基于ML的用户风险识别技术与应用

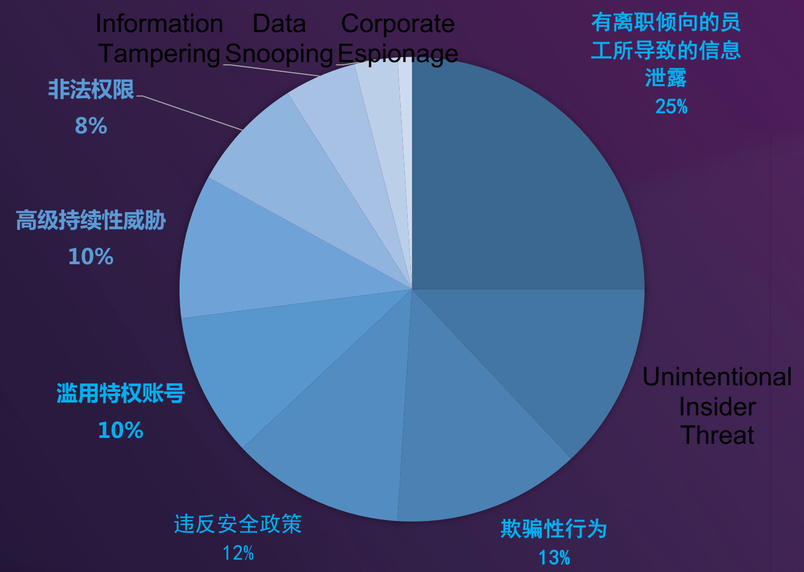
陈建

平安集团 首席信息安全官

2019年8月30日

2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

企业内部：用户行为风险领域



UEBA: 适用的风险场景

2019世界人工智能安全高端对话

2019 High-level Dialogue on World AI Security

2019世界人工智能安全高端对话

2019 High-level Dialogue on World AI Security

Skyeye-UEBA实时预警员工风险平台

2019世界人工智能安全高端对话

2019 High-level Dialogue on World AI Security

应用层

事件处理 | 员工风险看板 | 智能 实时 动态 | 图关联搜索 | 可视化报表

智能决策响应 | 实时监控和预警 | | 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

实时引擎层			离线分析和查询	离线模型平台	基础服务
实时计算引擎	实规则引擎	实时模型引擎	ES日志平台	Spark	黑/白/灰名单
专家规则库	员工特征库		Zeeplin	机器学习Mlib	风控锁

- 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
考勤	上网行为记录	应用访问日志	系统画像
职场信息	HDLP日志	业务埋点日志	
行为轨迹	进程信息	数据库访问日志	
就职信息	IM记录	堡垒机日志	
岗位信息	USB读写记录	网络异常流量	
基线考核	打印记录		
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

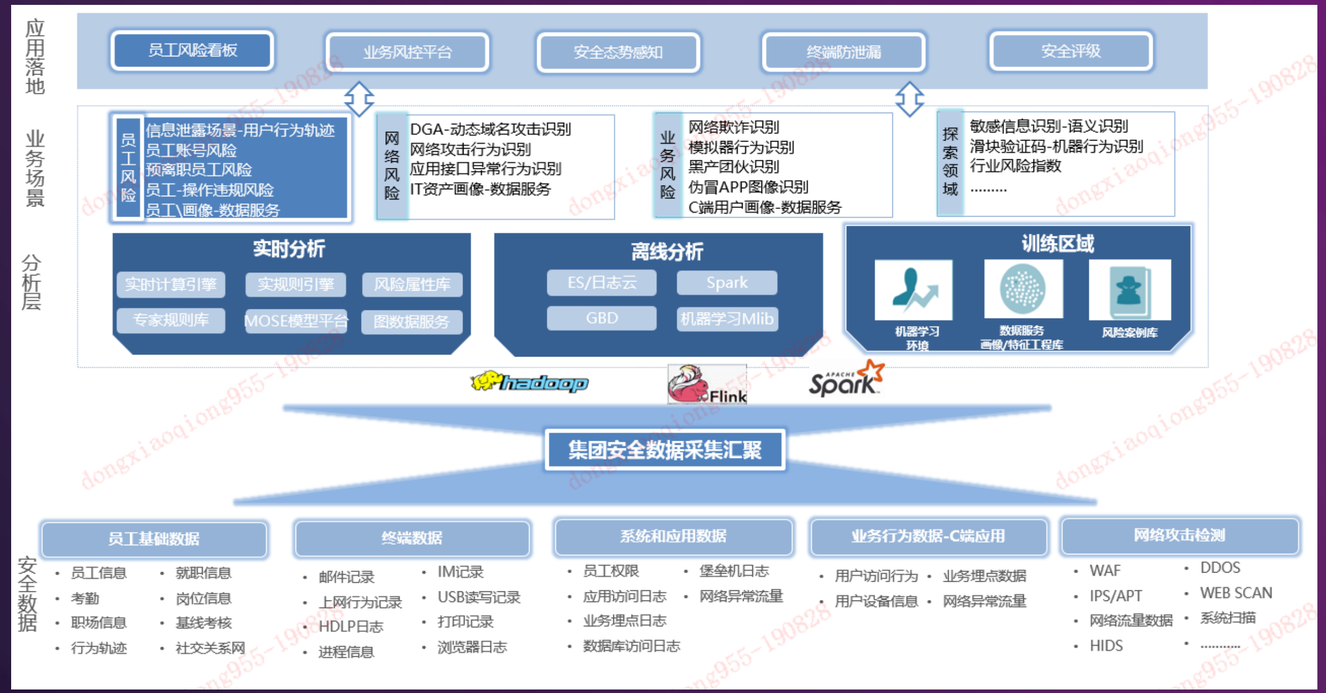
门禁 | 双因素认证 | 离职员工管理 | 打印管理 | IM监控 | EDR | 远程访问管控

- 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

2019世界人工智能安全高端对话

2019 High-level Dialogue on World AI Security

平安集团信息安全AI实践



WAIC 2019世界人工智能大会 WORLD ARTIFICIAL INTELLIGENCE CONFERENCE

2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

终端运营演进路线与挑战

<20 风险用户
历史负样本积累

终端运营1.0

- 30+ 专业公司 业务形态差异
- 30万+ 员工
- 600+ 员工操作场景
- 10T+ 员工行为数据/每天
- 15+ 终端测 安全认证、管控工具
- 1M+ 事件预警
- 8 终端运营工程师

终端运营2.0

- 1 监控产品
- 800+ 线上检测规则
- 2000+ 事件预警量 /每日
- 4000+ 拦截风险预警 /半年

终端运营3.0

- 1000- 事件“准确”预警量<1000
- 30万+ 员工如何工作？异常行为是什么？
- 800+ 规则更新效率-能提升吗？

WAIC 2019世界人工智能大会 WORLD ARTIFICIAL INTELLIGENCE CONFERENCE

2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

WAIC 2019世界人工智能大会 WORLD ARTIFICIAL INTELLIGENCE CONFERENCE

2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

用户风险场景-模型分析尝试

UEBA

人力相关数据	AD/UM数据	业务访问数据
上网数据	终端采集：HDLP数据	

实施方向及模式

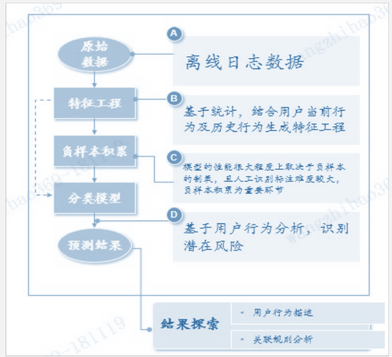
定位导向与要求

交流学习：通过与专业公司的业务访谈与沟通交流，学习相关业务逻辑，建立严密的反馈机制，保证模型的持续迭代。

＋

赋能：在实现基本的安全事件预警机制后，赋能给专业公司，使得专业公司建立适合自己业务场景的模型，细化风险类别。

模型流程



利用日志数据结合业务逻辑，识别潜在的员工风险及安全事件

设计规划	目标	**员工风险行为预警**
	达成结果	**实时预测员工风险行为，及时发现安全事件**
	服务对象	**员工风险看板**
	设计理念	**模型可抽象为可复用的方法论**
难点挑战	数据量大	**数据量10T+每天， 数据零散，没有丰富的有效字段**
	用户行为	**用户行为是什么？风险员工行为是什么？**
	业务复杂	**对应的业务系统庞杂，设计涉及 600+**
	无负样本	**历史安全事件为某领域内的个例，不可复用**
解决方案	数据改造	**改造接入日志数据，保证基本字段一致**
	数据处理	**数据预处理流程标准化**
	业务行为	**进行业务访谈，确认敏感行为及业务逻辑**
	样本确认	**无监督+专家研判**

2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

“模型设计”核心思想——可复用

WAIC
2019世界人工智能大会
WORLD ARTIFICIAL INTELLIGENCE CONFERENCE
2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

“模型”进化

无监督模型训练

用户特征/群组特征
访问时间 –访问量/访问间隔/历史访问情况

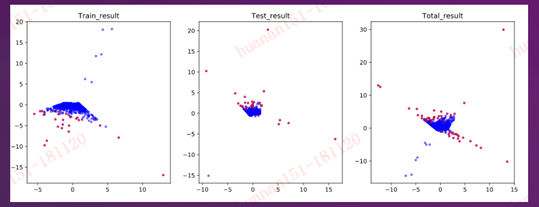
IP-常用IP：IP C段
IP数量访问量等统计
IP C段数量访问量等统计

业务访问特征-
topN：功能节点访问频率/访问量
敏感业务节点：敏感业务节点访问频率/访问量
业务逻辑：特定业务节点-业务逻辑判断
查询/订单操作比率

负样本积累
/反馈

专家研判

用户行为偏离



风险行为：访问频率、访问量超高、IP偏离等

检测结果

用户	时间	访问量	用户历史访问量	群组历史访问量	常用IP C段
G********0	2018-10-09 17	13673	308.54	900	10.66.221

用户	时间	访问量	用户历史访问量	群组历史访问量	常用IP C段
P*******6	2018-10-09 10	4329	6478.58	1749	36.7.110

结果说明

用户G********0于2018-10-09 17时，访问量较大，超过个人历史行为，超过群组历史行为。常用IP C段为：10.66.221

用户P*********6于2018-10-09 10时，访问量较大，超过群组历史行为。存在IP（IP C段）变动情况，常用IP C段为：36.7.110

WAIC
2019世界人工智能大会
WORLD ARTIFICIAL INTELLIGENCE CONFERENCE

2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

特征丰富，补充用户行为属性

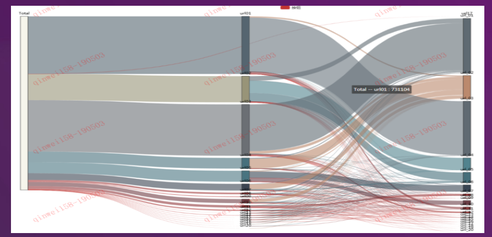
用户行为属性：

员工动机+意愿+能力→ Risk Score

无监督模型训练

特征、正常用户行为探索

用户访问路径



输出形式：<用户需要知道异常是什么?>

用户	时间	描述
S**********0	2019-01-03 15	用户：S**********0于2019-01-03 15时,存在url平均访问量异常，访问量偏离该用户历史行为,访问量偏离该用户所在群组历史行为,等异常行为。
G**********0	2019-01-03 14	用户：G**********0于2019-01-03 14时,存在访问量异常,url访问数量异常,IP频繁变动,访问量偏离该用户所在群组历史行为,等异常行为。
X**********9	2019-01-02 09	用户：X**********9于2019-01-0209时,存在访问量异常,url访问数量异常,IP频繁变动,访问量偏离该用户所在群组历史行为,等异常行为。

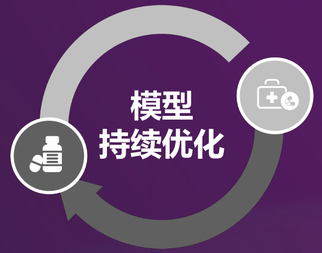
结果输出

用户：S**********0于2019-01-03 15时,存在url平均访问量异常，访问量偏离该用户历史行为,访问量偏离该用户所在群组历史行为,等异常行为。

用户：G**********0于2019-01-03 14时,存在访问量异常,url访问数量异常,IP频繁变动,访问量偏离该用户所在群组历史行为,等异常行为。

用户：X**********9于2019-01-0209时,存在访问量异常,url访问数量异常,IP频繁变动,访问量偏离该用户所在群组历史行为,等异常行为。

“模型”进化

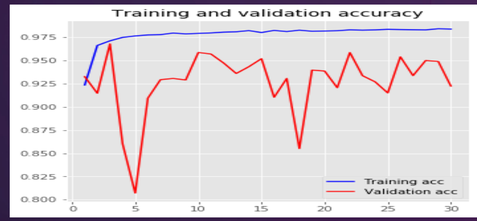


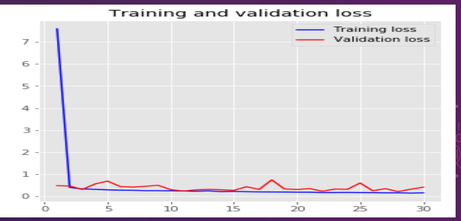
无监督模型训练

有监督模型训练

		预测		
实际		1	0	合计
	1	30	3	33
	0	0	53630	53630
	合计	30	53633	53663

计算指标	指标说明	指标结果
AccuracyRate	准确率= (TP+TN)/(TP+TN+FN+FP)	99.9%
ErrorRate	误分率=(FN+FP)/(TP+TN+FN+FP)	0.1%
Recall	召回率=TP/(TP+FN)	90.9%
Precision	查准率=TP/(TP+FP)	99.9%





WAIC 2019世界人工智能大会 WORLD ARTIFICIAL INTELLIGENCE CONFERENCE
2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

数据处理/特征工程-通用化

WAIC 2019世界人工智能大会 WORLD ARTIFICIAL INTELLIGENCE CONFERENCE

2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

模型结果-可解释性

输出形式：识别异常用户并提供一定的风险描述

用户	时间	描述
SU********0	2019-01-03 15	用户：SU********0于2019-01-03 15时,存在url平均访问量异常，访问量偏离该用户历史行为,访问量偏离该用户所在群组历史行为,等异常行为。
GO********0	2019-01-03 14	用户：G*********0于2019-01-03 14时,存在访问量异常,url访问数量异常,IP频繁变动,访问量偏离该用户所在群组历史行为,等异常行为。
X**********9	2019-01-02 09	用户：X**********9于2019-01-0209时,存在访问量异常,url访问数量异常,IP频繁变动,访问量偏离该用户所在群组历史行为,等异常行为。
Y**********7	2019-01-04 10	用户：Y**********7于2019-01-04 10时,存在访问量异常,IP频繁变动,url平均访问量异常，访问量偏离该用户历史行为,访问量偏离该用户所在群组历史行为,等异常行为。
X**********5	2019-01-02 10	用户：X*********5于2019-01-02 10时,存在url访问数量异常,IP频繁变动,访问量偏离该用户所在群组历史行为,等异常行为。
Y**********7	2019-01-04 11	用户：Y**********7于2019-01-04 11时,存在访问量异常,IP频繁变动,url平均访问量异常，访问量偏离该用户所在群组历史行为,等异常行为。
X**********5	2019-01-02 11	用户：X**********5于2019-01-02 11时,存在访问量异常,IP频繁变动,url平均访问量异常，访问量偏离该用户所在群组历史行为,等异常行为。
Z**********0	2019-01-02 16	用户：Z**********0于2019-01-02 16时,存在访问量异常,IP频繁变动,url平均访问量异常，访问量偏离该用户历史行为,等异常行为。

用户研判与反馈，负样本积累

事件	模型异常	反馈异常	核实异常比例
2019年02周	50	24	0. 48
2019年01周	50	27	0. 54
2019年03周	50	23	0. 46
2019年04周	57	40	0. 70
2019年05周	50	32	0. 64
2019年06周	41	25	0. 61
2019年07周	50	25	0. 5

基于用户反馈结果：确认存在异常行为总结归纳为以下情况

存在被拦截请求	存在多IP同时访问	存在使用外挂嫌疑	存在账号共用	订单查询/成交比异常	高频操作
11	73	3	70	20	10

2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

模型优化与探索

1

特征处理效率提升：

1、底层数据统计动作前置，数据入库同时生成统计信息及指标；

2

丰富特征

1、加工和探索更多的用户行为特征：用户业务访问路径

2、多模型结合：员工预离职预测，探索预离职员工信息泄露概率

3、用户行为属性和操作属性的标签化

3

模型探索和优化方向

1、“知己”模型的探索实践：用户的正常访问行为数据化，找出偏离正常行为的风险事件

2、不同场景用“恰当的方式”来解决，投入产出适配

WAIC 2019世界人工智能大会 WORLD ARTIFICIAL INTELLIGENCE CONFERENCE
2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

WAIC
2019世界人工智能大会
WORLD ARTIFICIAL INTELLIGENCE CONFERENCE

2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security

谢 谢

THANK YOU
FOR WATCHING

WAIC
2019世界人工智能大会
WORLD ARTIFICIAL INTELLIGENCE CONFERENCE

2019世界人工智能安全高端对话
2019 High-level Dialogue on World AI Security