UEBA在企业安全中的实践

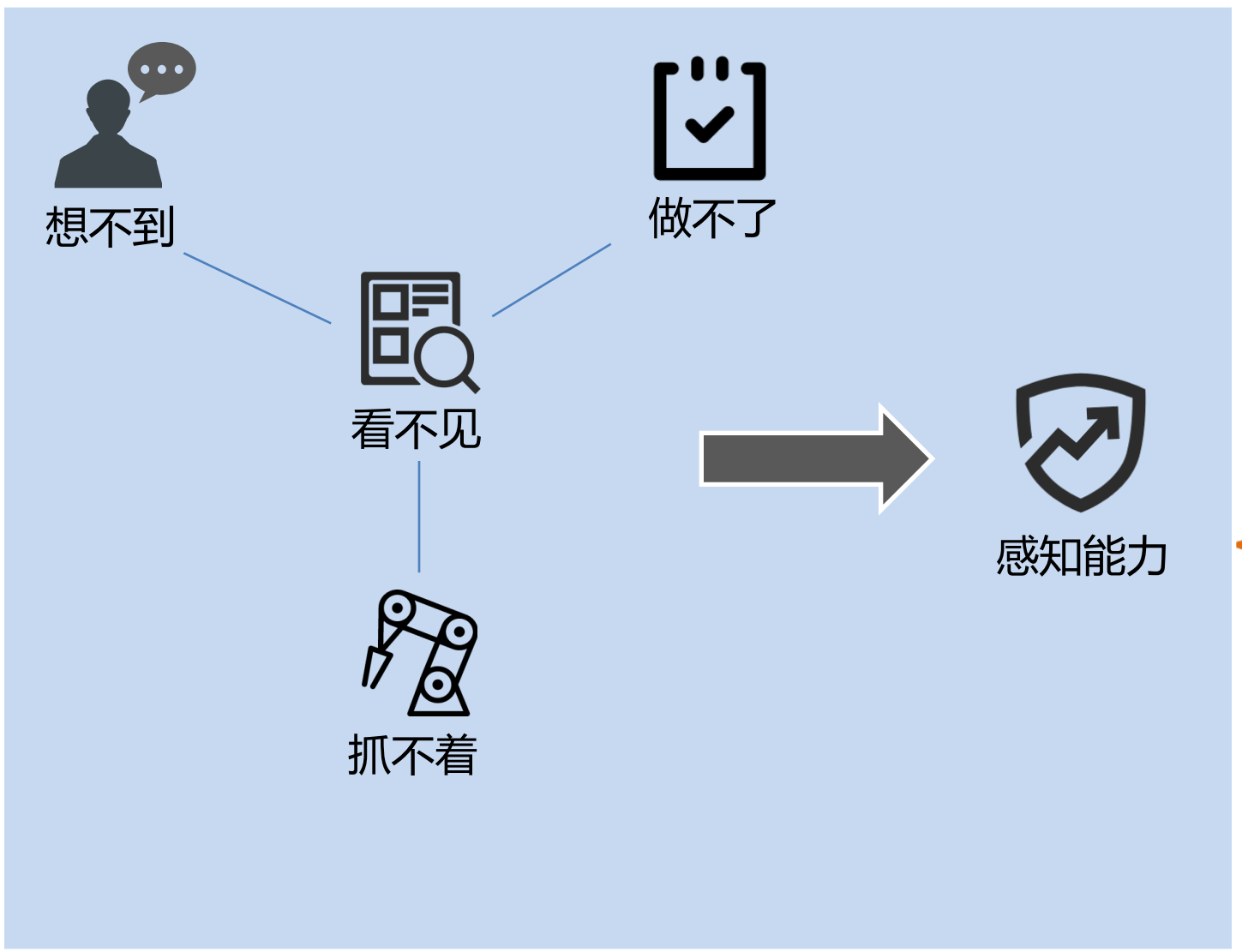
数据驱动，AI赋能

陈建

2018年4月

企业信息安全的风险关注点

- 交易欺诈风险
- 黑客攻击风险
- 员工操作风险
- 数据泄密风险
- 法律合规风险
- 人员/组织风险



- 基础安全能力
- 安全运营能力
- 可视化能力

企业信息安全的技术全景图

什么是UEBA（User and Entity Behavior Analytics）

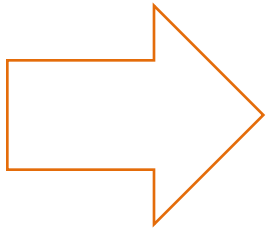
UBA

分析用户点击、购买等行为

智能推荐

标签画像

机器学习



UEBA

终端

应用

系统

基线

社交

网络流量

网络设备

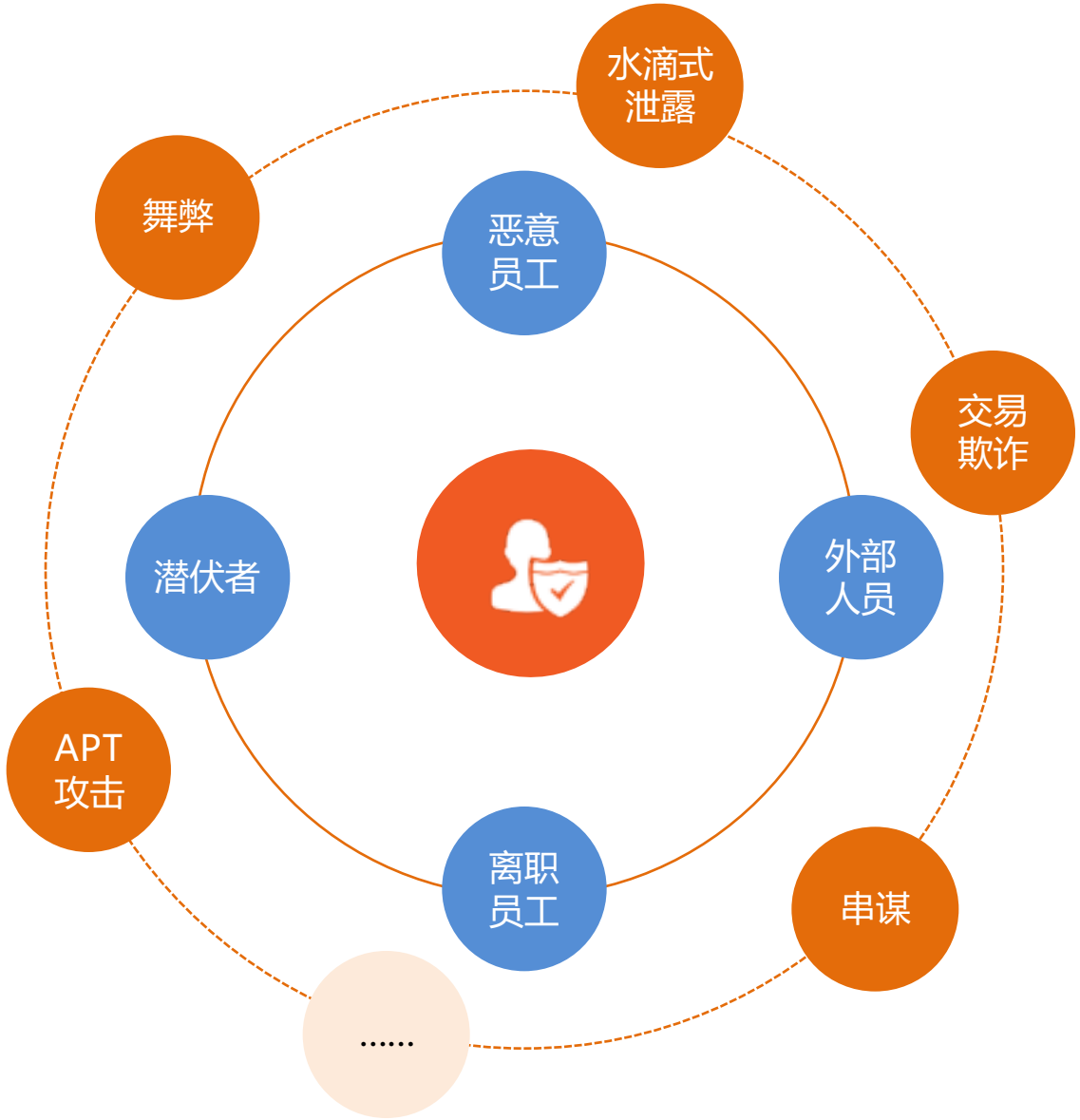
数据库

画像

机器学习/AI

UEBA适用的风险场景

- 内部渗透风险
- 员工舞弊风险
- 交易欺诈风险
- 数据泄露风险



员工风险感知平台

应用层

事件处理 | 员工风险看板 | 图关联搜索 | 可视化报表

智能决策响应 | 实时监控和预警 | **智能 实时 动态** | 案件库 | 证据保全

- 对安全事件、员工操作风险、业务风险进行可视化预警，支持定制化管理

分析层

实时分析层	离线分析和查询	离线模型平台	基础服务
实时计算	ES日志平台	Spark	黑/白/灰名单
规则管理	Zeeplin	机器学习Mlib	风控锁
规则引擎			
模型平台			

- 告警规则/模型、风险预警模型
- 引入AI，预警智能化
- 支持实时和离线分析

数据层

员工基础数据	终端数据	系统和应用数据	画像
• 员工信息	• 邮件记录	• 员工权限	• 员工画像
• 就职信息	• IM记录	• 堡垒机日志	• 系统画像
• 考勤	• 上网行为记录	• 应用访问日志	
• 岗位信息	• USB读写记录	• 网络异常流量	
• 职场信息	• HDLP日志	• 业务埋点日志	
• 基线考核	• 打印记录	• 数据库访问日志	
• 行为轨迹	• 进程信息		
• 社交关系网	• 浏览器日志		

- 建立可扩展的数据安全日志平台
- 收集包括不仅限于终端、系统、网络和应用等方面的全方位数据

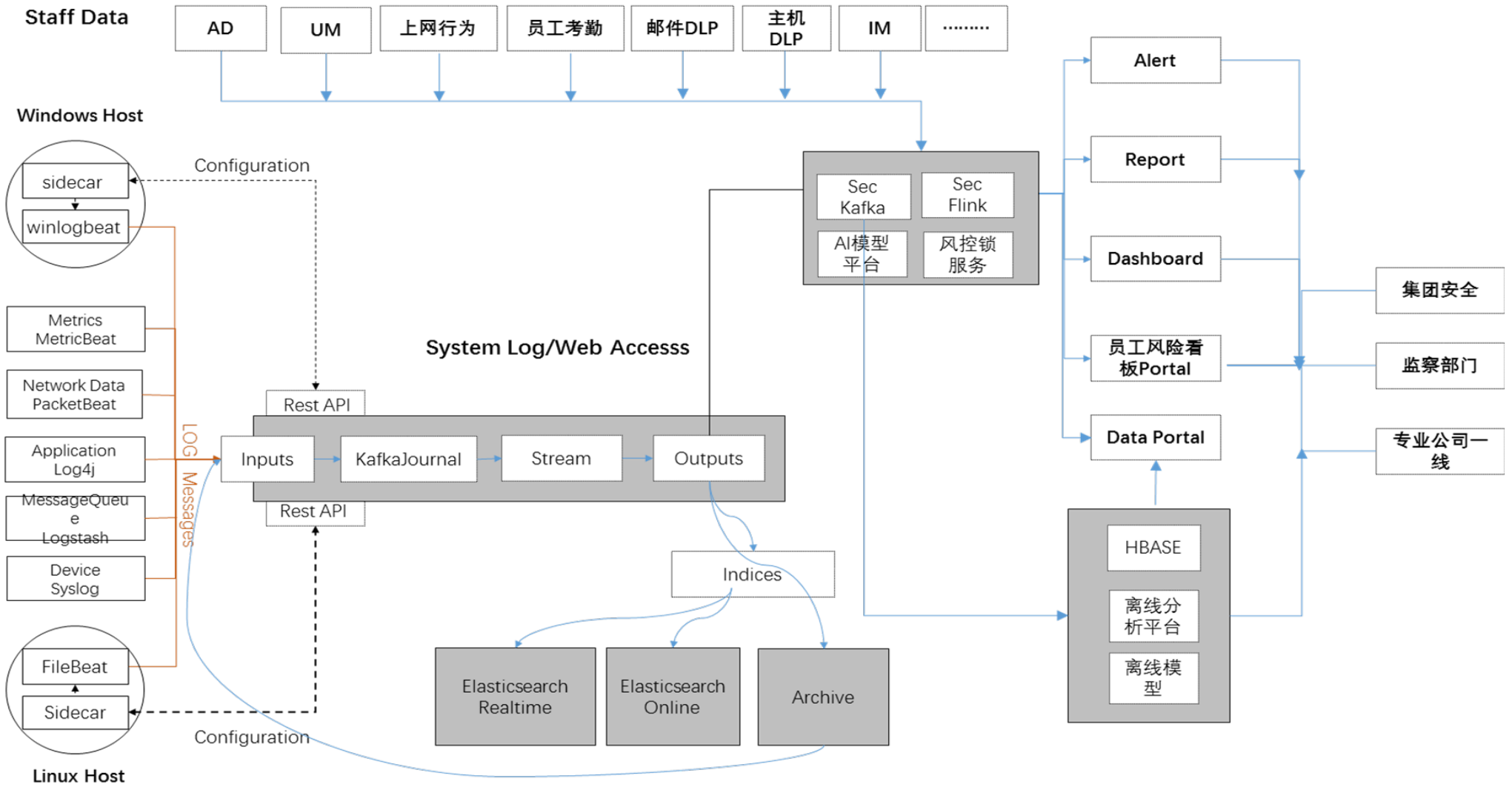
控制层

人脸识别 | 账号认证 | 权限管理 | 终端DLP | 邮件DLP | 上网行为管控 | USB管控

门禁 | 双因素认证 | 离职员工管理 | 打印管理 | IM监控 | EDR | 远程访问管控

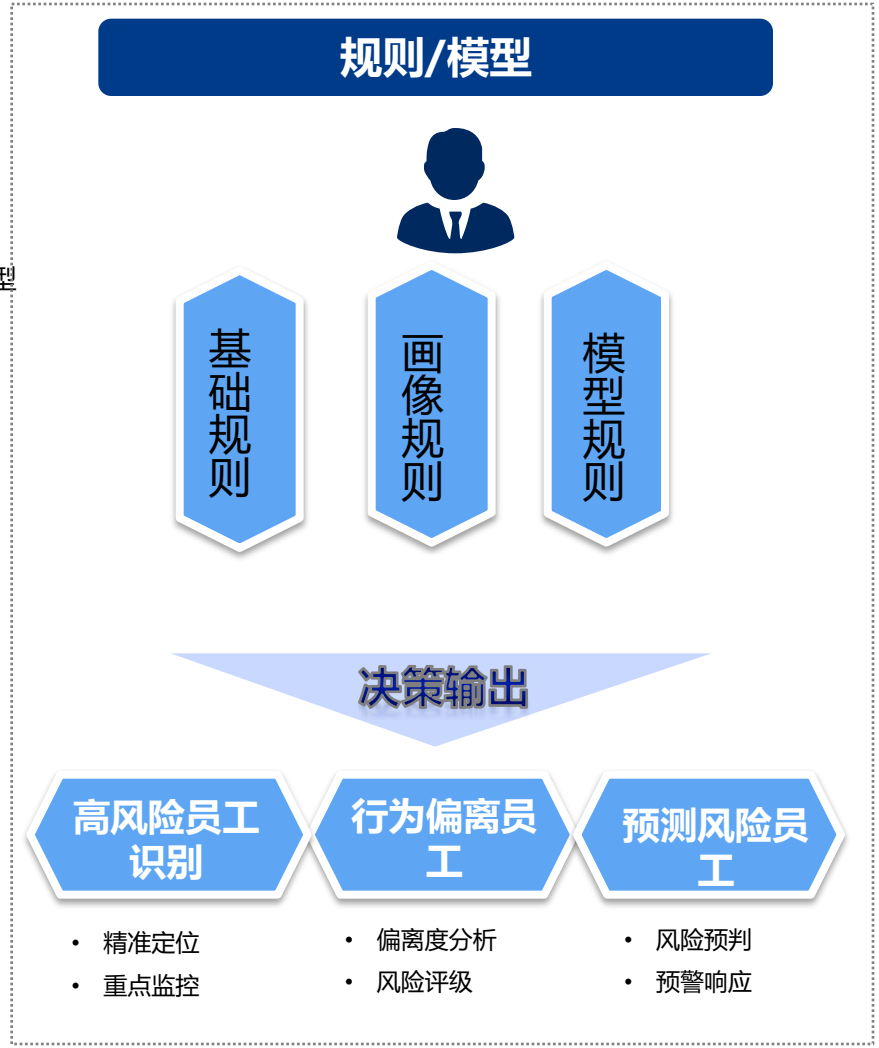
- 通过终端、网络等各层的安全控制能力进行数据收集和实时响应

技术架构


Staff Data
AD
UM
上网行为
员工考勤
邮件DLP
主机 DLP
IM
.....
Windows Host
sidecar
winlogbeat
Configuration
Metrics MetricBeat
Network Data PacketBeat
Application Log4j
MessageQueue Logstash
Device Syslog
FileBeat
Sidecar
Linux Host
LOG Messages
System Log/Web Accesss
Rest API
Inputs
KafkaJournal
Stream
Outputs
Rest API
Indices
Elasticsearch Realtime
Elasticsearch Online
Archive
Sec Kafka
Sec Flink
AI模型平台
风控锁服务
Alert
Report
Dashboard
员工风险看板Portal
Data Portal
HBASE
离线分析平台
离线模型
集团安全
监察部门
专业公司一线

基于数据和模型，实时、智能识别“风险”员工

Logistic模型
数据挖掘
深度学习
聚类算法
神经网络
迁移学习
关联分析
……

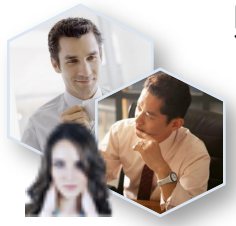


应用场景示例，依据风险等级智能决策并启动响应机制

员工信息泄露动机： 离职跳槽
风险识别：具有离职倾向的员工风险识别方法

A员工

司龄——18个月
性别——男
职级——专员
考勤——朝九晚六，上下班准时
上网行为-关注内容-招聘相关
绩效考核-绩效评级D
日常工作习惯-朝九晚六，不爱加班
近期：开始加班
权限：申请开通USB、外发邮件权限
常用设备：借助其他员工设备登陆账号
系统访问：登陆系统频率超出日常习惯、频繁访问客户信息相关页面；



账号风险-账号共享/账号盗用

- 同一账号当天内被不同IP成功登陆
- 同IP访问不同AD/UM账号
- 该账号在“新设备上”登录
- 账号在“非常工作职场”、“非所属专业公司”的登录
- AD账号通过外网IP登陆的监控等

规则引擎

动态决策

智能决策

实时响应

Risk Score：95
High risk

- 账号冻结、权限控制
- 预警+风险核查
- 业务系统整改

数据交互、报告通知、监控优化

平台原型（1/4）

风险大盘

员工风险看板

风险事件

员工行为轨迹

UEBA的那些“坑”

基础数据的“脏、乱、差”

传说的高大上，UEBA严重依赖高质量的数据，企业需要有数据治理的基础，有统一的数据字典

技术选型的复杂

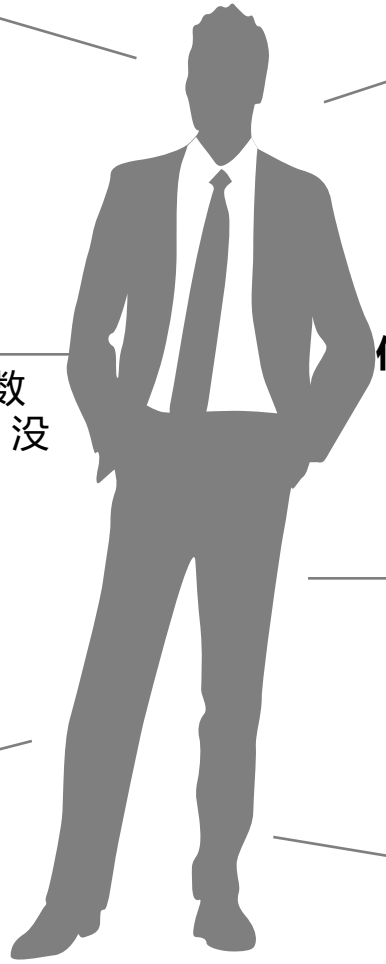
绞尽脑汁做出的技术选项，却经常屈服于数据本身的时效性

基础架构能力的缺失

说说你到底要多快，可靠高性能的大数据平台是UEBA依赖的核心基础设施，没有它就是一堆死数据

权限控制的痛苦

你说谁可以看，集团范围的推广尤其要平衡各方面的利益



业务和安全的博弈

和业务部门偶尔好基友，经常小冤家，**磕磕绊绊，相约到老**

脆弱的运营能力

想说爱你不容易，运营能力是风控系统能发挥作用的核心所在，规则和模型需要调优，案件需要反馈

商业安全产品的不开放

理想丰满，现实骨感，厂商产品的开放性是个大问题

平安慧安全

谢 谢