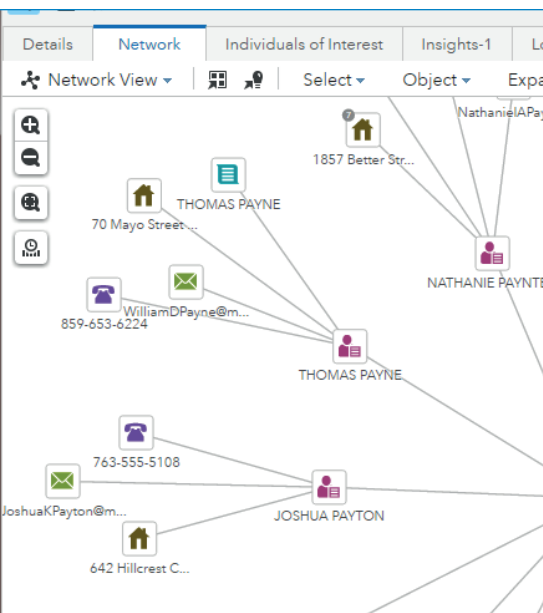


SAS® Visual Investigator

Szybka i efektywna analiza śledcza na masowych danych



Przeznaczenie

SAS Visual Investigator to zaawansowane narzędzie analityczne umożliwiające integrację i analizę danych pochodzących z różnych źródeł. Jest przeznaczony dla organizacji, w których wymagane jest szybkie podejmowanie decyzji na podstawie skutecznej analizy danych. Zaliczamy do nich przede wszystkim instytucje stojące na straży porządku publicznego, ochrony granic, zakłady ubezpieczeń oraz banki.

Bezpośrednimi użytkownikami narzędzia są analitycy śledczy, analitycy biznesowi oraz śledczy z obu tych obszarów. Narzędzie umożliwia pracę grupową, co sprzyja szybszej identyfikacji wzorców, anomalii i trendów ukrytych w danych. Charakteryzuje się prostym w obsłudze interfejsem użytkownika.

Rozwiązanie inne niż wszystkie

W przeciwieństwie do tradycyjnych narzędzi, które do rozpoczęcia analizy wymagają identyfikacji punktu zaczepienia i oferują na tym etapie jedynie możliwość wyszukiwania, SAS Visual Investigator – obok możliwości stosowania metody tradycyjnej – wykorzystuje zaawansowaną analitykę, umożliwiającą automatyczne wykrywanie nieznanym wcześniej związków.

Tradycyjna metoda prowadzenia analiz, polegająca na intuicyjnym przeszukiwaniu danych, niesie ze sobą ryzyko niewłaściwego wykorzystania czasu i zasobów. Brak klarownego punktu startowego lub klarownej hipotezy dla analizy zazwyczaj skutkuje jej wydłużeniem oraz stawia pod znakiem zapytania jej skuteczność. Nieefektywna analiza jest zagrożeniem dla organizacji. W grę wchodzi tutaj przede wszystkim aspekt finansowy, skuteczność sprostania wymaganiom wynikającym z działalności organizacji oraz z regulacji prawnych, a także reputacja.

Podczas gdy inne narzędzia umożliwiają jedynie podejście tradycyjne, oparte na wyszukiwaniu, SAS Visual Investigator wykorzystuje zaawansowaną analitykę, umożliwiającą automatyczną identyfikację punktu startowego dla analizy w postaci alertu. Alert wskazuje obiekt o podejrzanej charakterystyce, na którą wpływają cechy danego obiektu oraz cechy sieci obiektów z nim powiązanych. Alerty są kategoryzowane i, w zależności od kategorii, przesyłane do grup wyspecjalizowanych analityków, dla których są inicjalnie widoczne jako lista

uporządkowana w zależności od ważności alertów. Narzędzie umożliwia jednoczesną analizę wielu alertów przez różnych analityków. Jednym z dostępnych widoków alertu jest interaktywny diagram powiązań, ułatwiający dalsze prowadzenie analizy.

Dzięki zoptymalizowanym funkcjom administracyjnym, które zostały udostępnione użytkownikom, mogą oni łatwo adaptować narzędzie do zmieniających się wymagań biznesowych. Prace dostosowawcze mogą zostać wykonane przez dział IT organizacji użytkownika, bez potrzeby ingerencji dostawcy. Funkcje, takie jak wyszukiwanie i wizualizacja danych czy interaktywne generowanie sieci powiązań, pozwalają szybko identyfikować obszary wymagające dalszej analizy oraz dostosować narzędzie do zmieniającej się charakterystyki nadużyć lub przestępstw i wymagań wynikających z nowych regulacji prawnych. Łatwo dostępne, dobrze zarządzane i aktualne dane umożliwiają analitykom uzyskanie całościowego obrazu obiektów, relacji, sieci, wzorców, zdarzeń, trendów i anomalii.

Korzyści

- **Wzrost efektywności.** SAS Visual Investigator 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.
- **Możliwość adaptacji 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 i dostosowanie do zmian w strukturze organizacji.

- **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 kustomizacji, 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 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 rezultatów 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 alertów skutkuje szybkim zrozumieniem kontekstu, w którym osadzony jest dany alert. Analitycy mogą wydawać dyspozycje dotyczące alertów, zakładać sprawy w celu wykonania pogłębionej analizy, podejmować na bieżąco decyzje dotyczące obiektów, stanowiących przedmiot zainteresowania.

The screenshot displays the SAS Visual Investigator interface. At the top, there is a navigation bar with 'Home', 'Alerts', and 'Search' options. Below this is a 'Customer Profile' dropdown menu. The main area features a table of alerts with columns for Score, Alert ID, Customer Name, Customer ID, Customer Status, Regulatory Disclosure Indicator, and counts for AML, Sanctions, and Fraud alerts. The alert with ID 47911915 is highlighted in blue.

Score	Alert ID	Customer Name	Customer ID	Customer S...	Regulatory Disclosure Indicator	AML Alerted Customers	Sanctions Alerted Customers	Fraud Alerted Customers
9938	Alert_44329495	CHARLES READE	47045153	Active	false	7	6	8
9880	Alert_18730775	ABEL MEERTENS	431907738	Active	false	2	1	2
9864	Alert_47911915	ANTONIO HENDRICK	2282025133	Active	false	1	2	3
9836	Alert_45085241	GUDVIN SKURDAL	3690482493	Active	false	3	0	0
9830	Alert_16778987	LUKE COBURN	4531620821	Active	false	0	0	3
9804	Alert_48984404	ANGUS FOCKEN	541058273	Active	false	1	1	1
9785	Alert_19761777	CONNOR SEABROOK	608773768	Active	false	3	4	1
9782	Alert_14066391	NOAH OFERRALL	3394042888	Active	false	0	2	1
9740	Alert_41501475	GEPPE HERNÁNDEZ	176548693	Active	false	1	0	2
9728	Alert_16862268	VINCENZO UDINESE	286159675	Active	false	4	7	6

Below the table, there are three panels:

- Scorecard:** Shows a score of 9864 and three categories: Confirmed AML alerts in network, Confirmed sanctions alerts in network, and Confirmed fraud alerts in network.
- Alert Information:** Provides details for Alert ID: Alert_47911915, including object type, ID, score, queue, status (ACTIVE), hold, suppress, productive, and update information.
- Network:** A diagram showing the customer 'ANTON...' connected to several accounts: 128120..., 898982..., 850805..., and 279903... The alert 'Alert_47911915' is also shown in the network.

Rysunek 1. Do określania priorytetu alertów służą kolejki i strategie, dzięki którym mogą być one analizowane w odpowiedniej sekwencji i czasie. Opcje wizualizacji rozszerzają zrozumienie kontekstu poszczególnych alertów.

Zarządzanie alertami i przepływem pracy

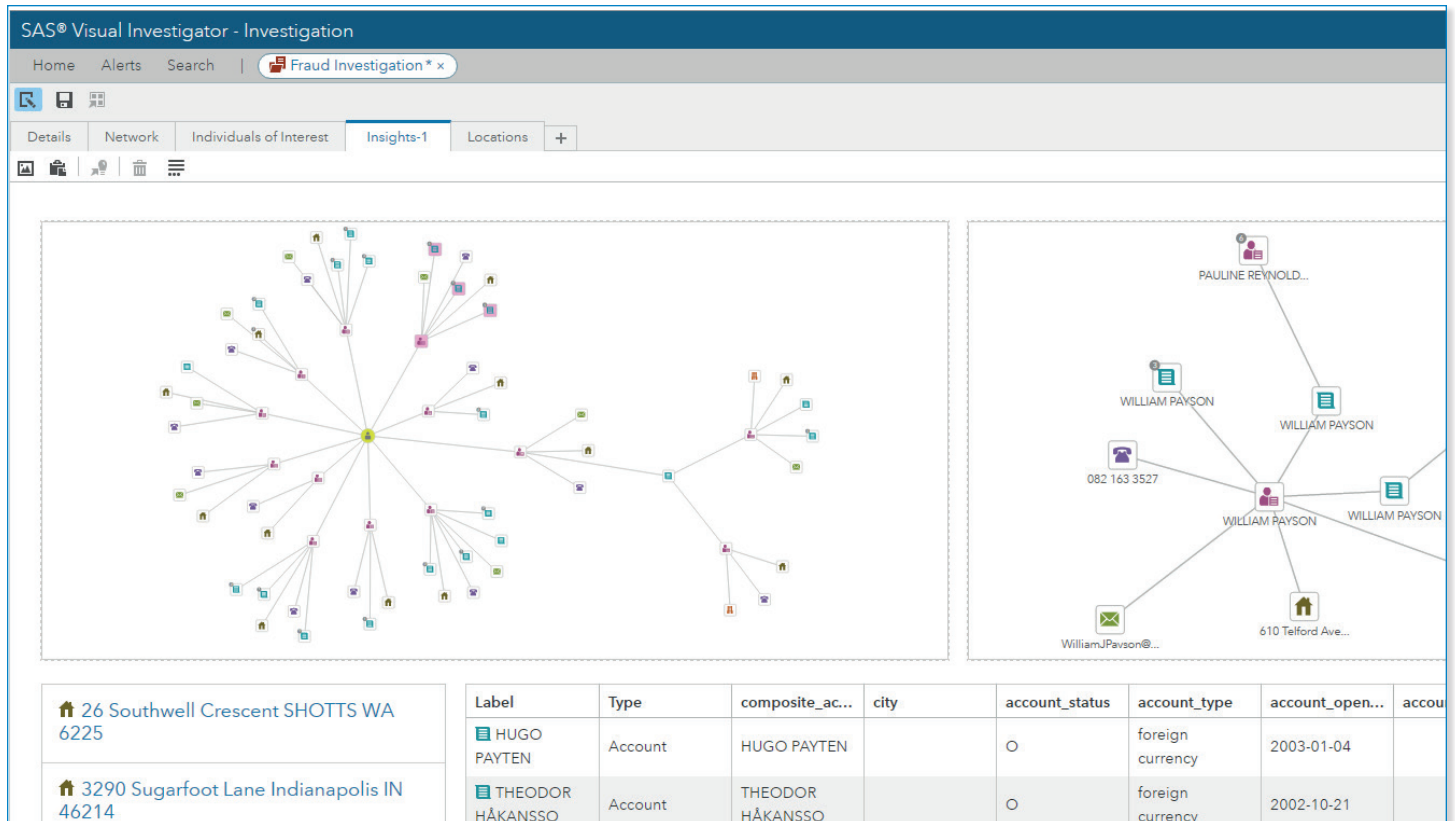
Menedżerowie mogą nadawać priorytet działaniom analitycznym, monitorować produktywność i skuteczność analityków oraz dostosowywać strategię analityczną do nowych, pojawiających się wzorców nadużyć i przestępstw.

Wyszukiwanie

Dostępne jest wyszukiwanie pełnotekstowe oraz wyszukiwanie na mapach. Po uprzednim zaindeksowaniu, przeszukiwane są wszystkie dane, przechowywane zarówno w źródłach zewnętrznych, jak i wewnętrznej bazie danych. Wyszukiwanie pełnotekstowe można zawęzić do wskazanych pól danego typu obiektu poprzez zdefiniowanie formatki wyszukiwania. Wyniki wyszukiwania można filtrować, przeglądać i przysyłać do przestrzeni roboczej w celu dalszej analizy.

Moduł analityczny i moduł dokumentacji wyników

Moduł analityczny to przestrzeń robocza, gdzie analitycy mogą gromadzić dane istotne dla śledztwa i prowadzić bieżącą analizę. Przestrzeń robocza udostępnia funkcjonalność analityczną w interaktywnych widokach analizowanych danych (widok diagramu powiązań, chronologiczny, geoprzestrzenny, tabelaryczny). Moduł dokumentacji wyników analizy służy do rejestracji widoków obszaru roboczego lub ich fragmentów oraz do udokumentowania wyników poszczególnych etapów analizy oraz wyników końcowych. Umożliwia również wprowadzanie notatek.

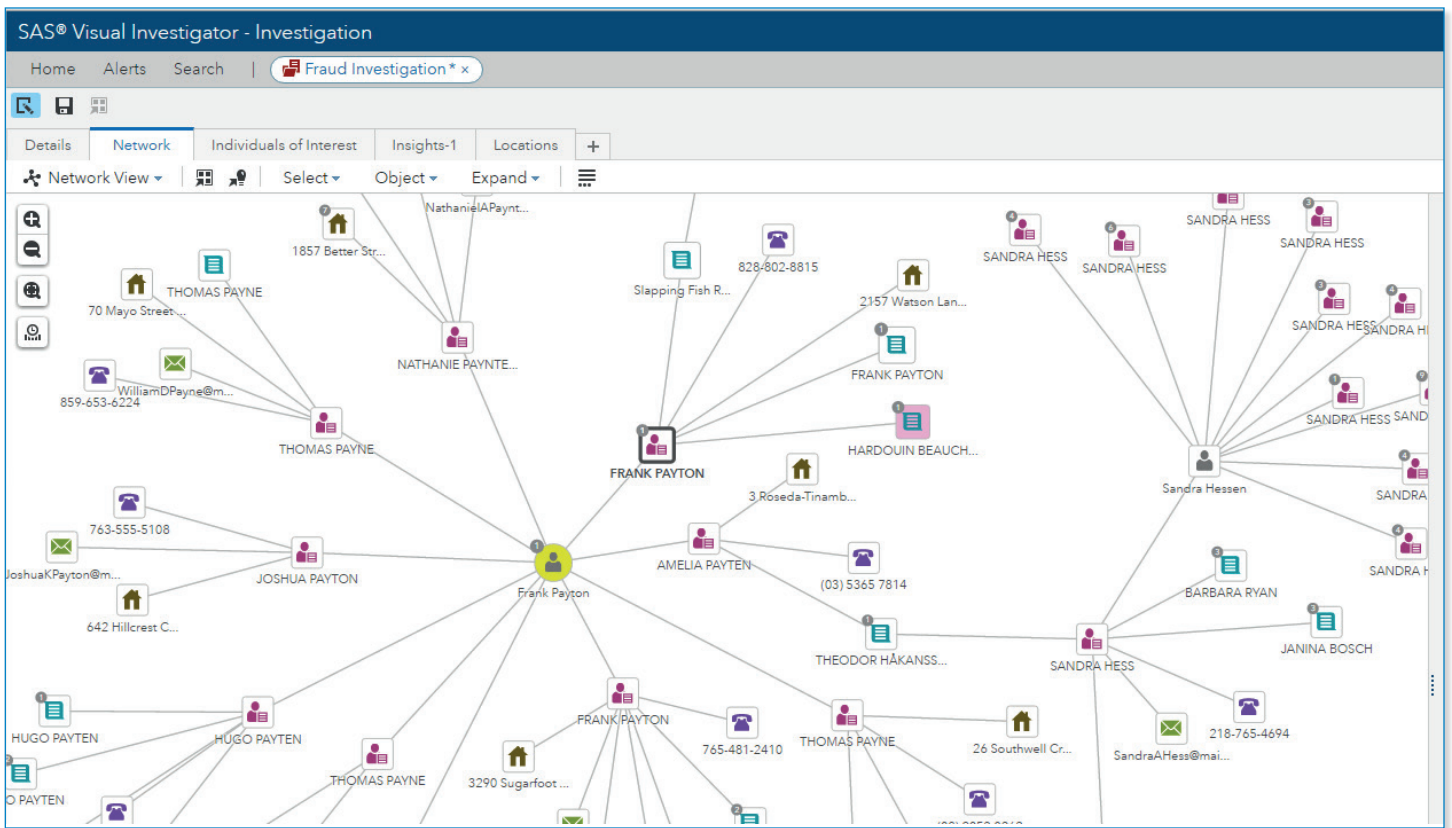


Rysunek 2. Moduł dokumentacji wyników analizy.

Interaktywny diagram powiązań

Pozwala na wizualizację i interaktywną eksplorację sieci powiązań w celu szybkiej identyfikacji związków ukrytych w danych. Udostępnia możliwość stosowania miar centralności sieci społecznej. Obliczenie pośrednictwa, bliskości czy wpływu dla poszczególnych obiektów diagramu skutkuje określeniem roli, którą te obiekty spełniają w sieci, co może wskazać nowy kierunek analizy. Także możliwość obserwacji zmian zachodzących w sieci w badanym okresie oraz różne widoki elementów tworzących sieć ułatwiają identyfikację nieoczywistych i złożonych relacji pomiędzy osobami, miejscami, zdarzeniami i innymi obiektami.

Analitycy mają również do dyspozycji tradycyjną funkcjonalność, taką jak rozwijanie obiektów o powiązania z innymi obiektami wskazanego typu, wyszukiwanie ścieżek, przeszukiwanie diagramu, ukrywanie obiektów, czy zmianę właściwości układu diagramu w celu zwiększenia jego czytelności.



Rysunek 3. Analitycy mogą oglądać dane na diagramie powiązań i korzystać z funkcjonalności, takiej jak rozwijanie wybranych obiektów o połączenia do wskazanych typów obiektów, badanie sieci z wykorzystaniem funkcji analizy sieci społecznej, czy zmiana właściwości układu diagramu.

Przykładowe obszary zastosowań

- Ubezpieczenia - wykrywanie nadużyć w ubezpieczeniach komunikacyjnych, majątkowych i życiowych.
- Instytucje porządku publicznego i ochrony granic - analiza kryminalna, wsparcie działań śledczych, przeciwdziałanie terroryzmowi, analiza PNR, wspomaganie wykrywania przestępstw celnych.
- Bankowość - wspomaganie wykrywania nadużyć w zakresie wniosków kredytowych i nadużyć prowizyjnych.

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

