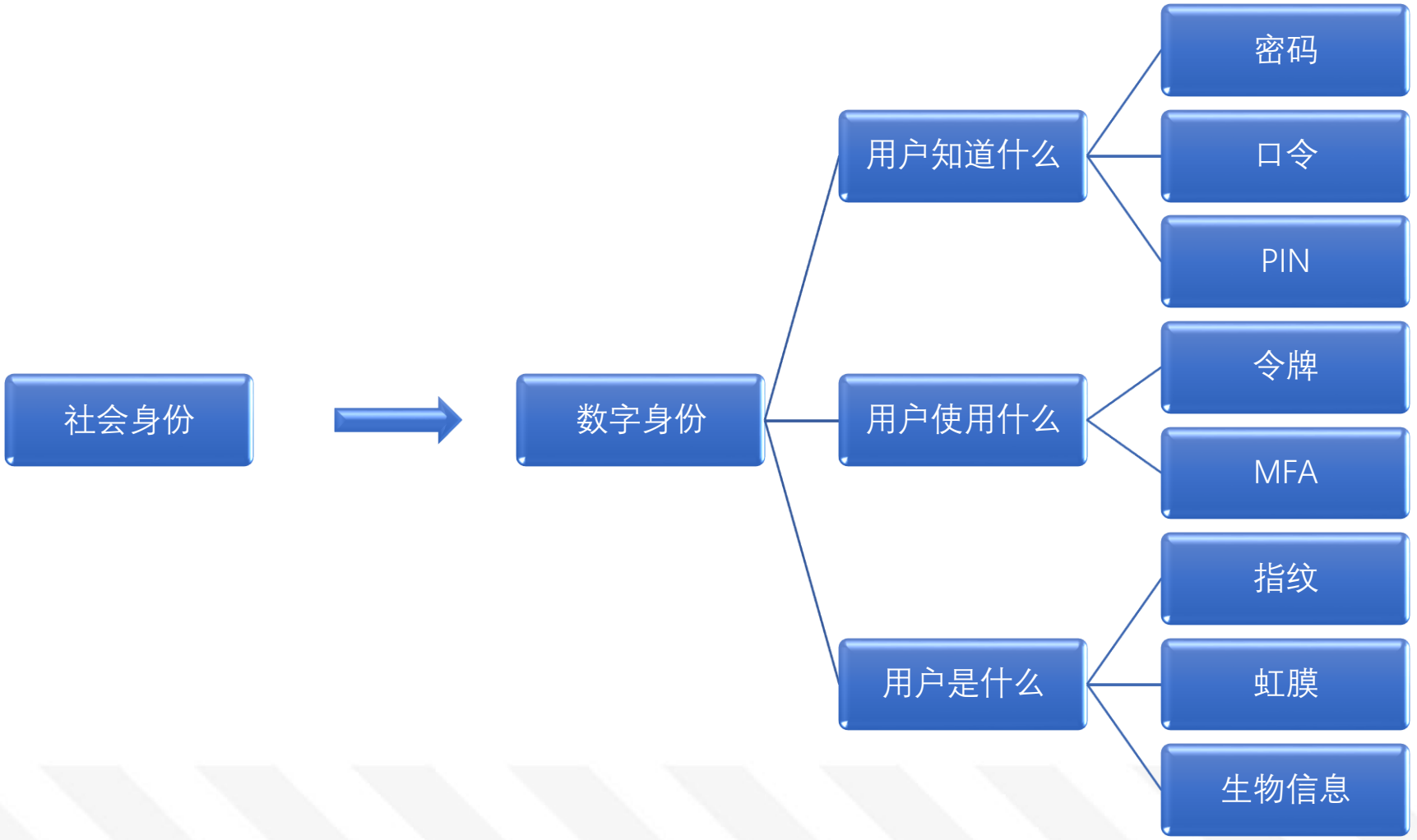
网络安全创新大会
Cyber Security Innovation Summit

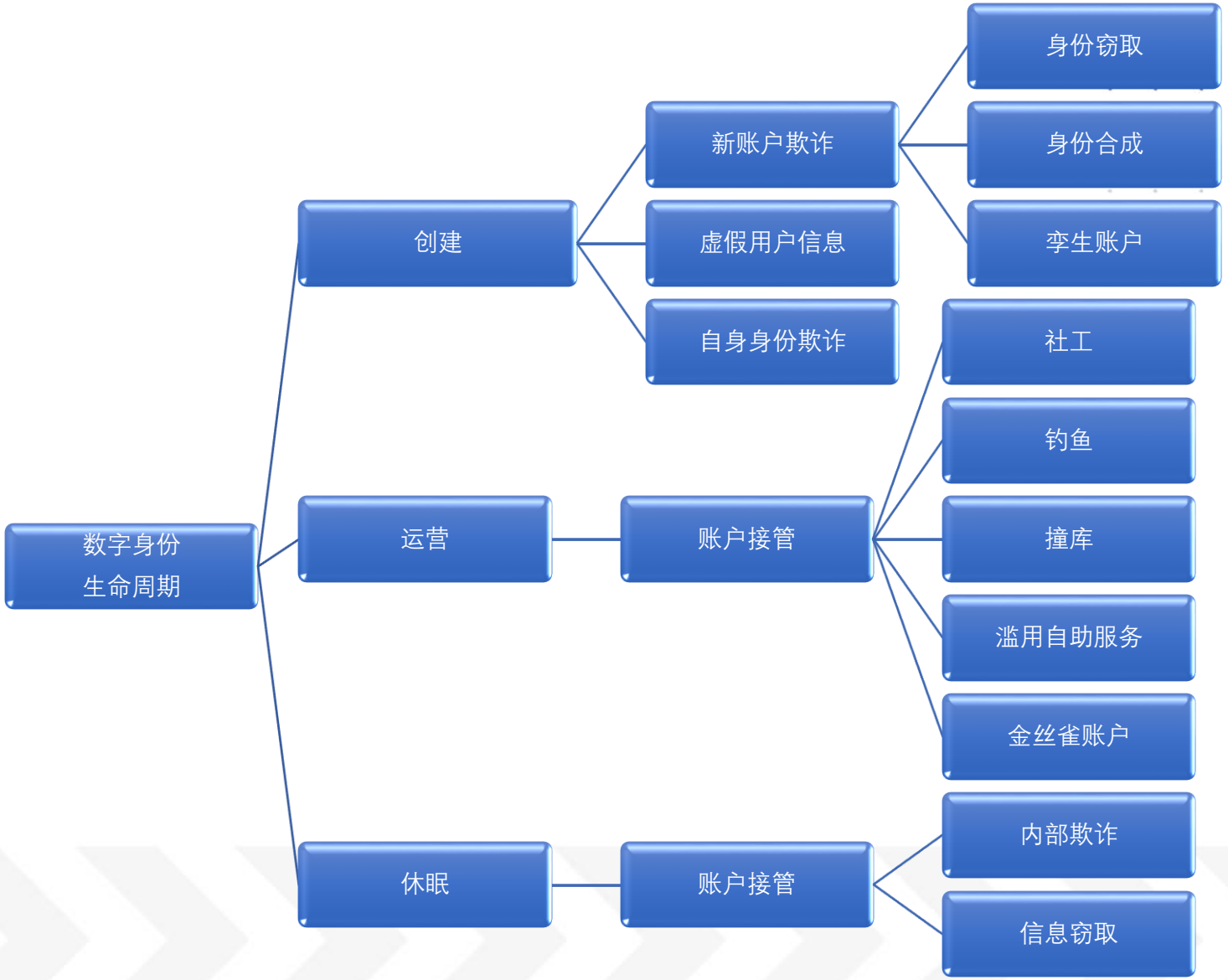
设备指纹与闭环AI防欺诈引擎

陈玉奇 F5亚太区安全架构师

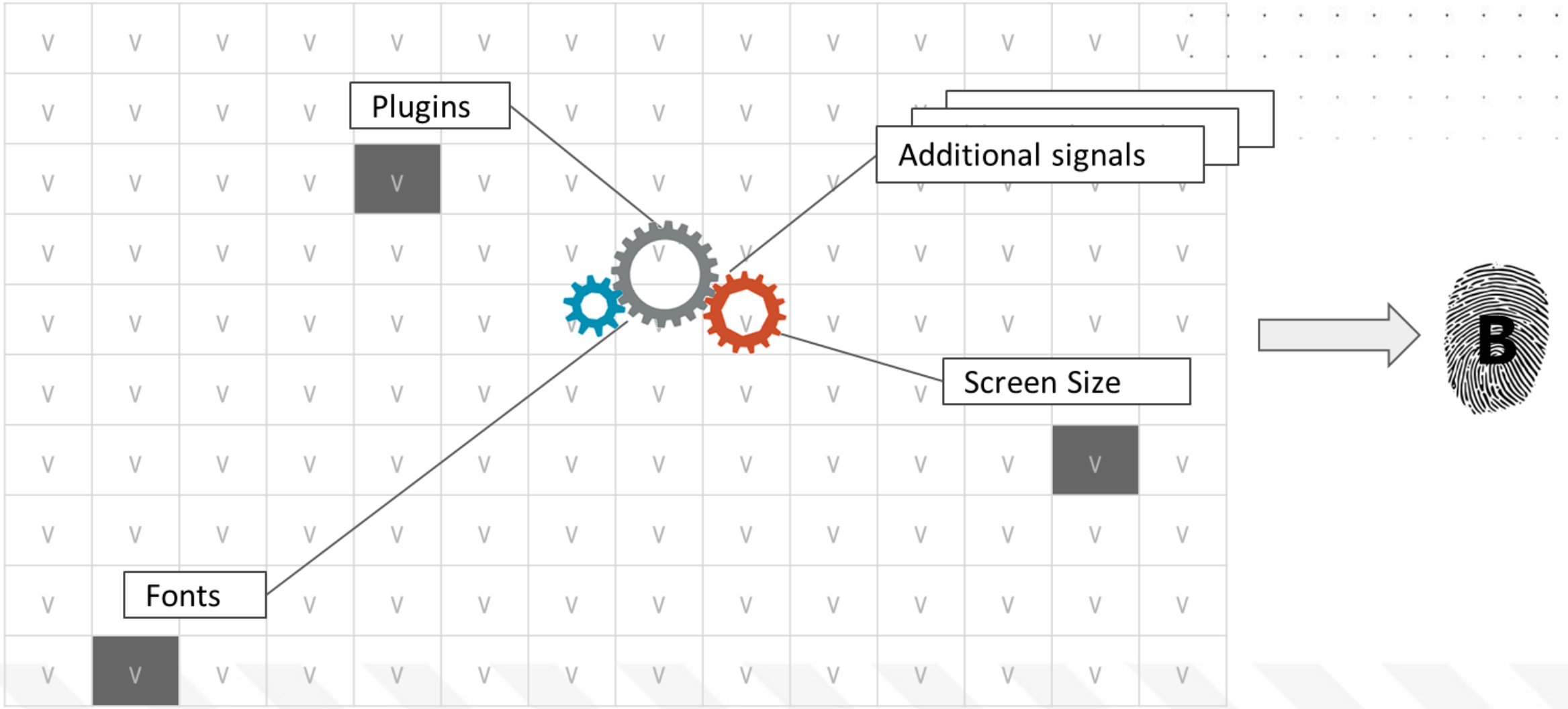
数字身份凭证



数字身份凭证生命周期安全挑战



数字身份和设备指纹



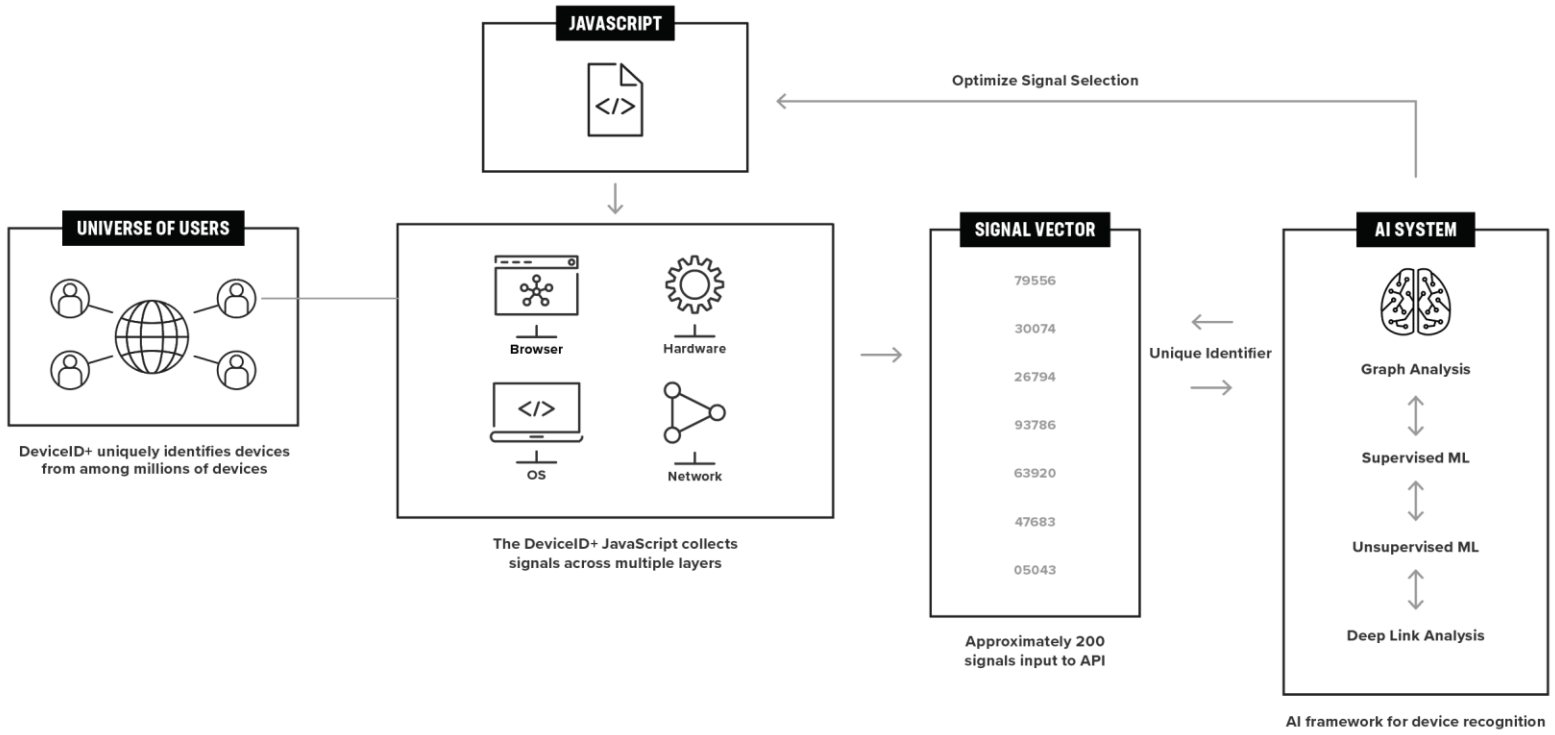
设备指纹形成

主动遥测信息收集 + 被动信息内容收集 = 设备指纹

JS模糊处理 + VM字节随机化 = 机密性与完整性

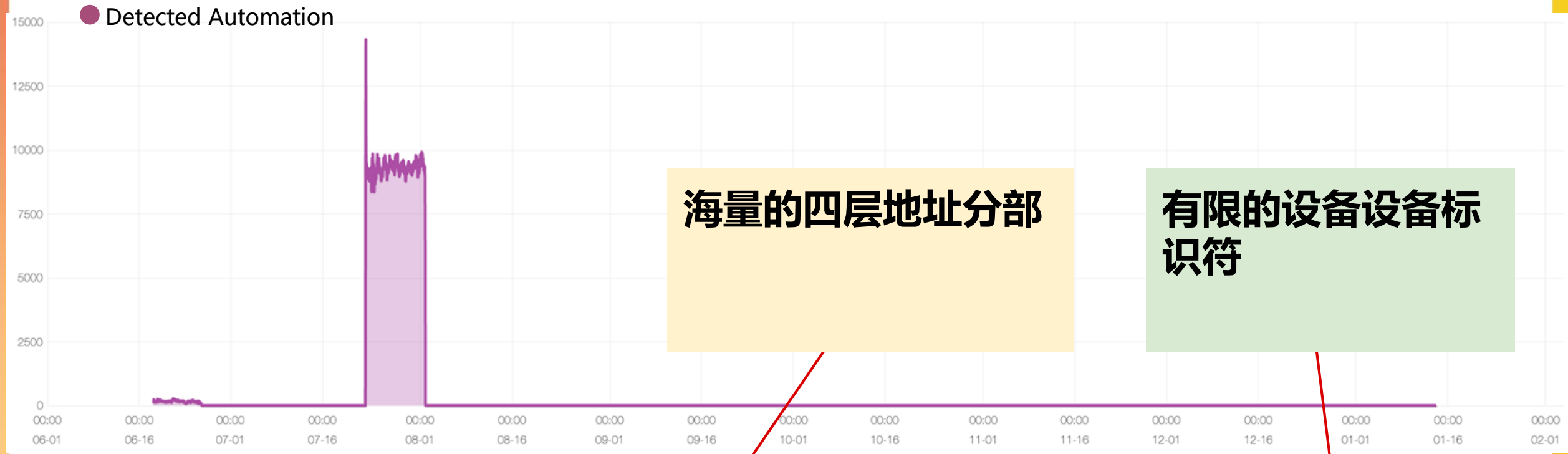
多维度设备信息收集 + 数据信息提炼和维护 = 唯一性

AI/ML信号提炼，消除杂音 + 海量数据增强 = 增加精确性



有趣的案例

网络安全创新大会
Cyber Security Innovation Summit



海量的四层地址分部

有限的设备设备标识符

2.2M
Post请求数

629K IPs　**9K** 网络域　**1** 国家

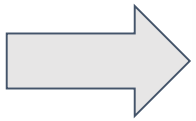
2
设备指纹

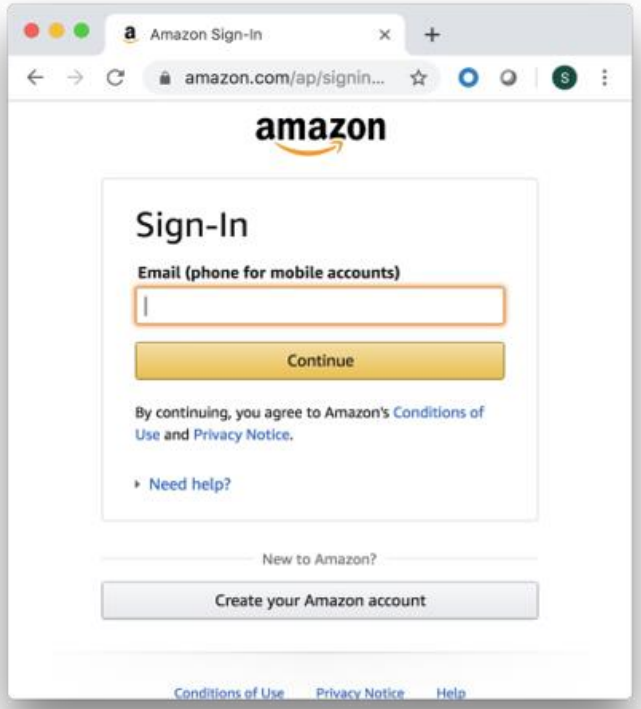
设备指纹 —— 用户分组

User1 = 合法用户

User2 = 欺诈者

User3 = 恶意自动化程序





通过设备指纹输入SIEM去区分不同用户，并且赋予不同安全策略 （零信任最佳实践）

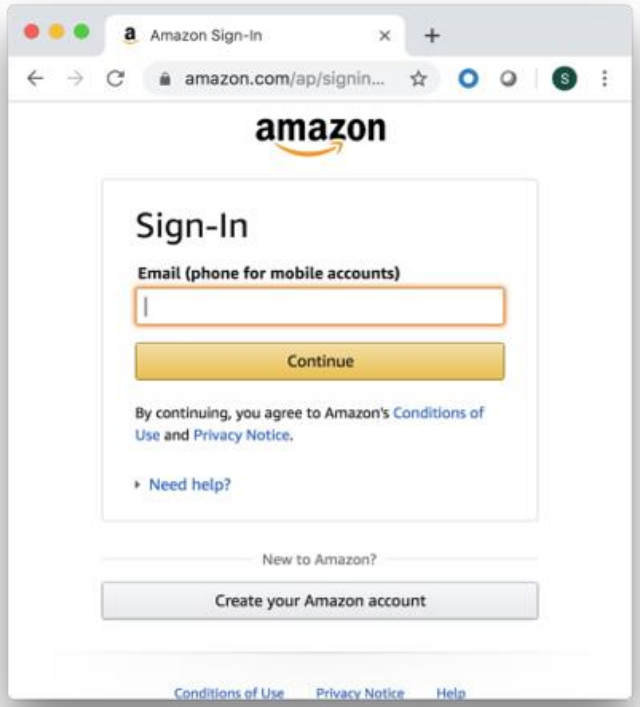
设备指纹 —— 快速用户登录

User1 = 合法用户

User2 = 欺诈者

User3 = 恶意自动化程序

有针对性性阻断



降低用户登录难度，减少可能出现的失败和欺诈

防止“记住我”的客户端登录风险，扩展合法用户会话

防欺诈更多应该解决的问题

你是人类用户么?

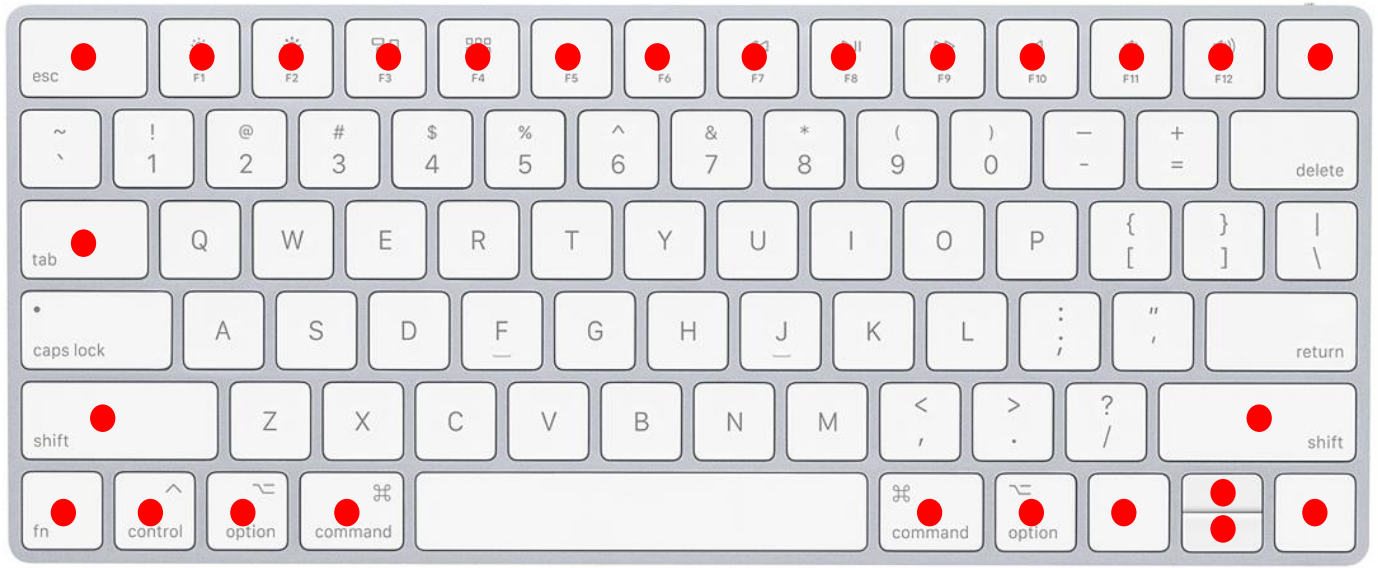
你是你宣称的这个人么?

你是好人还是坏人?

某些用户行为指标

49% **0.6%**

不常见的按键使用



但是单一指标很高的FP/FN，需要ML/AI来降噪

用户行为数据	欺诈者	正常用户
用户名口令的复制粘贴	42%	2%
地址信息粘贴	52%	3%
更高的按键之间的时长	44%	13%
登录页面的时长	52%	17%
Cookie变化时间更短	55%	24%
至少一项可疑设备信息	16%	7%
更高的多账户访问行为	Yes	No

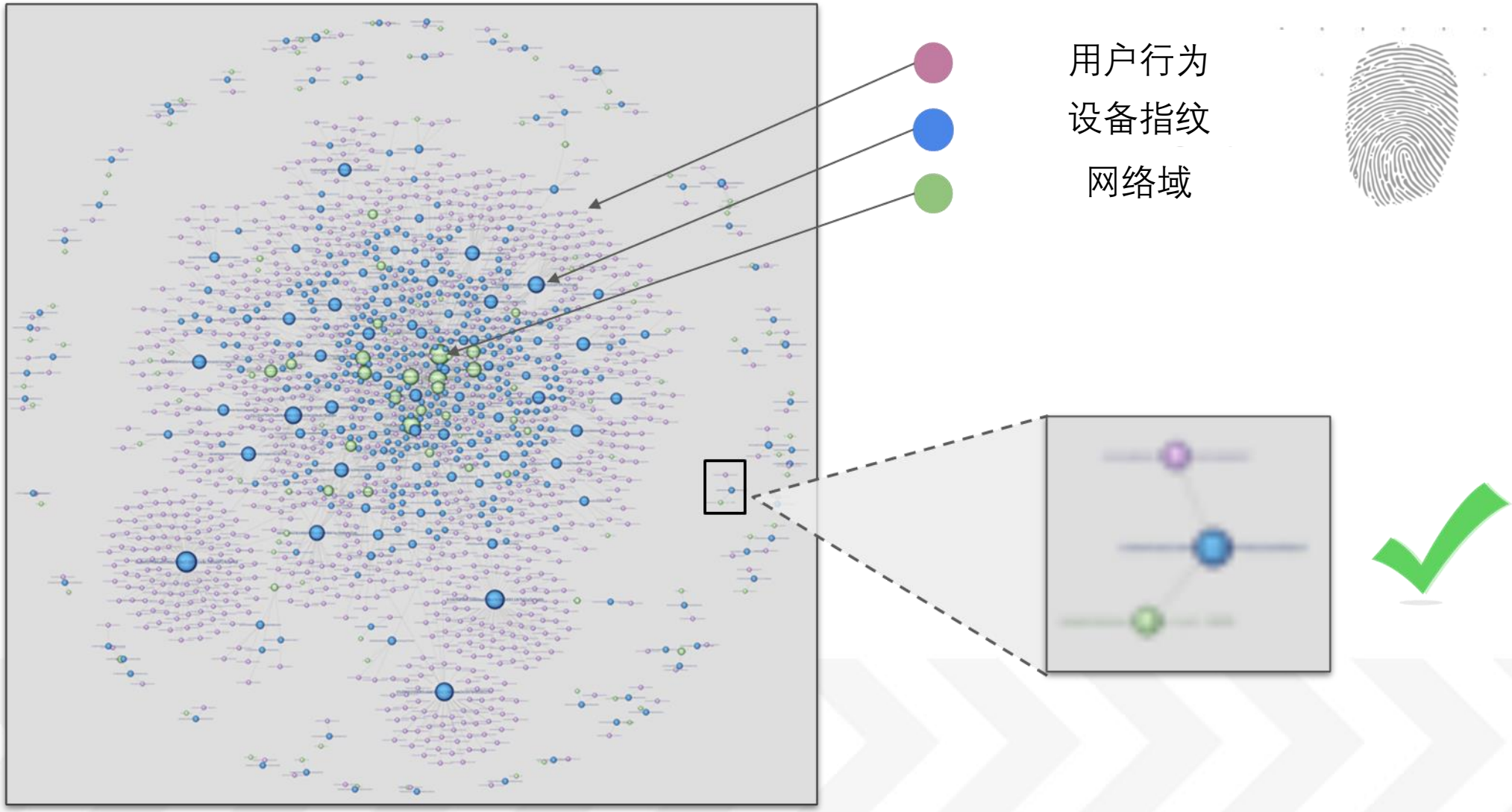
用户行为复合指标

Blue Bar	Key-down.
Orange Bar	Key-up.
Red Circle	Mouse-click.
Green Tick	Captured mouse event.
Dashed Line	High speed movement between two points.
Brown Square	Long pause.
Grey Line	Transition from non-mouse event to mouse event.

Key-down, key-up events

Mouse events & Mouse click

AI聚合分析

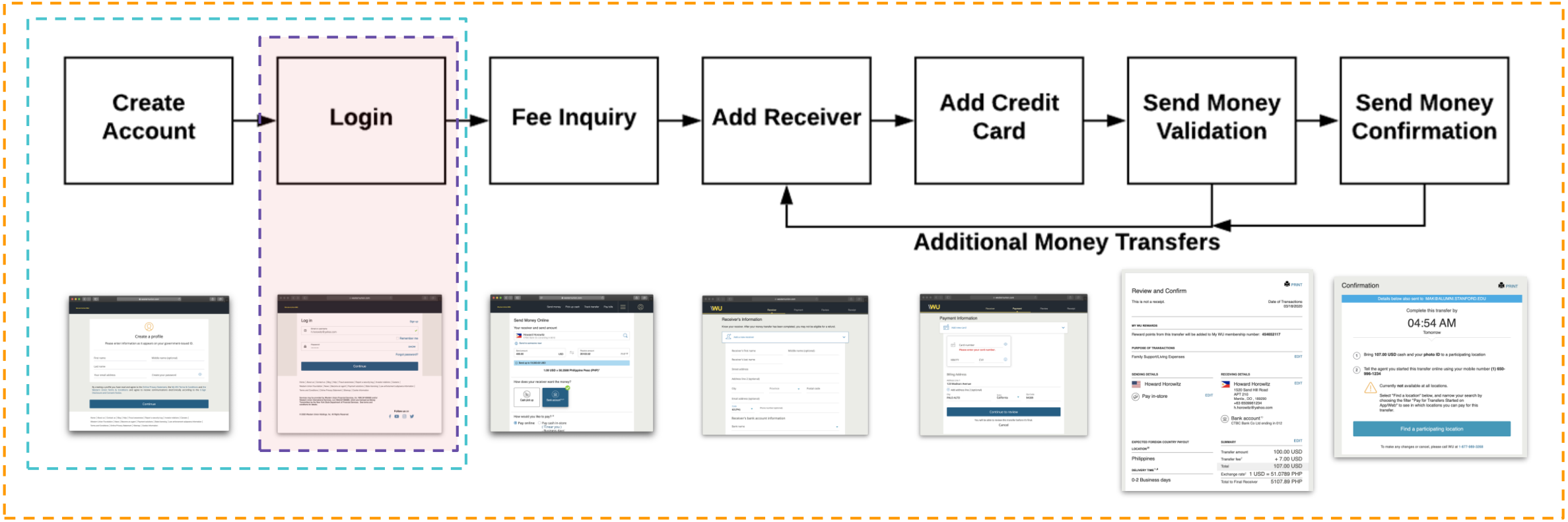


用户行为

设备指纹

网络域

实现全流程闭环的防欺诈引擎

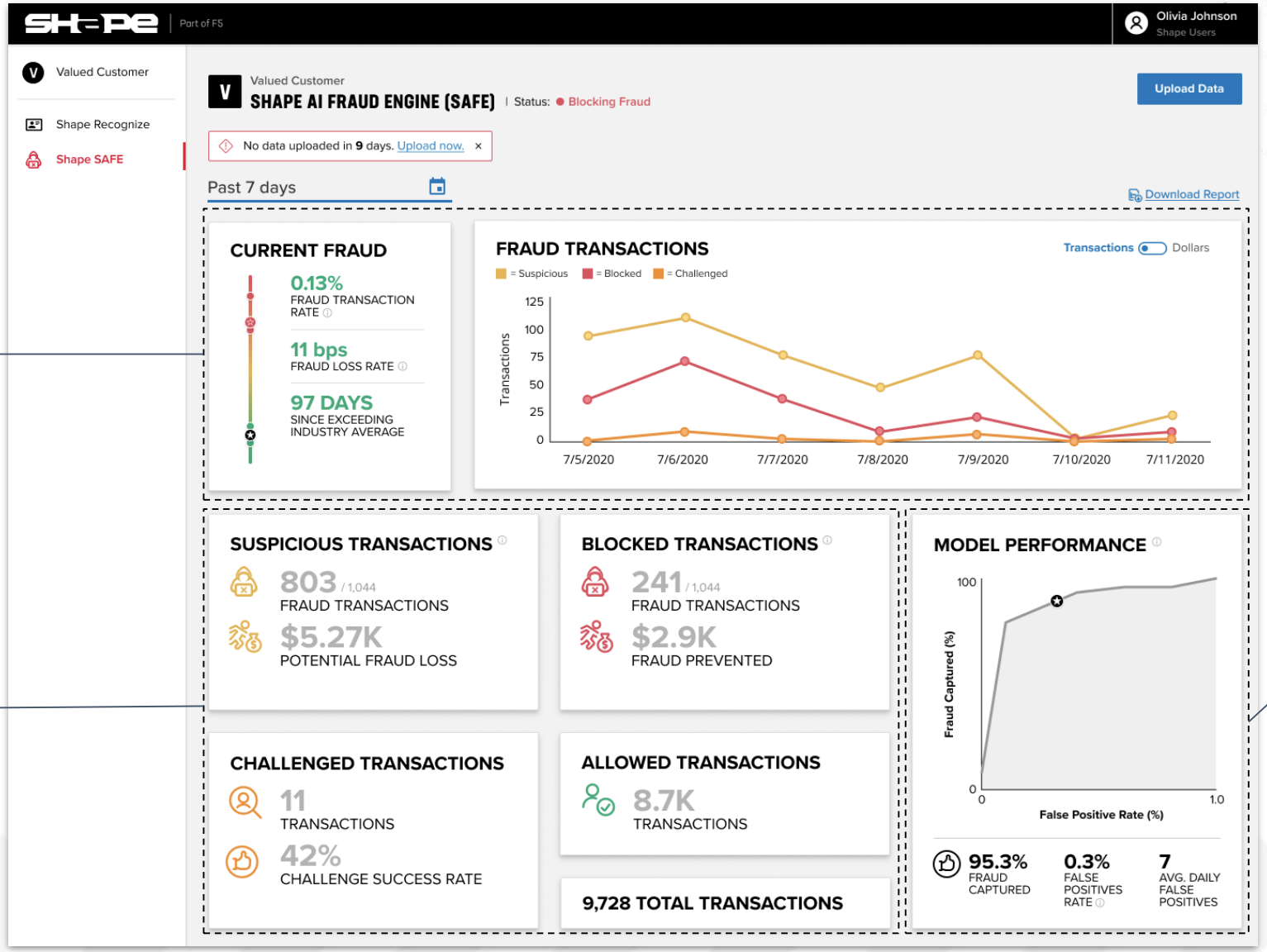


机器人还是人类? **你是你所声称的人么?** **你是好人还是坏人?**

有预测、有现状、有收益

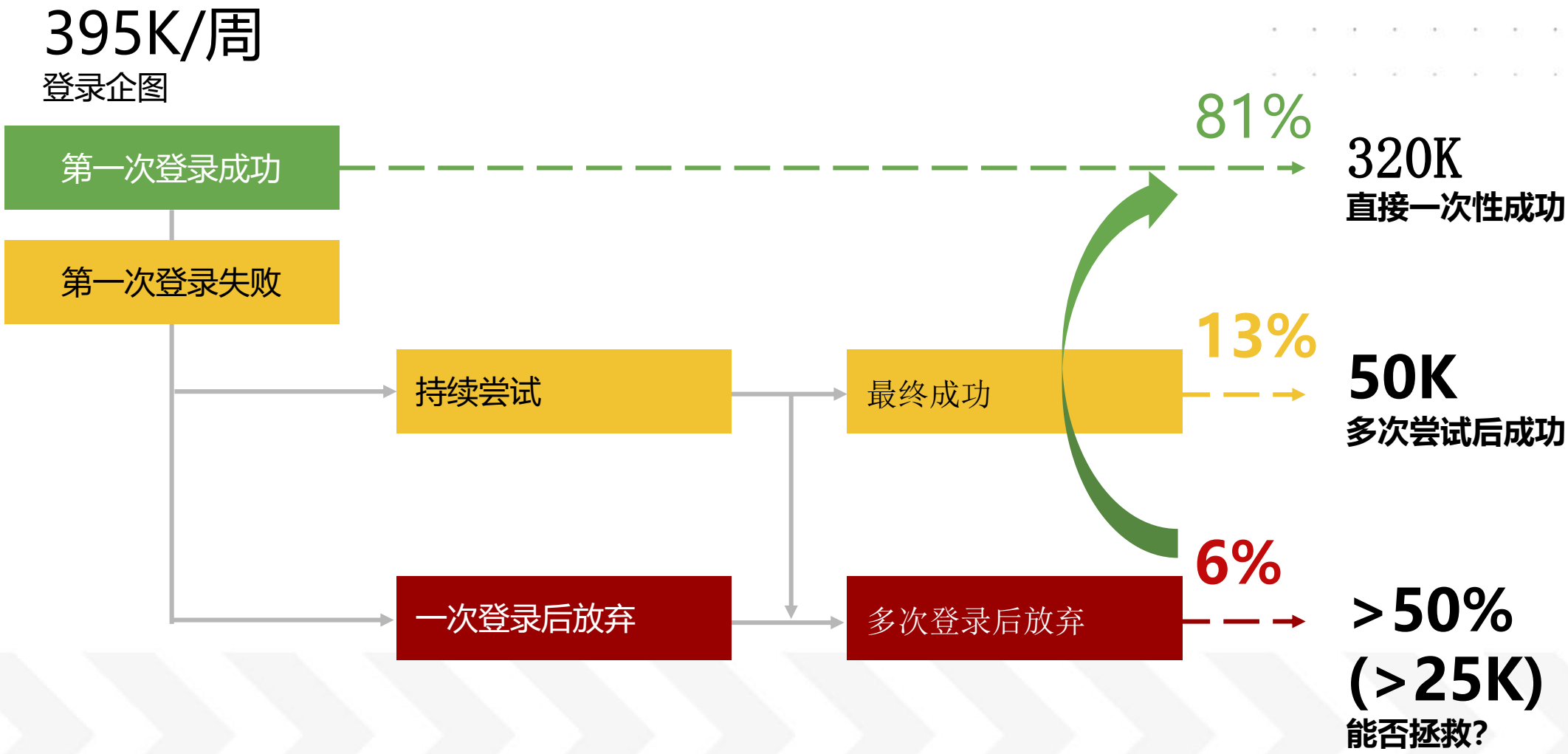
•1、当前的被欺诈级别

•2、建议采取的措施



3、到底防止多少欺诈，挣了多少钱

题外话 —— 识别登录在闭环中的价值



网络安全创新大会
Cyber Security Innovation Summit

THANKS