SHIELD

SHIELD para Plataformas de Mobilidade

A plataforma de Inteligência de Fraude baseada na identificação de dispositivos da SHIELD detecta a origem da fraude com o **SHIELD Device ID** e **inteligência de fraude** acionável, ajudando as plataformas de mobilidade a se anteciparem a ameaças sofisticadas de fraude enquanto protegem usuários e motoristas.

Trusted by

inDrive Careem ROUTE ... and more

"A inDrive está comprometida em lutar contra a injustiça e com a promoção da transparência e da equidade no setor de mobilidade e transporte. Nossa parceria com a SHIELD nos permite manter-nos fiéis à nossa missão de ajudar as pessoas, garantindo os mais altos padrões de confiança para todos, enquanto continuamos crescendo em ritmo acelerado."

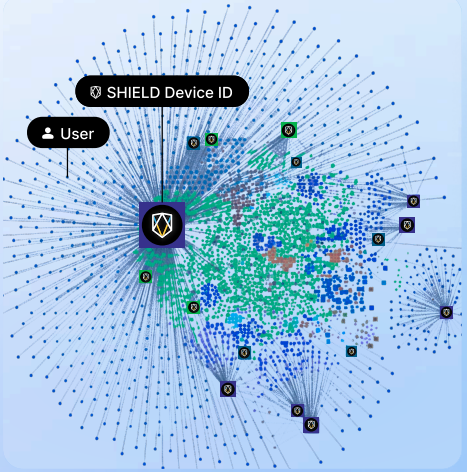
Arsen Tomsky
CEO & Fundador, inDrive

Our Solution

Plug-and-Play | Sem códigos adicionais | Não requer PII

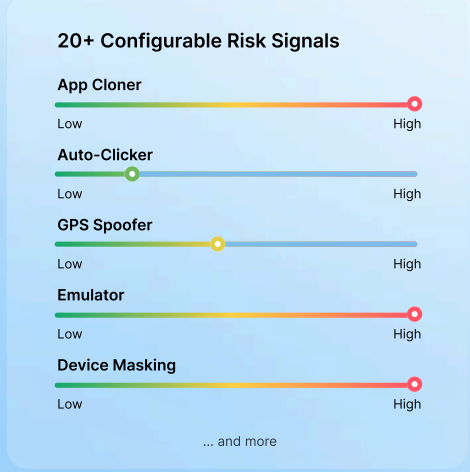
SHIELD Device ID

persistently identifies the root of fraud & fake accounts >99.9% accuracy



SHIELD Fraud Intelligence

real-time actionable insights into fraudulent activity



Use Cases

Elimine conluio entre motoristas e passageiros

O que é conluio entre motoristas e passageiros?

Os fraudadores criam múltiplas contas falsas de motoristas e passageiros em larga escala, utilizando ferramentas maliciosas para explorar os sistemas de transporte por aplicativo e obter vantagens indevidas. Isso pode incluir manipulação de tarifas, corridas falsas, falsificação de localização, aumento artificial de preços por demanda e muito mais.

Elimine as corridas falsas

Fraudadores em conluio completam viagens sem transportar passageiro real. Isso geralmente é feito para explorar o sistema e obter bônus, recompensas ou inflar artificialmente seus ganhos.

Elimine a falsificação de localização

Motoristas desonestos utilizam falsificadores de GPS para parecerem estar mais próximos dos passageiros, prejudicando motoristas legítimos e aumentando os tempos de espera.

Interrompa a manipulação

Redes de fraude manipulam a demanda combinando contas falsas e falsificadores de GPS para gerar aumentos artificiais nas tarifas em locais específicos, elevando os preços em benefício próprio.

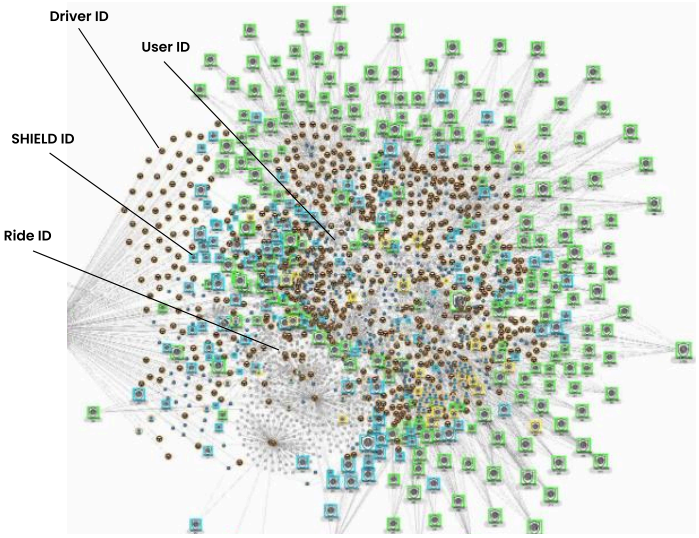
SHIELD Fraud Intelligence

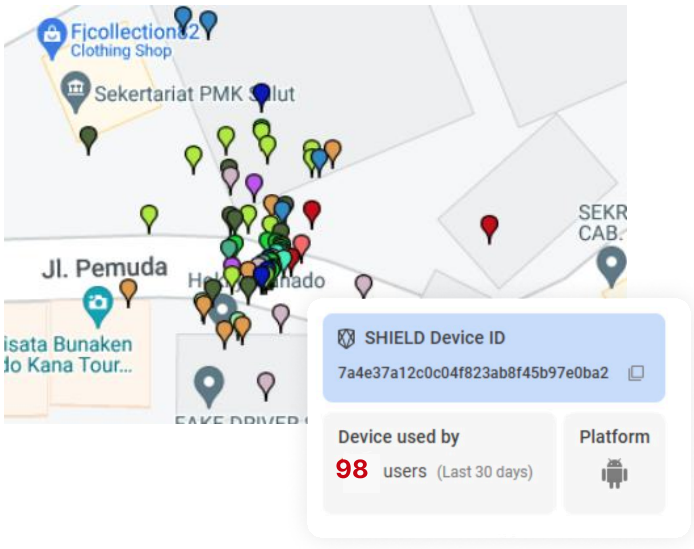
Falsificadores de GPS
Clonadores de app
Emuladores
Reset de fábrica
Dispositivos com jailbreak
Apps manipulados

How it Works

Fraudadores costumam usar um único dispositivo para criar múltiplas contas de motoristas e usuários em larga escala. Eles exploram identidades roubadas, aplicativos manipulados, clonadores de apps, autoclickers e emuladores para executar seus esquemas. Ao controlar tanto contas de motoristas quanto de passageiros, manipulam preços e monopolizam corridas.

A SHIELD identifica contas interconectadas originadas do mesmo dispositivo, detectando redes complexas de fraude e interrompendo ataques coordenados. Em um caso, descobrimos um grupo de **98 motoristas e usuários vinculados a um único dispositivo**, dentro de um raio de 5 metros. Uma investigação mais profunda revelou que esses motoristas haviam compartilhado múltiplas corridas em um único dia.





Use Cases

Interrompa a falsificação de localização

O que é falsificação de localização?

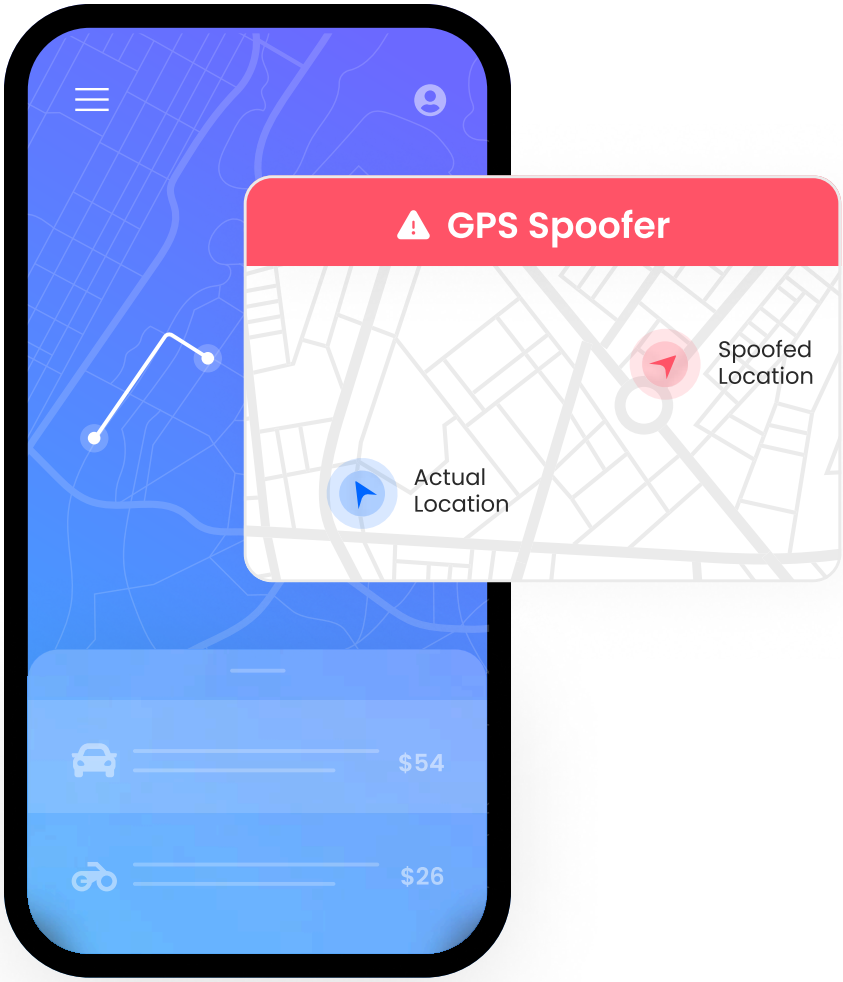
A falsificação de localização acontece quando motoristas manipulam sua posição de GPS utilizando softwares ou técnicas não autorizadas. Isso compromete as operações da plataforma, permitindo que motoristas manipulem preços, burlem regras de trânsito ou adulterem informações das corridas. Localizações falsas podem gerar perda de receita, queda na qualidade do serviço e quebra de confiança entre usuários e a plataforma.

Bloqueie esquemas de motoristas

Esquemas fraudulentos de motoristas exploram as plataformas de mobilidade para inflar ganhos por meio de fraudes coordenadas. Ao interromper a falsificação de localização, você garante uma competição justa entre motoristas, promovendo um ecossistema mais íntegro.

Ofereça experiências seguras para os usuários

Proteja os usuários contra motoristas fraudulentos e garanta informações corretas sobre viagens, preços e confiabilidade. Isso fortalece a confiança entre sua plataforma e os usuários, criando uma experiência segura e transparente.



Use Cases

Elimmine abuso de promoção

O que é abuso de promoção?

Os fraudadores podem criar diversas contas falsas para se aproveitar de códigos de cadastro de novos usuários e de indicações. Esse tipo de fraude distorce os esforços de marketing da plataforma, gerando perdas significativas de receita e reduzindo a efetividade dos programas legítimos de indicação.

SHIELD Fraud Intelligence

Clonador de apps
Emuladores
Reset de fábrica
Dispositivos com jailbreak
Apps manipulados
Auto-clicker

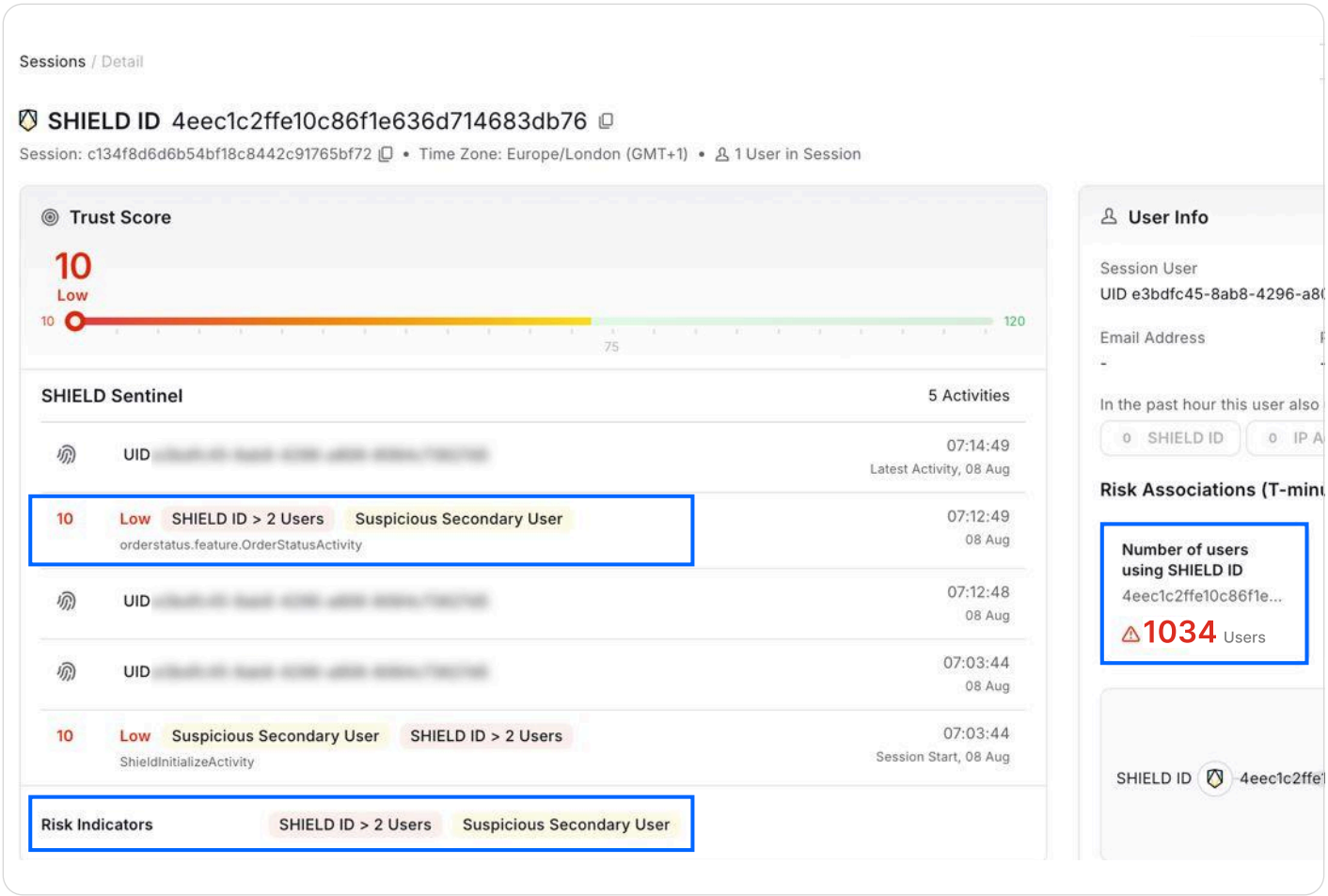
How it Works

Eles criam múltiplas contas em larga escala com o uso de identidades roubadas, aplicativos manipulados, clonadores de apps e emuladores.

Normalmente, utilizam essas contas falsas para:

- Aproveitar bônus de cadastro para novos usuários
- Explorar códigos de indicação referindo contas que eles mesmos controlam
- Resgatar várias vezes viagens grátis ou cupons promocionais em contas diferentes

A SHIELD identifica dispositivos vinculados a múltiplas contas de usuários por meio do SHIELD Device ID e detecta as ferramentas usadas pelos fraudadores para automatizar e escalar esse processo.



*Todos os dados foram randomizados