SAS® Visual Investigator

Szybka i efektywna analiza śledcza na masowych danych

Kto używa SAS® Visual Investigator?

SAS Visual Investigator jest przeznaczony dla organizacji które w walce z nieprawidłowościami korzystają z szerokich, wielowymiarowych danych. Zaliczamy do nich na przykład instytucje stojące na straży porządku publicznego, ochrony granic, zakłady ubezpieczeń, banki, operatorów telekomunikacyjnych. Bezpośrednimi użytkownikami narzędzia są analitycy biznesowi, analitycy śledczy oraz pracownicy operacyjni działający w terenie.

Do czego służy SAS® Visual Investigator?

SAS Visual Investigator jest zaawansowanym rozwiązaniem umożliwiającym integrację i analizę danych pochodzących z różnych źródeł. Umożliwia wykrywanie nadużyć i nieprawidłowości za pomocą zaawansowanych technik dochodzeniowych oraz na podstawie spostrzeżeń własnych analityka. Użytkownicy mogą wykonywać szczegółowe analizy śledcze, odkrywać nieznane wzorce i dostosowywać platformę do indywidualnych i organizacyjnych potrzeb. Rozwiązanie jest przystosowane do instalacji w chmurze.

Jakie korzyści daje SAS® Visual Investigator?

Organizacje stoją przed wyzwaniem polegającym na zwiększeniu wydajności wykrywania nadużyć przy rosnącej ich liczbie oraz coraz bardziej skomplikowanych schematach. SAS Visual Investigator pomaga skutecznie odpowiedzieć na to wyzwanie poprzez generowanie komunikatywnych alertów wskazujących nieprawidłowości i udostępnienie narzędzi umożliwiających pracę grupową, szybką analizę i podjęcie właściwych decyzji.

Wykorzystanie zawansowanej analityki SAS i uczenia maszynowego w połączeniu z interaktywnym interfejsem dla analityków śledczych umożliwia szybkie i skuteczne prowadzenie analiz oraz podział i przypisywanie zadań w zależności od aktualnych potrzeb. Możliwa jest również bezpośrednia współpraca z systemami zewnętrznymi za pomocą interfejsów programistycznych.

Dzięki zoptymalizowanym funkcjom administracyjnym, które zostały udostępnione użytkownikom, mogą oni łatwo adaptować narzędzie do zmieniających się wymagań rynku, takich jak wymagania regulatorów, i wymagań biznesowych, w tym potrzeb audytu wewnętrznego. Prace dostosowawcze mogą być w szerokim zakresie wykonywane przez użytkowników biznesowych.

Funkcjonalność analityczna obejmuje między innymi wyszukiwanie pełnotekstowe i przestrzenne, analizę tekstu, wielowymiarowe wizualizacje, automatyczną budowę sieci i analizę transakcji.

Zintegrowane, łatwo dostępne, dobrze zarządzane i aktualne dane umożliwiają analitykom oraz śledczym uzyskanie całościowego obrazu relacji, sieci, wzorców, zdarzeń, trendów i anomalii oraz znalezienie się o krok do przodu przed oszustami.

Korzyści z zastosowania

- **Możliwość łatwego dostosowania narzędzia do specyficznych wyzwań biznesowych.** Dzięki konfigurowalnemu modelowi danych i elastyczności rozwiązania możliwe jest szybkie dostosowanie narzędzia do nowych trendów i wymagań biznesowych, uzyskanie dostępu do nowych źródeł danych, dostosowanie do zmian w strukturze organizacji i rozszerzenie zastosowań o nowe obszary.
- **Wzrost efektywności.** Nasze rozwiązanie zapewnia automatyzację procesów związanych z zarządzaniem danymi, klasyfikację i wstępną ocenę alertów oraz system workflow. Wszystkie te elementy istotnie skracają proces decyzyjny. Prosty w obsłudze interfejs użytkownika umożliwia import danych uzupełniających do wewnętrznej bazy danych, wykonywanie złożonych wyszukiwań, korzystanie podczas analizy z interaktywnych widoków tych samych danych, takich jak diagram powiązań, widok chronologiczny, widok geoprzestrzenny i widok tabelaryczny.
- **Łatwe wykorzystanie wszystkich danych.** W przeciwieństwie do podejścia tradycyjnego, skutkującego ponoszeniem dodatkowych kosztów tworzenia modeli danych, ETL czy koniecznością każdorazowego udziału pracowników dostawcy przy wymaganej kastomizacji, nasze podejście umożliwia wykorzystanie danych źródłowych bez potrzeby importowania ich do SAS Visual Investigator, bez względu na ich wielkość i strukturę. Takie rozwiązanie umożliwia analitykom pracę na aktualnych danych, które mogą być rozproszone w obrębie danej organizacji.

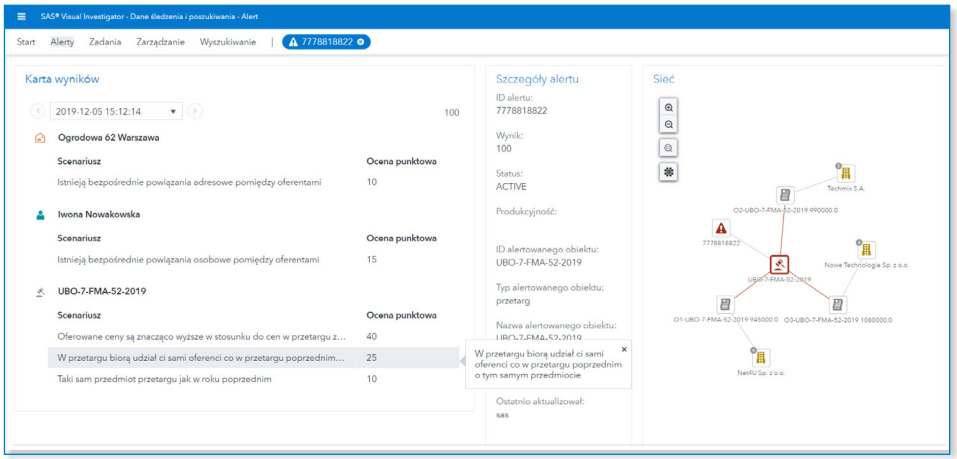
- **Minimalizacja całkowitego kosztu eksploatacji dzięki opcji instalacji w chmurze oraz możliwościom konfiguracyjnym.** Architektura SAS Visual Investigator umożliwia przetwarzanie danych w dowolnym miejscu, bez utraty funkcjonalności analitycznej.
- **Komunikatywność narzędzia.** Zdajemy sobie sprawę, że od analityków śledczych nie należy oczekiwać wiedzy dotyczącej różnicy między prawdopodobieństwem testowym a testem t. Położyliśmy duży nacisk na komunikatywność narzędzia. Przykładowo, powody wygenerowania alertu zawsze podawane są w zrozumiałej dla wszystkich formie opisowej.

Przegląd funkcjonalności

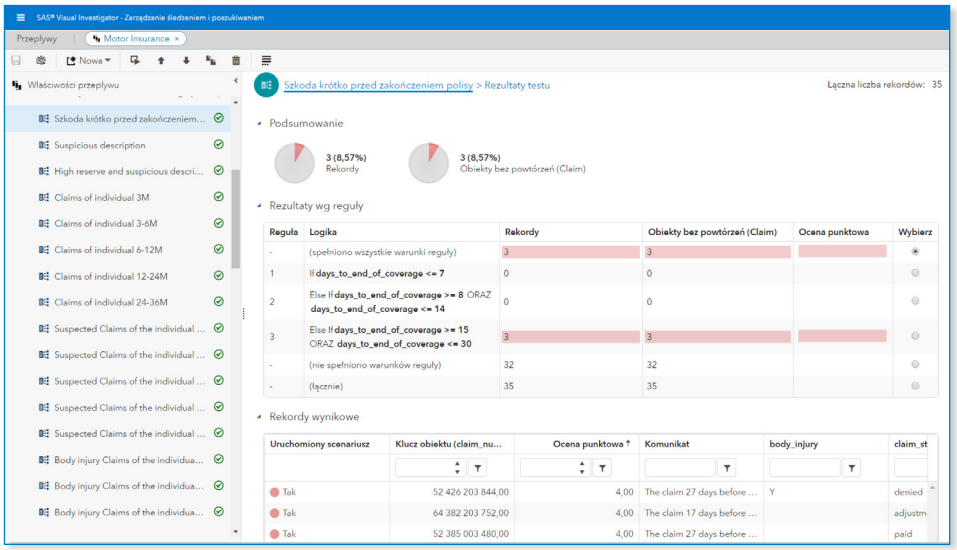
SAS Visual Investigator jest prostym w obsłudze narzędziem, służącym do prowadzenia analiz śledczych i zarządzania cyklem życia śledztwa. Wspiera podejmowanie odpowiednich działań na podstawie szybkich decyzji wynikających z wyników analizy. Został zaprojektowany z myślą o wydajności i efektywności.

Poniżej zaprezentowano najważniejsze cechy charakterystyczne i funkcjonalne narzędzia.

- **Alerty:** Zapewniono funkcjonalność umożliwiającą wykrywanie podejrzanych zjawisk i generowanie alertów dzięki wykorzystaniu reguł biznesowych i scenariuszy. Alerty generowane są automatycznie na podstawie aktualnych danych. Sposób wizualizacji skutkuje szybkim zrozumieniem kontekstu, w którym osadzony jest dany alert. Analitycy mogą wydawać dyspozycje, zakładać sprawy w celu wykonania pogłębionej analizy, podejmować na bieżąco decyzje dotyczące obiektów stanowiących przedmiot zainteresowania.
- **Zarządzanie alertami i workflow:** Menedżerowie mogą nadawać priorytet działaniom analitycznym, monitorować produktywność i skuteczność analityków oraz dostosowywać strategie analityczne do nowych, pojawiających się wzorców nadużyć.
- **Elastyczna adaptacja do zmieniających się potrzeb biznesowych:** Administratorzy mogą szybko udostępniać nowe zasoby informacyjne korzystając z interaktywnych narzędzi, bez konieczności tworzenia niestandardowych interfejsów.
- **Ukierunkowana analiza śledcza:** Obszary robocze umożliwiają gromadzenie i analizę danych istotnych dla śledztwa, pochodzących z alertów lub wyszukiwania. W ramach obszaru roboczego dostępne są interaktywne widoki tych samych danych, takie jak diagram powiązań, chronologiczny, tabelaryczny, szczegółowy, mapy. Moduł dokumentacji wyników umożliwia rejestrację widoków obszaru roboczego lub ich fragmentów oraz udokumentowanie wyników analizy.



Rysunek 1: Analitycy mogą zapoznać się z regułami, które spowodowały wygenerowanie alertu oraz z oceną punktową. Mogą eksplorować skojarzoną sieć powiązań i wyświetlać inne informacje, które pomagają ocenić alert i podjąć odpowiednie działania.



Rysunek 2: Analitycy mogą tworzyć i testować scenariusze służące do identyfikacji podejrzanych zdarzeń i anomalii w danych oraz do generowania alertów.

Przegląd funkcjonalności

Wyszukiwanie

Po uprzednim zaindeksowaniu, przeszukiwane mogą być wszystkie dane, przechowywane zarówno w źródłach zewnętrznych, jak i wewnętrznej bazie danych. Wyniki wyszukiwania można filtrować, przeglądać i przesyłać do przestrzeni roboczej w celu dalszej analizy.

Cechy charakterystyczne:

- **Wyszukiwanie pełnotekstowe:** Wymaga wpisania poszukiwanego tekstu w pole wyszukiwania. Wyrazy stanowiące tekst zapytania są łączone domyślnie opera-

torem OR. Przeszukiwane są wszystkie obiekty istniejące w bazie danych.

- **Filtrowanie wyników wyszukiwania:** Wyniki można filtrować po typach obiektów i zawartości pól. Obiekty nie spełniające kryterium zadanego przez filtry nie będą widoczne na liście wyników. Filtry i ich ustawienia określane są podczas konfiguracji typów obiektów.
- **Wyszukiwanie według formatki obiektu:** Wymaga wpisania wyszukiwanego tekstu w co najmniej jedno pole formatki. Teksty wpisane w różne pola są łączone domyślnie za pomocą operatora AND. Wyszukane zostaną tylko te obiekty których zawartość poszczególnych pól odpowiada tekstowi podanemu w polach formatki wyszukiwania.
- **Asystent budowy zapytań:** Narzędzie umożliwia tworzenie zaawansowanych zapytań, dotyczących jednego lub kilku typów obiektów, bez znajomości składni. Warunki można zadawać na poziomie pól obiektów a stosowane operatory zależą od typu danego pola.
- **Wyszukiwanie na mapach:** Wyszukiwanie można ograniczyć do obszaru wskazanego na mapie poprzez nasienie odpowiedniego kształtu. Na mapie zostaną pokazane obiekty spełniające kryteria wyszukiwania i posiadające współrzędne.
- **Inspektor obiektów:** Wyświetla w odrębnym panelu skrótowe informacji o obiekcie zaznaczonym na liście wyników wyszukiwania.
- **Zaznaczanie wyników wyszukiwania:** Wyszukane obiekty można zaznaczać na liście wyników korzystając z filtrów lub wyszukiwarki tekstów etykiet, a następnie przesłać je do przestrzeni roboczej w celu dalszej analizy.

Scenariusze

Intuicyjny interfejs użytkownika umożliwia tworzenie reguł i scenariuszy generujących alerty przeznaczone do oceny przez analityka. Interfejs umożliwia:

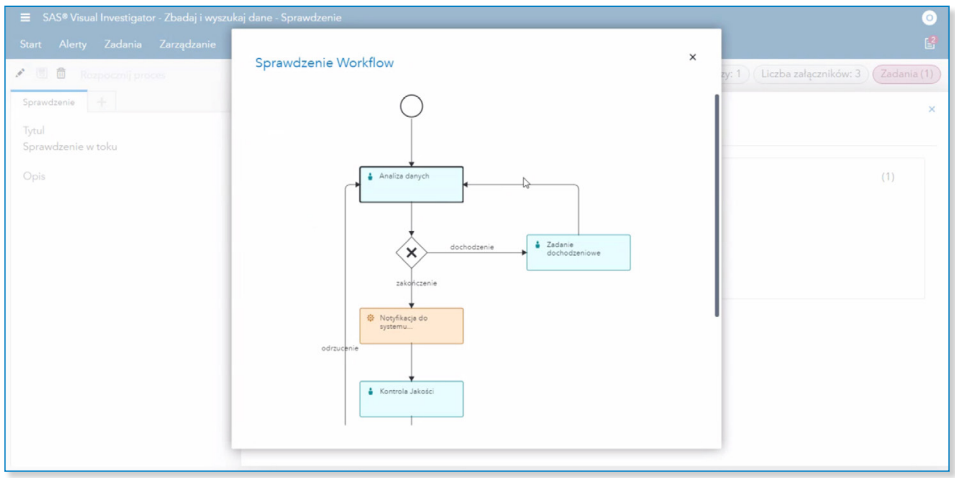
- Tworzenie scenariuszy przy użyciu konstruktora reguł, tabeli decyzyjnej lub kodu SAS.
- Modyfikację parametrów scenariuszy, w zależności od uprawnień.
- Testowanie scenariuszy i wyliczania oceny punktowej.
- Generowanie oceny punktowej na podstawie scenariuszy.
- Uruchamianie w trybie wsadowym lub ręczne.

Alerty

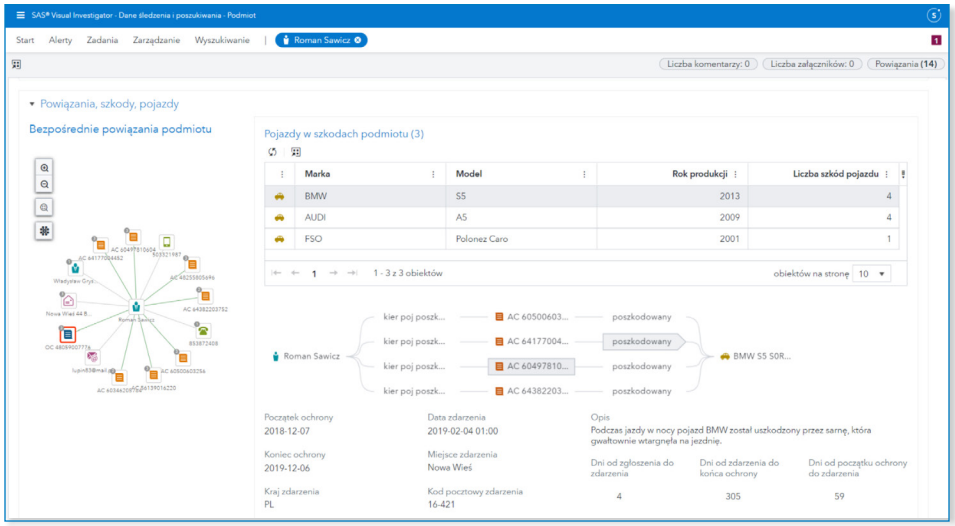
Zapewniono funkcjonalność umożliwiającą wykrywanie podejrzanych zjawisk i generowanie alertów dzięki wykorzystaniu reguł biznesowych i scenariuszy. Alerty generowane są automatycznie na podstawie aktualnych danych. Dzięki możliwościom integracyjnym alerty można ładować z systemów zewnętrznych (obukierunkowa komunikacja).

Funkcjonalność dotycząca alertów umożliwia:

- Określenie priorytetu alertów i przypisywanie ich do użytkowników lub grup.
- Wizualizację alertów umożliwiającą szybkie zrozumienie kontekstu, w których są osadzone.
- Wzbogacenie alertów o powiązane obiekty i dodatkowe dane.
- Eskalacje alertów poprzez zmianę kolejek i priorytetów.
- Ustawienie opcji automatycznej dyspozycji.



Rysunek 3: Administratorzy mogą tworzyć schematy przepływu pracy, co umożliwia użytkownikom codzienną pracę w podziale na zadania.



Rysunek 4: Analitycy i śledczy mogą zapoznawać się ze szczegółami danego obiektu i obiektów powiązanych w widoku strony, dostosowanym do aktualnych potrzeb.

- Zarządzanie i kontrolę wykonania dyspozycji.
- Oznaczenie alertu w celu wykonania pogłębionej analizy.

SAS® Mobile Investigator

SAS Mobile Investigator jest aplikacją umożliwiającą korzystanie z SAS Visual Investigator z urządzeń mobilnych. Użytkownicy mogą wyszukiwać dane, odbierać i wykonywać zadania, tworzyć nowe treści i zarządzać dochodzeniami z dowolnego miejsca. Dodatkowo dostępne są usługi urządzeń mobilnych, takie jak wykrywanie lokalizacji na mapie.

Administratorzy mogą zapewnić dostęp mobilny użytkownikom pracującym w terenie korzystając z narzędzi administracyjnych SAS Visual Investigator, umożliwiających zarządzanie aplikacją oraz jej konfigurację.

Analityka

Zastosowana analityka wspiera użytkowników w wielu obszarach. Przykładowo, umożliwia łatwą identyfikację obiektów o takiej samej zawartości wskazanych pól, co skutkuje wyłapaniem potencjalnych duplikatów. Często pozwala to na ogląd sytuacji z nowej perspektywy znacznie upraszczając śledztwo. Kolejnym przykładem jest możliwość stosowania miar centralności sieci społecznej, takich jak bliskość czy pośrednictwo. Miary centralności wskazują obiekty spełniające w sieci określone role, co znacznie ułatwia ocenę i stawianie hipotez, szczególnie w przypadku dużych sieci. Wizualizacja sieci powiązań których elementami są osoby, zdarzenia, miejsca, rzeczy itp. oraz funkcjonalność analityczna, umożliwiają użytkownikom identyfikację nieoczywistych związków między obiektami, prześledzenie ich powstawania w czasie oraz wykrywanie wzorców.

Pracę z siecią umożliwia analitykom interaktywny diagram powiązań. Poszczególne obiekty lub ich grupy można rozwijać o nowe obiekty. Obiekty nieistotne dla analizy można usuwać z diagramu. Dostępne są również automatyczne układy diagramu zwiększające jego czytelność. Diagram lub jego fragmenty można przesyłać do modułu dokumentacji wyników analizy.

Najważniejsza funkcjonalność

Wyszukiwanie
- Wyszukiwanie pełnotekstowe.
- Wyszukiwanie według formatki obiektu.
- Asystent budowy zaawansowanych zapytań.
- Wyszukiwanie na mapach, eksploracja i wizualizacja.
- Filtrowanie wyników wyszukiwania.
- Wizualizacja analizy tekstu.

Alerty
- Zarządzanie i audyt.
- Określanie priorytetów i kolejek alertów.
- Wzbogacenie alertów o dodatkowe dane.
- Wizualizacja alertu i obiektów składowych umożliwiającą szybkie zrozumienie kontekstu.
- Opcje dyspozycji alertów - zarządzanie i kontrola.
- Zakładanie spraw na podstawie alertów.

Analityka
- Identyfikacja obiektów o takiej samej zawartości wskazanych pól.
- Miary centralności sieci społecznej, przejrzysta wizualizacja wyników.
- Rozwijanie obiektów o obiekty połączone.
- Ikony dla typu obiektu w zależności od zawartości pól i dodatkowe oznaczenia graficzne.

Analiza transakcji
- Wizualizacja sieci transakcji.

Analiza śledcza
- Interaktywne obszary robocze.
- Dokumentacja wyników analizy.
- Wydruk wyników.
- Interaktywne widoki danych (diagram powiązań, chronologiczny, tabelaryczny, szczegółowy, mapy).

Zarządzanie sprawami
- Workflow.
- Możliwość dodawania załączników.
- Konfiguracja strony startowej w zależności od uprawnień użytkownika.
- Szablony wydruku.

Scenariusze
- Tworzenie scenariuszy przy użyciu konstruktora reguł, tabeli decyzyjnej lub kodu SAS.
- Modyfikacja parametrów scenariuszy, w zależności od uprawnień.
- Testowanie scenariuszy.
- Generowanie oceny punktowej na podstawie scenariuszy.
- Uruchamianie w trybie wsadowym lub ręczne.

Cechy charakterystyczne:

- **Diagram powiązań:** Wizualizacja i eksploracja sieci, automatyczne układy diagramu, identyfikacja grup ściślej powiązanych ze sobą obiektów, wykrywanie nieoczywistych związków.
- **Rozwijanie:** Dotyczy obiektu lub grupy obiektów, które można rozwijać o jeden lub dwa poziomy, o obiekty lub powiązania wskazanego typu, powiązania transakcyjne, inne obiekty zgodne z kryteriami zapytania formułowanego podczas rozwijania.
- **Analityka sieciowa:** Wskazanie obszarów sieci wymagających zainteresowania analityka za pomocą miar centralności.
- **Oznaczenia graficzne elementów sieci:** Różne ikony dla różnych typów obiektów oraz zróżnicowanie ikon dla jednego typu obiektu w zależności od zawartości pola, np. do typu obiektu pojazd można przypisać różne ikony w zależności od rodzaju pojazdu. Zróżnicowanie kolorów i innych właściwości w zależności od typu połączeń. Zróżnicowanie oznaczeń graficznych skutkuje szybszym i lepszym zrozumieniem danych.

Przestrzeń robocza

Przestrzeń robocza umożliwia analitykom gromadzenie, wizualizację, eksplorację i analizowanie danych dotyczących ich dochodzenia. Do przestrzeni roboczej wskazanego lub nowotworzonego obiektu, takiego jak np. Dochodzenie czy Sprawa, można dodawać dane stanowiące przedmiot zainteresowania analityka. Jeden obiekt może posiadać wiele przestrzeni roboczych. W ramach przestrzeni roboczej dostępne są różne widoki danych (diagram powiązań, chronologiczny, tabelaryczny, szczegółowy, mapy). Widoki są interaktywne względem siebie, co oznacza że obiekt zaznaczony w jednym widoków zachowuje status zaznaczenia po przełączeniu widoku na inny.

Najważniejsza funkcjonalność (c.d.)

Administracja i konfiguracja

- Otwarty model danych.
- Łatwe dołączanie nowych źródeł danych.
- Projektowanie stron i formatek obiektów przy pomocy narzędzia udostępniającego metodę przeciągnij i upuść.
- Definiowanie typów obiektów i połączeń.
- Możliwość eksportu i importu konfiguracji.
- Konfiguracja wyszukiwania.
- Model zabezpieczeń na poziomie encji.
- Definiowanie modelu wizualizacji chronologicznej i wizualizacji na mapach.
- Widok obiektu wzbogacany o dane z obiektów powiązanych.
- Uprawnienia użytkowników.
- Workflow i monitorowanie zadań.
- Audyt.

SAS® Mobile Investigator

- Zdalny dostęp z urządzeń mobilnych.
- Wykrywanie lokalizacji/usługi urządzeń mobilnych.
- Wyszukiwanie danych.
- Przyjmowanie i realizacja zadań w ramach workflow.
- Tworzenie nowych treści.
- Administracja aplikacji mobilnej - projektowanie dedykowanych stron i formatek obiektów, zarządzanie właściwościami.

Konfigurowalność

Dzięki konfigurowalnemu modelowi danych i elastyczności rozwiązania możliwe jest szybkie dostosowanie narzędzia do nowych trendów i wymagań biznesowych, uzyskanie dostępu do nowych źródeł danych i dostosowanie do zmian w strukturze organizacji.

Cechy charakterystyczne:

- Otwarty model danych, umożliwiający szybkie dostosowanie narzędzia do nowych wymagań biznesowych.
- Interaktywne narzędzie projektowania stron i formatek.
- Konfiguracja i zarządzanie alertami w połączeniu z możliwością zdefiniowania workflow.
- Możliwość eksportu i importu konfiguracji ułatwiająca utrzymanie spójności pomiędzy różnymi środowiskami.

Ponadto dostępne są standardowe funkcje administracyjne, takie jak indeksowanie i import danych.

W celu kontaktu z lokalnym biurem SAS, odwiedź stronę: sas.com/poland