LexisNexis®
RISK SOLUTIONS

ZNACZENIE ANALIZY BEHAWIORALNEJ DO CELÓW ANTYFRAUDOWYCH I JEJ WYKORZYSTANIE W ZGODZIE Z REGULACJAMI EUROPEJSKIMI

MACIEJ JAMIOŁKOWSKI, COUNTRY MANAGER

Forum Usług Płatniczych, Październik 2023 r.

O LEXISNEXIS RISK SOLUTIONS

- Oferujemy szerokie portfolio produktów do zarządzania ryzykiem: KYC, AML, antyfraud, płatności, orkiestracja danych

- Mamy wielosektorowe i międzynarodowe doświadczenie

  Fraud nie jest ograniczony do jednej branży lub regionu. Analizujemy cyfrowe tożsamości użytkowników Internetu, w oparciu o ich interakcje z serwisami i aplikacjami na całym świecie.
  W ten sposób powstaje sieć powiązań pomiędzy użytkownikami i ich akcjami

  Tak szerokie spojrzenie umożliwia o wiele większą precyzję w podejmowaniu decyzji antyfraudowych

6000+
klientów na całym świecie

180+
krajów, w których mamy klientów

4,4 mld
urządzeń w sieci

3 mld
cyfrowych tożsamości

LexisNexis® RISK SOLUTIONS

O LEXISNEXIS RISK SOLUTIONS

- **Globalne repozytorium danych**

  W sercu naszego rozwiązania jest współdzielone repozytorium danych o zdarzeniach fraudowych

  Obecnie widzimy ruch z 244 na 249 krajów, co oznacza, że nawet jeśli w danym kraju nie mamy żadnego klienta, mamy informacje o cyfrowych tożsamościach użytkowników z tego kraju, korzystających z międzynarodowych serwisów

- **Międzypodmiotowa wymiana danych o fraudzie i zaufanych użytkownikach**

  Mamy sprawdzone, bezpieczne rozwiązanie do współdzielenie danych pomiędzy podmiotami, rozszerzające obraz cyfrowych tożsamości o dodatkowy kontekst

6000+
klientów na całym świecie

180+
krajów, w których mamy klientów

4,4 mld
urządzeń w sieci

3 mld
cyfrowych tożsamości

LexisNexis® RISK SOLUTIONS

~~BIOMETRIA BEHAWIORALNA?~~

ANALIZA BEHAWIORALNA

LexisNexis®
RISK SOLUTIONS

RÓŻNICE POMIĘDZY BIOMETRIĄ I ANALIZĄ BEHAWIORALNĄ

Czym są dane biometryczne

Odcisk palca

Tęczówka i siatkówka

Kształt i wyraz twarzy

Głos

NIE zbieramy danych biometrycznych w żadnej formie do celów antyfraudowych

Termin *biometria behawioralna* w kontekście antyfraudowym jest jedynie marketingowym hasłem używanym przez branżę.

W praktyce **nie ma nic wspólnego** z właściwą biometrią.

LexisNexis® RISK SOLUTIONS

RÓŻNICE POMIĘDZY BIOMETRIĄ I ANALIZĄ BEHAWIORALNĄ

Zajmujemy się analizą zachowania użytkownika,
na podstawie jego interakcji z urządzeniem

Klawiatura

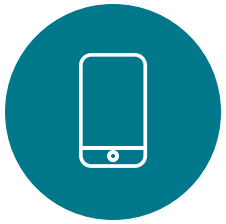
- Użycie skrótów klawiszowych
- Kopiuj-wklej
- Autouzupełnienie
- Błędy i kasowanie
- Rytm pisania
- Długość wpisywania

Myszka

- Interakcje z serwisem
- Wyjście myszy poza stronę
- Szybkość ruchów
- Krzywizna ruchów
- Kliknięcia

Ekran dotykowy

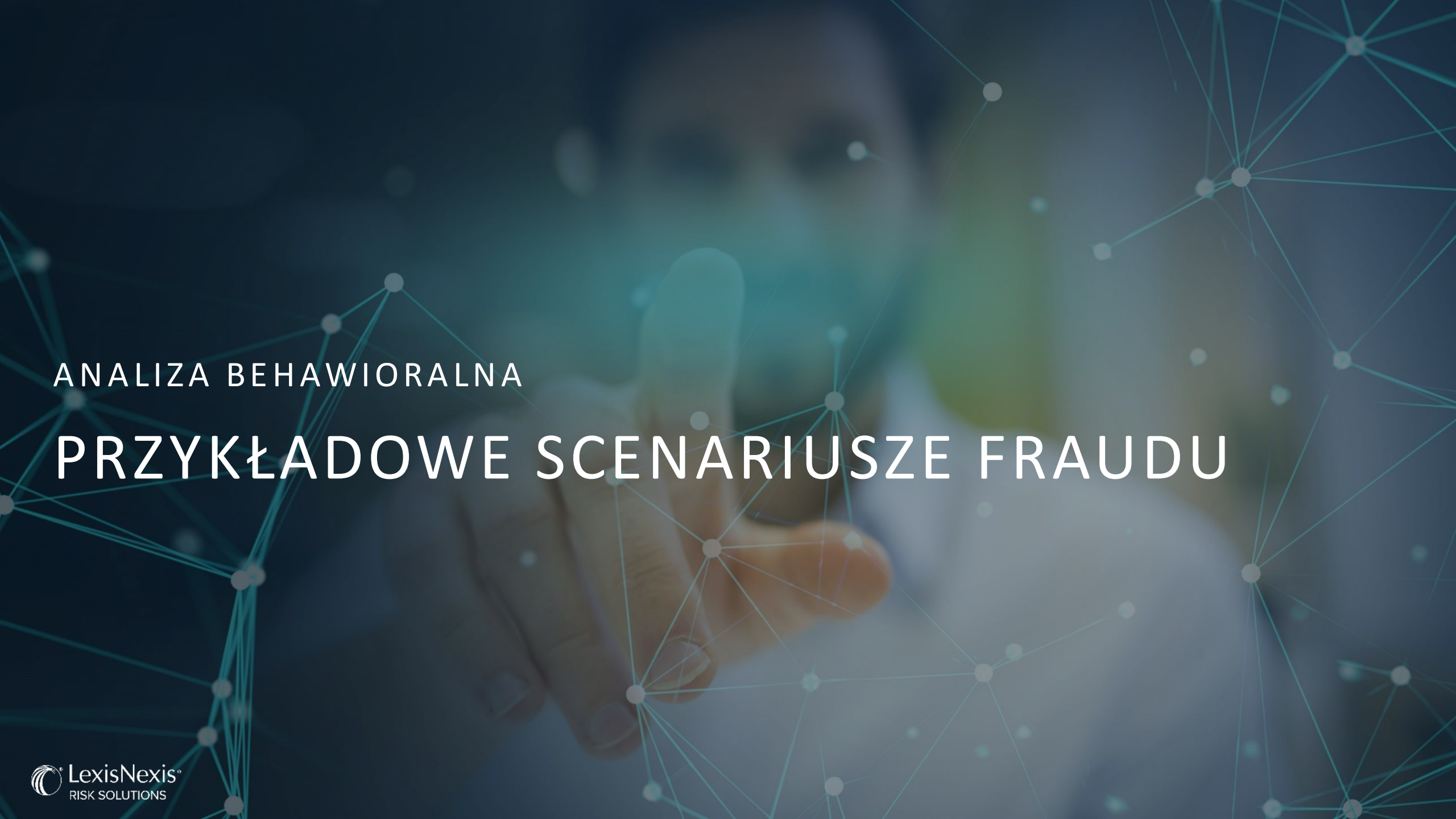
- Gesty
- Dotknięcia i przesunięcia
- Siła nacisku
- Rozmiar i obszar dotyku



Wskaźniki mobilne

- Położenie urządzenia
  - akcelerometr
  - żyroskop
- Aktywne połączenia
- Potencjalne instruowanie

LexisNexis®
RISK SOLUTIONS



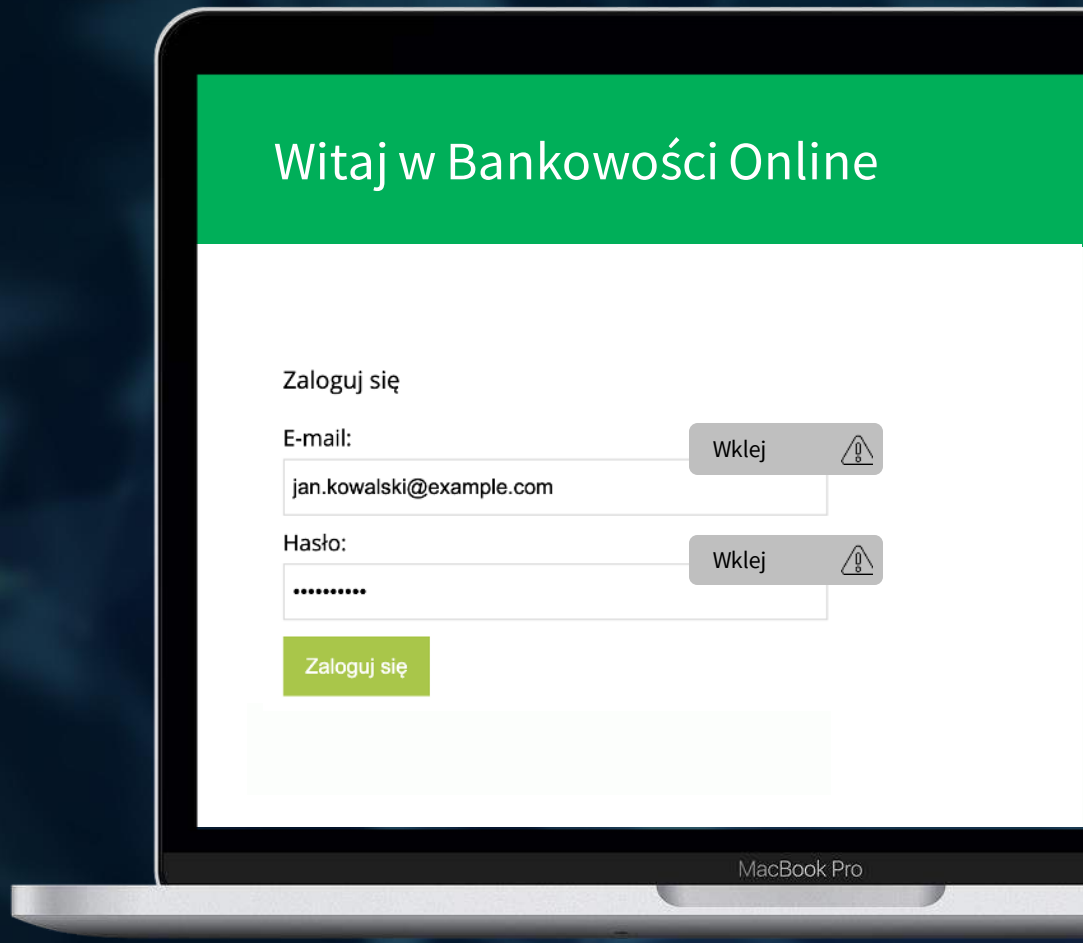
ANALIZA BEHAWIORALNA

PRZYKŁADOWE SCENARIUSZE FRAUDU

LexisNexis® RISK SOLUTIONS

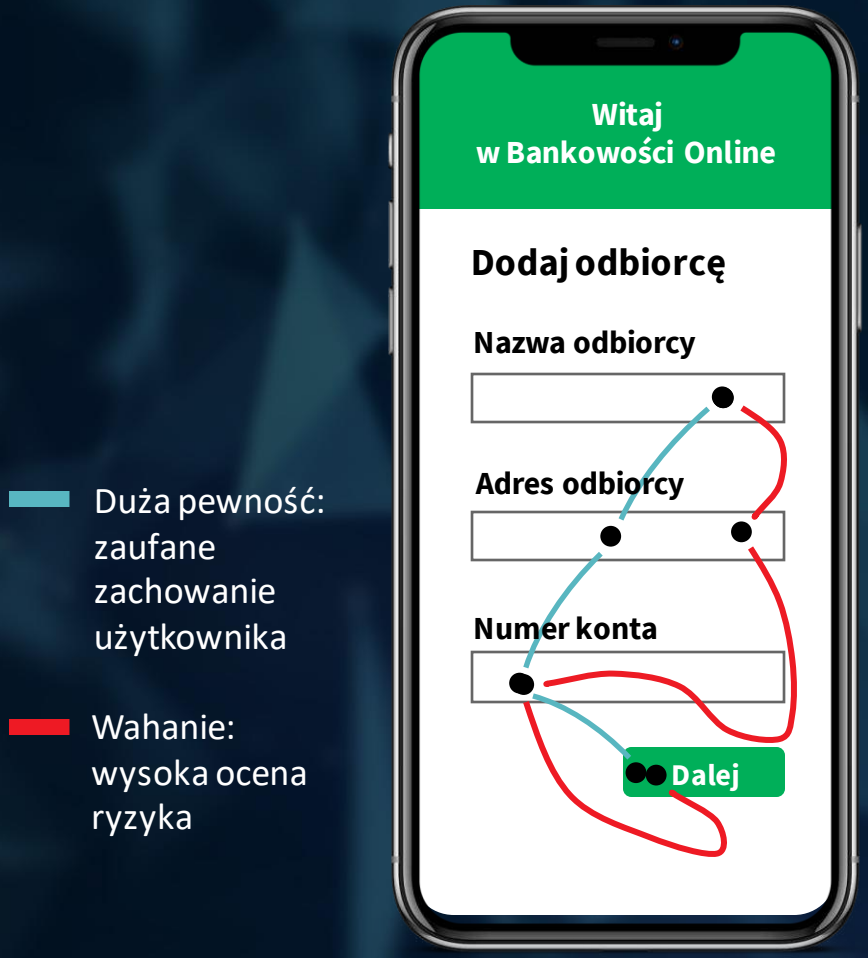
PRZEJĘCIA KONT PRZEZ OSZUSTA I BOTY

- Przeważnie przy przejęciu konta skradzione dane logowania są kopiowane i wklejane. Wiarygodni użytkownicy zazwyczaj wpisują te dane ręcznie lub korzystają z funkcji autouzupełniania
  - Myszka wychodząca poza stronę może wskazywać na kopiowanie danych z zewnętrznego źródła
- Ataki BOTów są z kolei zautomatyzowane i bardzo szybkie, często mierzone w milisekundach. Dane logowania są wklejane przez specjalne skrypty
  - Niektóre boty próbują naśladować pisanie przez użytkownika, ale tempo jest szybsze niż możliwości człowieka
- Przy próbie przejęcia konta porównujemy profil behawioralny z danej sesji, do wcześniej zbudowanego profilu użytkownika. Z pewnym prawdopodobieństwem, jesteśmy w stanie określić czy to profil tej samej osoby czy nie.



ATAKI SOCJOTECHNICZNE (AKTYWE POŁĄCZENIA)

- Podczas ataku socjotechnicznego, analiza urządzenia czy połączenia sieciowego staje się nieskuteczna, ponieważ manipulowany użytkownik wykonuje polecenia oszusta na swoim urządzeniu, podłączony do swojej sieci.
- Ofiara ataków socjotechnicznych zachowuje się inaczej, zarówno w przeglądarce, jak i aplikacji mobilnej
- Podczas ataków socjotechnicznych, przesuwanie palca lub kursora zazwyczaj trwa dużej i wykazuje się większą krzywizną ruchu
    - Wskazuje to na niepewność i wahanie wynikające z instruowania, nietypowe przy normalnym poruszaniu się użytkownika w serwisie



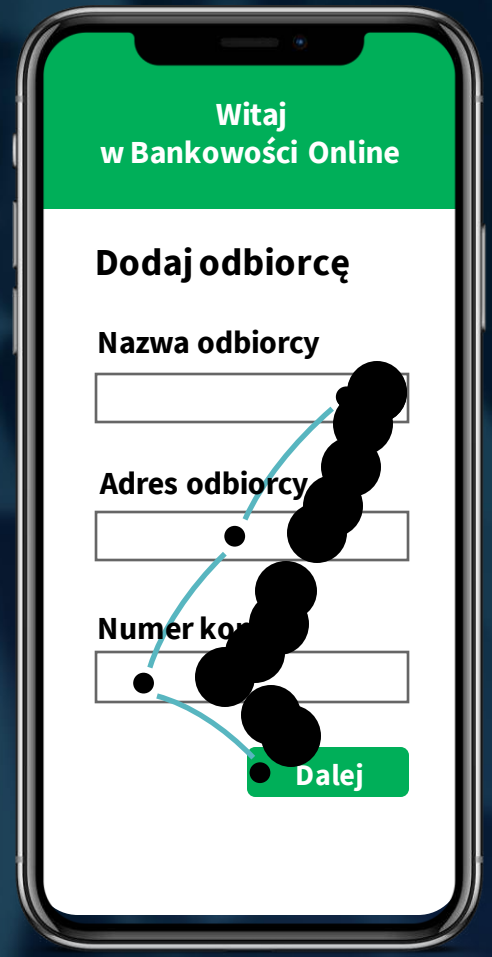
LexisNexis® RISK SOLUTIONS

NARZĘDZIA ZDALNEGO DOSTĘPU (RAT, RDP)

- W związku z kompresją danych w trakcie przesyłania, ruchy palca lub kursora są dużo mniej płynne przy użyciu narzędzi zdalnego dostępu (RAT)
    - Rozmiar dotyku i kursora są znacząco (nienaturalnie) większe przy zastosowaniu narzędzi RAT na urządzeniach mobilnych
- Analiza behawioralna jest wsparciem w detekcji narzędzi zdalnego dostępu, nawet kiedy detekcja otwartych portów jest niemożliwa lub mało wiarygodna. Analiza ta daje informacje o faktycznym wykorzystaniu RAT w sesji użytkownika, przyczyniając się do znacznej redukcji poziomu *false positives*

Normalny rozmiar dotyku i płynne ruchy

Nienaturalnie duży rozmiar dotyku i "rwane" ruchy



LexisNexis® RISK SOLUTIONS

EUROPEJSKIE PODEJŚCIE DO ANALIZY BEHAWIORALNEJ

Chcemy wesprzeć dyskusję na temat regulacji, dzieląc się naszym globalnym doświadczeniem

27 Krajów w Unii Europejskiej

Dziesiątki Regulatorów i prawodawców

120+ Tyle banków i instytucji finansowych, operujących w różnych systemach regulacyjnych w całej Europie, wspiera LexisNexis Risk Solutions

Żaden z tych podmiotów nie zbiera wyraźnych zgód na profilowanie behawioralne

LexisNexis® RISK SOLUTIONS

EUROPEJSKIE PODEJŚCIE DO ANALIZY BEHAWIORALNEJ

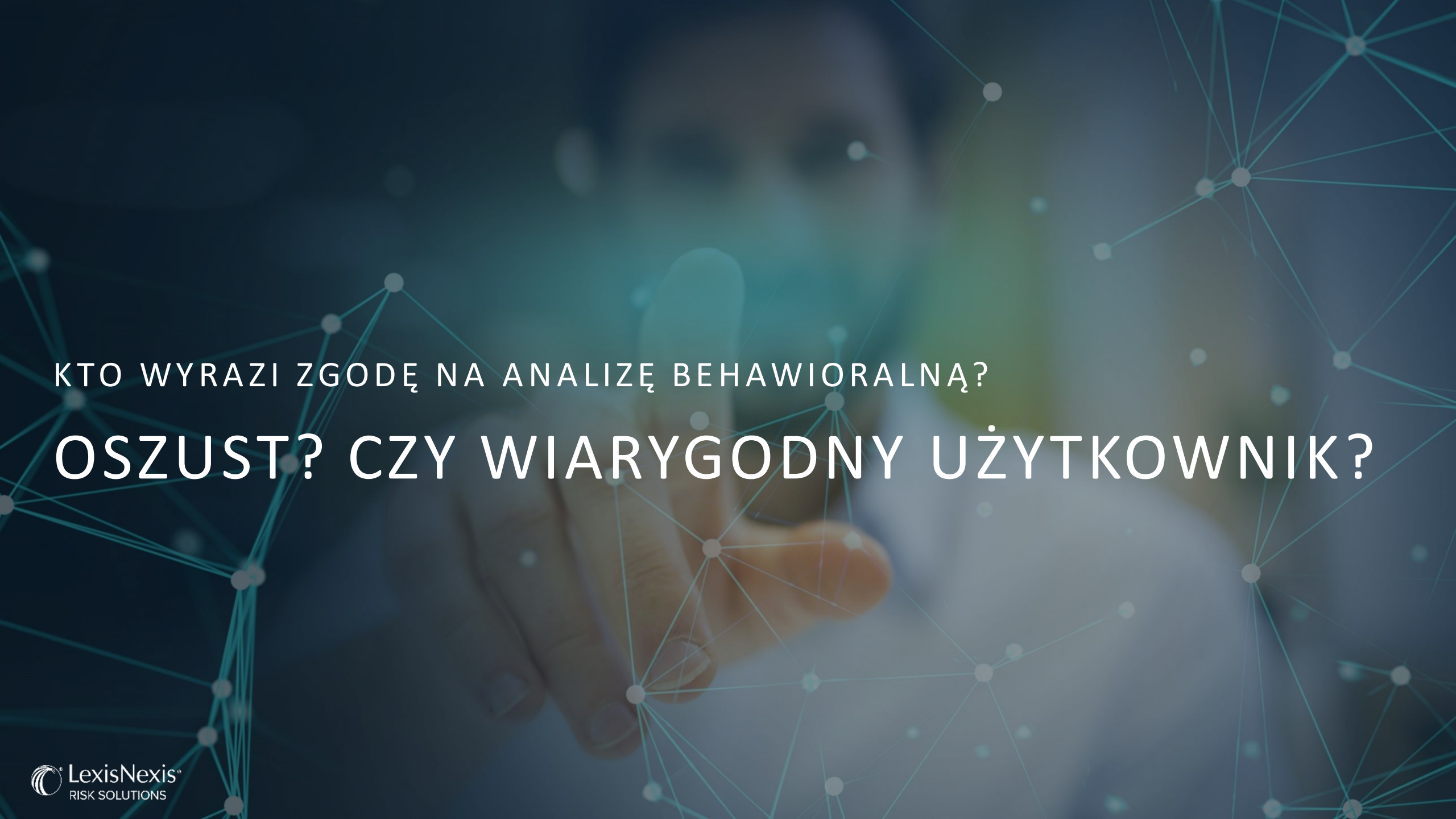
- $Weryfikacja \neq identyfikacja$
  RODO, art. 4 , ust. 14

  Weryfikacja czy użytkownik wykazuje cechy zaufania lub ryzyka, na podstawie jego analizy, nie oznacza możliwości identyfikacji konkretnego użytkownika w myśl Rozporządzenia o Ochronie Danych Osobowych

- Nie używamy danych biometrycznych, czyli **nie dochodzi do przetwarzania szczególnych kategorii danych osobowych.** Nie zachodzi zatem potrzeba zbierania zgód
  RODO, art. 9

- Zgodność przetwarzania z prawem:
  - (c) obowiązek prawny
  - (f) uzasadniony interes

  RODO, art. 6



KTO WYRAZI ZGODĘ NA ANALIZĘ BEHAWIORALNĄ?

OSZUST? CZY WIARYGODNY UŻYTKOWNIK?

LexisNexis®
RISK SOLUTIONS

44 202 711 zł

Tyle wyniosła wartość fraudu na poleceniach przelewu w Polsce, w pierwszym kwartale 2023 r.*
Dalsza zwłoka z udoskonalaniem zabezpieczeń spowoduje jedynie wzrost strat

LexisNexis®
RISK SOLUTIONS

**Informacja o transakcjach oszukańczych dokonywanych przy użyciu bezgotówkowych instrumentów płatniczych w I kwartale 2023 r., Narodowy Bank Polski*

LexisNexis®
RISK SOLUTIONS

DETEKCJA FRAUDU MONITORING TRANSAKCJI

AML & CFT KYC & KYB ORKIESTRACJA DANYCH

MACIEJ JAMIOŁKOWSKI
COUNTRY MANAGER
+48 509 997 924
MACIEJ.JAMIOLKOWSKI@LEXISNEXISRISK.COM

ANALIZA CYFROWEJ TOŻSAMOŚCI UŻYTKOWNIKA

ANALIZA BEHAWIORALNA ANALIZA ADRESU EMAIL