Jak skutecznie wnioskować o środki z KPO?

Opracowane przez KAMSOFT S.A. kompendium wiedzy jest narzędziem, które pomaga zrozumieć, jakie rozwiązania i produkty najlepiej wpisują się w cele określone w KPO. Służy ono jako przewodnik w skomplikowanych procesie aplikowania o środki finansowe, wskazując na najlepsze praktyki i strategie, które mogą zwiększyć szanse na sukces w ramach prowadzonych lub planowanych naborów.

Zestaw informacji dostarcza praktycznych wskazówek i przykładów wypełnienia formularza wniosku, ułatwiając sprawne aplikowanie o środki na e-zdrowie w ramach naboru.

Zawarte poniżej rozwiązania i typy usług wyśmienicie wpisują się w nurt bieżących oczekiwań jednostek finansujących, w szczególności kładąc nacisk na zwiększenie szeroko rozumianego bezpieczeństwa dodatkowo oferując wskazówki dotyczące uzupełniania kluczowych sekcji formularza aplikacyjnego KPO. Podane dane służą jedynie jako przykłady zastosowania rozwiązań, którymi pragniemy zachęcić Państwa do bezpośredniego kontaktu z KAMSOFT S.A. celem wypracowania modelu możliwie najlepiej spełniającego Państwa aktualne potrzeby.

Dokument podzielony jest na następujące bloki, zgodnie z wytycznymi jakie Ministerstwo Zdrowia przekazało w ramach planowanego podziału środków dla Inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”:

Maksymalny udział wsparcia w wydatkach kwalifikowalnych na poziomie przedsięwzięcia wynosi 100% ze środków RRF.

Nie jest wymagane wniesienie wkładu własnego – finansowego, osobowego lub rzeczowego przez Wnioskodawcę.

Wnioskodawca jest zobowiązany do zabezpieczenia środków własnych, z których pokryje wartość podatku VAT

W przypadku pytań prosimy o kontakt : medycyna@kamsoft.pl z tytułem CYBERBEZPIECZEŃSTWO lub o kontakt ze wskazanymi opiekunami handlowymi.

Cyberbezpieczeństwo

A. Cyberbezpieczeństwo

W tym punkcie KAMSOFT S.A. w swojej ofercie ma nowatorskie rozwiązania, znacząco wspomagające pracę Szpitala w zakresie szeroko rozumianego wsparcia cyber-bezpieczeństwa, głównie w zakresie integracji usług IT, w szczególności w odniesieniu do wskaźnika D21G. Zachęcamy do zapoznania się z oferowanymi rozwiązaniami.

Zakup lub rozwój systemu kopii bezpieczeństwa – oferowane rozwiązania w zakresie usług i rozwiązań systemowych

Oferowane rozwiązanie	Opis funkcjonalny	Uzyskane korzyści
KSerwisSO	- Kompleksowe zarządzanie backupem systemu operacyjnego środowiska serwerowego - Analiza stanów w zakresie rozwiązań IT oraz IoT	- backup środowisk administracyjnych oraz uruchomieniowych środowisk systemów operacyjnych umożliwiający wdrożenie funkcji disaster and recovery oraz minimalizację czasu niezbędnego na procedury odtworzeniowe - konfiguracja kopii zapasowej w modelu 3-2-1 - okresowa weryfikacja/test procesu odtwarzania z kopii zapasowej, raport z procedur odtworzeniowych - weryfikacja urządzeń podpiętych do sieci szpitalnej - sprawdzanie oprogramowania zainstalowanego w ramach organizacji na komputerach
KSerwisSBD	Kompleksowe zarządzanie backupem systemu bazodanowego środowiska ZSI opartego na bazie danych Oracle. Narzędzie zapewni ciągłość działania, dzięki regularnym aktualizacjom i nadzorem nad bazą danych. Dodatkowo wdrożone monitorowanie rozwiązanie wykorzystuje elastyczny mechanizm powiadomień, który pozwala użytkownikom konfigurować alerty e-mail dla praktycznie każdego zdarzenia. Pozwala to na szybką reakcję na problemy z serwerem. Udostępniane raporty i alerty pozwalają na optymalne planowanie zasobów pod kątem uzyskiwanej wydajności.	- konfiguracja kopii zapasowej w modelu 3-2-1 - odtwarzanie baz danych - zarządzanie archiwalnymi bazami danych - - okresowa weryfikacja/test procesu odtwarzania z kopii zapasowej, raport z procedur odtworzeniowych - zarządzanie i monitoring optymalizacyjny bazy danych pod kątem zintegrowanych środowisk informatycznych - monitoring incydentów bazodanowych - proaktywne działania zwiększające bezpieczeństwo danych gromadzonych w bazach danych - kwartalne raporty ze stanu bazy danych wraz z wytycznymi - wdrożenie rozwiązań klasy SEHA

KSSecurity Plus	Zapewnienie dodatkowej izolacji serwera bazodanowego i bezpośredniego dostępu do serwera bazodanowego w sieci wewnętrznej, wymagającego dodatkowego uwierzytelnienia z wykorzystaniem MFA. Mechanizm pozwala na znaczące ograniczenie ryzyka prób uzyskania dostępu do serwera bazodanowego bezpośrednio z sieci wewnętrznej (po włamaniu do sieci wewnętrznej lub prób sabotażu)	- wdrożenie dodatkowego mechanizmu zabezpieczającego wymagającego autoryzacji z wykorzystaniem MFA w celu uzyskania połączenia administracyjnego z serwerem bazodanowym, - zarządzanie i monitoring wdrożonego mechanizmu oraz realizowanych połączeń bazodanowych,
KSPerformance	Kompleksowe zarządzanie wydajnością systemu bazodanowego środowiska ZSI opartego na bazie danych Oracle. Narzędzie zapewni ciągłość działania dzięki monitorowaniu bieżącej wydajności serwerów bazodanowych, podsystemu dyskowego, zajętości bazy danych oraz obciążenia interfejsów sieciowych. Pozwoli na uzyskanie informacji o ewentualnym rosnącym zapotrzebowaniu na zasoby oraz konieczności rozważenia modernizacji czy konserwacji infrastruktury w celu zapewnienia dalszego wydajnego działania.	- konfiguracja mechanizmu gromadzenia metryk wydajnościowych, - zarządzanie i monitoring wskaźników wydajnościowych, - monitoring incydentów wydajnościowych, - proaktywne działania wpływające korzystnie na wydajność eksploatowanego silnika bazodanowego, - optymalizacja wydajności systemowej bazy danych - kwartalne raporty wydajnościowe ze obciążenia silnika bazy danych wraz z rekomendacjami.
KSerwisGOD	W ramach wdrażanych rozwiązań możliwe jest też : - automatyczne wykrywanie serwerów i urządzeń sieciowych - rozproszone monitorowanie ze scentralizowaną administracją WEB - wsparcie dla mechanizmów odpytywania i pułapkowania - wsparcie dla tworzenia dzienników audytowych dla działu IT - ocena konfiguracji - wykrywanie złośliwego oprogramowania - integralności plików - aktywne wykrywanie zagrożenia - analiza danych dziennika - wykrywanie luk w zabezpieczeniach - reagowanie na incydenty monitorowanie - utrzymanie higieny IT - ochrona obciążeń roboczych - weryfikacja konfiguracji portów tcp/udp pod kątem zarządzania bezpieczeństwem sieci - zarządzanie bezpieczeństwem i aktualnością końcówek systemów Windows	- tworzenie zindywidualizowanych, pod klienta, scenariuszy dla monitorowania infrastruktury - tworzenie personalizowanych dashbordów z kluczowymi KPI w zakresie nadzoru - Instalacja dodatkowych template'ów, np bazodanowych - ustawienie triggerów alarmujących wyznaczone osoby o awariach - rozbudowane raporty z analiz dla wykorzystania przez dział IT do planowania bezpieczeństwa oraz ew. inwestycji - ustawienie wykresów pokazujących potencjalne ataki ddos na infrastrukturę klienta - ustawienie kanałów powiadamiania klienta o awariach (email, sms (wymagana wykupiona usługa bramka sms u klienta), inne) - zwiększenie zabezpieczeń sieciowych poprzez eliminację zbędnego ruchu - wdrożenie polityki WSUS - mechanizmy ELK do analizy i przechowywania logów zdarzeń, które są nie tylko proaktywne ale również mają dużą wartość dowodową w zakresie analiz potencjalnych zdarzeń – zapewnienie zgodności z NIS2

	- zarządzalność monitoringiem logów, których w placówce jest niezwykle dużo i sam fakt ich realnego odseparowania już jest wartością dodaną - zarządzalność ruchem internetowych, który stwarza ponad 85% zagrożeń w ramach polityk cyberbezpieczeństwa - proaktywne wykrywanie zagrożeń i włamań w oparciu o definiowane reguły zachowań - check alive – weryfikacja zdarzeń awaryjnych sprzetu	- wdrożenie polityki nadzorczej nad szeroko rozumianym API poprzez uruchomienie WAF i API Gateways, które skoncentrowane na kontroli ruchu HTTP pozwalają na skuteczniejsze budowanie zabezpieczeń a także wskazywanie tzw. słabych punktów i budowania pierwszej linii obrony. Wdrożone rozwiązanie ma w swym celu wykraczać poza proste blokady portów, głównie dzięki zastosowaniu nieszablonowych sygnatur zagrożeń z wykorzystaniem AI i wskazań środków naprawczych - uruchomienie proaktywnego rozwiązania umożliwiającego analizę anomalii zachowań (w kontekście działania danej placówki) - graficzny podgląd urządzeń w sieci w podziale na aktywne i nieaktywne - powiadomienia o awariach sprzętowych - testy infrastruktury sieciowej
Sprzęt do backupu wraz z niezbędnymi licencjami (serwery backupu, serwery NAS, macierze, biblioteki taśmowe)	- Backup plików, systemów operacyjnych, baz danych, maszyn wirtualnych oraz aplikacji. - Obsługa różnych typów backupów: pełny, przyrostowy, różnicowy. - Harmonogramowanie zadań backupowych zgodnie z wymaganiami klienta. - Centralne zarządzanie procesami backupu i odtwarzania. - Przechowywanie kopii zapasowych w środowisku sieciowym z wysoką dostępnością. - Obsługa systemów taśmowych umożliwiająca szybki dostęp do danych na taśmach.	- Ochrona przed utratą danych (Tworzenie kopii zapasowych chroni dane przed przypadkowym usunięciem, awarią sprzętu, atakami ransomware lub innymi zagrożeniami) - Redundancja (Dzięki zastosowaniu macierzy dyskowych (RAID) i bibliotek taśmowych, dane są przechowywane z wielopoziomowym zabezpieczeniem) - Izolacja backupów (Backupy offline (np. na taśmach) są odporne na ataki typu ransomware, co zapewnia dodatkowy poziom ochrony) - Rozwiązanie można łatwo skalować w miarę rozwoju biznesu, dodając nowe serwery, macierze, przestrzeń na NAS lub taśmy do biblioteki. - Możliwość backupu zarówno systemów fizycznych, jak i wirtualnych (np. VMware, Hyper-V), oraz integracja z aplikacjami biznesowymi i bazami danych.

		- Biblioteki taśmowe oferują tanią i trwałą opcję archiwizacji, szczególnie dla danych przechowywanych zgodnie z wymogami prawnymi - Automatyczne zarządzanie polityką przechowywania danych zapewnia zgodność z wymogami dotyczącymi retencji. - Backupy przechowywane na macierzach i serwerach NAS umożliwiają szybkie przywracanie plików lub całych systemów

Przykład wypełnienia fiszki projektowej

Zakładane cele:

Celem wdrożenia oprogramowania jest zapewnienie ciągłości działania systemów informatycznych. Całość rozwiązania podzielona jest na trzy produkty, z których każdy może być indywidualnie konfigurowany. Począwszy od bazowego zakresu związanego z audytem i wskazaniami dot. środowisk serwerowych oraz aktualnego stanu IT, poprzez zaawansowany mechanizm zarządzania kopiami zapasowymi baz danych, które to rozwiązanie umożliwia regularne aktualizacje baz zapasowych a także systemów operacyjnych dla krytycznej infrastruktury serwerowej, które są zawsze gotowe do przejęcia funkcji bazy głównej w przypadku awarii lub utraty danych. Dzięki temu organizacje minimalizują ryzyko przestojów, chronią kluczowe dane i utrzymują wysoką dostępność kluczowych systemów medycznych, co jest szczególnie istotne w środowiskach wymagających niezawodności operacyjnej. Duży nacisk kładziony jest tu również na proaktywne działania mające na celu nie tylko uruchomienie, ale i przede wszystkim utrzymywanie systemów w ciągłej gotowości w stanie optymalnego działania, co jak pokazują raporty audytowe w placówkach medycznych niejednokrotnie pozostawiają wiele do poprawy. Wdrożenie najbardziej rozbudowanych mechanizmów i usług monitorowania nie tylko pozwala działać prewencyjnie w zakresie optymalizacji i bezpieczeństwa, ale przede wszystkim pozwala na wdrażanie wytycznych NIS2 co jest szczególnie istotne nie tylko z perspektywy placówek świadczących usługi krytyczne, ale każdego podmiotu medycznego, który jest świadomy zagrożeń oraz racjonalnie szacuje ryzyka biznesowe w swojej organizacji.

Wdrożenie oprogramowania zwiększa bezpieczeństwo danych medycznych i stabilność infrastruktury IT. Oprócz tego możliwe do osiągnięcia pełne, proaktywne monitorowanie bazy danych również w zakresie wspierania procesów D&R a także optymalizacji. Testowe odtworzenia na wskazanej infrastrukturze wg. zasady : wykonaj i sprawdź. Również zestawy optymalizacyjne jak i wiedza ekspercka, przekazana końcowym użytkownikom pozwala na wielowymiarowe ujęcie polityki bezpieczeństwa w najbardziej newralgicznych miejscach, co docelowo przekłada się na zupełnie nową, obecnie prawie niespotykaną jakość i zarządzanie ryzykami po stronie działów IT oraz Zarządu Szpitala.

W ramach projektu zakłada się (wskaźniki na poziomie produktu):

- Zakup usług oraz licencji i oprogramowania niezbędnego oprogramowania

- Szkolenie personelu (personel techniczny)
- Wdrożenie i uruchomienie rozwiązania
- Analiza wymagań biznesowych i technicznych (Zdefiniowanie, jakie problemy rozwiązanie ma adresować (np. ochrona przed utratą danych, zgodność z regulacjami).
- Określenie obszarów środowiska IT, które będą objęte backupem (serwery, NAS, macierze, aplikacje) oraz wymagań technicznych (rodzaj danych do backupu (pliki, bazy danych, maszyny wirtualne); Ilość danych (obecnie i w przewidywanym wzroście); Czas okna backupowego i czas odtworzenia danych (RPO i RTO); Wymagania dotyczące retencji i archiwizacji)
- Inwentaryzacja obecnej infrastruktury (Ocena aktualnych zasobów, Serwery fizyczne i wirtualne, obecne systemy backupu, magazyny danych i sieć)
- Identyfikacja braków lub problemów (np. niska przepustowość sieci, brak redundancji).
- Wybór rozwiązania technologicznego (Komponenty sprzętowe - Serwery backupu, Serwery NAS jako przestrzeń na backup, Macierze dyskowe i biblioteki taśmowe)
- Wybór odpowiedniego narzędzia (np. Veeam, Commvault, Veritas, Acronis).
- Projekt mechanizmów zapewniających ciągłość działania (RAID, replikacja danych).
- Określenie polityki przechowywania na różnych nośnikach (szybki backup na macierze, archiwizacja na taśmy).
- Przygotowanie harmonogramu wdrożenia
- Plan migracji - przeniesienie istniejących backupów (jeśli dotyczy).
- Polityki backupu i zarządzania danymi - rodzaje backupów (pełny, różnicowy, przyrostowy); częstotliwość backupów i harmonogram; Retencja danych; plan tworzenia kopii zapasowych w różnych lokalizacjach (np. chmura, offsite).
- Testowanie rozwiązania - Sprawdzenie wydajności backupów przy maksymalnym obciążeniu; weryfikacja poprawności i szybkości odtwarzania danych; testowanie procedur odzyskiwania danych w sytuacjach awaryjnych.
- Dokumentacja techniczna - Opis architektury; instrukcje instalacji i konfiguracji; polityka backupu i retencji; instrukcje odtwarzania danych.
- Szkolenie zespołu IT - Obsługa rozwiązania; Zarządzanie zadaniami backupowymi; Monitorowanie statusu backupów i raportowanie

Osiągane korzyści (wskaźniki na poziomie rezultatu):

- Regularne tworzenie i aktualizacja kopii zapasowych baz danych Oracle oraz administracja i proaktywne działanie optymalizacyjne.
- Zgodność z wymogami NIS2 w zakresie bezpieczeństwa danych.
- Oszczędność czasu pracy lekarzy lub personelu odpowiadającego za jakość
- Adresacja wymogów cyberbezpieczeństwa
- Optymalizacje systemów pod kątem best practices
- Wdrożenie skutecznych sposobów zarządzania infrastrukturą oraz jej bieżący monitoring – również w trybach 24h
- Realny wkład i wsparcie przy kreowaniu polityki IT w organizacji
- Korzystanie z rozwiązania do backupu opartego na serwerach backupu, serwerach NAS, macierzach dyskowych lub bibliotekach taśmowych przynosi klientowi szereg korzyści, które poprawiają bezpieczeństwo danych, efektywność operacyjną oraz zgodność z regulacjami.
- Ochrona przed utratą danych - Tworzenie kopii zapasowych chroni dane przed przypadkowym usunięciem, awarią sprzętu, atakami ransomware lub innymi zagrożeniami.

- Redundancja - Dzięki zastosowaniu macierzy dyskowych (RAID) i bibliotek taśmowych, dane są przechowywane z wielopoziomowym zabezpieczeniem.
- Izolacja backupów - Backupy offline (np. na taśmach) są odporne na ataki typu ransomware, co zapewnia dodatkowy poziom ochrony.
- Możliwość backupu zarówno systemów fizycznych, jak i wirtualnych (np. VMware, Hyper-V), oraz integracja z aplikacjami biznesowymi i bazami danych.
- Tworzenie kopii w różnych lokalizacjach geograficznych lub w chmurze zapewnia dodatkowy poziom ochrony w razie klęski żywiołowej

B. Cyberbezpieczeństwo

W tym punkcie KAMSOFT S.A. w swojej ofercie ma nowatorskie rozwiązania, znacząco wspomagające pracę Szpitala w zakresie szeroko rozumianego wsparcia cyber-bezpieczeństwa, głównie w zakresie integracji usług IT, w szczególności w odniesieniu do wskaźnika D21G. Zachęcamy do zapoznania się z oferowanymi rozwiązaniami.

Zakup lub rozwój systemów firewall – oferowane rozwiązania

Oferowane rozwiązanie	Opis funkcjonalny	Uzyskane korzyści
Firewall sprzętowy	Firewall jest monitorowaną i kontrolowaną granicą między siecią użytkownika a resztą Internetu. Zadanie zapory sieciowej polega na zapobieganiu cyberzagrożeniom i złośliwemu lub niechcianemu ruchowi sieciowemu spoza własnej sieci. Wdrożenie firewalla stanowi budowę pierwszej linii obrony przed cyberatakiem.	- Ochrona danych wrażliwych w sieci komputerowej placówki - Filtracja i blokowanie niechcianego ruchu sieciowego z zewnątrz - Kontrola dostępu użytkowników i urządzeń do sieci wewnętrznej placówki - Monitorowanie ruchu sieciowego

Przykład wypełnienia fiszki projektowej

Zakładane cele :

- Ochrona przed atakami zewnętrznymi: Firewalle blokują nieautoryzowany dostęp do sieci, chroniąc przed atakami hakerów i złośliwym oprogramowaniem.
- Kontrola dostępu: Firewalle umożliwiają zarządzanie, kto i co może uzyskać dostęp do sieci, co pomaga w utrzymaniu bezpieczeństwa i zgodności z politykami firmy.
- Monitorowanie ruchu sieciowego: Firewalle mogą monitorować i analizować ruch sieciowy, co pozwala na wykrywanie i reagowanie na podejrzane aktywności.
- Zapobieganie wyciekom danych: Firewalle mogą zapobiegać nieautoryzowanemu przesyłaniu danych na zewnątrz sieci, chroniąc wrażliwe informacje.
- Zarządzanie przepustowością: Firewalle mogą kontrolować przepustowość sieci, priorytetyzując ważne aplikacje i usługi, co poprawia wydajność sieci.
- Zgodność z przepisami: Wiele regulacji wymaga stosowania firewalli jako części strategii bezpieczeństwa, co pomaga w spełnianiu wymogów prawnych.

W ramach projektu zakłada się:• Analiza potrzeb: Zidentyfikowanie specyficznych potrzeb i wymagań sieciowych, w tym rodzajów danych, które będą chronione, oraz potencjalnych zagrożeń.

- Wybór odpowiedniego firewalla: Wybór firewalla, który najlepiej odpowiada potrzebom organizacji, biorąc pod uwagę funkcje, skalowalność i koszty.
- Planowanie architektury sieci: Określenie, gdzie firewall będzie umieszczony w sieci, aby zapewnić optymalną ochronę i wydajność.
- Konfiguracja polityk bezpieczeństwa: Ustalenie i skonfigurowanie polityk bezpieczeństwa, które będą kontrolować ruch sieciowy, w tym reguły dostępu, filtrowanie treści i monitorowanie ruchu.
- Testowanie i walidacja: Przeprowadzenie testów, aby upewnić się, że firewall działa zgodnie z oczekiwaniami i skutecznie chroni sieć przed zagrożeniami.
- Szkolenie personelu: Zapewnienie odpowiedniego szkolenia dla personelu IT, aby mogli skutecznie zarządzać i monitorować firewall.
- Monitorowanie i utrzymanie: Regularne monitorowanie działania firewalla i aktualizowanie go, aby zapewnić ciągłą ochronę przed nowymi zagrożeniami.
- Dokumentacja: Sporządzenie szczegółowej dokumentacji dotyczącej konfiguracji, polityk bezpieczeństwa i procedur zarządzania firewallem.

Osiągane korzyści :

- Ochrona danych pacjentów: Firewalle pomagają chronić wrażliwe dane medyczne przed nieautoryzowanym dostępem i cyberatakami. To jest szczególnie ważne w kontekście danych osobowych i medycznych, które są bardzo cenne i mogą być celem ataków.
- Zapobieganie atakom z zewnątrz: Firewalle blokują nieautoryzowany ruch przychodzący i wychodzący, co pomaga zapobiegać atakom z zewnątrz, takim jak ataki typu DDoS (Distributed Denial of Service) czy próby włamań.
- Kontrola dostępu: Firewalle umożliwiają kontrolowanie, które urządzenia i użytkownicy mają dostęp do sieci, co pomaga w zarządzaniu uprawnieniami i minimalizowaniu ryzyka wewnętrznych zagrożeń.
- Monitorowanie ruchu sieciowego: Firewalle mogą monitorować ruch sieciowy i wykrywać podejrzane aktywności, co pozwala na szybkie reagowanie na potencjalne zagrożenia.
- Zgodność z przepisami: Wiele przepisów dotyczących ochrony danych, takich jak RODO (GDPR), wymaga stosowania odpowiednich środków bezpieczeństwa, w tym firewalli, aby chronić dane osobowe pacjentów.
- Zwiększenie wydajności sieci: Firewalle mogą również pomóc w zarządzaniu ruchem sieciowym, co może prowadzić do zwiększenia wydajności sieci poprzez blokowanie niepotrzebnego ruchu i priorytetyzowanie ważnych danych.

C. Cyberbezpieczeństwo

W tym punkcie KAMSOFT S.A. w swojej ofercie ma nowatorskie rozwiązania, znacząco wspomagające pracę Szpitala w zakresie szeroko rozumianego wsparcia cyber-bezpieczeństwa, głównie w zakresie integracji usług IT, w szczególności w odniesieniu do wskaźnika D21G. Zachęcamy do zapoznania się z oferowanymi rozwiązaniami.

Zakup lub rozwój systemów poczty elektronicznej wraz z systemami bezpieczeństwa – oferowane rozwiązania

Oferowane rozwiązanie	Opis funkcjonalny	Uzyskane korzyści
System poczty elektronicznej	kompleksowe rozwiązanie do zarządzania pocztą elektroniczną i ułatwienie współpracy w ramach firmy.	- zaawansowane funkcje zabezpieczeń, takie jak weryfikacja dwuetapowa, ochrona przed spamem i phishingiem, oraz regularne kopie zapasowe - możliwość dodawania i usuwania kont użytkowników, tworzenia aliasów adresów e-mail, oraz zarządzania grupami mailowymi i urządzeniami podłączonymi do konta - integracja z innymi aplikacjami biznesowymi, takimi jak kalendarze, narzędzia do zarządzania projektami i dokumentami, co ułatwia współpracę i organizację pracy - automatyczne sortowanie wiadomości, zaawansowane filtry i reguły, oraz możliwość korzystania z własnej domeny

Przykład wypełnienia fiszki projektowej

Zakładane cele:

- Szybka i efektywna komunikacja: Poczta elektroniczna umożliwia natychmiastowe przesyłanie wiadomości, co przyspiesza procesy decyzyjne i komunikację wewnętrzną oraz zewnętrzną.
- Łatwość archiwizacji i wyszukiwania: Wiadomości e-mail można łatwo przechowywać i archiwizować, co ułatwia dostęp do ważnych informacji i dokumentów w przyszłości.
- Niskie koszty: W porównaniu do tradycyjnych metod komunikacji, takich jak poczta tradycyjna czy telefon, poczta elektroniczna jest znacznie tańsza.

- Możliwość załączania plików: E-maile pozwalają na przesyłanie załączników, takich jak dokumenty, zdjęcia czy prezentacje, co ułatwia współpracę i wymianę informacji.
- Zwiększona produktywność: Dzięki możliwości automatyzacji odpowiedzi, filtrowania wiadomości i integracji z innymi narzędziami, poczta elektroniczna może znacząco zwiększyć produktywność pracowników.
- Globalny zasięg: Poczta elektroniczna umożliwia komunikację z osobami na całym świecie, co jest szczególnie ważne w kontekście globalnych operacji biznesowych.
- Bezpieczeństwo: Nowoczesne systemy poczty elektronicznej oferują zaawansowane funkcje bezpieczeństwa, takie jak szyfrowanie wiadomości i ochrona przed spamem oraz phishingiem.

.

W ramach projektu zakłada się:

- Analiza potrzeb: Zidentyfikowanie specyficznych wymagań organizacji, takich jak liczba użytkowników, rodzaje przesyłanych danych oraz wymagania dotyczące bezpieczeństwa i zgodności z przepisami.
- Wybór odpowiedniego systemu: Wybór systemu poczty elektronicznej, który najlepiej odpowiada potrzebom organizacji, biorąc pod uwagę funkcje, skalowalność, koszty oraz wsparcie techniczne.
- Planowanie infrastruktury: Określenie wymagań sprzętowych i sieciowych, takich jak serwery, przestrzeń dyskowa, przepustowość sieci oraz redundancja, aby zapewnić niezawodność i wydajność systemu.
- Konfiguracja polityk bezpieczeństwa: Ustalenie i wdrożenie polityk bezpieczeństwa, takich jak szyfrowanie wiadomości, filtrowanie spamu, ochrona przed phishingiem oraz zarządzanie uprawnieniami użytkowników.
- Migracja danych: Planowanie i przeprowadzenie migracji istniejących danych pocztowych do nowego systemu, z minimalnym zakłóceniem dla użytkowników.
- Testowanie i walidacja: Przeprowadzenie testów, aby upewnić się, że system działa zgodnie z oczekiwaniami i spełnia wszystkie wymagania dotyczące wydajności i bezpieczeństwa.
- Szkolenie użytkowników: Zapewnienie odpowiedniego szkolenia dla użytkowników, aby mogli efektywnie korzystać z nowego systemu poczty elektronicznej.
- Monitorowanie i utrzymanie: Regularne monitorowanie działania systemu, aktualizowanie oprogramowania oraz reagowanie na wszelkie problemy, aby zapewnić ciągłą ochronę i wydajność.
- Dokumentacja: Sporządzenie szczegółowej dokumentacji dotyczącej konfiguracji systemu, polityk bezpieczeństwa, procedur zarządzania oraz instrukcji dla użytkowników.

Osiągane korzyści :

- Zwiększona efektywność komunikacji: Nowoczesne systemy poczty elektronicznej oferują zaawansowane funkcje, takie jak automatyzacja odpowiedzi, filtrowanie wiadomości i integracja z innymi narzędziami, co pozwala na szybszą i bardziej efektywną komunikację.

- Lepsze zarządzanie danymi: Systemy poczty elektronicznej mogą pomóc w lepszym zarządzaniu danymi, umożliwiając łatwe przechowywanie, wyszukiwanie i archiwizowanie wiadomości. To jest szczególnie ważne w kontekście zgodności z przepisami dotyczącymi ochrony danych.
- Zwiększone bezpieczeństwo: Nowoczesne systemy poczty elektronicznej oferują zaawansowane funkcje bezpieczeństwa, takie jak szyfrowanie wiadomości, filtrowanie spamu i ochrona przed phishingiem, co pomaga chronić wrażliwe informacje przed nieautoryzowanym dostępem.
- Skalowalność: Rozwój systemów poczty elektronicznej pozwala na skalowanie infrastruktury w miarę wzrostu organizacji, co zapewnia, że system będzie w stanie obsłużyć rosnącą liczbę użytkowników i wiadomości.
- Integracja z innymi narzędziami: Nowoczesne systemy poczty elektronicznej mogą być zintegrowane z innymi narzędziami i aplikacjami, takimi jak kalendarze, systemy zarządzania projektami i platformy do współpracy, co zwiększa efektywność pracy zespołowej.
- Poprawa wizerunku firmy: Profesjonalny system poczty elektronicznej z własną domeną może poprawić wizerunek firmy, zwiększając jej wiarygodność i profesjonalizm w oczach klientów i partnerów biznesowych

D. Cyberbezpieczeństwo

W tym punkcie KAMSOFT S.A. w swojej ofercie ma nowatorskie rozwiązania, znacząco wspomagające pracę Szpitala w zakresie szeroko rozumianego wsparcia cyber-bezpieczeństwa, głównie w zakresie integracji usług IT, w szczególności w odniesieniu do wskaźnika D21G. Zachęcamy do zapoznania się z oferowanymi rozwiązaniami.

Zakup usług i urządzeń do segmentacji sieci i separacji sieci – oferowane rozwiązania

Oferowane rozwiązanie	Opis funkcjonalny	Uzyskane korzyści
Przełączniki Ethernet oraz routery warstwy L2/L3	- Zastosowanie urządzeń, które zarządzają ruchem pakietów w sieci lokalnej operując na drugiej warstwie modelu TCP/IP, oraz przy okazji modelu OSI/ISO. - Możliwość utworzenia sieci VLAN co pozwala w sposób efektywny segmentować sieć, czyli podzielić ją na mniejsze elementy, które w sposób logiczny są od siebie odseparowane - Segmentacja pozwala zatrzymać cały ruch sieciowy pomiędzy wybranymi częściami sieci komputerowej lub definiować parametry ruchu względem takich kryteriów, jak np. rodzaj ruchu, źródło, miejsce docelowe – zgodnie politykami segmentacji sieci	- Zwiększenie bezpieczeństwa: Segmentacja sieci ogranicza obszar ataku, co utrudnia intruzom przemieszczanie się po całej sieci w przypadku naruszenia zabezpieczeń. - Lepsze zarządzanie ruchem sieciowym: Podział sieci na mniejsze segmenty pozwala na bardziej efektywne zarządzanie ruchem. Można przypisywać specyficzne polityki zarządzania ruchem do poszczególnych segmentów, co ułatwia monitorowanie i kontrolowanie przepływu danych - Segmentacja pomaga w zarządzaniu ryzykiem wewnętrznym, takim jak nieautoryzowany dostęp - Zgodność z regulacjami - Szybsze wykrywanie i reagowanie na incydenty - Optymalizacja zasobów i wydajności - lepsze zarządzanie zasobami sieciowymi, takimi jak przepustowość, moc obliczeniowa i pamięć - Segmentacja wspiera skalowalność infrastruktury IT, umożliwiając łatwiejsze dodawanie nowych urządzeń i usług bez konieczności przebudowy całej sieci

Przykład wypełnienia fiszki projektowej

Zakładane cele :

- Zwiększone bezpieczeństwo danych: Segmentacja sieci pozwala na izolowanie wrażliwych informacji w określonych segmentach, co utrudnia dostęp do nich dla potencjalnych atakujących.
- Lepsza kontrola dostępu: Dzięki segmentacji można precyzyjnie kontrolować, kto i co ma dostęp do poszczególnych części sieci, co minimalizuje ryzyko nieautoryzowanego dostępu.
- Poprawa wydajności sieci: Segmentacja pomaga w zarządzaniu ruchem sieciowym, redukując zatory i optymalizując przepływ danych, co prowadzi do lepszej wydajności całej sieci.
- Łatwiejsze zarządzanie i utrzymanie: Podział sieci na mniejsze segmenty ułatwia zarządzanie i rozwiązywanie problemów, ponieważ administratorzy mogą skupić się na konkretnych obszarach bez wpływu na całą sieć.
- Zgodność z przepisami: Segmentacja sieci pomaga w spełnianiu wymogów regulacyjnych poprzez izolowanie danych i kontrolowanie dostępu.
- Szybsza reakcja na incydenty: W przypadku naruszenia bezpieczeństwa, segmentacja umożliwia szybsze zidentyfikowanie i izolowanie zagrożonego segmentu, co minimalizuje wpływ na resztę sieci

.

W ramach projektu zakłada się:

- Analiza potrzeb: Zidentyfikowanie specyficznych wymagań organizacji, takich jak liczba urządzeń, rodzaje przesyłanych danych oraz wymagania dotyczące bezpieczeństwa i zgodności z przepisami.
- Wybór odpowiednich narzędzi i technologii: Wybór technologii i urządzeń, które najlepiej odpowiadają potrzebom organizacji, biorąc pod uwagę funkcje, skalowalność, koszty oraz wsparcie techniczne.
- Planowanie architektury sieci: Określenie, jak segmentacja będzie wdrażana w istniejącej infrastrukturze sieciowej, w tym identyfikacja kluczowych punktów segmentacji i strategii routingu.
- Konfiguracja polityk bezpieczeństwa: Ustalenie i wdrożenie polityk bezpieczeństwa, które będą kontrolować ruch sieciowy między segmentami, w tym reguły dostępu, filtrowanie treści i monitorowanie ruchu.
- Testowanie i walidacja: Przeprowadzenie testów, aby upewnić się, że segmentacja działa zgodnie z oczekiwaniami i skutecznie chroni sieć przed zagrożeniami.
- Szkolenie personelu: Zapewnienie odpowiedniego szkolenia dla personelu IT, aby mogli skutecznie zarządzać i monitorować segmentację sieci.
- Monitorowanie i utrzymanie: Regularne monitorowanie działania segmentacji i aktualizowanie konfiguracji, aby zapewnić ciągłą ochronę przed nowymi zagrożeniami.
- Dokumentacja: Sporządzenie szczegółowej dokumentacji dotyczącej konfiguracji segmentacji, polityk bezpieczeństwa i procedur zarządzania.

Osiągane korzyści:

- Zwiększone bezpieczeństwo: Segmentacja pozwala na oddzielenie różnych części sieci, co utrudnia potencjalnym atakującym dostęp do całej sieci. W przypadku naruszenia bezpieczeństwa, atak jest ograniczony do jednego segmentu.
- Lepsza wydajność: Dzięki segmentacji można zmniejszyć ilość ruchu w sieci, co prowadzi do mniejszych opóźnień i lepszej wydajności. Mniej urządzeń w jednym segmencie oznacza mniej kolizji i bardziej efektywne przesyłanie danych.
- Łatwiejsze zarządzanie: Segmentacja ułatwia zarządzanie siecią, ponieważ administratorzy mogą kontrolować i monitorować mniejsze, bardziej zdefiniowane części sieci. To pozwala na szybsze wykrywanie i rozwiązywanie problemów.
- Izolacja problemów: W przypadku awarii lub problemów z wydajnością, segmentacja pozwala na szybkie zidentyfikowanie i izolowanie problematycznego segmentu, co minimalizuje wpływ na resztę sieci.
- Zgodność z przepisami: W niektórych branżach segmentacja sieci jest wymagana do spełnienia określonych standardów bezpieczeństwa i zgodności z przepisami

E. Cyberbezpieczeństwo

W tym punkcie KAMSOFT S.A. w swojej ofercie ma nowatorskie rozwiązania, znacząco wspomagające pracę Szpitala w zakresie szeroko rozumianego wsparcia cyber-bezpieczeństwa, głównie w zakresie integracji usług IT, w szczególności w odniesieniu do wskaźnika D21G. Zachęcamy do zapoznania się z oferowanymi rozwiązaniami.

Zakup usług wdrożenia polityki zarządzania hasłami i dostępem do systemów informatycznych – oferowane rozwiązania w zakresie usług i rozwiązań

Oferowane rozwiązanie	Opis funkcjonalny	Uzyskane korzyści
KSMFA	Zastosowanie dwuskładnikowego uwierzytelniania, co wymiernie poprawia bezpieczeństwo danych	- zwiększenie bezpieczeństwa w wykorzystanych aplikacjach - uproszczenie polityki zarządzania hasłami
KSSDS	System dostępu serwisowego – zapewnia uwierzytelnienie, logowanie aktywności oraz zapewnienie rozliczalności realizowanych czynności serwisowych	- zwiększa bezpieczeństwo w trakcie realizacji działań serwisowych
KSDomain	Wdrożenie rozwiązania domenowego	- skuteczne zarządzanie urządzeniami oraz użytkownikami w sieci

Przykład wypełnienia fiszki projektowej

Zakładane cele :

Celem nadrzędnym jest wdrożenie rozwiązań opartych o MFA (Multi-Factor Authentication), czyli uwierzytelnianie wieloskładnikowe. To metoda zabezpieczenia, która wymaga od użytkownika podania co najmniej dwóch różnych czynników weryfikacyjnych, aby uzyskać dostęp do systemu, konta lub aplikacji. Główne założenie MFA: Tradycyjne logowanie oparte tylko na haśle może być podatne na ataki (np. phishing, brute force, wycieki danych). MFA zwiększa bezpieczeństwo, wymagając dodatkowych potwierdzeń, które utrudniają nieautoryzowany dostęp. Warto dodać, że NIS 2 kładzie nacisk na cyberhigienę i bezpieczeństwo, a MFA stanowi część bardziej rozbudowanego podejścia do ochrony przed nieautoryzowanym dostępem oraz cyberatakami. Organizacje objęte dyrektywą muszą nie tylko wdrożyć MFA, ale również monitorować, audytować i utrzymywać odpowiednie mechanizmy weryfikacji tożsamości użytkowników, aby zapewnić zgodność z regulacjami i minimalizować ryzyko ataków.

Trzy główne typy czynników uwierzytelniania:

Coś, co wiesz (ang. *Something you know*):

- Hasło, PIN, odpowiedź na pytanie bezpieczeństwa.

Coś, co masz (ang. *Something you have*):

- Telefon (kod SMS lub aplikacja autoryzująca, np. Google Authenticator),
- Token sprzętowy (np. klucz bezpieczeństwa USB, jak YubiKey),
- Certyfikat cyfrowy na urządzeniu.

Coś, czym jesteś (ang. *Something you are*):

- Biometria (np. odcisk palca, rozpoznawanie twarzy, skan tęczówki).

W ramach oferowanych rozwiązań opieramy się głównie o dwa pierwsze założenia, głównie z uwagi na brak realnych regulacji prawnych pozwalających na przechowywanie danych trzeciego typu przez Szpitale dla potrzeb logowania. Poprzez wdrożenie MFA uzyska się nie tylko znacznie większą wiarygodność logowań do systemów informatycznych, ale również możliwe będzie uproszczenie polityki zarządzania oraz zmianami haseł. Należy również wyraźnie zaznaczyć, że dyrektywa NIS2 wprost wskazuje na wymóg stosowania skutecznych środków ochrony dostępu do systemów IT, w tym mechanizmów silnego uwierzytelniania, takich jak MFA, w celu minimalizacji ryzyka nieautoryzowanego dostępu.

Dodatkowo poprzez wdrożenie rozwiązań domenowych możliwe jest centralne zarządzanie użytkownikami, urządzeniami i zasobami w organizacji, co znacząco ułatwia administrację i oszczędza czas. Dzięki domenie można wdrażać polityki bezpieczeństwa, takie jak kontrola haseł czy ograniczenia dostępu, które obowiązują w całej sieci. Umożliwia także scentralizowaną kontrolę dostępu do zasobów, takich jak foldery, drukarki czy aplikacje, zwiększając bezpieczeństwo i wydajność pracy. Dodatkowo, domena pozwala zautomatyzować procesy, takie jak instalacje oprogramowania czy aktualizacje, co redukuje czas i koszty zarządzania IT.

W ramach projektu zakłada się (wskaźniki na poziomie produktu):

- Zakup usług oraz licencji i oprogramowania niezbędnego oprogramowania
- Szkolenie personelu (personel techniczny)
- Wdrożenie i uruchomienie rozwiązania

Osiągane korzyści (wskaźniki na poziomie rezultatu):

- Spełnienie wymogu NIS2 w zakresie zabezpieczeń autoryzacyjnych.
- Wspomaganie oraz optymalizacja polityki zarządzania użytkownikami.
- Oszczędność czasu pracy lekarzy lub personelu dzięki wdrożeniu SSO
- Centralne zarządzanie użytkownikami
- Centralna kontrola dostępu do urządzeń

Cyberbezpieczeństwo

W tym punkcie KAMSOFT S.A. w swojej ofercie ma nowatorskie rozwiązania, znacząco wspomagające pracę Szpitala w zakresie szeroko rozumianego wsparcia cyberbezpieczeństwa, głównie w zakresie integracji usług IT, w szczególności w odniesieniu do wskaźnika D21G. Zachęcamy do zapoznania się z oferowanymi rozwiązaniami.

Zakup lub rozwój systemów opartych na rozwiązaniach co najmniej klasy EndPoint Detection and Response w architekturze serwera – oferowane rozwiązania w zakresie usług i rozwiązań

Oferowane rozwiązanie	Opis funkcjonalny	Uzyskane korzyści
KEDR	Systemy **Endpoint Detection and Response (EDR)** to zaawansowane rozwiązania z zakresu cyberbezpieczeństwa, które są zaprojektowane do monitorowania, wykrywania i reagowania na zagrożenia w punktach końcowych sieci, takich jak komputery, laptopy, serwery czy urządzenia mobilne. Punkty końcowe (ang. *endpoints*) są często celem cyberataków, dlatego zabezpieczenie ich ma kluczowe znaczenie w ochronie organizacji. Planujemy wdrożyć i skonfigurować rozwiązanie, które odgrywa kluczową rolę w nowoczesnym cyberbezpieczeństwie, zapewniając wykrywanie zagrożeń w czasie rzeczywistym i szybką reakcję na incydenty na poziomie punktu końcowego. Pomaga organizacjom proaktywnie bronić się przed różnymi cyberzagrożeniami, w tym złośliwym oprogramowaniem, oprogramowaniem wymuszającym okup, zaawansowanymi trwałymi zagrożeniami (APT) i zagrożeniami wewnętrznymi. - wsparcie dla tworzenia dzienników audytowych dla działu IT - ocena konfiguracji - wykrywanie złośliwego oprogramowania - integralności plików - aktywne wykrywanie zagrożenia - analiza danych dziennika - wykrywanie luk w zabezpieczeniach - reagowanie na incydenty monitorowanie	**Monitorowanie w czasie rzeczywistym**: EDR zbiera dane z punktów końcowych w czasie rzeczywistym, rejestrując działania użytkowników, procesy systemowe, zmiany w plikach, czy ruch sieciowy. **Zaawansowana analiza zagrożeń**: System EDR wykorzystuje technologie takie jak sztuczna inteligencja (AI), uczenie maszynowe (ML) i analitykę behawioralną, aby wykrywać nietypowe wzorce aktywności, które mogą wskazywać na zagrożenia. **Wykrywanie i reagowanie na incydenty**: Po wykryciu potencjalnego zagrożenia system umożliwia natychmiastową reakcję, np. izolację zainfekowanego urządzenia, zatrzymanie podejrzanego procesu czy usunięcie złośliwego oprogramowania. **Gromadzenie danych do analizy śledczej**: System EDR zapisuje szczegółowe dane o zdarzeniach na punktach końcowych, co pozwala na ich analizę w przypadku incydentów bezpieczeństwa. **Integracja z innymi systemami bezpieczeństwa**: EDR współpracuje z systemami typu SIEM (*Security Information and Event Management*) czy XDR (*Extended Detection and Response*), tworząc kompleksowe rozwiązania ochronne. Wdrażane rozwiązania mogą być dwuetapowe : wskazania lub wręcz wymuszanie zdarzeń. EDR analizuje, monitoruje oraz zapisuje informacje o działaniu systemu oraz procesów na urządzeniu końcowym. Dzięki

	- utrzymanie higieny IT Zastosowane rozwiązania możliwe są do wykorzystania jako komponent w stosach monitorowania.	wdrożonym na końcówkach agentom daje dużą widoczność i wiedzę o lokalnych zdarzeniach na stacjach roboczych i serwerach. Pozwala na wykrywanie zagrożeń ukrytych na przykład w pamięci komputera, co dla innych systemów jest praktycznie niemożliwe. Przeszukiwanie incydentów i zebranych danych z końcówek · Ocena ryzyka i różne poziomy alarmowania. Wykrywanie podejrzanej aktywności. Blokowanie złośliwego działania. Threat hunting. Integracja z innymi systemami, w szczególności w zakresie monitorowania i prezentacji danych. - tworzenie zindywidualizowanych, pod klienta, scenariuszy dla monitorowania infrastruktury - tworzenie personalizowanych dashbordów z kluczowymi KPI w zakresie nadzoru Dzięki rozwiązaniu otrzymamy możliwość dostosowania wyglądu i ustawienia wizualizacji a także alertów, które zostaną wywołane, gdy określone warunki zostaną spełnione.

Przykład wypełnienia fiszki projektowej

Zakładane cele :

Głównym celem wdrożenia rozwiązania jest wdrożenie i eksploatacyjne użytkowanie zestawu mechanizmów i usług, które są zaprojektowane do monitorowania, wykrywania jak również reagowania na zagrożenia w punktach końcowych sieci, takich jak komputery, laptopy, serwery czy urządzenia mobilne. Zgodnie z raportami podatności, głównie punkty końcowe są często celem cyberataków, dlatego zabezpieczenie właśnie ich ma kluczowe znaczenie w ochronie organizacji. Realizacja takich założeń bez odpowiednich narzędzi oraz często przy braku kwalifikacji jest skazane na niepowodzenie lub tylko fragmentaryczne sukcesy. Skuteczne wdrożenie ale także wytworzenie w dziale IT oraz organizacji należytych i pożądanych nawyków, wsparte rozwiązaniami wraz proaktywnym monitoringiem pozwala zarówno na skuteczny monitoring jak i zaawansowaną analizę zagrożeń. Zintegrowania rozwiązania z systemami/zespołami monitorującymi pracę w trybie 24h oraz uruchomienie odpowiednich watch dogów pozwala na wykrywanie zagrożeń w czasie rzeczywistym i szybką reakcję na incydenty na poziomie punktu końcowego. Dzięki temu nie tylko kultura organizacyjna w ramach IT oraz IoT w szpitalu znacząco wzrasta ale przede wszystkim zwiększa się bezpieczeństwo jednostki przetwarzającej dane osobowe i dane wrażliwe.

W ramach projektu zakłada się (wskaźniki na poziomie produktu):

- Zakup usług oraz licencji i oprogramowania niezbędnego oprogramowania
- Szkolenie personelu (personel techniczny)
- Wdrożenie i uruchomienie rozwiązania
- Wykorzystanie centrum analizy i wsparcia dla działów IT szpitala
- Proaktywne monitorowanie rozwiązań objętych wdrożeniem

Osiągane korzyści (wskaźniki na poziomie rezultatu):

- Ocena wykorzystania infrastruktury IT + wskazania rozbudowy
- Monitoring końcówek pod kątem bezpieczeństwa
- Aktywne wykrywanie zagrożeń
- Opracowanie polityki bezpieczeństwa
- Identyfikacja luk w systemie oraz w zabezpieczeniach

F. Cyberbezpieczeństwo

W tym punkcie KAMSOFT S.A. w swojej ofercie ma nowatorskie rozwiązania, znacząco wspomagające pracę Szpitala w zakresie szeroko rozumianego wsparcia cyber-bezpieczeństwa, głównie w zakresie integracji usług IT, w szczególności w odniesieniu do wskaźnika D21G. Zachęcamy do zapoznania się z oferowanymi rozwiązaniami.

Przeprowadzenie szkoleń pracowników w zakresie oferowanych rozwiązań – oferowane rozwiązania

Oferowane rozwiązanie	Opis funkcjonalny	Uzyskane korzyści
KSStep1	Szkolenie z zakresu zaawansowanej administracji systemem Oracle pod kątem optymalizacji i skutecznego zarządzania posiadanym rozwiązaniem	- wiedza z zakresu administracji Oracle - najlepsze praktyki w zarządzaniu Oracle - troubleshoting – jak radzić sobie z typowymi problemami - backup – jak nim zarządzać – wiedza z zakresu administracji
KSStep2	Szkolenie z zakresu zabezpieczeń środowiska ZSI	- wiedza z zakresu kreowania polityki bezpieczeństwa - poszukiwanie słabych punktów systemów ZSI - bezpieczne zarządzanie integracjami - wdrożenie zabezpieczeń RODO - wprowadzenie metodyki zarządzania sprzętem IT oraz IoT

Przykład wypełnienia fiszki projektowej

Zakładane cele :

Głównym celem wdrożenia rozwiązania jest wdrożenie i eksploatacyjne użytkowanie zestawu mechanizmów i usług oraz polityk bezpieczeństwa, która jest niezwykle istotna z perspektywy zarządzania IT oraz IoT w ramach placówek służby zdrowia, ze szczególnym uwzględnieniem operatorów usługi krytycznej. Dodatkowo dyrektywa NIS2 wymaga aby dział IT był skutecznie przeszkolony oraz wyedukowany z zakresu zarządzania pod kątem bezpieczeństwa szeroko rozumianym zintegrowanym systemem informatycznym, którym administruje. Niezależnie od przyjętej opcji związanej z zarządzaniem infrastrukturą serwerową (outsourceing czy inhouse) zespół IT musi być partnerem do rozmów. Ponadto dział IT musi kreować bezpieczną, skuteczną i przewidywalną politykę bezpieczeństwa i z tego też tytułu jednym z celów jest nabycie wiedzy aby wyrównać poziomy kompetencyjne działów IT szpitala oraz dostawców IT aby mogli oni skutecznie komunikować się pomiędzy sobą a rozmowa była partnerska. Dodatkowo rosnące wykorzystanie szeroko rozumianego IoT w placówkach medycznych stawia przed działami IT nowe, zupełnie dotąd nieobsługiwane zadania.

Przykład wypełnienia fiszki projektowej

Zakładane cele :

.

W ramach projektu zakłada się:

- Szkolenie personelu (personel techniczny)
- Wdrożenie i uruchomienie rozwiązania lub usług o ile będą konieczne
- Wykorzystanie centrum analizy i wsparcia dla działów IT szpitala
- Zbudowanie kompetencji w szeregach działów IT, które pozwolą na skuteczną i bezpieczną komunikację z dostawcami
- Zbudowanie świadomości i kompetencji oraz jej wykorzystanie dla wykreowania odpowiedniej polityki bezpieczeństwa w organizacji

Osiągane korzyści :

- Umiejętność opracowanie polityki bezpieczeństwa
- Umiejętność identyfikacja luk w systemie oraz w zabezpieczeniach
- Twarde kompetencje w zakresie zarządzania ZSI
- Rozbudowanie zakresów wiedzy i umiejętności z zakresu administracji bazami danych
- Uzyskanie twardych umiejętności w zakresie nadzoru nad backupem

Integracja z systemami e-Zdrowia

G. Integracja z systemami e-Zdrowia

W tym punkcie KAMSOFT S.A. w swojej ofercie ma nowatorskie rozwiązania, znacząco wspomagające pracę Szpitala w zakresie szeroko rozumianego wsparcia integracji z systemami e-Zdrowia, w szczególności w odniesieniu do wskaźnika D21G. Zachęcamy do zapoznania się z oferowanymi rozwiązaniami. W ramach punktu dot. integracji z systemami e-Zdrowia, scalono wszystkie trzy wskazane zadania, które prezentowane są poniżej :

Doprowadzenie do wymiany i raportowania obowiązujących i nowych rodzajów EDM (w sumie 18 rodzajów EDM) – oferowane rozwiązania

Budowa lub rozbudowa repozytorium danych medycznych na potrzeby przechowywania i wymiany danych medycznych – oferowane rozwiązania

Podniesienie rozwiązań HIS do nowszych wersji systemu, pod warunkiem integracji z P1 – oferowane rozwiązania

Oferowane rozwiązanie	Opis funkcjonalny	Uzyskane korzyści
KS-EDMSuite	EDM, czyli elektroniczna dokumentacja medyczna to współczesny sposób zarządzania informacją o zdrowiu pacjentów oraz o przebiegu ich leczenia. Kompletna i wiarygodna informacja to podstawa do merytorycznej analizy stanu zdrowia, wspierania decyzji terapeutycznych oraz automatyzacji umożliwiającej odciążenie lekarza od mozolnego poszukiwania kluczowych informacji w gąszczu danych. Teraz system może pomóc wyłuskać te informacje, które w kontekście pacjenta są kluczowe w danym momencie. EDM stanowią dokumenty wytworzone w jednolitym formacie określonym przez zdefiniowany centralnie szablon (HL7 CDA), które są podpisane jednym z przewidzianych przez ustawę o systemie informacji w ochronie zdrowia rodzajów podpisu elektronicznego.	- integracja z SIM/P1 - integracja z placówkami w ramach wymiany EDM - EDM dostępny dla Pacjenta - zgodność z wymogami CeZ w ramach wskazanych EDM w formacie HL7CDA PIK
e-repozytorium	Lokalne repozytorium EDM jako bezpieczna alternatywa oraz wygodne miejsce przechowywania EDM wraz z dokumentami Pacjenta.	- full text search – czyli wdrożony mechanizm wyszukiwania wg naturalnego zapisu i pytania skierowanego do repozytorium - odseparowane, niezależne repozytorium lokalne jako kopia oraz miejsce do udostępniania danych EDM - spełnienie wymogów NIS2 Podział funkcjonalny – business first – wysokopoziomowo Specjalizowana funkcjonalność – spójna dla wszystkich systemów EDM Full Text Search

		Tagowanie dokumentów Możliwość nałożenia filtrowania – usługa aplikowania zgód Wymiana dokumentacji w ramach organizacji Zautomatyzowana integracja z usługami publicznymi Pełne API Możliwość łatwego / samodzielnego zintegrowania z rozwiązaniami in-house Zarządzanie dokumentacją Dedykowane punkty dostępu dla audytorów Dedykowane punkty dostępu dla instytucji kontrolujących / organów ścigania Dedykowane punkty dostępu dla CRO Monitorów Archiwizowanie Podział odpowiedzialności za kluczowe zasoby informacyjne (masters-slaves) Separacja obciążenia / zarządzanie wydajnością Compliance / Privacy by design Warstwa audytu wykorzystania API Odrębny ITS na potrzeby integracji Opcjonalne archiwum
Moduły wytwarzania i podpisywania EDM	Rozwiązania rozbudowujące ZSI, w ramach których wytwarzana jest kompletna EDM wraz z opcjami składania podpisów cyfrowych pod dokumentacją	- umożliwienie tworzenia i podpisywania EDM Systemy informatyczne wspierające prace personelu medycznego placówek umożliwiają realizację procesów digitalizacji dokumentacji medycznej i obsługi dokumentów w postaci elektronicznej. Ich w pierwszej kolejności zakup, dostawa, szkolenie personelu i ostatecznie wdrożenie przekłada się na wzrost liczby dokumentów wytwarzanych w postaci elektronicznej przez personel medyczny. Systemy te powinny umożliwiać szybkie wprowadzanie danych bezpośrednio przez specjalistów medycznych, co w efekcie powinno skutecznie ograniczyć stosowanie dokumentacji papierowej. Wzrost liczby przetwarzanych dokumentów w formie cyfrowej poprawia jakość dokumentacji, jej dostępność i zarządzanie jej archiwizacją, usprawniając przy tym jej przepływ, dostępność, zarządzanie oraz minimalizując ryzyka powstawania błędów

Zintegrowany System Informatyczny	Rozbudowa obecnie eksploatowanego systemu o moduły lub obszary podnoszące poziom integracji wewnętrznej.	Systemy zintegrowane zapewniają interoperacyjność i możliwość transferu danych pomiędzy różnymi elementami - systemami dziedzinowymi, które funkcjonują w ramach podmiotu. Kompletna integracja wewnętrzna eksploatowanego przez placówkę systemu jest kluczowym elementem skutecznej integracji z systemami zewnętrznymi i pozwoli w efekcie na sprawne raportowanie i przesyłanie danych do systemów centralnych – np. Platforma P1, zapewniając zgodność z aktualnym stanem prawnym.
Zamawianie leków on-line		- zwiększenie dostępności e-usług oferowanych pacjentowi poprzez integrację z IKP (pacjent.gov.pl) - odciążenie personelu pomocniczego placówki medycznej poprzez automatyzację procesów związanych z obsługa kontaktu z pacjentem w zakresie przedłużania recept - odciążenie personelu medycznego placówki medycznej poprzez automatyzację procesów związanych z wstępnym wprowadzeniem do systemu zapotrzebowania wskazanego przez pacjenta (wybór leków, dawkowania, etc.)
Aktualizacja rozwiązań HIS	Zaktualizowanie wymaganych funkcjonalnie bloków lub fragmentów systemów, które do tej pory nie były w całości w części objęte funkcjonalnością umożliwiającą wytwarzanie EDM zgodnie ze wskazanymi 18toma typami EDM. Dodatkowo utrzymanie systemowe przez okres trwałości projektu	- rozbudowanie systemu o brakujące elementy EDM - zapewnienie subskrypcji aktualizacji systemu na czas trwałości projektu

Przykład wypełnienia fiszki projektowej

Zakładane cele :

Na dzień składania wniosków Centrum e-Zdrowia (CEZ) wskazuje 18 rodzajów Elektronicznej Dokumentacji Medycznej (EDM), które są kluczowe dla systemu ochrony zdrowia w Polsce. Poniżej wymieniona lista tych dokumentów:

1. **E-recepta**

2. **E-skierowanie**
3. **Karta informacyjna z leczenia szpitalnego**
4. **Karta przebiegu ciąży**
5. **Orzeczenie o niezdolności do pracy** (np. ZUS ZLA)
6. **Opis badania diagnostycznego, w tym laboratoryjnego**
7. **Opis badania obrazowego**
8. **Karta odmowy przyjęcia do szpitala**
9. **Karta zgonu**
10. **Plan leczenia**
11. **Informacja o stanie zdrowia pacjenta**
12. **Zaświadczenie lekarskie** (np. o stanie zdrowia pacjenta)
13. **Karta zabiegu operacyjnego**
14. **Protokół operacyjny**
15. **Karta anestezjologiczna**
16. **Informacja o zastosowanej chemioterapii**
17. **Karta wizyty ambulatoryjnej**
18. **Dokumentacja szczepień ochronnych**

Należy zauważyć, że większość placówek nie prowadzi ww. dokumentów w formie EDM a nawet jeżeli prowadzi to często jest to tzw. Level 1, czyli z formatem HL7CDA PIK ma to wspólną tylko i wyłącznie kopertę. Celem niniejszego wdrożenia ma być doprowadzenie do wdrożenia przez Szpital wszystkich wymaganych 18tu typów dokumentów (o ile takie są w obiegu) oraz miarodajnego opomiarowania sytuacji przed i po, aby możliwe było sprawdzenie jak wygląda nie tylko samo wdrożenie ale przede wszystkim skuteczne użytkowanie przez personel szpitala funkcjonalności umożliwiających tworzenie EDM.

Przykład wypełnienia fiszki projektowej

Zakładane cele :

Wskazane dokumenty są ustandaryzowane i mają być dostępne w formie cyfrowej w ramach krajowego systemu informacji medycznej. Ich wdrożenie ma na celu usprawnienie procesów leczenia, poprawę komunikacji między podmiotami medycznymi oraz zwiększenie dostępności danych dla pacjentów. Wdrożenie obejmie również 5 letnie utrzymanie repozytoriów danych EDM wraz z ich wytwarzaniem.

W ramach projektu zakłada się:

- Spełnienie wymogów legislacyjnych w ramach udostępnienia funkcjonalności wytwarzania wskazanych 18tu typów dokumentów EDM
- Wdrożenie i przeszkolenie personelu z zakresu użytkowania systemów w ramach EDM również w zakresie skutecznego pobierania i udostępniania EDM
- Standaryzacja prowadzonej dokumentacji medycznej
- Wdrożenie nadzoru nad jakością ale również terminowością wytwarzania EDM w ramach szpitala
- Zapewnienie aktualizacji na czas trwania projektu

Osiągane korzyści :

- Zgodność z wymogami CeZ w ramach wymogów EDM wg standardu HL7CDA PIK
- Wdrożenie lokalnego e-repozytorium EDM
- Usprawnienie obiegu dokumentów medycznych i EDM w ramach szpitala
- Ułatwiony dostęp do EDM dla uprawnionego personelu medycznego
- Ułatwiony proces decyzyjny i diagnostyczny oraz poprawa jakości leczenia dzięki dostępowi do EDM pacjenta nie tylko w ramach swojej placówki ale także w ramach systemu P1
- Wygoda dla Pacjentów – integracja z systemami P1 daje nie tylko wgląd pacjenta do IKP ale również umożliwia m.in. zamawianie przedłużeń leków stale zażywanych
- Wymienność EDM pomiędzy placówkami
- Zapewniona aktualizacja systemów na czas trwania projektu

Digitalizacja dokumentacji medycznej

H. Digitalizacja dokumentacji medycznej

W tym punkcie KAMSOFT S.A. w swojej ofercie ma nowatorskie rozwiązania, znacząco wspomagające pracę Szpitala w zakresie szeroko rozumianego wsparcia tworzenia EDM oraz ucyfrowienia dokumentów prowadzonych papierowo, w szczególności w odniesieniu do wskaźnika D21G. Zachęcamy do zapoznania się z oferowanymi rozwiązaniami. W ramach punktu dot. digitalizacji przedstawiamy je zagregowane do dwóch punktów :

Wdrożenie rozwiązań umożliwiających zasilenie systemu P1 danymi medycznymi zgromadzonymi w systemie HIS – oferowane rozwiązania

Digitalizacja papierowej dokumentacji medycznej przechowywanej w podmiocie (zakup sprzętu i wynagrodzenie) – oferowane rozwiązania

Oferowane rozwiązanie	Opis funkcjonalny	Uzyskane korzyści
KS-EDMSuite	EDM, czyli elektroniczna dokumentacja medyczna to współczesny sposób zarządzania informacją o zdrowiu pacjentów oraz o przebiegu ich leczenia. Kompletna i wiarygodna informacja to podstawa do merytorycznej analizy stanu zdrowia, wspierania decyzji terapeutycznych oraz automatyzacji umożliwiającej odciążenie lekarza od mozolnego poszukiwania kluczowych informacji w gąszczu danych. Teraz system może pomóc wyłuskać te informacje, które w kontekście pacjenta są kluczowe w danym momencie. Wdrożenie EDMSuite jest konieczne dla placówek, które chcą tworzyć EDM i zasilać platformę P1. EDM stanowią dokumenty wytworzone w jednolitym formacie określonym przez zdefiniowany centralnie szablon (HL7 CDA), które są podpisane jednym z przewidzianych przez ustawę o systemie informacji w ochronie zdrowia rodzajów podpisu elektronicznego.	- komunikacja z P1 - integracja z placówkami w ramach wymiany EDM - EDM dostępny dla Pacjenta - zgodność z wymogami CeZ w ramach wskazanych EDM w formacie HL7CDA PIK - możliwość ucyfrowienia dokumentów papierowych do formatu elektronicznego
e-repozytorium	Lokalne repozytorium EDM jako bezpieczna alternatywa oraz wygodne miejsce przechowywania EDM wraz z dokumentami Pacjenta.	- full text search – czyli wdrożony mechanizm wyszukiwania wg naturalnego zapisu i pytania skierowanego do repozytorium - odseparowane, niezależne repozytorium lokalne jako kopia oraz miejsce do udostępniania danych EDM - spełnienie wymogów NIS2 Podział funkcjonalny – business first – wysokopoziomowo Specjalizowana funkcjonalność – spójna dla wszystkich systemów EDM Full Text Search

		Tagowanie dokumentów Możliwość nałożenia filtrowania – usługa aplikowania zgód Wymiana dokumentacji w ramach organizacji Integracja dokumentacji z przejmowanych podmiotów (w ramach połączeń i fuzji) Zautomatyzowana integracja z usługami publicznymi Pełne API Możliwość łatwego / samodzielnego zintegrowania z rozwiązaniami in-house Zarządzanie dokumentacją Dedykowane punkty dostępu dla audytorów Dedykowane punkty dostępu dla instytucji kontrolujących / organów ścigania Dedykowane punkty dostępu dla CRO Monitorów Archiwizowanie Podział odpowiedzialności za kluczowe zasoby informacyjne (masters-slaves) Separacja obciążenia / zarządzanie wydajnością Compliance / Privacy by design Warstwa audytu wykorzystania API Odrębny ITS na potrzeby integracji Opcjonalne archiwum
Moduły wytwarzania i podpisywania EDM	Rozwiązania rozbudowujące ZSI, w ramach których wytwarzana jest kompletna EDM wraz z opcjami składania podpisów cyfrowych pod dokumentacją	- umożliwienie tworzenia i podpisywania EDM Systemy informatyczne wspierające prace personelu medycznego placówek umożliwiają realizację procesów digitalizacji dokumentacji medycznej i obsługi dokumentów w postaci elektronicznej. Ich w pierwszej kolejności zakup, dostawa, szkolenie personelu i ostatecznie wdrożenie przekłada się na wzrost liczby dokumentów wytwarzanych w postaci elektronicznej przez personel medyczny. Systemy te powinny umożliwiać szybkie wprowadzanie danych bezpośrednio przez specjalistów medycznych, co w efekcie powinno skutecznie ograniczyć stosowanie dokumentacji papierowej. Wzrost liczby przetwarzanych dokumentów w formie cyfrowej poprawia jakość dokumentacji, jej dostępność i zarządzanie jej archiwizacją,

		usprawniając przy tym jej przepływ, dostępność, zarządzanie oraz minimalizując ryzyka powstawania błędów.
Zintegrowany System Informatyczny	Rozbudowa obecnie eksploatowanego systemu o moduły lub obszary podnoszące poziom integracji wewnętrznej.	Systemy zintegrowane zapewniają interoperacyjność i możliwość transferu danych pomiędzy różnymi elementami - systemami dziedzinowymi, które funkcjonują w ramach podmiotu. Kompletna integracja wewnętrzna eksploatowanego przez placówkę systemu jest kluczowym elementem skutecznej integracji z systemami zewnętrznymi i pozwoli w efekcie na sprawne raportowanie i przesyłanie danych do systemów centralnych – np. Platforma P1, zapewniając zgodność z aktualnym stanem prawnym.
Skaner lub urządzenie wielofunkcyjne wraz z licencją skanowania dokumentów.	Digitalizacja dokumentacji medycznej. Cała obsługa wykonywana jest przy pomocy panelu urządzenia, a dokumenty są automatycznie umieszczane we właściwych kartotekach pacjenta w systemie medycznym bez uruchamiania systemu medycznego.	- umożliwienie tworzenia i podpisywania EDM - szybki i niezawodny sposób skanowania dokumentacji pacjentów; - archiwizacja dokumentów pacjenta bezpośrednio w systemie medycznym bez konieczności jego uruchamiania - ergonomiczna obsługa skanowanych dokumentów przez panel urządzenia. - podpięcie skanowanego dokumentu pod kartotekę pacjenta i wybrany typ dokumentacji; - możliwość logowania: PIN, login i hasło, kartą - możliwość podpisania dokumentów certyfikatem ZUS - możliwość zarządzania wieloma przychodniami z poziomu jednego panelu administracyjnego - możliwość tworzenia ról dostępu użytkownika do firm, urządzeń, funkcji systemu - kompletna informacja o pacjencie w centralnym systemie medycznym

Przykład wypełnienia fiszki projektowej

Zakładane cele :

Na dzień składania wniosków Centrum e-Zdrowia (CEZ) wskazuje 18 rodzajów Elektronicznej Dokumentacji Medycznej (EDM), które są kluczowe dla systemu ochrony zdrowia w Polsce. Poniżej wymieniona lista tych dokumentów:

1. **E-recepta**
2. **E-skierowanie**
3. **Karta informacyjna z leczenia szpitalnego**
4. **Karta przebiegu ciąży**
5. **Orzeczenie o niezdolności do pracy** (np. ZUS ZLA)
6. **Opis badania diagnostycznego, w tym laboratoryjnego**
7. **Opis badania obrazowego**
8. **Karta odmowy przyjęcia do szpitala**
9. **Karta zgonu**
10. **Plan leczenia**
11. **Informacja o stanie zdrowia pacjenta**
12. **Zaświadczenie lekarskie** (np. o stanie zdrowia pacjenta)
13. **Karta zabiegu operacyjnego**
14. **Protokół operacyjny**
15. **Karta anestezjologiczna**
16. **Informacja o zastosowanej chemioterapii**
17. **Karta wizyty ambulatoryjnej**
18. **Dokumentacja szczepień ochronnych**

Należy zauważyć, że większość placówek nie prowadzi ww. dokumentów w formie EDM a nawet jeżeli prowadzi to często jest to tzw. Level 1, czyli z formatem HL7CDA PIK ma to wspólną tylko i wyłącznie kopertę. Celem niniejszego wdrożenia ma być doprowadzenie do wdrożenia przez Szpital wszystkich wymaganych 18tu typów dokumentów (o ile

takie są w obiegu) oraz miarodajnego opomiarowania sytuacji przed i po, aby możliwe było sprawdzenie jak wygląda nie tylko samo wdrożenie ale przede wszystkim skuteczne użytkowanie przez personel szpitala funkcjonalności umożliwiających tworzenie EDM.

Dodatkowo wskazać należy, że w szpitalach funkcjonuje niezliczona ilość karteczek, jako zleceń, uwag, które skutecznie omijają wdrażany obieg dokumentacji EDM w ramach ZSI. To pole, które nie jest opisane jako HL7CDA PIK i leży w chwili obecnej w pełnej jurysdykcji producentów systemów. Możliwe jest uruchamianie użytkowników do takiej pracy, która z kolej znacząco wzbogaci zasoby EDM w ramach przetwarzalnej i interpretowalnej informacji o Pacjencie.

Przykład wypełnienia fiszki projektowej

Zakładane cele :

Wskazane dokumenty są ustandaryzowane i mają być dostępne w formie cyfrowej w ramach krajowego systemu informacji medycznej. Ich wdrożenie ma na celu usprawnienie procesów leczenia, poprawę komunikacji między podmiotami medycznymi oraz zwiększenie dostępności danych dla pacjentów. Wdrożenie obejmie również 5 letnie utrzymanie repozytoriów danych EDM wraz z ich wytwarzaniem.

Ucyfrowienie dokumentacji poprzez zarówno objęcie obecnych dokumentów poza obiegiem EDM w ramach ZSI oraz wskanowanie papierowej dokumentacji medycznej do systemu i odłożenie jej w lokalnym repozytorium (w tym w zakresie świadomych zgód pacjenta).

W ramach projektu zakłada się:

- Spełnienie wymogów legislacyjnych w ramach udostępnienia funkcjonalności wytwarzania wskazanych 18tu typów dokumentów EDM
- Wdrożenie i przeszkolenie personelu z zakresu użytkowania systemów w ramach EDM również w zakresie skutecznego pobierania i udostępniania EDM
- Standaryzacja prowadzonej dokumentacji medycznej
- Ucyfrowienie dokumentacji papierowej
- Wdrożenie nadzoru nad jakością ale również terminowością wytwarzania EDM w ramach szpitala
- Zapewnienie aktualizacji na czas trwania projektu

Osiągane korzyści :

- Zgodność z wymogami CeZ w ramach wymogów EDM wg standardu HL7CDA PIK
- Wdrożenie lokalnego e-repozytorium EDM
- Usprawnienie obiegu dokumentów medycznych i EDM w ramach szpitala
- Ułatwiony dostęp do EDM dla uprawnionego personelu medycznego
- Ułatwiony proces decyzyjny i diagnostyczny oraz poprawa jakości leczenia dzięki dostępowi do EDM pacjenta nie tylko w ramach swojej placówki ale także w ramach systemu P1

- Wygoda dla Pacjentów – integracja z systemami P1 daje nie tylko wgląd pacjenta do IKP ale również umożliwia m.in. zamawianie przedłużeń leków stale zażywanych
- Wymienność EDM pomiędzy placówkami
- Zapewniona aktualizacja systemów na czas trwania projektu
- Repozytorium EDM
- Ucyfrowienie papierowej dokumentacji i w efekcie zwiększenie jej dostępności w ramach uprawnionych osób

Wdrożenie rozwiązań AI

I. Wdrożenie rozwiązań AI

W tym punkcie KAMSOFT S.A. w swojej ofercie ma nowatorskie rozwiązania, również wykorzystujące AI. W ramach dofinansowań KPO Ministerstwo Zdrowia przewiduje jedynie integrację z modelami AI wypracowanymi w ramach platformy centralnej. Wobec czego integracji poddane będą rozwiązania HIS wskazane w ramach możliwych przypadków użycia integracji . Punkty referencyjne z opracowanych i dostępnych materiałów MZ prezentują się następująco :

Integracja z opracowanymi przez CeZ w ramach Platformy Usług Inteligentnych narzędziami opartymi na sztucznej inteligencji, wspomagającymi proces podejmowania decyzji przez lekarza– oferowane rozwiązania

Integrację z centralnym repozytorium danych medycznych opracowanym i udostępnionym przez CeZ – oferowane rozwiązania

Oferowane rozwiązanie	Opis funkcjonalny	Uzyskane korzyści
KS-EDMSuite	W ramach integracji z rozwiązaniami dot. EDM wykorzystywany jest interfejs integracyjny EDMSuite. Spodziewamy się, że podobnie zostaną zaimplementowane usługi integracyjne z centralnym repozytorium – jednak z uwagi na brak jakichkolwiek wytycznych na tym etapie ze strony CeZ nie jest możliwe opisanie dalszych wymagań	Dojrzałe, funkcjonujące skutecznie na rynku rozwiązanie umożliwiające integrację z rozwiązaniami P1 – zakłada się jego wykorzystanie przy integracji z AI opracowanym przez CeZ
Dedykowana integracja via CustomAPI	Dedykowana integracja z usługami AI do wspomagania procesów medycznych – brak opisu interfejsu po stronie CeZ na chwilę obecną uniemożliwia wyspecyfikowanie funkcjonalności	Opracowane wg. określonych wytycznych CeZ API
Pharmindex Open z asystentem AI dla przychodni szpitalnych	W ramach integracji, AI w Pharmindex Open ułatwi wyłuskanie z opisów Pharmindex informacji, które mogą być szczególnie istotne w farmakoterapii pacjenta jak stosowanie produktu u dzieci, osób starszych, pytania dodatkowe do wywiadu z pacjentem, zaproponowanie dodatkowych badań itp. AI pomaga w wygenerowaniu informacje w oparciu o rzetelną wiedzę zgromadzoną w Pharmindex i nie rozszerza jej o inne źródła.	Bezpieczeństwo farmakoterapii pacjenta, Oszczędność czasu. Informacja oparta o rzetelne, aktualizowane na bieżąco źródło.