Business Intelligence Insight

Bottomline

Cyber Fraud & Risk Management

Modułowa i nowoczesna platforma skutecznie zapobiegająca nadużyciom i zabezpieczająca przed wyrafinowanymi atakami cyberprzestępców, zagrożeniami wewnętrznymi, oszustwami płatniczymi i praniem pieniędzy.

Cyber Fraud & Risk Management

Następna linia obrony

Nie ma dnia bez informacji w mediach o kolejnym naruszeniu danych.

Bez względu na to, czy naruszenie polega na tym, że pracownik banku przekierowuje płatności na swój rachunek osobisty, systemy firmowe zostają przejęte przez grupę przestępczą czy informacje o stanie zdrowia pacjentów zostają wykradzione z placówki medycznej, cyberbezpieczeństwo stanowi obecnie najważniejsze wyzwanie dla każdej branży.

Stopień zaawansowania cyberataków stale rośnie, podobnie jak ich wpływ finansowy. Mówiąc wprost, tradycyjne rozwiązania zabezpaieczające, takie jak zapobieganie włamaniom i systemy analiz dzienników, nie wystarczą do obrony przed tymi zagrożeniami.

Zapewnienie większego bezpieczeństwa

Rozwiązania „Cyber Fraud and Risk Management" firmy Bottomline Technologies w zakresie nadużyć finansowych w cyberprzestrzeni i zarządzania ryzykiem umożliwiają firmom aktywne monitorowanie aktywności użytkowników, reagowanie na ostrzeżenia w czasie rzeczywistym oraz eliminowanie zagrożeń inicjowanych przez zewnętrznych hakerów, jak i złośliwych użytkowników wewnętrznych. Połączenie tych możliwości zapewnia silną linię obrony i lepsze bezpieczeństwo.

Ten pierwszy tego typu wieloplatformowy system nadzoru zapewnia dogłębne monitorowanie działań użytkowników końcowych w aplikacjach firmowych w całym przedsiębiorstwie. Specjaliści ds. bezpieczeństwa, inspektorzy ds. nadużyć i audytorzy wewnętrzni mogą wykorzystywać rozwiązania dotyczące nadużyć finansowych w cyberprzestrzeni i zarządzania ryzykiem Cyber Fraud and Risk Management, aby osiągnąć następujące cele o krytycznym znaczeniu:

Śledzenie zachowań w czasie rzeczywistym — Zachowania użytkowników końcowych można śledzić w wielu aplikacjach, kanałach i platformach, niezależnie od tego, czy znajdują się one na komputerze mainframe, czy w chmurze. Następnie, zachowania te są profilowane przez skuteczny system analityczny, który koreluje działania w celu generowania alertów w czasie rzeczywistym na temat podejrzanych zdarzeń. Dzięki możliwości analizy w wielu różnych kanałach, aplikacjach oraz typach płatności (np. call center, e-bankowość, POS, mobile, ATM, centra płatnicze, SWIFT, ISO20022, itp.), CFRM zapewnia przedsiębiorstwom elastyczność i skuteczność tak bardzo potrzebną, by wyprzedzić rozwój wydarzeń we współczesnym, szybko zmieniającym się środowisku zagrożeń.

Dogłębne monitorowanie — System rejestruje szczegółową ścieżkę audytu, umożliwiając pełny wgląd w działania użytkownika końcowego dzięki wizualnemu odtworzeniu każdego ekranu, uderzenia w klawisz i ciągu ekranów w podstawowych aplikacjach biznesowych. Korzystając z funkcji wyszukiwania podobnych do wyszukiwarki Google, inspektorzy mogą dokładne prześledzić działania użytkowników, zapewniając zgodność z przepisami GLBA, HIPAA, PCI i innymi regulacjami, które wymagają ścieżki audytu potwierdzającej dostęp do poufnych danych klientów.

Lepsze zarządzanie sprawami — Podejrzane zdarzenia mogą być badane za pośrednictwem przyjaznego dla użytkownika interfejsu internetowego, umożliwiającego inspektorom lepsze zarządzanie procesem dochodzenia i jego dokumentowanie. Wszystkie informacje dotyczące danego alertu, sprawy lub profilu można skompilować w ramach jednego, połączonego widoku z elastycznymi opcjami bardziej szczegółowego przeglądania danych dla każdego powiązanego podmiotu.
Wdrożenie rozwiązań Cyber Fraud and Risk Management jest proste. Nie wymaga żadnych zmian w infrastrukturze firmy, dodatkowych kosztów, nie oznacza pogorszenia wydajności serwerów lub sieci, ani zmian dla klientów. To bezpieczeństwo „łatwe w obsłudze".

Bezpieczeństwo dla każdej branży

Rozwiązania Cyber Fraud & Risk Management skutecznie ostrzegają zespoły ds. bezpieczeństwa oraz compliance funkcjonujące we wszystkich branżach o wystąpieniu podejrzanych zachowań:

Bankowość

Ponieważ sektor bankowy nieustannie dąży do modelu działalności online, instytucje finansowe muszą nie tylko walczyć z nadużyciami, które są powszechne od wielu lat, ale muszą również chronić swoje portale skierowane do klientów przed atakami typu „man-in-the-middle" czy DDoS. Rozwiązania CFRM dostosowane do potrzeb instytucji finansowych mogą pomóc w wykrywaniu tych nadużyć dzięki rozwiązaniom w zakresie oszustw wewnętrznych (Insider Fraud), oszustw czekowych (Check Fraud) oraz nadużyć i bezpieczeństwa w Internecie (Web Fraud & Security).

Służba zdrowia

Służba zdrowia szybko stała się głównym celem cyberataków. Placówki służby zdrowia przechowują więcej danych osobowych niż jakiekolwiek inne podmioty, a takie dane stanowią kopalnię złota dla potencjalnych złodziei. Ponadto, placówki służby zdrowia podlegają dodatkowej presji w zakresie przestrzegania przepisów rządowych, takich jak ustawy HIPAA i HITECH. Rozwiązanie Healthcare Privacy and Data Security dotyczące ochrony prywatności i bezpieczeństwa danych w służbie zdrowia zapewnia prywatność pacjentów i umożliwia przestrzeganie przepisów, chroniąc wysoce wrażliwe dane w dokumentacjach pacjentów przed zagrożeniami wewnętrznymi i zewnętrznymi.

Przedsiębiorstwa

Firmy działające we wszystkich branżach stoją w obliczu wielu wyzwań związanych z utrzymaniem bezpiecznej sieci. Od zabezpieczenia systemu ERP po ograniczanie ryzyka nadużyć związanych z płatnościami, przedsiębiorstwa potrzebują silnej linii obrony przed zagrożeniami pojawiającymi się w cyberprzestrzeni. Rozwiązania firmy Bottomline: „Accounts Payable Fraud" (oszustwa dotyczące zobowiązań płatniczych), „Insider Fraud" (oszustwa wewnętrzne) oraz „Web Fraud & Security" (nadużycia i bezpieczeństwo w Internecie) umożliwiają firmom stworzenie solidnych postaw bezpieczeństwa, dzięki wykrywaniu podejrzanych zachowań zaraz po ich zainicjowaniu.

BI Insight S.A. www.biinsight.pl

Rozwiązania Cyber Fraud & Risk Management firmy Bottomline:

Przeciwdziałanie praniu pieniędzy. Zwalczanie procederu prania pieniędzy i finansowania terroryzmu dzięki monitorowaniu transakcji finansowych pod kątem podejrzanej działalności oraz list sankcyjnych.

Kontrola i zarządzanie obszarem compliance. Zarządzanie zgodnością z przepisami, takimi jak ustawy Sarbanes-Oxley, HIPAA/HITECH oraz Basel II-III/ Solvency.

Zarządzanie sprawami w przedsiębiorstwie. Automatyzacja i usprawnienie procesów tworzenia alertów i spraw, zarządzania nimi i ich badania.

Oszustwa w aplikacjach mobilnych i internetowych. Wykrywanie i blokowanie podejrzanych transakcji w kanałach internetowych i mobilnych z wykorzystaniem analizy zachowań i transakcji.

Nadużycia płatnicze. Wykrywanie wielu różnych nadużyć płatniczych i zapobieganie im.

Oszustwa wewnętrzne. Wykrywanie, blokowanie i śledzenie podejrzanej działalności użytkowników wewnętrznych w czasie rzeczywistym.

Monitorowanie zachowania użytkownika. Pociąganie upoważnionych użytkowników do odpowiedzialności, sprawdzanie podejrzanych zachowań, reagowanie w czasie rzeczywistym i zapobieganie kolejnym przestępstwom dzięki wieloplatformowemu „systemowi nadzoru".

Transaction Screening for Financial Services

Dynamiczne otoczenie regulacyjne

- Ustawa z dnia 1 marca 2018r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

- 4/5 dyrektywa UE w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu

- Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy (FATF)

- Brytyjska Ustawa o ściganiu przestępstw i przestępczości z 2017 r. (Policing and Crime Act 2017)

- Brytyjska Ustawa o dochodach z przestępczości z 2002 r. (Proceeds of Crime Act 2002)

Skuteczne filtrowanie transakcji w celu identyfikacji i ograniczenia ryzyka związanego z sankcjami

Wykrywanie i zapobieganie przestępstwom finansowym, takim jak finansowanie terroryzmu, pranie pieniędzy i przestępczość zorganizowana, stanowi coraz większe wyzwanie dla instytucji finansowych. Istnieje wymóg prawny w zakresie zapobiegania realizacji transakcji z jakąkolwiek osobą fizyczną lub podmiotem umieszczonym na liście osób i podmiotów podlegających sankcjom. Nieprzestrzeganie tego obowiązku może skutkować wysokimi grzywnami w zależności od skali naruszenia. Licencje bankowe mogą zostać cofnięte, a kierownictwo wyższego szczebla może zostać osobiście pociągnięte do odpowiedzialności. Respektowanie ograniczeń dotyczących listy sankcji może być trudne i kosztowne, biorąc pod uwagę wielkość i złożoność transakcji, struktury własności i rosnący handel transgraniczny. Przy 90-99% przypadków zgodności dających fałszywe alarmy, nie dziwi fakt, że w ostatnich latach wiele instytucji finansowych znacznie zwiększyło swoje zasoby w zakresie compliance.

Korzyści biznesowe

Rozwiązanie „Transaction Screening for Financial Services" firmy Bottomline w zakresie kontroli transakcji w ramach usług finansowych umożliwia instytucjom finansowym sprawdzenie strony inicjującej transakcję, beneficjenta i kontrahenta w przypadku wszystkich transakcji w czasie rzeczywistym w odniesieniu do listy sankcji celem ograniczenia ryzyka i uniknięcia kar administracyjnych. Rozwiązanie przetwarza dużą liczbę transakcji w ciągu kilku milisekund z zastosowaniem najbardziej aktualnych krajowych i międzynarodowych wykazów sankcji. Umożliwia to szybsze i bardziej skuteczne wykrywanie, badanie i eliminowanie potencjalnych naruszeń. Ponadto, upraszcza zarządzanie wieloma listami, eliminując nakłady pracy konieczne do obsługi dublujących się alertów i fałszywych alarmów.

Rozwiązanie Transaction Screening for Financial Services, w pełni zintegrowane z innymi rozwiązaniami CFRM w zakresie compliance oraz płatności:

- stanowi zintegrowaną platformę kontroli transakcji, wykrywania zdublowanych informacji i eliminowania potencjalnych naruszeń,
- zapewnia zgodność z krajowymi i międzynarodowymi listami sankcji, zapobiegając naruszeniom i wynikającym z nich karom,
- upraszcza proces zarządzania wieloma listami sankcji i ograniczania liczby fałszywych alarmów,
- zapewnia skuteczną automatyzację, aby zminimalizować nakłady pracy manualnej i wspiera skalowalność,
- jest łatwe w obsłudze, można je szybko wdrożyć, jest tanie w użytkowaniu i zapewnia szybki zwrot z inwestycji.

Możliwości produktu

Kontrola w czasie rzeczywistym transakcji, dla których czas jest istotny

Rozwiązanie „Transaction Screening for Financial Services" firmy Bottomline umożliwia instytucjom filtrowanie transakcji w czasie rzeczywistym i wdrażanie środków zaradczych przed przetworzeniem i realizacją płatności.

Monitorowanie wszystkich zleceń płatniczych

Rozwiązanie oferuje instytucjom finansowym pojedynczą platformę do kontroli wielu rodzajów płatności, takich jak ISO20022, SWIFT, SEPA, SIC4, Bacs, Cheques i Faster Payments. Dzięki temu instytucje mogą zachować konkurencyjność, oferując najszerszą gamę rodzajów transakcji.

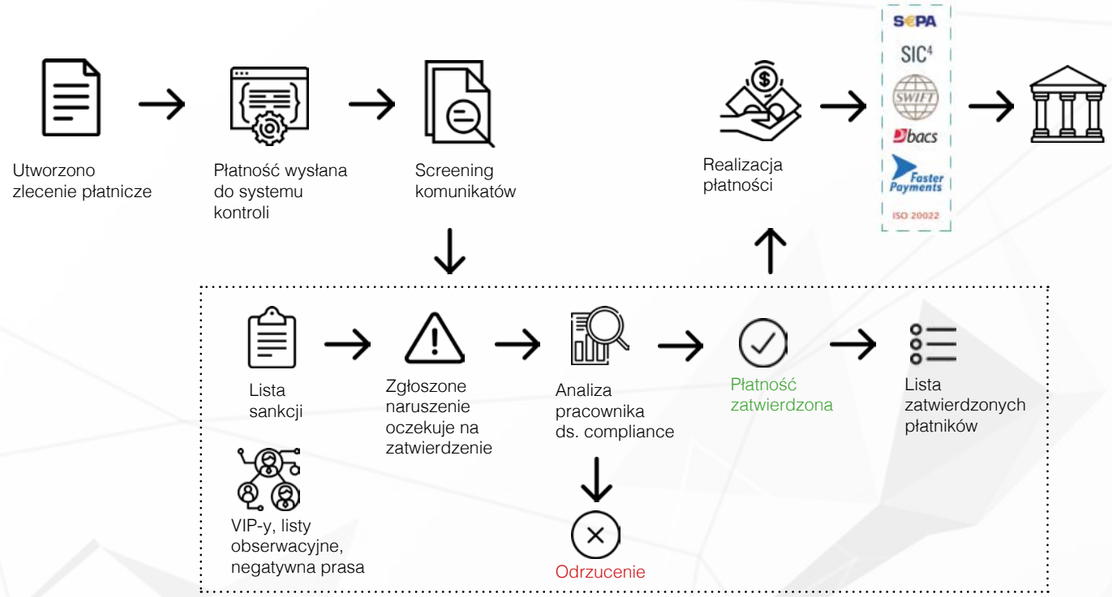
Lista sankcji i zasięg jurysdykcji

Instytucje muszą respektować lokalne i międzynarodowe listy sankcji. Rozwiązanie zapewnia obsługę najważniejszych list sankcji, takich jak wykazy UE, OFSI, ONZ, OFAC, a także kluczowych krajów, w tym Szwajcarii, Chin, Kanady, Australii, Singapuru, Japonii i wielu innych.

Szybka i aktualna ochrona

Rozwiązanie firmy Bottomline w zakresie monitorowania transakcji umożliwia sprawdzanie pojedynczych nazw lub plików wsadowych. Ilekroć lista sankcji zostaje zaktualizowana, rozwiązanie automatycznie dodaje każdy nowy podmiot (osobę fizyczną, firmę lub kraj) do bazy danych sankcji, zapewniając lepszą ochronę i zdolność reagowania na nowe zagrożenia i ryzyka.

Schemat filtrowania transakcji



Rozwiązanie Transaction Screening for Financial Services oferuje kompleksową ochronę przed naruszeniami sankcji poprzez screening wszystkich transakcji w czasie rzeczywistym. Ogranicza ryzyko naruszenia sankcji i upraszcza eliminowanie nadużyć.

Cyber Fraud & Risk Management: Secure Payments

Ochrona płatności w aplikacjach, kanałach i dla różnych typów płatności

Cyber Fraud & Risk Management umożliwia firmom i instytucjom finansowym ograniczanie ryzyka, zapobieganie nadużyciom oraz spełnianie wymogów zgodności z przepisami za pośrednictwem elastycznej platformy, która może być rozbudowywana, i która zapewnia doskonałą ochronę przed nadużyciami.

CFRM to innowacyjny, kompleksowy pakiet rozwiązań dla firm w zakresie zarządzania nadużyciami, który obejmuje wszechstronne metody przechwytywania danych, wielokanałową analizę oraz alerty w czasie rzeczywistym. Dzięki temu, firmy mogą wykrywać i zapobiegać oszustwom wewnętrznym i zewnętrznym w czasie rzeczywistym oraz lepiej spełniać wymogi w zakresie zgodności z przepisami dotyczącymi wykrywania nadużyć.

Platforma CFRM firmy Bottomline jest elastyczna i może być w znacznym stopniu rozbudowywana dzięki modelowi szybkiej aktywacji, co zapewnia firmom następujące korzyści:

- lepszy wgląd i kontrolę,
- szybsze dochodzenia w sprawie nadużyć,
- szybsze podejmowanie decyzji.

Obejmuje inteligentne uczenie maszynowe, wykrywanie oparte na regułach oraz profilowanie behawioralne w celu wykrywania anomalii i monitorowania aktywności użytkowników końcowych, a także transakcji w aplikacjach i kanałach w całej instytucji. System śledzi całą aktywność użytkownika końcowego w wielu środowiskach, m.in. w komputerach typu mainframe, w sieci, w rozwiązaniach mobilnych, a także produktach wewnętrznych i zewnętrznych.

Rozwiązania CFRM

Bezpieczne płatności

- Aplikacje
- Kanały
- Typy płatności
- PSD2 RTS

Przestrzeganie prawa

- Przeciwdziałanie praniu pieniędzy
- Kontrola pod kątem sankcji
- „Poznaj swojego klienta” / CDD
- Zarządzanie sprawami w przedsiębiorstwie

Analiza zachowania użytkownika

- Wykrywanie zagrożeń wewnętrznych
- Wykrywanie intruzów

Najważniejsze cechy platformy CFRM

Blokowanie podejrzanych transakcji w czasie rzeczywistym

Wraz z rozwojem systemów rozliczenowych i przelewów bankowych, monitorowanie w czasie rzeczywistym, generowanie ostrzeżeń i blokowanie transakcji stanowią niezbędne komponenty skutecznego rozwiązania. W przypadku wykrycia podejrzanych transakcji czy okoliczności, transakcje mogą zostać automatycznie wstrzymane do chwili ich wyraźnego zatwierdzenia przez upoważnionego analityka lub specjalistę ds. płatności. Ponadto, jeśli podejrzana działalność nie jest powiązana z określoną transakcją, ale występuje podczas sesji online lub mobilnej, może zostać uruchomione bardziej zaawansowane uwierzytelnianie, w ramach którego użytkownik musi udzielić odpowiedzi zanim będzie mógł zrealizować ryzykowne płatności.
System CFRM może również wysyłać powiadomienia do innych systemów uwierzytelniających, aby uruchomić dodatkowe uwierzytelnianie lub hasła jednorazowe.

Analiza nadużyć z inteligentnym uczeniem maszynowym

Dzięki połączeniu nadzorowanego i nienadzorowanego uczenia maszynowego z wykrywaniem opartym na regułach i profilowaniem behawioralnym, CFRM stale ulepsza swój system analityczny i uwzględnia adaptacyjne informacje w czasie rzeczywistym w ramach wykrywania nadużyć.
Wykorzystując dużą wiedzę firmy Bottomline w zakresie płatności i nadużyć, system analityczny CFRM stosuje inteligentne uczenie maszynowe, aby firmy mogły odpowiednio wcześnie reagować na zmieniające się i złożone systemy nadużyć, ograniczyć liczbę fałszywych alarmów i chronić swoje płatności. Jest to połączone z wykrywaniem opartym na regułach i profilowaniem behawioralnym w celu szybkiego zabezpieczenia się przed znanymi nieuczciwymi zachowaniami oraz atakami na transakcje płatnicze.

Wielokanałowe śledzenie zachowań

Zachowanie klientów, kont, pracowników i innych podmiotów jest śledzone i profilowane przez system analityczny, który koreluje działania między różnymi kanałami, takimi jak bankowość elektroniczna, rozwiązania mobilne, Automatyczny System Rozrachunkowy (ACH), przelewy, czeki, call center i inne, a także generuje w czasie rzeczywistym alerty dotyczące podejrzanych lub nietypowych zdarzeń.

Dochodzenia i zarządzanie sprawami

Podejrzane zdarzenia mogą być badane w Investigation Center, tj. skutecznym, internetowym, badawczym interfejsie użytkownika, umożliwiającym analitykom zarządzanie procesem dochodzeniowym i jego dokumentowanie, wyświetlanie wszystkich informacji dotyczących alertów, spraw lub profili w ramach jednego, skonsolidowanego widoku z elastycznymi opcjami bardziej szczegółowego przeglądania danych dla każdego powiązanego podmiotu.

Wizualne odtworzenie informacji

System, w sposób nieinwazyjny rejestruje szczegółową ścieżkę audytu, umożliwiając pełny wgląd w działania użytkownika końcowego dzięki wizualnemu odtworzeniu każdego ekranu, modyfikacji użytkownika i ciągu ekranów w podstawowych aplikacjach biznesowych. System obejmuje również funkcję wyszukiwania podobną do wyszukiwarki Google w celu przeszukiwania treści każdego ekranu i sesji użytkownika, umożliwiając analitykom natychmiastowe uzyskanie odpowiedzi na pytania, takie jak: który użytkownik uzyskał dostęp do określonego numeru konta w danym czasie, a następnie odtworzenie dokładnych działań użytkownika ekran po ekranie. Funkcja ta umożliwia przestrzeganie przepisów GLBA, SOX, PCI i innych, które wymagają szczegółowej ścieżki audytu potwierdzającej dostęp do poufnych danych klientów.

Moduł bezpiecznych płatności Secure Payments

Rozwiązanie Secure Payments w zakresie bezpiecznych płatności umożliwia ochronę płatności w różnych aplikacjach, kanałach i dla różnych typów płatności.
Dzięki systemowi Secure Payments instytucje finansowe mogą:

- wykrywać nieuczciwe płatności w czasie rzeczywistym,
- blokować płatności przed ich realizacją,
- zabezpieczać sesje online i w aplikacjach mobilnych oraz aktywność na koncie,
- obsługiwać wszystkie typy płatności i kanały w ramach jednego rozwiązania dla przedsiębiorstw,
- spełniać wymagania dotyczące zgodności z przepisami.

Dzięki gotowej bibliotece wstępnie zbudowanych integracji i obsłudze różnorodnych formatów płatności, rozwiązanie „Secure Payments" zapewnia ciągłą elastyczność w zakresie kompleksowych analiz behawioralnych, ostrzegania w czasie rzeczywistym i blokowania transakcji, umożliwiając firmom ograniczanie ryzyka, zapobieganie nadużyciom i realizację wymogów w zakresie zgodności z obowiązującymi przepisami.

APLIKACJE

Platformy bankowe
Centra płatnicze
Biura obsługi
TMS
ERP

KANAŁY

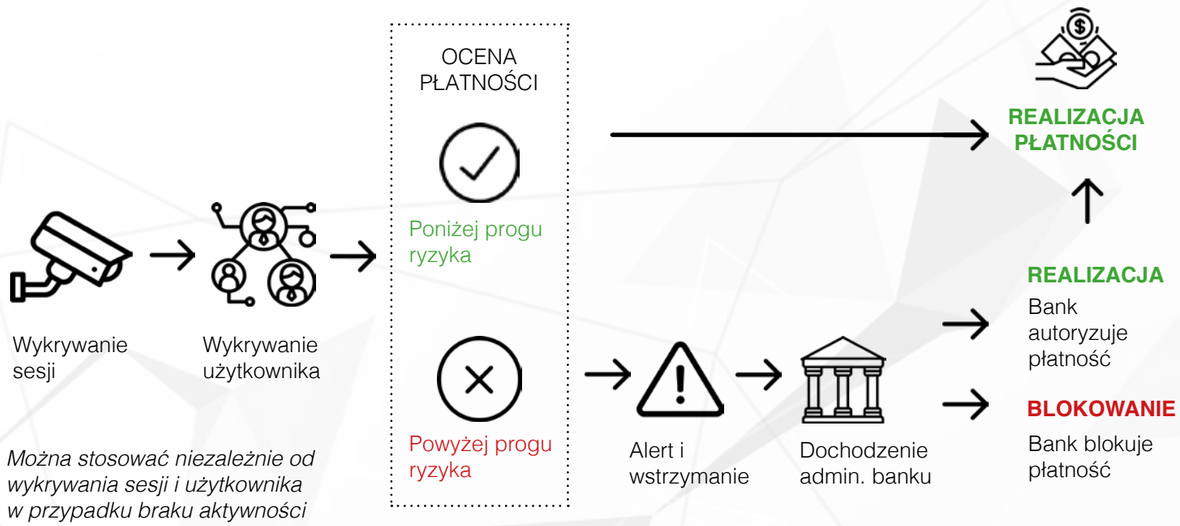
Punkt sprzedaży
Oddział
Internet
Centrum telefoniczne
Portale
Host2Host
Rozwiązania mobile
Bankomaty
IVR
Przelewy

TYPY PŁATNOŚCI

CH
BACS
Bill Pay
Czek
ISO 20022
ISO 8583
SEPA
SIC4
SWIFT

Rozwiązanie Secure Payments CFRM skutecznie identyfikuje ataki w ramach niektórych najbardziej zaawansowanych systemów nadużyć, takich jak wysyłanie fałszywych biznesowych wiadomości e-mail (Business Email Compromise, BEC) oraz ataki wielokanałowe i pozwala znacznie je ograniczyć.

Secure Payments - proces od zainicjowania sesji do rozliczenia



Można stosować niezależnie od wykrywania sesji i użytkownika w przypadku braku aktywności online.

Cyber Fraud & Risk Management: Payement Fraud for SWIFT

Rozwiązanie w czasie rzeczywistym dla zagrożeń w czasie rzeczywistym

Nadużycia, stały temat w mediach, stają się coraz szybsze i bardziej wyrafinowane, występują w bankach i instytucjach finansowych, wywierając istotny wpływ zarówno na finanse, jak i na reputację. Do tej pory reakcja ze strony społeczności biznesowej bywała różna, ale obecnie sieć się zacieśnia. Organizacje, instytucje i organy regulacyjne aktywizują sektor finansowy, by stawił czoła bardzo realnemu zagrożeniu związanemu z nadużyciami, a dostawcy technologii przodują w inwestowaniu w bezpieczeństwo i rozwiązania w zakresie wykrywania oszustw, aby chronić finanse swoich klientów.

Jednym z głośnych incydentów była sprawa SWIFT, w której hakerzy uzyskali dostęp do globalnej sieci płatniczej SWIFT w celu realizacji nieuczciwych transakcji. Interfejs SWIFT wykorzystywany przez instytucje finansowe został zhakowany, a hakerzy wykorzystywali luki w systemach inicjowania przelewów bankowych przed wysyłaniem komunikatów w sieci SWIFT.

W odpowiedzi SWIFT wydało nowy zestaw standardów bezpieczeństwa, które zapewnią większe bezpieczeństwo systemu finansowego. Jest to tzw. „SWIFT Customer Security Program" (CSP). W ramach tego programu SWIFT wprowadziło obligatoryjne i zalecane środki kontroli, które będą stanowić podstawę bezpieczeństwa dla całej społeczności SWIFT.

Monitoring, wykrywanie i reagowanie w czasie rzeczywistym

Jako światowy lider od prawie 30 lat w branży przetwarzania płatności biznesowych, firma Bottomline Technologies jest w stanie oferować rozwiązania dla banków i instytucji finansowych, które umożliwiają nie tylko zapewnienie zgodności z nowymi standardami SWIFT, ale także realizację długoterminowej strategii w zakresie oszustw, dzięki lepszej ochronie i możliwościom wykrywania nadużyć.

Payment Fraud for SWIFT Interfaces dotyczące nadużyć płatniczych w systemie SWIFT, element Financial Messaging Risk and Compliance to innowacyjne rozwiązanie obejmujące kompleksowe przechwytywanie danych, monitorowanie zachowań, analizy bezpieczeństwa sieci i cenzurowanie transakcji w czasie rzeczywistym. Wyjątkowa funkcja monitorowania użytkowników i realizacji płatności w systemie SWIFT jednocześnie umożliwia szybkie wykrywanie niestandardowych działań. Dzięki połączeniu dynamicznego profilowania, scoringu i prognostycznych analiz ryzyka, wysyłamy ostrzeżenia i zapobiegamy realizacji transakcji przed wystąpieniem strat.

Krytyczne możliwości w ramach proaktywnej strategii ochrony przed nadużyciami

- Identyfikacja zagrożeń w czasie rzeczywistym, dzięki rejestrowaniu całego ruchu w sieci, w ramach analizy działań użytkowników i rejestracji płatności SWIFT MT 1xx oraz 2xx, a także wysyłanie alertów w reakcji na podejrzane zachowania lub nawet blokowanie transakcji.

- Wykrywanie wielu zagrożeń w ramach monitorowania aktywności w zakresie logowania, danych transakcji i zachowań użytkowników. Dzięki identyfikacji podejrzanych lub nietypowych działań, to rozwiązanie może wykrywać kolejne, pojawiające się zagrożenia.

- Skrócenie czasu dochodzenia dzięki rejestracji całej ścieżki audytu sesji użytkownika i umożliwieniu analitykom wyszukiwania danych w wyszukiwarce działającej podobnie jak Google. We współpracy z narzędziem GTExchange firmy Bottomline, rozwiązanie to umożliwia również natychmiastowe odtworzenie interakcji użytkownika, zapewniając analitykom szybki i kompleksowy wgląd.

- Zapewnienie efektywności operacyjnej dzięki Investigation Center, które obejmuje pulpity nawigacyjne, wstępnie zdefiniowane raporty i możliwość tworzenia raportów ad-hoc, a także umożliwia zarządzanie sprawami w przypadku alertów wymagających dalszej analizy.

- Zapewnienie zgodności z programem SWIFT Customer Security Program, szczególnie w zakresie środka kontroli 6.4 w ramach CSP dotyczącego rejestrowania i monitorowania zachowań użytkowników oraz środka kontroli 2.9A w ramach CSP dotyczącego środków kontroli transakcji biznesowych.

Podczas gdy standardowy raport na koniec dnia dotyczący incydentów może wskazywać na nadużycia, które już zostały dokonane i skutkować podjęciem pilnych działań zaradczych, rozwiązanie Payment Fraud for SWIFT oferuje skuteczne proaktywne monitorowanie aktywności, alerty i blokowanie transakcji, dzięki czemu Państwa instytucja finansowa będzie znacznie lepiej chroniona.
Dzięki łatwej integracji z Państwa obecnym interfejsem SWIFT i systemem wysyłania komunikatów finansowych, rozwiązanie umożliwia reagowanie na coraz bardziej wyrafinowane próby nadużyć, chroniąc i wzmacniając krytyczne procesy płatnicze Państwa firmy.

Dzięki połączeniu dynamicznego profilowania, scoringu i prognostycznych analiz ryzyka, wysyłamy ostrzeżenia i zapobiegamy realizacji transakcji przed wystąpieniem strat.

Nieuczciwe zmowy pracowników
narażają firmy na znaczne ryzyko

Nadużycia stanowią coraz poważniejsze zagrożenie dla przedsiębiorstw na całym świecie, zmniejszając integralność i bezpieczeństwo danych, zaufanie konsumentów i uczciwość marki.

Według Stowarzyszenia Biegłych ds. Przestępstw i Nadużyć Gospodarczych (ACFE) około połowa przypadków oszustw wewnętrznych dotyczy wielu sprawców, którzy zawarli zmowę, aby popełnić oszustwo, a faktyczne straty z tytułu nadużyć znacznie rosną, gdy w proceder zaangażowanych jest wielu oszustów. Jednym z powodów dla których straty są większe jest fakt, że gdy w nieuczciwy proceder zaangażowanych jest kilka osób istnieje więcej okazji do popełnienia oszustwa a także łatwiej jest ominąć środki kontroli mające na celu przeciwdziałanie nadużyciom i dłużej ukrywać nieuczciwe praktyki.

Firmy inwestują we wdrażanie mechanizmów kontrolnych, takich jak wymóg by transakcje powyżej określonych progów były zatwierdzane przez drugiego pracownika i uniemożliwienie tej samej osobie reaktywacji konta oraz przelania środków. Jednakże koordynując swoje działania pracownicy mogą współpracować w celu obejścia tych mechanizmów.

Oto pięć metod, które mogą pomóc w identyfikacji nadużyć i zmowy pracowników.

1. Monitorowanie wszystkich działań użytkowników

Aby wykryć potencjalne oszustwa wewnętrzne, firmy muszą monitorować i rozpoznawać nietypowe zachowania pracowników w czasie rzeczywistym. Podejrzane zachowanie można wykryć za pomocą systemów monitorowania, które śledzą wszelkie nietypowe zmiany dokonywane przez pracowników w systemach informatycznych. Niestety nadużycie może zostać wykryte dopiero po poniesieniu szkody.

Lepszym sposobem zapobiegania nadużyciom jest monitorowanie wyszukiwań danych w celu wykrycia, **czy pracownicy planują oszustwo**. Na przykład, jeśli pracownik banku próbuje „wyczyścić" uśpione konto, pierwszym krokiem jest próba wyszukania nieaktywnych kont z wysokimi saldami. Monitorując wyszukiwania użytkowników inspektorzy mogą ustalić, czy pracownicy szukają potencjalnych celów, zanim uśpione konto zostanie ponownie aktywowane lub środki zostaną przelane.

2. Porównanie zachowania danej osoby w stosunku do odpowiedniej grupy porównawczej

Pracownicy próbujący dopuścić się nadużycia są zwykle zaznajomieni z wprowadzonymi środkami kontroli i mogą próbować je obejść. Na przykład, pracownicy banku znający próg dla transakcji, którego przekroczenie skutkuje wysłaniem alertu dotyczącego potencjalnie podejrzanej działalności, mogą wypłacać mniejsze kwoty w dłuższym okresie czasu aby uniknąć wykrycia takiego procederu.

Narzędzie analityczne, które wykorzystuje inteligentne uczenie maszynowe, by szybko identyfikować normalne zachowania poszczególnych osób i potrafi porównać je z normalnym zachowaniem innych pracowników pełniących podobne funkcje w tym samym dziale lub w innych działach może skuteczniej wykrywać wszelkie próby nadużyć. Na przykład, pracownik back office próbuje wyszukać konta nieaktywne przez określony czas (tuż przed ich automatycznym oznaczeniem jako „uśpione"). Takie zachowanie może zostać uznane za podejrzane w porównaniu z typowymi wyszukiwaniami przeprowadzanymi przez pracowników na podobnych stanowiskach.

3. Korelowanie działań w różnych kanałach i systemach w całej firmie

Firmy zazwyczaj przydzielają różne funkcje różnym pracownikom tak, by ograniczyć możliwości popełniania nadużycia. Na przykład, w bankach zwykle tylko pracownicy back office mogą reaktywować nieaktywne konto, ale nie mogą przelewać środków. Z kolei kasjerzy mogą przelewać środki, ale nie mogą zmieniać statusu kont. Zmowa między pracownikiem back office i kasjerem umożliwiłaby im „czyszczenie" uśpionych kont. W celu wykrywania takich nadużyć, system przeciwdziałania nadużyciom finansowym musi monitorować i korelować całą działalność w back office, systemach transakcyjnych, oddziałach, kanałach elektronicznych i innych systemach.

4. Wykrywanie podobieństw w działaniach pracowników

Sytuacja, gdy dwóch pracowników realizuje nadmierne działania na tych samych kontach klientów może wyraźnie wskazywać na zmowę, szczególnie jeśli są oni jedynymi pracownikami, którzy mają dostęp do tych kont. Na przykład, jeśli pracownik back office i kasjer stale przeglądają te same konta, może to oznaczać, że współpracują w celu przejęcia tych kont. Jednym ze sposobów identyfikowania i zapobiegania nadużyciom tego typu jest powiadamianie analityków ds. nadużyć o wszelkich sytuacjach, gdy kilku pracowników realizuje podejrzane transakcje na tych samych kontach, za pomocą systemowego rozwiązania do wykrywania takich praktyk. Dzięki temu narzędziu, w połączeniu z inteligentnym uczeniem maszynowym i profilowaniem behawioralnym możliwe jest ustalanie w sposób kompleksowy, podobieństw dotyczących działań pracowników.

5. Stosowanie narzędzi wizualnych w celu ustalenia powiązań między pracownikami, kontami klientów i podejrzanymi działaniami

Analizy to za mało. Ponieważ zmowa dotyczy kilku pracowników i podejrzanych zdarzeń, wizualna analiza powiązań może być bardzo skuteczna. Może pomóc ujawnić skomplikowane scenariusze, które trudno jest wykryć za pomocą tradycyjnych metod prezentacji, takich jak tabele i wykresy. Stosowanie narzędzi, które umożliwiają grupowanie zdarzeń i identyfikację tendencji z użyciem wizualizacji, przyspiesza dochodzenie w sprawie nadużycia i rozstrzygnięcie danej sprawy.

Monitorując i analizując wszystkie działania pracowników i szukając oznak ich współpracy, firmy mogą wykrywać podejrzaną działalność, zanim stracą pieniądze lub ich reputacja zostanie naruszona. Istnieją inne korzyści wynikające z wdrożenia skutecznego systemu śledzenia. Prawdopodobieństwo, że pracownicy dopuszczą się nadużycia jest mniejsze, gdy wiedzą oni, że istnieje większe prawdopodobieństwo, że zostaną przyłapani. Co więcej, jeśli nadużycie zostanie wykryte, gdy straty są jeszcze niewielkie można uniknąć większych problemów.

W celu ograniczenia ryzyka oszustw wewnętrznych rekomendowane jest wdrożenie Insider Fraud - jednego z modułów CFRM.

BI Insight S.A. www.biinsight.pl

Insider Fraud
fraudy wewnętrzne

Wprowadzenie do modułu Insider Fraud

System wykrywania oszustw wewnętrznych Insider Fraud identyfikuje i śledzi wszelką podejrzaną aktywność pracowników poprzez monitorowanie wszystkich działań podejmowanych przez użytkownika i weryfikowanie ich w odniesieniu do zestawu wcześniej zdefiniowanych reguł. Kiedy działanie lub wzorzec działań pracownika zostaną określone na podstawie reguł jako potencjalnie nieuczciwe, generowany jest alert dla analityków w celu analizy alertu i uruchomienia dochodzenia. Takie reguły mogą uwzględniać wiele różnych czynników i punktów dotyczących danych, ponieważ system monitoruje działania w czasie rzeczywistym, jak również dane historyczne, może on wykrywać wiele różnych systemów nadużyć, jednocześnie pozwalając zmniejszyć liczbę fałszywych alarmów.

Ponieważ system monitoruje zachowania pracowników, dla wszystkich użytkowników tworzone są profile, co pozwala ustalić, czy działania pracowników są potencjalnie podejrzane, czy też stanowią część ich normalnej pracy. Na przykład, jeśli jakiś pracownik został wyznaczony do pracy tylko z kontami VIP, nie chcielibyśmy, aby alerty były wysyłane za każdym razem, gdy taki pracownik wejdzie na konto VIP. Zamiast tego, system „nauczy się", że jest to fałszywy alarm i doda go do profilu użytkownika. Profilowanie może również służyć do wykrywania podejrzanego zachowania, np. jeśli jakiś użytkownik zwykle przegląda kilka rekordów dziennie, a następnie zaczyna przeglądać wiele innych rekordów, może to zostać oznaczone jako podejrzana aktywność, skierowana do zweryfikowania przez analityka.

Moduł Insider Fraud obejmuje gotowy zestaw ponad 120 sprawdzonych reguł opracowanych na podstawie wieloletniego doświadczenia w zakresie wykrywania oszustw wewnętrznych, a także informacji zwrotnych od klientów. Konkretne reguły wdrażane przez każdego klienta zostaną dostosowane do każdej firmy z osobna w zależności od jej wielkości i struktury. Ponadto stale udostępniane są nowe reguły, z których firmy mogą korzystać, ponieważ taktyki stosowane przez cyberprzestępców ciągle się zmieniają. Użytkownicy systemu mogą dodawać nowe reguły w prosty, nieskomplikowany sposób.

Wszystkie alerty generowane przez system są wyświetlane w Investigation Center, gdzie mogą być śledzone i zarządzane np. przez analityków lub koordynatorów ds. compliance. Alerty zawierają szczegółowe informacje na temat konkretnej sytuacji, która wywołała alert. Alert obejmuje również dodatkowe informacje, np. wcześniejsze powiązane alerty i inne dane historyczne, które mogą być przydatne dla osoby badającej sprawę. Taka kombinacja informacji zapewnia wszystkie istotne dane wymagane do rozpoczęcia dochodzenia w sprawie nadużycia.

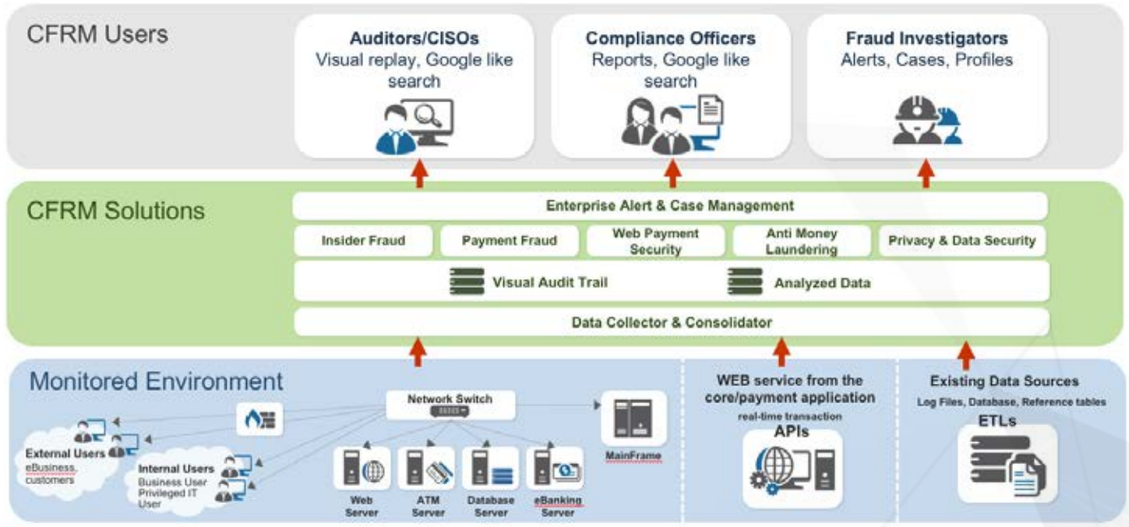
120

sprawdzonych reguł

Przechwytywanie danych

Tradycyjne systemy zarządzania nadużyciami finansowymi opierają się zazwyczaj na danych już istniejących w firmie, takich jak pliki dziennika i bazy danych, dlatego analiza w ich ramach jest ograniczona ze względu na dostarczone dane oraz czas, w którym te dane są dostarczane. Wykrywanie różnego rodzaju oszustw wewnętrznych i zewnętrznych może odbywać się o wiele skuteczniej i z niższymi wskaźnikami fałszywych alertów, jeśli informacje o zapytaniach użytkowników są uwzględniane w analizowanych danych. Na przykład, można wykryć przygotowania do kradzieży z nieaktywnych kont i zapobiec temu zdarzeniu odpowiednio wcześnie, śledząc nadmierną liczbę zapytań dotyczących uśpionych kont uruchomionych przez danego pracownika. Ponadto, pliki dziennika zwykle nie zawierają informacji o aktywności uprzywilejowanych użytkowników IT. CFRM przechwytuje dane dotyczące aktywności bezpośrednio z sieci firmowej, zapewniając dogłębny wgląd w aktywność użytkownika. Dane przechwycone z sieci są uzupełniane danymi zebranymi z tradycyjnych źródeł, takich jak pliki dzienników i bazy danych.

Architektura Rozwiązania CFRM



Schemat nr 1

Podsłuchiwanie sieci (sniffing)

CFRM rejestruje aktywność użytkowników końcowych za pomocą serwerów firmowych i komunikacji między serwerami (np. komunikatów SWIFT) poprzez nieinwazyjne podsłuchiwanie ruchu w sieci (tzw. sniffing). Podsłuchiwanie polega na podłączeniu czujnika CFRM Sensor do głównych przełączników sieci firmowej przez porty zdublowane lub urządzenia TAP.

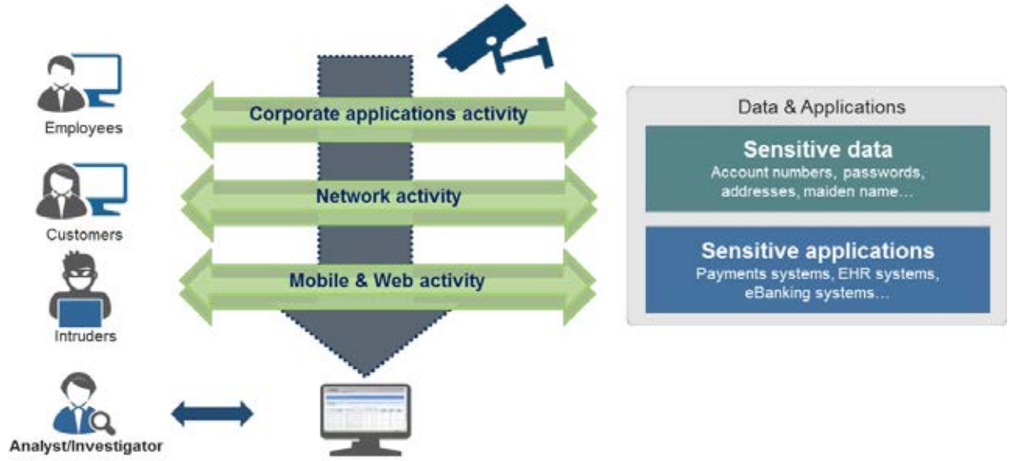
Zapisane sesje użytkownika i komunikaty międzyserwerowe są analizowane i rekonstruowane w czasie rzeczywistym, umożliwiając wizualne odtworzenie aktywności użytkownika ekran po ekranie.
CFRM monitoruje aktywność na wielu platformach:

- Protokół ekranu IBM Mainframe — 3270 na SNA, TCP/IP (TN3270) i Enterprise Extender
- Protokół ekranu IBM iSeries — 5250 na SNA, TCP/IP (TN5250), i MPTN
- Komunikaty klient/serwer i międzyserwerowe — TCP/IP, MQ Series, MSMQ, IBM mainframe SNA LU0 i LU6.2, SMB
- HTTP, HTTPS, Usługi Internetowe
- Telnet/ VT100 i inne typy VT, SSH
- Formularze Oracle
- FTP
- Dostęp do bazy danych: Oracle (SQLNET), DB/2 (DRDA) i MS SQL (TDS)
- SWIFT, FIX i ISO8583. Monitorowanie innych protokołów aplikacji można łatwo skonfigurować.
- Citrix/RDP

System może monitorować różne typy użytkowników końcowych:

- Użytkownicy biznesowi
- Uprzywilejowani użytkownicy IT
- Użytkownik zewnętrzny uzyskujący dostęp do systemów firmowych za pośrednictwem Internetu (np. klienci korzystający z bankowości elektronicznej).

Jak widać na schemacie nr 2, system CFRM monitoruje dane przesyłane między użytkownikami i aplikacjami w nieinwazyjny sposób. Można w nim tworzyć alerty i dochodzenia, aby zapobiegać nadużyciom. Posiada również łatwy w obsłudze i przyjazny interfejs użytkownika, w którym pracownicy mogą np. definiować parametry dla reguł.



Schemat nr 2

Wykorzystując nieinwazyjną technikę monitorowania sieci system CFRM nie wymaga żadnych zmian w infrastrukturze firmy, nie generuje żadnego ryzyka i nie skutkuje obniżeniem wydajności serwerów, sieci oraz aplikacji klienckich.

Zbieranie danych z plików dzienników i innych źródeł

System CFRM może przechwytywać dane z plików tekstowych i binarnych, plików dzienników, tabel bazy danych, plików XML i CSV, kolejek wiadomości i innych źródeł. System można skonfigurować w celu analizowania zebranych danych za pomocą złożonych układów, które mogą być dynamiczne lub oparte na słowniku danych. Dane zebrane z plików dzienników lub innych źródeł mogą być wykorzystywane do analiz, w raportach i dochodzeniach, podobnie jak dane przechwytywane podczas podsłuchiwania sieci. Zebrane dane mogą być analizowane w czasie rzeczywistym i korelowane przez silnik reguł (rule engine) z informacjami przechwyconymi w ramach podsłuchiwania sieci. Korzystanie ze sniffingu sieciowego nie jest obligatoryjne. W niektórych wdrożeniach wszystkie dane wymagane do analizy pochodzą z plików dzienników lub innych źródeł bez stosowania podsłuchiwania sieci.

Analiza danych

System zapewnia gotową funkcję indeksowania dowolnego tekstu i konfigurowalną analizę procesów użytkownika.

1. Indeksowanie dowolnego tekstu

CFRM analizuje treść zapisanych ekranów / stron internetowych i identyfikuje nagłówki, podpisy pól i wartości dla ekranu / strony internetowej. Wszystkie te informacje są przechowywane w systemowej bazie danych i mogą być indeksowane do wyszukiwania dowolnego tekstu w stylu podobnym do wyszukiwarki Google. Dzięki temu można, na przykład, wyszukiwać wszystkich użytkowników, którzy uzyskali dostęp do określonego konta klienta w danym okresie. Wyszukiwanie to można przeprowadzić na danych zapisanych z określonej platformy (np. Internetu) lub na danych zapisanych z kilku platform (np. komputer mainframe, klient/serwer, Internet, AS/400 itp.).

2. Analiza procesów użytkownika

Jedną z wyjątkowych funkcji CFRM jest analiza aktywności użytkowników końcowych i identyfikacja procesów biznesowych przeprowadzanych przez użytkowników. Odbywa się to w dwóch etapach — identyfikacja konkretnych ekranów i identyfikacja procesów biznesowych, które obejmują zidentyfikowane ekrany.

- Identyfikacja ekranów / stron internetowych
  Osoba wdrażająca system może zidentyfikować konkretny ekran, określając pewien tekst lub kilka ciągów tekstowych (np. nazwę transakcji i/lub nagłówek ekranu), które pojawiają się w określonych miejscach na ekranie. Definicja ekranu może również obejmować kilka pól do rejestrowania przez system zgodnie z ich lokalizacjami na ekranie. Gdy wdrażający wprowadzi definicję ekranu w repozytorium CFRM, system zacznie sprawdzać każdy zarejestrowany ekran pod kątem tej definicji w czasie rzeczywistym.

- Identyfikacja procesów biznesowych (zdarzenia w ramach aktywności użytkownika)
  Zdarzenie w ramach aktywności użytkownika to transakcja biznesowa realizowana przez użytkownika poprzez uzyskanie dostępu do jednego lub kilku ekranów aplikacji. Osoba wdrażająca system może zidentyfikować zdarzenie w ramach aktywności użytkownika, ustalając scenariusz, w którym użytkownik przechodzi z ekranu na ekran w celu wykonania określonej funkcji biznesowej.

Należy zauważyć, że nie ma potrzeby identyfikowania ekranów/ stron internetowych w celu wykonywania funkcji wyszukiwania i odtwarzania. Identyfikacja jest wymagana tylko w przypadku ekranów/ stron internetowych obejmujących procesy biznesowe, które osoba wdrażająca chciałaby zidentyfikować i jest przeprowadzana w dwóch głównych celach:

- Uruchomienie reguł biznesowych w silniku reguł w celu wykrycia podejrzanego zachowania użytkownika/ działań na koncie.
- Utworzenie ścieżki audytu transakcji biznesowych z konkretnymi informacjami przechwyconymi z transakcji. Taka ścieżka audytu jest zwykle w postaci tabeli generowanej automatycznie przez CFRM, w której każdy wiersz dotyczy jednego wystąpienia ekranu lub zdarzenia w ramach aktywności użytkownika. Przechwytywane informacje mogą obejmować np. identyfikator użytkownika, numer konta, imię i nazwisko/ nazwę klienta, kwotę transakcji, działania wykonane przez użytkownika końcowego (dodawanie, aktualizowanie, usuwanie), itp. Taka szczególna ścieżka audytu stanowi dodatek do ogólnej ścieżki audytu generowanej automatycznie przez CFRM poprzez rejestrowanie kompletnych sesji użytkownika.

Zdarzenia w ramach aktywności użytkownika są definiowane z zastosowaniem kreatora, który prowadzi użytkownika przez proces. Wszystkie elementy, m.in. zdarzenia w ramach aktywności użytkownika, ekrany, pola itp. są przechowywane w repozytorium CFRM.

Profilowanie, scoring i alerty

Mechanizm analityczny oferuje bardzo elastyczny i adaptowalny model danych, który umożliwia zaawansowane obliczenia i korelacje w czasie rzeczywistym. Model danych może obejmować statyczne i dynamiczne informacje na temat podmiotów różnych typów, m.in. pracowników, kont, klientów i innych. Można go dostosować do danego procesu i wymagań firmy.
Dane przechwytywane przez system z różnych źródeł są przesyłane do silnika reguł w znormalizowany sposób, więc platforma, z której dane zostały przechwycone i sposób w jaki zostały one przechwycone, stają się przejrzyste dla mechanizmu analitycznego.

Mechanizm analityczny akceptuje dwa typy danych wejściowych:

- zdarzenia w ramach aktywności użytkownika, które są nieustannie przechwytywane przez system z różnych kanałów danych. Zdarzenia te są mapowane w mechanizmie analitycznym jako Fakty,
- dane z zewnętrznych baz danych i plików, np. wskazanie kont należących do celebrytów lub kierownictwa firmy. Informacja tego typu zwykle nie jest wyświetlana na ekranach użytkownika przechwyconych przez system, ale jest istotna dla wykrycia podejrzanego zachowania. Informacje otrzymane ze źródeł zewnętrznych są mapowane jako Podmioty biznesowe, np. Użytkownik, Klient, Konto, itp.

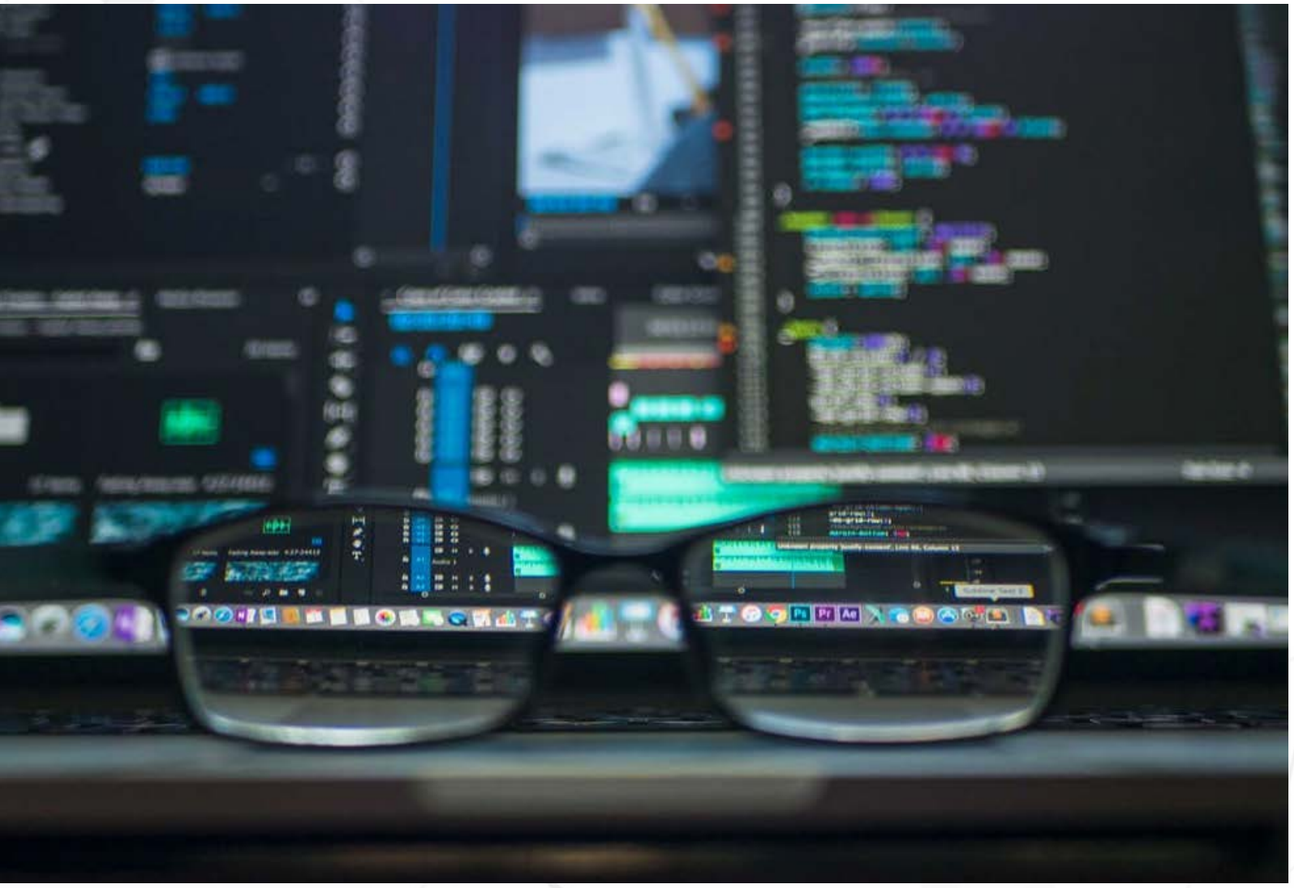
Jedną z wyjątkowych funkcji CFRM jest stosowanie nowych reguł do zarejestrowanych danych historycznych. Jest to możliwe, ponieważ cała aktywność użytkownika jest rejestrowana i przechowywana niezależnie od tego, czy jest podejrzana, czy nie. Dzięki temu audytorzy wewnętrzni mogą sprawdzić, czy we wcześniej zarejestrowanych danych firmy nie pojawiły się nowe potencjalne scenariusze nadużyć (których wcześniej nie przewidziano).

Profilowanie

Mechanizm oferuje profilowanie użytkowników końcowych i grup użytkowników końcowych, kont i grup kont, klientów i grup klientów oraz wszelkich innych podmiotów. System obejmuje wstępnie zdefiniowany zestaw wskaźników profilu, który można dostosować do szczególnych wymagań firmy.

Oto kilka przykładów wskaźników profilu użytkownika:

- średnia liczba kont, do których użytkownik uzyskał dostęp, dziennie w ciągu ostatnich 3 miesięcy,
- średnia liczba nieaktywnych kont, do których użytkownik uzyskał dostęp, tygodniowo w ciągu ostatnich 3 miesięcy,
- średnia liczba zmian adresu konta, tygodniowo w ciągu ostatnich 3 miesięcy,
- średnia liczba zmian beneficjenta konta, tygodniowo w ciągu ostatnich 3 miesięcy,
- średnia liczba zmian częstotliwości wysyłania wiadomości dla konta, tygodniowo w ciągu ostatnich 3 miesięcy,
- średnia liczba zmian atrybutów nieaktywnych kont, tygodniowo w ciągu ostatnich 3 miesięcy,
- średnia liczba zapytań o nazwy klientów, tygodniowo w ciągu ostatnich 3 miesięcy,
- średnia łączna kwota przelewów pieniężnych, dziennie w ciągu ostatnich 3 miesięcy,
- średnia liczba przelewów pieniężnych, dziennie w ciągu ostatnich 3 miesięcy,
- średnia liczba zmian atrybutu konta i zmian powrotnych w ciągu 48 godzin, miesięcznie w ciągu ostatnich 3 miesięcy.



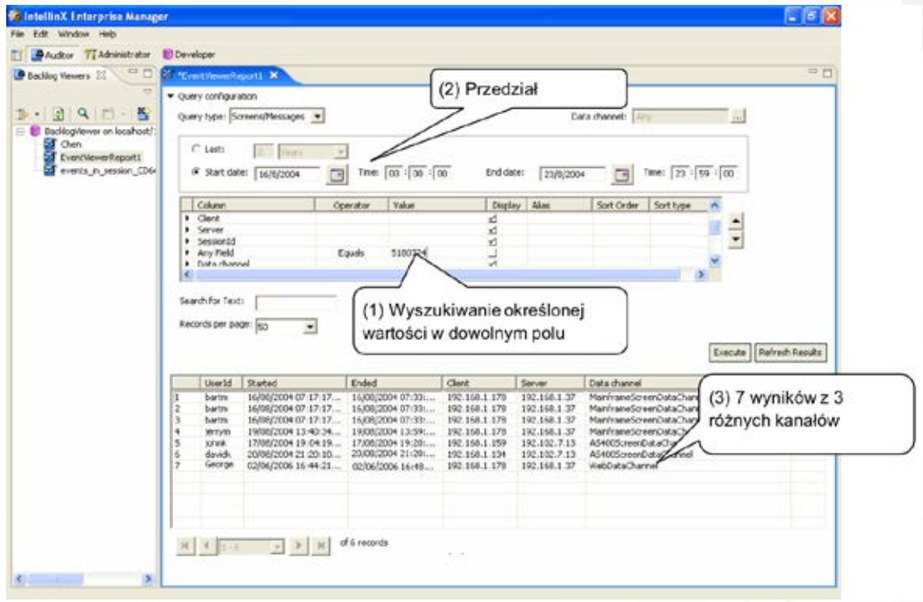
Odtwarzanie danych i wyszukiwanie na wielu platformach

Wyszukiwanie danych o aktywności użytkownika na wielu platformach (podobne do wyszukiwania w Google)

Funkcja wyszukiwania danych na różnych platformach umożliwia analitykom wyszukiwanie dowolnego terminu w każdej monitorowanej aplikacji. Na przykład, można zidentyfikować wszystkich użytkowników, którzy uzyskali dostęp do określonego konta klienta w danym przedziale czasowym. Wyszukiwanie to można łatwo przeprowadzić na danych zapisanych z określonej platformy (np. Internet) lub na danych zapisanych z kilku platform (np. komputer mainframe, klient/serwer, Internet, AS/400, dostęp do bazy danych itp.).

Poniższy zrzut ekranu przedstawia wyszukiwanie przeprowadzone przez analityka w ramach wyszukiwania podobnego do wyszukiwania w Google, w celu znalezienia wszystkich użytkowników, którzy uzyskali dostęp do określonego konta o numerze „5180774”(1) w dowolnym polu, na dowolnym ekranie lub platformie w całej firmie. Wyszukiwanie można również przeprowadzić w określonym przedziale czasowym(2). W rezultacie system wyświetlił u dołu ekranu siedem ekranów użytkowników, na których pojawiła się określona wartość. Dla każdego ekranu system wyświetla kanał danych(3), z którego zarejestrowano dany ekran: komputer mainframe, AS/400 lub Internet.

Z wyników na poniższej liście analityk może wybrać dowolny ekran do odtworzenia, aby dowiedzieć się dlaczego uzyskano dostęp do konta o tym numerze.



Odtwarzanie danych

System CFRM umożliwia również wizualne odtworzenie działań użytkownika ekran po ekranie. Dzięki temu analityk może przejść bezpośrednio do ekranów, które uruchomiły alarm, i przewijać je do tyłu lub do przodu, aby w pełni zrozumieć rzeczywiste zachowanie użytkownika i kontekst jego działań. Funkcja ta umożliwia analitykowi dokładne zbadanie sprawy w prosty i szybki sposób.

Przykładowe reguły

Jedną z najczęstszych reguł stosowanych w systemie jest sytuacja, w której pracownicy uzyskują dostęp do większej liczby rekordów klientów niż inni użytkownicy. Może to oznaczać, że pracownik zbiera informacje pod dalsze nieuczciwe działania. W tym przypadku mechanizm analityczny śledzi, ile razy każdy użytkownik uzyskał dostęp do danego rekordu w określonym przedziale czasowym. System oblicza również średnią liczbę kont, na które wchodzono, dla każdej grupy pracowników. Na podstawie tych dwóch rodzajów danych system może generować alerty, gdy dany pracownik wyszukuje znacznie więcej rekordów niż jego współpracownicy pełniący podobne funkcje. Alerty można uściślić, uwzględniając czas, w którym nastąpiła nadmierna liczba wyszukiwań (czy było to poza normalnymi godzinami pracy) oraz profil kont klientów, do których uzyskano dostęp (konta celebrytów lub członków kierownictwa banku).

Wyciek poufnych informacji/kradzież danych:

- wyszukiwanie informacji o kontach/klientach częściej niż średnia przewidywana częstotliwość,
- nadmierna liczba wydruków dotyczących konta/klienta,
- nadmierna liczba wyszukiwań pospolitych nazwisk,
- nadmierna liczba szczegółowych wyszukiwań informacji bez późniejszej transakcji pieniężnej,
- niewłaściwe zachowanie na danym stanowisku (np. wyszukiwanie danych poza godzinami pracy, sprawdzanie kont innych działów, wyszukiwanie informacji o kontach z innych województw/regionów/krajów),
- wyszukiwanie informacji o kliencie będącym na aktywnej liście klientów prestiżowych (VIP),
- pobieranie dużej liczby informacji.

Defraudacja:

- na koncie przeprowadzane są transakcje określonego typu o dużej łącznej wartości,
- na koncie przeprowadzanych jest zbyt wiele operacji określonego typu,
- w oddziale przeprowadzanych jest zbyt wiele operacji określonego typu na kontach danego rodzaju,
- na własnym koncie pracownika przeprowadzanych jest zbyt wiele operacji określonego typu,
- pracownik realizuje transakcję na koncie, na którym ostatnio nie przeprowadzano żadnych operacji,
- pracownik dokonuje wypłat z kont, które mogą przejść na własność Skarbu Państwa po bezdziedzicznej śmierci posiadacza konta.

Wewnętrzne przejęcie konta:

- wielokrotne logowanie do konta z wielu różnych adresów IP jednocześnie,
- logowanie z nowego adresu IP,
- logowanie z innego kraju,
- nietypowe zachowanie w pracy (np. wyszukiwanie danych poza godzinami pracy, sprawdzanie kont innych działów, wyszukiwanie informacji o kontach z innych województw/regionów/krajów),
- pracownik zalogował się bez wczytania karty identyfikacyjnej.

Naruszenia zasad

- uzyskiwanie dostępu do kont współpracowników,
- otwieranie wielu kont o niskim lub zerowym saldzie,
- wyszukiwanie informacji o kliencie będącym na aktywnej liście klientów prestiżowych (VIP),
- przeprowadzanie nadmiernej liczby operacji zwrotu środków w ciągu ostatnich 7 dni,
- dokonywanie przelewów pieniężnych na własny rachunek,
- dokonywanie zwrotów opłat na własny rachunek,
- wyszukiwanie informacji o kontach/klientach częściej niż średnia przewidywana częstotliwość,
- przeprowadzanie transakcji na własny rachunek.

Dowiedz się więcej na

www.biinsight.pl

HISTORIA:

- Rok powstania - 2006
- Ponad 30 klientów

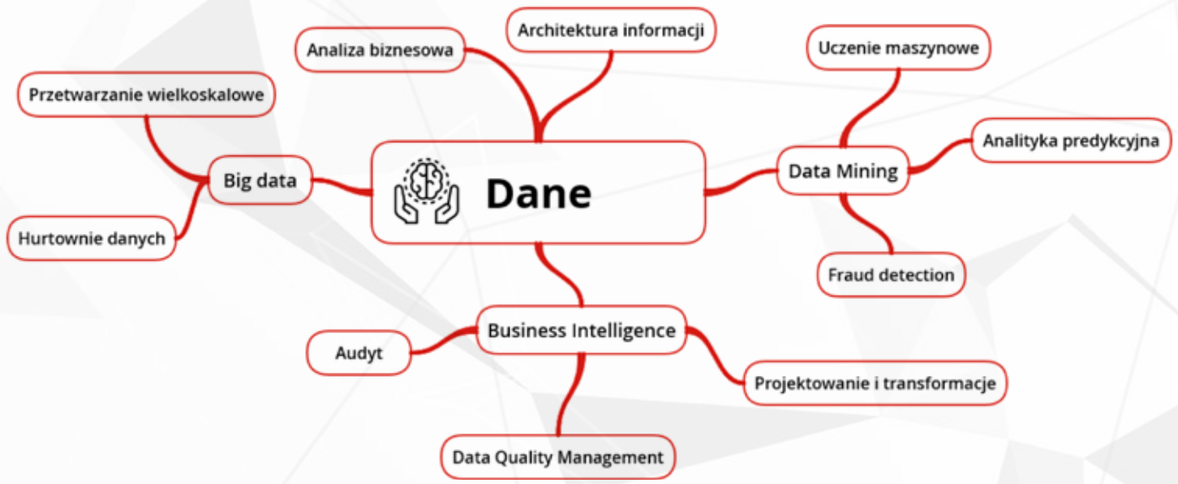
DZIŚ:

- 20 konsultantów z obszarów:

- Business Intelligence
- Data Warehouse
- Big Data
- Fraud Management
- Data Quality & Governance
- segmentacji behawioralnej oraz projektowania i budowy webowych systemów aplikacyjnych

- Stabilność finansowa

Obszar działania



Obszary kompetencji

Rozwiązania Business Intelligence (raportowanie operacyjne, zarządcze, hierarchiczne KPI)
- Oracle BI, SAP BusinessObjects, IBM Cognos, MicroStrategy, SAS (analizy i raportowanie w ładzie korporacyjnym),
- MS SQL Server Analysis Services, MS SQL Server Reporting Services
- MS PowerBI, Qlik, Tableau, Oracle Data Visualization (analiza eksploracyjna i ad-hoc)

Dedykowane Hurtownie Danych i procesy zasilania
- autorskie komponenty BI Insight DWH – zestaw gotowych komponentów służących do budowy oraz zasilania Hurtowni Danych
- Oracle Data Integrator, IBM Data Stage, Informatica, Talend, SAP Data Integrator, MS Integration Services
- Oracle GoldenGate - replikacja danych w trybie „real-time”

biDQM (Data Quality Monitoring)
- poprawność, spójność i jakość danych
- autorskie rozwiązanie zapewniające odpowiednią jakość danych w hurtowni danych

Zaawansowana analiza danych
- silniki wielowymiarowe: IBM SPSS, Oracle Essbase, IBM TM1, MS Analysis Services
- Python, R

BigData, machine learning, analizy behawioralne i segmentacyjne (massive data store and analysis)
- Hadoop (Cloudera, HortonWorks)
- Vertica Analytics Platform

Fraud Management
- wykrywanie i przeciwdziałanie nadużyciom
- specjalizowana platforma Bottomline Cyber Fraud and Risk Management
- dedykowane rozwiązania ze szczególnym uwzględnieniem możliwości analitycznych oraz gotowym zestawem analiz zbudowanym z wykorzystaniem narzędzi klasy BI

Data Security (techniczne dostosowanie systemów bazodanowych do regulacji RODO)
- Oracle Active Data Guard,
- Oracle DB Vault,
- Oracle Transparent Data Encryption

Aplikacje webowe
- Projektowanie i budowa aplikacji (mobilnych, cloud ready) w technologiach: Oracle APEX, .Net

Cyber Fraud & Risk Management

Data Governance

Business Intelligence

Data Warehouse

Big Data

BI Insight S.A.
ul. Władysława Jagiełły 4/U3
02-495 Warszawa
KRS 0000267338
NIP 522-28-29-670
REGON 140680503