LexisNexis®
RISK SOLUTIONS

LexisNexis® Behavioral Biometrics

Histórias de sucesso dos clientes

Behavioral Biometrics é o termo usado para descrever a maneira como um usuário online interage com o seu desktop, celular ou notebook através do teclado, mouse e/ou tela touchscreen. O LexisNexis® Behavioral Biometrics foi projetado como uma melhoria para o produto LexisNexis® ThreatMetrix® existente com o objetivo de:

- Acrescentar uma camada adicional de defesa contra tomada de decisão sobre fraudes e risco ao combinar a forma como um usuário interage com o seu dispositivo à inteligência de identidade digital existente.
- Melhorar a definição do perfil de comportamento de alto risco associado a fraudadores, *bots* automatizados, engenharia social e ataques de acesso remoto.
- Construir, com o passar do tempo, uma visão mais clara do comportamento do usuário legítimo, identificando com confiança os desvios de um padrão já estabelecido.
- Identificar perfis confiáveis e de comportamento de alto risco para melhor prever práticas fraudulentas em tempo quase real.

As principais vantagens incluem:

Integração estreita: o LexisNexis Behavioral Biometrics está completamente integrado no portal atual do LexisNexis ThreatMetrix®, simplificando o alinhamento com recursos de inteligência de identidade digital e promovendo implementação direta.

Abordagem Caixa Branca:

- Dados do Behavioral Biometrics relacionados às interações com o mouse, o teclado e o dispositivo móvel estão disponíveis para uso, de acordo com as políticas e as regras.
- Modelos e pontuações de Machine Learning para diferentes categorias de risco são oferecidos com códigos de razão associados para expor a lógica por trás da classificação. Os atributos de Behavioral Biometrics podem ser usados independentes ou em combinação com os de identidade digital.

Privacidade por design: teclas alfanuméricas não são registradas, portanto não há coleta de dados sobre senha ou informações pessoalmente identificáveis (PII).

Baixo atrito: implementado como parte do payload do JavaScript do LexisNexis ThreatMetrix existente. Sem degradação de desempenho ou impacto na latência quando o Behavioral Biometrics é ativado.

Business Case do Behavioral Biometrics:

Tome decisões confiáveis sobre riscos que envolve cada vez mais a disposição de várias peças de inteligência de maneira a impor poucas restrições a usuários bons e confiáveis. O desafio para os negócios digitais é que os fraudadores costumam imitar o comportamento do usuário legítimo, seja imitando clientes verdadeiros, treinando *bots* automatizados para se comportarem como humanos ou persuadindo pessoas a iniciar operações com o seu nome.

Os dados do Behavioral Biometrics oferecem uma outra dimensão de inteligência às organizações, capturando como um usuário final se comporta com o seu dispositivo. Fornece esse conhecimento juntamente com inteligência de identidade digital relacionada a reputação do dispositivo, inteligência de localização, padrões de comportamento operacionais e ameaças conhecidas, ajudando as empresas a diferenciar melhor entre usuários confiáveis e ameaças em potencial.

O Behavioral Biometrics em ação: História de sucesso 1

Dois Bancos Nível 1 na região EMEA (Europa, Oriente Médio e África) apresentaram resultados imediatos após a integração do Behavioral Biometrics a criações de novas contas e às páginas de cadastros de novos canais.

PROBLEMA COMERCIAL

A criação de novas contas e os cadastros de novos canais apresentam um ponto de risco significativo na jornada do cliente, à medida que os fraudadores tentam monetizar credenciais roubadas ou interceptar um cadastro bancário móvel/online para ganhar acesso a contas de bons clientes.

A VANTAGEM DO BEHAVIORAL BIOMETRICS

Os fraudadores obtêm listas de credenciais de identidade roubadas ou interceptadas e usam esses dados para realizar cadastros fraudulentos em novos produtos ou serviços. A captura de dados de identidade digital (ex.: integridade e localização do dispositivo), assim como a forma com a qual um usuário insere dados no aplicativo, ajuda a diferenciar entre o comportamento genuíno do usuário e dos fraudadores usando identidades roubadas.

RESULTADOS

BANCO A:

70%
De taxa de fraude encontrada em uma regra a qual identificou padrões recorrentes de comportamento de alto risco em campos específicos no processo de solicitação de cartão de crédito.

92%
De todas as fraudes foram interrompidas a partir da regra nova implementada.

BANCO B:

66%
De taxa de fraude encontrada em novos cadastros de aplicativos móveis que usaram padrões específicos de comportamento de alto risco.

75%
De taxa de fraude encontrada na página de redefinir senha, quando as funções específicas do teclado foram usadas.

O Behavioral Biometrics em ação: História de sucesso 2

Organização de serviços financeiros dos EUA modela comportamento de alto risco para novas solicitações de cartão de crédito.

PROBLEMA COMERCIAL

A detecção de tentativas fraudulentas de solicitação de cartão de crédito ajuda essa organização de serviços financeiros a reduzir o prejuízo causado por fraudes e a minimizar as demandas operacionais associadas à gestão de estornos a comerciantes.

A VANTAGEM DO BEHAVIORAL BIOMETRICS

Descobriu-se que um fraudador se comportou de maneira muito diferente à de um usuário confiável ao preencher um formulário de inscrição. Uso do mouse, cadência do teclado e o tempo gasto preenchendo os campos ajudaram na identificação de solicitações de alto risco antes delas serem processadas.

Usando essa inteligência, a equipe de serviços profissionais LexisNexis ThreatMetrix criou um modelo de fraude sob medida no Behavioral Biometrics, combinando dados brutos de biometria comportamental com a análise comportamental refinada da LexisNexis ThreatMetrix.

RESULTADOS

Aumento entre
10 e 20%

Este modelo de fraude personalizado ajudou a aumentar a detecção de fraudes em 10% a 20%, além de recursos de identidade digital existentes.

OU

1/3

Redução de um terço nos casos de falsos positivos.

O Behavioral Biometrics em ação: História de sucesso 3

Empresa global de viagem diferencia entre avaliações confiáveis e fraudulentas usando atributos do Behavioral Biometrics.

PROBLEMA COMERCIAL

Avaliações fraudulentas podem representar um grande desafio para muitas empresas de serviços de viagem. Os criminosos escrevem e publicam comentários enganosos para aumentar a credibilidade de ofertas de viagens falsas ou para oferecer vantagens infundadas.

A VANTAGEM DO BEHAVIORAL BIOMETRICS

Viajantes legítimos tendem a escrever avaliações geralmente bem pensadas, ao passo que os fraudadores costumam produzir comentários falsos em massa, por vezes alterando detalhes importantes. Essa diferença de comportamento ajudou essa agência de viagens a identificar quais comportamentos indicavam uma avaliação falsa.

RESULTADOS

4x

Análises de tempo ajudaram a revelar padrões de comportamento de avaliações que foram consideradas quatro vezes mais prováveis de serem fraudulentas.

2x

Análises de dados de teclado revelaram que avaliações que não foram escritas do zero tinham quase duas vezes mais probabilidade de serem rejeitadas.

O Behavioral Biometrics em ação: História de sucesso 4

Troca de criptomoedas consegue diferenciar, com segurança, tráfego humano de não humano.

PROBLEMA COMERCIAL

Troca de criptomoedas tornou-se um alvo-chave para ataques de *bot* automatizados tentando invadir contas de bons usuários para acessar moedas digitais.

A VANTAGEM DO BEHAVIORAL BIOMETRICS

Por natureza, o tráfego de *bots* costuma apresentar um padrão uniforme de interação com negócios digitais, com características que podem ser identificadas como semelhantes a máquinas em vez de humanos. O isolamento dessas características comportamentais forneceu à troca de criptomoedas um sinal confiável sobre se o usuário acessando a conta era humano ou *bot.*

RESULTADOS

O tráfego de *bots* apresentou uma velocidade de acesso **mais homogênea** em cada interação.

Humanos exibiram **pequenas variações** na velocidade de acesso com o passar do tempo.

O Behavioral Biometrics em ação: História de sucesso 5

Empresa de jogos online protege pagamentos detectando comportamento de alto risco em tempo quase real.

PROBLEMA COMERCIAL

Empresas de jogos são grandes alvos de criminosos cibernéticos em busca de lucros com fundos fraudulentos, lavagem de dinheiro e monetização com cartões de créditos roubados.

A VANTAGEM DO BEHAVIORAL BIOMETRICS

Análises de dados de teclados revelaram que fraudadores em posse de dados de cartões de créditos roubados exibiram padrões de comportamento consistentes únicos e distintos aos de como consumidores legítimos inserem os seus dados.

RESULTADOS

32%

De fraudes foram identificadas pela empresa de jogos para pagamentos através da nossa tecnologia identificou que essas contas estavam atreladas a cartões de créditos roubados.

Principais recursos do Behavioral Biometrics


Coleta de dados de mouse e teclado.


Coleta de dados de sensor e tela touchscreen.


Um módulo móvel dedicado de kit de desenvolvimento de software (SDK).


Atributos como detecção de copia e cola, mouse fora da tela, elementos da tela e tempo gastos nos campos de preenchimentos.


Uma pontuação geral de biometria comportamental, de fraudador, de anomalia, de *bot*, de acesso remoto, de engenharia social e de códigos de razão associados.


Histórico de detecção de anomalia.


Recursos de agrupamento de fraudes.


Uma interface de usuário intuitiva acessada através do portal LexisNexis ThreatMetrix.

Para mais informações, acesse
risk.lexisnexis.com/fraudes

LexisNexis®
RISK SOLUTIONS

Sobre a LexisNexis Risk Solutions

A LexisNexis® Risk Solutions aproveita o poder dos dados e das análises avançadas para fornecer informações que ajudam empresas e governos a reduzir risco e melhorar a tomada de decisões, beneficiando pessoas no mundo todo. Fornecemos soluções de dados e de tecnologia para uma grande variedade de setores, inclusive de seguros, serviços financeiros, assistência médica e governos. Com sede na área metropolitana de Atlanta, Geórgia, contamos com escritórios por todo o planeta e fazemos parte do RELX (LSE: REL/NYSE: RELX), fornecedor global de análises baseadas em informações e ferramentas de tomada de decisão para clientes profissionais e empresas. Para mais informações, acesse www.risk.lexisnexis.com e www.relx.com.

As nossas soluções de serviços financeiros auxiliam organizações a prevenir crimes financeiros, atender às regulamentações, mitigar riscos comerciais, aprimorar a eficiência operacional e aumentar a rentabilidade.

Este documento tem somente fins educativos e não garante a funcionalidade e os recursos dos produtos identificados da LexisNexis. A LexisNexis não garante que este documento esteja completo e sem erros.