Numer sprawy: **IGM.271.3.2026**

# Szczegółowy Opis Przedmiotu Zamówienia

na ***Dostawę oprogramowania do agregacji logów i rozbudowa systemu backup, związana z realizacją projektu w ramach grantu Cyberbezpieczny Samorząd dla Gminy Łabiszyn i jej jednostek organizacyjnych***

# Spis treści

# 1. Zestawienie ilościowe.

**Część nr 2 – Dostawa oprogramowania informatycznego.**

| Lp. | Nazwa | Ilość |
|---|---|---|
| 1. | Zakup oprogramowania do agregacji logów | 1 szt. |
| 2. | Rozbudowa systemu backup | 1 szt. |

## 2. Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum" oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać

Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.

10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowania overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne

opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

# 3. Opis przedmiotu zamówienia

## 3.1. Wymagania ogólne.

1. Dostarczone oprogramowanie musi być wolne od wad prawnych i fizycznych oraz nienoszące oznak użytkowania.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego oprogramowania.
3. Niedopuszczalne są produkty prototypowe, oprogramowanie nie może znajdować się na liście „end-of-sale", „end-of-support", „end-of-life" producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wykonawca zapewni dostawę oprogramowania do wskazanej lokalizacji w siedzibie Zamawiającego.
5. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
6. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
7. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
8. Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:
    a. Instalacja ma odbyć się na komputerach oraz serwerach wskazanych przez Zamawiającego, a w przypadku jeżeli dostarczone oprogramowanie działa w modelu rozwiązania chmurowego to Wykonawca jest zobligowany do konfiguracji oprogramowania w chmurze Wykonawcy bądź Producenta oferowanego oprogramowania.
    b. Zamawiający dopuszcza instalację i wdrożenie zdalne przy wykorzystaniu narzędzia Wykonawcy, z zastrzeżeniem, że Wykonawca jest zobowiązany dostarczyć oprogramowanie do zdalnej pracy umożliwiające szyfrowanie połączeń oraz nagrywanie sesji serwisowych.
    c. W przypadku jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.

d. Wykonawca, pomimo zapewnienia serwisu producenta zobowiązany będzie do udzielania pomocy technicznej Zamawiającemu przez okres gwarancji.
e. Usługa wsparcia wdrożenia obejmuje:
    i. przeprowadzenie analizy przedwdrożeniowej,
    ii. pomoc przy instalacji silnika bazy danych – jeżeli będzie wymagana instalacja,
    iii. rejestracja produktu – jeżeli wymagana,
    iv. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
    v. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
    vi. konfigurację oprogramowania,
    vii. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
    viii. szkolenie administratorów z zakresu pracy z programem,
    ix. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połącznie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.

9. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia oprogramowania – wymagania minimalne:
    a. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
        i. scenariusze testowe, procedury oraz wzory raportów testów,
        ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
        iii. opis koncepcji realizacji prac,
        iv. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
    b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
        i. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni roboczych od dnia zawarcia umowy,
        ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
        iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
        iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
        v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,

vi. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.

c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery". Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.

10. Wymagania licencyjne dla dostarczonego oprogramowania:
    a. Licencjobiorcą licencji będą: Urząd Miejski w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Zakład Wodociągów i Kanalizacji w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Miejski Zespół Oświaty, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Miejski Ośrodek Pomocy Społecznej, ul. Szubińska 1, 89-210 Łabiszyn; Zespół Szkół w Łabiszynie, ul. Nadnotecka 2, 89-210 Łabiszyn zgodnie ze wskazaniem poniżej.
    b. Zamawiający dopuszcza udzielenie licencji w wersji papierowej i/lub elektronicznej. W przypadku jeżeli producent oprogramowania nie wystawia licencji w zakresie oferowanego oprogramowania Wykonawca powinien dostarczyć stosowne oświadczenie producenta oprogramowania bądź jego dystrybutora.
    c. Licencje muszą obowiązywać do dnia 30.06.2026 r. niezależnie od modeli dystrybucji poszczególnych producentów oferowanego oprogramowania.
    d. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
    e. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do przeniesienia oprogramowania na inny serwer/komputer.
    f. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
    g. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
    h. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
    i. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym urządzeniu klienckim (licencja nie może być przypisana do komputera/urządzenia).
    j. Licencja oprogramowania nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji ze zgromadzonych danych.

k. Wykonawca zapewni gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.

11. Wymagania gwarancyjne i serwisowe dla dostarczonego oprogramowania w formie licencji czasowych lub subskrypcyjnych:
    a. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie do dnia 30.06.2026 r.
    b. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w oprogramowaniu do serwisu producenta lub jego dystrybutora.
    c. Serwis producenta musi zostać zapewniony przez Wykonawcę do dnia 30.06.2026 r.
    d. Serwis polega na świadczeniu usługi wsparcia technicznego udzielonego przez producenta lub autoryzowanego dystrybutora producenta w języku polskim i objąć musi minimum:
        i. dostęp do najnowszych wersji oprogramowania,
        ii. wsparcie telefoniczne w zakresie oferowanego oprogramowania zespołu inżynierów technicznych,
        iii. wsparcie w prawidłowym i zgodnym z wymaganiami producenta użytkowaniu oprogramowania,
        iv. przyjmowanie i realizacja zgłoszeń serwisowych,
        v. doradztwo techniczne w zakresie konfiguracji i optymalizacji oprogramowania,

        w przypadku jeżeli w dalszej części niniejszego dokumentu zdefiniowano wymogi serwisu lub gwarancji w innym zakresie powyższe wymogi są obowiązujące i należy potraktować jako podstawowe, precyzowane przez dodatkowe wymagania opisane w dalszej części dokumentu.

12. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi", „powinien", „możliwość" określając w ten sposób wymaganą funkcjonalność oprogramowania.

## 3.2. Zakup oprogramowania do agregacji logów (1 szt.) – Część 2.

Minimalne parametry funkcjonalne oprogramowania do agregacji logów:

1. System musi umożliwiać zbieranie logów z szerokiego spektrum źródeł, takich jak systemy operacyjne (Linux, Windows, macOS), aplikacje, urządzenia sieciowe, bazy danych, serwery webowe, oraz platformy chmurowe (np. AWS, Azure, Google Cloud), a także z innego oprogramowania do zbierania logów.
2. System musi wspierać zbieranie logów w różnych formatach, w tym min. syslog, plain text zapewniając możliwość monitorowania standardowych i niestandardowych źródeł danych.
3. System musi centralizować logi z wszystkich podłączonych źródeł umożliwiając ich łatwe zarządzanie i analizę w jednym miejscu.
4. System musi oferować zaawansowane funkcje filtracji i transformacji logów.
5. System musi posiadać funkcję normalizacji logów pochodzących z różnych źródeł umożliwiając standaryzację danych i ich późniejszą korelację.
6. System musi posiadać mechanizm korelacji zdarzeń, który umożliwia łączenie i analizowanie zdarzeń pochodzących z różnych źródeł w celu wykrywania bardziej złożonych zagrożeń.

7. System musi wspierać tworzenie i zarządzanie regułami korelacji, które mogą być dostosowywane do specyficznych potrzeb organizacji, a także grupowane według źródła logów, rodzaju zagrożenia lub poziomu krytyczności.
8. System musi umożliwiać hierarchizację reguł umożliwiając tworzenie bardziej zaawansowanych strategii wykrywania zagrożeń.
9. System musi posiadać silniki detekcji zagrożeń, które analizują logi w czasie rzeczywistym, identyfikując złośliwe działania, próby włamań, naruszenia polityk bezpieczeństwa oraz inne anomalie.
10. System musi wspierać wykrywanie zagrożeń opartych zarówno na sygnaturach, jak i na anomaliach umożliwiając szybkie reagowanie na nowe i nieznane wcześniej zagrożenia.
11. System musi posiadać funkcję wykrywania specyficznych rodzajów ataków, takich jak brute force, ataki DDoS, próby eskalacji uprawnień, ataki typu SQL injection, czy próby przejęcia kont użytkowników.
12. System musi umożliwiać dynamiczne przypisywanie poziomów krytyczności do wykrytych zdarzeń pozwalając na priorytetyzację incydentów bezpieczeństwa.
13. System musi generować alarmy w czasie rzeczywistym, z możliwością ich wysyłania przez e-mail, webhooki, do systemów SIEM lub innych systemów zarządzania incydentami.
14. System musi oferować możliwość korelacji i łączenia alarmów zapewniając pełny kontekst zdarzenia i redukcji liczbę fałszywych alarmów.
15. System musi umożliwiać archiwizację wszystkich zebranych logów z możliwością ich przeszukiwania w celu przeprowadzania analizy historycznej oraz audytów po incydencie.
16. System musi posiadać funkcję generowania raportów zgodności z regulacjami, takimi jak PCI DSS, GDPR oraz inne z możliwością dostosowywania tych raportów do specyficznych wymagań Zamawiającego.
17. System musi oferować możliwość tworzenia niestandardowych raportów, które mogą zawierać szczegółowe zestawienia zdarzeń, analizę trendów oraz ocenę skuteczności polityk bezpieczeństwa.
18. System musi posiadać wbudowaną integrację z Kibana umożliwiającą wizualizację danych logów, wykonywanie zapytań oraz przetwarzanie danych.
19. System musi udostępniać API RESTful pozwalające na integrację z zewnętrznymi systemami oraz automatyzację procesów związanych z analizą logów i zarządzaniem incydentami.
20. System musi oferować integrację z zewnętrznymi bazami danych zagrożeń, takimi jak VirusTotal, w celu automatycznego sprawdzania logów związanych z plikami pod kątem znanych zagrożeń.
21. System musi wspierać integrację z honeypotami pozwalając na wykrywanie i analizowanie prób ataków na pułapki umożliwiając lepsze zrozumienie działań atakujących.
22. System musi posiadać funkcję geolokalizacji IP w analizowanych logach umożliwiając identyfikowanie podejrzanych połączeń z nieautoryzowanych lokalizacji.
23. System musi oferować interaktywne dashboardy do monitorowania logów w czasie rzeczywistym z możliwością ich dostosowania do specyficznych potrzeb operacyjnych Zamawiającego.
24. System musi umożliwiać tworzenie spersonalizowanych widoków i filtrów, które pozwolą na szybką identyfikację incydentów i anomalii dostosowanych do potrzeb administratorów.
25. System musi posiadać mechanizmy autoryzacji i autentykacji użytkowników umożliwiając kontrolę dostępu do danych, konfiguracji oraz interfejsów zarządzających.
26. Zamawiający oczekuje dostawy oprogramowania na licencji typu „open source”. Zamawiający dopuszcza licencje komercyjne, jednak w takim przypadku Zamawiający oczekuje dostawy licencji

wieczystej, która nie będzie wymagała nigdy żadnych dodatkowych licencji w celu aktualizacji oprogramowania do najnowszej wersji.

Wdrożenie oprogramowania do agregacji logów – minimalny zakres prac Wykonawcy:

1. Wdrożenie powinno uwzględniać wszystkie funkcjonalności oprogramowania od zbierania logów po ich analizę, korelację i generowanie raportów.
2. Wdrożenie powinno odbyć się na rzecz i uwzględniając infrastrukturę poszczególnych jednostek biorących udział we wdrożeniu oprogramowania, tj. Urząd Miejski w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Miejski Ośrodek Pomocy Społecznej, ul. Szubińska 1, 89-210 Łabiszyn; Miejski Zespół Oświaty, ul. Plac 1000-lecia 1, 89-210 Łabiszyn; Zakład Wodociągów i Kanalizacji w Łabiszynie, ul. Plac 1000-lecia 1, 89-210 Łabiszyn.
3. W ramach wdrożenia należy przeprowadzić analizę wstępną, w ramach której:
    a. Należy przeprowadzić ocenę infrastruktury: Dokładnie zidentyfikować wszystkie urządzenia w sieci, w tym serwery, przełączniki, komputery, drukarki, routery, firewalle i inne urządzenia sieciowe. Wskazać, które z nich generują logi, które będą zbierane i analizowane przez oprogramowanie.
    b. Należy określić wymagania: Zidentyfikować specyficzne potrzeby i wymagania Zamawiającego, takie jak zgodność z regulacjami, kluczowe punkty monitorowania, typy zagrożeń, na które należy zwracać szczególną uwagę, oraz priorytety w zakresie analizy logów.
    c. Należy zaplanować odpowiedni sprzęt i zasoby: Ustalić odpowiednią infrastrukturę sprzętową i zasoby, które będą niezbędne do wdrożenia oprogramowania. Uwzględnić wymagania dotyczące serwera, pamięci masowej, sieci i innych zasobów, aby zapewnić wydajność systemu oraz odpowiednią konfigurację i wydajność maszyny wirtualnej.
4. Następnie prace wdrożeniowe obejmą przygotowanie środowiska, w ramach których:
    a. Należy zainstalować serwer centralny: Zainstalować i skonfigurować serwer centralny, który będzie odpowiedzialny za centralizację logów, ich przetwarzanie oraz zarządzanie oprogramowaniem. Serwer powinien mieć odpowiednią moc obliczeniową oraz wystarczającą przestrzeń dyskową do przechowywania zebranych logów – należy określić wszystkie niezbędne zasoby.
    b. Należy skonfigurować agentów na urządzeniach końcowych: Na wszystkich serwerach, komputerach oraz innych urządzeniach, które będą generować logi, zainstalować i skonfigurować agentów do zbierania danych. Agenci muszą być dostosowani do specyficznych systemów operacyjnych i urządzeń.
    c. Należy utworzyć połączenia sieciowe: Upewnić się, że wszyscy agenci są poprawnie połączeni z serwerem centralnym. Połączenia powinny być zabezpieczone, aby zapewnić integralność i poufność przesyłanych danych.
5. W następnym kroku prace wdrożeniowe powinny objąć konfigurację zbierania i przetwarzania logów, w ramach których:
    a. Należy skonfigurować zbieranie logów z różnych źródeł: Ustawić oprogramowanie tak, aby zbierało logi z serwerów, przełączników, routerów, firewalli oraz innych urządzeń sieciowych. Należy upewnić się, że logi są zbierane w czasie rzeczywistym, a system wspiera różnorodne formaty logów (np. syslog, JSON, plain text).
    b. Należy ustalić reguły filtracji i transformacji logów: Zdefiniować zasady filtracji, które określą, jakie logi mają być przechowywane i analizowane. Oprogramowanie powinno być

skonfigurowany do transformacji logów, tak aby dane były normalizowane i wzbogacane o dodatkowe informacje, takie jak metadane czy lokalizacja geograficzna.

c. Należy zaimplementować korektę i deduplikację logów: Zaimplementować mechanizmy deduplikacji, które będą eliminować powtarzające się zdarzenia, zapobiegając generowaniu zbędnych alarmów i umożliwiając bardziej efektywną analizę.

6. Następnie prace wdrożeniowe skupić się powinny na ustawieniu reguł korelacji i detekcji, w ramach których:
    a. Należy skonfigurować reguły korelacji: Ustawić reguły korelacji, które pozwolą na analizę logów pochodzących z różnych źródeł w celu wykrywania bardziej złożonych zagrożeń. Reguły te powinny być dostosowane do specyfiki sieci jednostek wdrażających oprogarmowanie.
    b. Należy zdefiniować sygnatury i anomalia: Zaimplementować reguły wykrywania zagrożeń zarówno na podstawie sygnatur, jak i anomalii. System powinien być w stanie identyfikować znane wzorce zagrożeń oraz odchylenia od normalnego zachowania systemu.
    c. Należy skonfigurować poziomy krytyczności: Określić poziomy krytyczności dla różnych rodzajów zdarzeń, aby umożliwić priorytetyzację alarmów. Dostosować poziomy krytyczności do wymagań Zamawiającego uwzględniając lokalne regulacje i polityki.
7. W ramach wdrożenia wymaganym od Wykonawcy jest implementacja mechanizmów alarmowania, w ramach których:
    a. Należy skonfigurować alerty w czasie rzeczywistym: Ustalić mechanizmy generowania alertów w czasie rzeczywistym, które będą informować administratorów o wykrytych zagrożeniach. Alerty powinny być wysyłane za pomocą e-maila.
    b. Należy ustawić logikę alarmów: Zdefiniować logikę, która będzie decydować, kiedy i w jaki sposób generowane są alarmy. Należy upewnić się, że alarmy są kontekstowe i że system łączy powiązane zdarzenia w celu zredukowania liczby fałszywych pozytywów.
8. W celu wdrożenia monitorowania i analizy historycznej:
    a. Należy skonfigurować dashboardy monitorujące: Utworzyć interaktywne dashboardy do monitorowania logów i alarmów w czasie rzeczywistym. Dashboardy powinny być dostosowane do potrzeb Zamawiającego umożliwiając łatwe śledzenie kluczowych wskaźników bezpieczeństwa.
    b. Należy skonfigurować mechanizmy archiwizacji i analizy logów: Skonfigurować mechanizmy archiwizacji logów, które pozwolą na ich długoterminowe przechowywanie i analizę historyczną. Należy zapewnić możliwość przeszukiwania archiwalnych logów w celu prowadzenia audytów i dochodzeń po incydentach.
    c. Należy zaimplementować generowanie raportów zgodności: Zaimplementować automatyczne generowanie raportów zgodności, które będą odzwierciedlać wymagania regulacyjne, takie jak RODO, i które będą regularnie dostarczane do odpowiednich wydziałów urzędu.
9. Dodatkowo należy przygotować oprogramowanie do integracji z innymi systemami poprzez konfigurację integracji z Elastic Stack umożliwiając wizualizację danych logów w Kibana, wykonywanie zaawansowanych zapytań w Elasticsearch oraz przetwarzanie danych przez Logstash. Dodatkowo, należy Zaimplementować API RESTful, które umożliwi integrację oprogramowania z innymi systemami zarządzania incydentami oraz automatyzację procesów związanych z analizą logów.

10. W końcowej fazie wdrożenia przed uruchomieniem produkcyjnym oprogramowania należy przeprowadzić testowanie i optymalizację oprogramowania, tj.:
    a. Wykonać testy funkcjonalne, aby upewnić się, że wszystkie komponenty modułu działają poprawnie. Testy powinny obejmować zbieranie logów, ich analizę, generowanie alarmów oraz integrację z innymi systemami.
    b. Przeprowadzić testy obciążeniowe, aby sprawdzić, czy system działa wydajnie nawet przy dużej ilości generowanych logów. Należy upewnić się, że serwer centralny jest w stanie obsłużyć przewidywaną ilość danych.
    c. Na podstawie wyników testów dokonać niezbędnych optymalizacji, takich jak dostosowanie filtrów, reguł korelacji czy poziomów krytyczności, aby system dział zgodnie z oczekiwaniami Zamawiającego.
11. W ramach wdrożenia oprogramowania do agregacji logów należy przeprowadzić szkolenie administratorów odpowiedzialnych za obsługę oprogramowania obejmujące wszystkie aspekty jego konfiguracji, monitorowania i zarządzania incydentami oraz sporządzić szczegółową dokumentację konfiguracji modułu, w tym opis wszystkich zdefiniowanych reguł, schematów połączeń oraz procedur zarządzania systemem.

## 3.3. Rozbudowa systemu backup (1 szt.)

Rozbudowa systemu backup składać się będzie z zapewnienia dla Miejskiego Ośrodka Pomocy Społecznej, ul. Szubińska 1, 89-210 Łabiszyn dwóch elementów:

1. Dostawa oprogramowania umożliwiającego backup w chmurze o parametrach minimum:
    a. Data obowiązywania licencji: 30 czerwca 2026 r.
    b. Ilość danych w chmurze: min. 5 TB.
    c. Brak kosztów transmisji danych.
    d. Szyfrowanie połączenia przesyłu i transferu danych.
    e. Dostępność danych na poziomie 99 % w danym roku.
    f. Do plików i folderów w usłudze chmury można uzyskać dostęp i nimi zarządzać poprzez witrynę www.
    g. Miejsce składowania danych na obszarze UE.

2. Aktualizacja posiadanego oprogramowania backup Ferro Backup System do najnowszej wersji oferowanej przez producenta w postaci licencji wieczystej umożliwiającej backup 20 stacji roboczych oraz jednego serwera fizycznego z maksymalnie 4 maszynami wirtualnymi wraz z zapewnieniem wsparcia producenta oprogramowania w okresie do 30.06.2026 r.
   lub dostawa równoważnej platformy oprogramowania backup zapewniającej wszystkie powyższe wymagania oraz poniżej wskazane kryteria równoważności:

    1. System musi tworzyć „samowystarczalne” archiwa do odzyskania których nie jest wymagana osobna baza danych.
    2. System musi mieć mechanizmy kompresji w celu zmniejszenia wielkości archiwów.
    3. System musi zapewniać backup jednoprzebiegowy.
    4. System musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania.
    5. System musi mieć możliwość uruchamiania skryptów przed i po zadaniu backupowym.

6. System musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
7. System musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej.
8. System musi wspierać backup maszyn wirtualnych.
9. System powinien zapewniać wykonywanie kopii zapasowych plików przechowywanych na urządzeniach pracujących pod kontrolą systemów Windows i Linux.
10. System powinien mieć możliwość pracy w programie z dowolnego miejsca bez potrzeby korzystania z Pulpitu zdalnego, jednoczesnej pracy z danym serwerem przez kliku administratorów.
11. System powinien mieć wbudowane następujące funkcje:
    a. Możliwość wykonania backupu całego systemu operacyjnego, łącznie z zainstalowanymi programami, sterownikami i danymi użytkownika, tak aby w przypadku awarii możliwe było odzyskanie działającego systemu operacyjnego i wszystkich zainstalowanych komponentów.
    b. Zautomatyzowane przywracanie systemu operacyjnego z serwerów (prosty sposób przywracania systemu operacyjnego z serwera kopii zapasowych poprzez sieć do uszkodzonego komputera). Możliwość przywrócenia po awarii systemu operacyjnego wraz z wszystkimi zainstalowanymi programami (ang. bare-metal restore), tak aby uruchomić system operacyjny bez potrzeby ponownej instalacji i konfiguracji.
    c. Ochrona przed programami ransomware szyfrującymi pliki.
    d. Backup i odzyskiwanie maszyn wirtualnych Hyper-V oraz VMWare ESX, ESXi. Program powinien wykonywać kopie zapasowe zarówno zatrzymanych jak i uruchomionych maszyn wirtualnych.
    e. Certyfikaty SSL dla połączeń HTTPS – możliwość obsługi samopodpisanych certyfikatów oraz stosowania własnych certyfikatów SSL.
    f. Zabezpieczanie połączeń sieciowych w systemach archiwizacji danych - typu klient-serwer za pomocą reguł IPSec.
    g. Możliwość archiwizacja danych w chmurze.
    h. Backup plików PST (MS Outlook) - backup plików PST bez zamykania programu Outlook.
    i. Możliwość automatycznego backupu urządzenia przy zamykaniu systemu.
    j. Archiwizacja danych także na napędy taśmowe – możliwość replikacji na napędy taśmowe.
    k. Możliwość backupu na dysk sieciowy - składowanie kopii na urządzeniach typu NAS szybkim i wydajnym protokołem iSCSI.
    l. Możliwość instalacji serwera backupu pod systemem Linux i Mac OS.
    m. Możliwość wydajnego i pewnego backupu baz danych i plików poczty (Microsoft SQL Server, Microsoft Exchange Server, Oracle, MySQL, InterBase, Firebird, Microsoft Access, dBase, Paradox oraz plików programów pocztowych: Microsoft Outlook, Outlook Express, Mozilla Thunderbird).
    n. Możliwość archiwizacji otwartych i zablokowanych plików.
    o. Możliwość szyfrowania archiwów (w tym AES 256).

p. Możliwość wykonywania archiwizacji pełnej i różnicowej, także różnicowej na poziomie fragmentów plików (archiwizowane są tylko te części plików, które zostały zmodyfikowane od czasu poprzednich archiwizacji a pozostałe są pomijane).
q. Możliwość generowania raportów i statystyk, które pomagają w analizie działania aplikacji (Raporty informujące o niewykonanych i opóźnionych zadaniach archiwizacji i statystyki zawierające informacje na temat szybkości i rozmiaru backupu z poszczególnych komputerów).
r. Możliwość wykonywania zadań archiwizacji w/g harmonogramu następującego typu: Na żądanie - zadanie archiwizacji będzie wykonywane tylko przez manualne uruchomienie zadania; Codziennie - zadanie archiwizacji będzie uruchamiane codziennie o wskazanej godzinie; Co określoną liczbę dni - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę dni; Co określoną liczbę godzin - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę godzin; Co określoną liczbę minut - zadanie archiwizacji będzie wykonywane automatycznie co określoną liczbę minut; W dni tygodnia - zadanie archiwizacji będzie wykonywane automatycznie w wybrane dni tygodnia; Czas rozpoczęcia - umożliwia ustalenie terminu rozpoczęcia zadania archiwizacji z dokładnością do jednej minuty; Następny termin - umożliwia ustalenie daty kolejnej archiwizacji; Zadania opóźnione mogą być pominięte i wykonane w następnym terminie, wykonane natychmiast po podłączeniu serwera; Przy zamykaniu systemu.
s. Dziennik zdarzeń służący do sprawdzania poprawności działania systemu i wyszukiwania przyczyn ewentualnych problemów – możliwość na bieżąco śledzenia generowanych zdarzeń, dotyczących działania całego systemu, takie jak: błędy, ostrzeżenia i informacje. Wszystkie zapisane zdarzenia można filtrować co najmniej według typu zdarzenia oraz nazwy komputera, którego dana informacja dotyczy.
t. Podczas wyboru plików i katalogów do archiwizacji pozwalać określić woluminy, maski lub pełne ścieżki do plików i katalogów, które mają być archiwizowane i te, które mają być wykluczone z archiwizacji.
u. Obsługę co najmniej następujących rodzajów archiwizacji: archiwizacja pełna; archiwizacja różnicowa; archiwizacja różnicowa na poziomie fragmentów plików.
v. Obsługę kopii rotacyjnych (wersjonowanie, retencja danych - pozwala określić, ile maksymalnie przechowywać archiwów na dysku, ile przechowywać kopii wstecz).
w. Obsługę replikacji archiwów - archiwa należące do wybranego zadania backupu mogą być powielane w inne miejsce, replikacja może być wykonywana na napędy dyskowe, optyczne i taśmowe.
x. Monitoring i kontrola pracy serwera backupu, powinna w łatwy i intuicyjny sposób umożliwić zatrzymanie i uruchomienie serwera backupu, możliwość wywołania wirtualnego wiersz poleceń na serwerze backupu i podłączonych stacjach roboczych.
y. Dziennik zdarzeń służy do sprawdzania poprawności działania Systemu i wyszukiwania przyczyn ewentualnych problemów. W zakładce Dziennik zdarzeń można na bieżąco śledzić wszystkie generowane zdarzenia dotyczące działania całego Systemu (serwera jak i stacji roboczych), takie jak: błędy, ostrzeżenia i informacje.
z. Wszystkie zapisane zdarzenia można filtrować według typu zdarzenia oraz nazwy urządzenia, którego dana informacja dotyczy.

aa. Wysyłanie alertów administracyjnych, zawierających raporty lub wybrane komunikaty z dziennika zdarzeń, wg ustalonego harmonogramu na wskazany adres e-mail lub np. do serwera syslog.
bb. Możliwy dostęp do zasobów sieciowych przez np. definiowanie ścieżki UNC, dyski sieciowe i dyski serwerów FTP, które mogą być wykorzystywane przez system jako: miejsce przechowywania archiwów, katalog docelowy replikacji, ścieżka zapisu alertów administracyjnych.
cc. Możliwe używania poleceń lokalnych, służących do rozszerzania funkcjonalności programu. Dzięki nim można automatycznie uruchamiać na serwerze backupu zewnętrzne programy, skrypty lub pliki wsadowe, wykonywać operacje na plikach, wykorzystywać komponenty ActiveX, sterować usługami Active Directory, itp.
dd. Program może być uruchamiany w trybie Usługi systemowej lub awaryjnie, także w trybie aplikacji użytkownika.
ee. Możliwe uruchomienie programu w trybie diagnostycznym oraz w trybie naprawy bazy danych.