości produktów zgodnie z przepisami o rękojmi za wady fizyczne rzeczy.



Cyberbezpieczny Samorząd

ZMIANY UMOWY

§9

1. Poza zmianami umowy dopuszczonymi na podstawie art. 455 ustawy pzp, dopuszcza się możliwość zmian postanowień zawartej umowy, w następujących przypadkach:
 - 1) gdy zmiana dotyczy urządzenia wymienionego w „Wykazie rzeczowo-finansowym” w przypadku wycofania go z produkcji i wprowadzeniu zamiennika o tych samych lub lepszych właściwościach. Warunkiem zmiany umowy w oparciu o wyżej wspomnianą okoliczność, jest konieczność przekazania Zamawiającemu oświadczenia producenta o wycofaniu z produkcji danego urządzenia wraz z oświadczeniem Wykonawcy o nazwie proponowanego zamiennika. Wykonawca musi załączyć także karty charakterystyki proponowanego zamiennika wraz z jego ceną jednostkową brutto, która nie może być wyższa niż cena jednostkowa brutto urządzenia wycofanego z produkcji.
 - 2) gdy zmiana dotyczy przedłużenia terminu wykonania przedmiotu umowy jeżeli:
 - a) wystąpią okoliczności, których strony nie były w stanie przewidzieć, pomimo zachowania należytej staranności, mające bezpośredni wpływ na termin realizacji przedmiotu umowy,
 - b) konieczność zmiany spowodowana jest okolicznościami pozostającymi poza kontrolą stron, dotyczy to w szczególności takich okoliczności jak zagrożenie epidemiologiczne, zamieszki, akty terroru, zamknięcie granic, rządowe ograniczenia międzynarodowego transportu, utrudnienia na lotniskach i granicach, tj.: okoliczności o charakterze tzw. siły wyższej. W czasie trwania siły wyższej Wykonawca odpowiada za wykonanie umowy na zasadach ogólnych kodeksu cywilnego. Wykonawca dołoży wszelkich starań, aby pomimo istnienia siły wyższej zapewnić ciągłość dostaw oraz zobowiązuje się informować Zamawiającego niezwłocznie i na bieżąco o wszelkich trudnościach związanych z dostarczeniem zamówionych przez niego urządzeń, o których mowa w §1.
2. Termin wykonania umowy może zostać przedłużony o okres, nie dłuższy niż, okres występowania okoliczności, o których mowa w ust. 1 pkt 2.
3. Wszelkie zmiany umowy możliwe będą wyłącznie gdy zostaną spełnione łącznie następujące warunki:
 - 1) wystąpienie okoliczności, o których mowa w ust. 1 zostało udokumentowane przez Wykonawcę,
 - 2) Zamawiający uzna i zaakceptuje w formie pisemnej pod rygorem nieważności, że wystąpiły okoliczności opisane w ust. 1 oraz w przypadku, o którym mowa w ust. 1 pkt 2, że wpłynęły one na termin wykonania przedmiotu umowy.
4. Zmiany umowy wymagają formy pisemnej pod rygorem nieważności, chyba że umowa stanowi inaczej.

POSTANOWIENIA DODATKOWE

§10

Strony zgodnie postanawiają, że Wykonawca nie może bez uprzedniej zgody Zamawiającego podejmować żadnych czynności w szczególności zawierać umów, zwłaszcza cesji i poręczenia, których skutkiem mogłoby być przejście na osobę trzecią, na podstawie umowy lub z mocy prawa wierzytelności przysługującej Wykonawcy w stosunku do Zamawiającego, albo wstąpienie osoby trzeciej w prawa zaspokojonego wierzyciela.

§11

Na podstawie art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L z 2016 r. Nr 119, str. 1), dalej „RODO”, informuję, że:

- 1) Administratorem Pani/Pana danych osobowych jest Starostwo Powiatowe w Rzeszowie, ul. Grunwaldzka, 15, 35 – 959 Rzeszów, które realizuje zadania Starosty Rzeszowskiego oraz Zarządu Powiatu. Kontakt telefoniczny: 17 23 00 651, kontakt e-mail: starostwo@powiat.rzeszowski.pl.



Cyberbezpieczny Samorząd

- 2) W zakresie dotyczącym ochrony danych osobowych może Pani/Pan kontaktować się pisemnie z Inspektorem Ochrony Danych pod adresem: ul. Grunwaldzka 15, 35 – 959 Rzeszów, lub za pomocą adresu e-mail: rodo@powiat.rzeszowski.pl.
- 3) Pani/Pana dane osobowe przetwarzane będą w celu:
 - a) zawarcia i wykonywania umowy zawartej z Administratorem (art. 6 ust. 1 lit. b RODO) oraz dokonania niezbędnych rozliczeń w związku z jej zawarciem – przez czas niezbędny do realizacji umowy, a po jej zakończeniu dane osobowe będą przetwarzane przez czas potrzebny na wykazanie prawidłowości wykonania wynikających z niej obowiązków do upływu terminów wskazanych w przepisach o archiwizacji;
 - b) wykonywania ustawowych obowiązków Administratora, w szczególności podatkowych i sprawozdawczych (art. 6 ust. 1 lit. c RODO) – przez czas niezbędny do realizacji ustawowych obowiązków Administratora;
- 4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy pzp, a także użytkownicy dostarczonych urządzeń;
- 5) Pani/Pana dane osobowe będą przechowywane przez okres określony zgodnie z Rozporządzeniem 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 (Dz. U. z 2011 r. Nr 14 poz. 67 ze zm.) lub w przypadku dofinansowania zadania ze środków zewnętrznych zgodnie z wytycznymi konkursu oraz umowy o dofinansowanie;
- 6) obowiązek podania Pani/Pana danych osobowych jest warunkiem koniecznym do zawarcia i realizacji umowy;
- 7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- 8) posiada Pani/Pan:
 - a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
 - b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą pzp oraz nie może naruszać integralności protokołu oraz jego załączników);
 - c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO (prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
 - d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- 9) nie przysługuje Pani/Panu:
 - a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
 - c) 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. b RODO.

§12

1. Wykonawca zobowiązany jest wypełnić obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO, wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał lub pozyska w celu zawarcia i realizacji umowy.
2. Wykonawca zobowiązany jest zastosować środki zabezpieczenia określone w art. 32 RODO w stosunku do danych osobowych pozyskanych w związku z realizacją niniejszej umowy.



Cyberbezpieczny Samorząd

- Wykonawca jest odpowiedzialny na zasadach ogólnych przepisów RODO, za szkody wyrządzone Zamawiającemu, osobie fizycznej, której dane osobowe zostały mu udostępnione lub innym osobom trzecim, w związku z nienależytym przetwarzaniem, bądź zabezpieczeniem tych danych.

§13

- Wykonawca zobowiązany jest do informowania Zamawiającego o zmianie formy prawnej prowadzonej działalności, o wszczęciu postępowania upadłościowego oraz zmianie 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.
- Wszelkie spory mogące wyniknąć na tle realizacji postanowień niniejszej umowy strony poddają rozstrzygnięciu sądu właściwego miejscowo dla Zamawiającego.
- W sprawach nieuregulowanych niniejszą umową, mają zastosowanie przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2024 r. poz.1061 ze zm.), ustawy pzp oraz postanowienia SWZ.
- Umowę sporządzono w trzech jednobrzmiących egzemplarzach, z przeznaczeniem dwóch egzemplarzy dla Zamawiającego oraz jednego egzemplarza dla Wykonawcy (*w przypadku zawarcia umowy w formie elektronicznej ust.4 zostanie usunięty*).

Zamawiający:

Wykonawca:

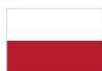
Kontrasygnata Skarbnika

Załącznik:

Wykaz rzeczowo-finansowy



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Wykaz rzeczowo-finansowy

Lp.	Określenie urządzenia/oprogramowania	Ilość	Stawka podatku VAT (%)	Wartość brutto (zł)
1	Serwer do SIEM PRODUCENT, NAZWA : Numer produktu lub kod producenta: Zainstalowany system operacyjny: LICENCJA na system operacyjny bezterminowa (wieczysta). OKRES GWARANCJI: 24 miesiące.	1 szt.	23	
2	Oprogramowanie SIEM PRODUCENT, NAZWA : LICENCJA: bezterminowa (wieczysta).	1 szt.	23	
RAZEM WARTOŚĆ BRUTTO				

Zamawiający:

Wykonawca:

