58同城

2021

58同城 第2届 安全技术沙龙

业务风控建设 & 应用安全实践

主办单位：58安全 58 CYBERSECURITY | 58安全应急响应中心 Security Response Center

指导单位：北京市朝阳区互联网协会

段枝宏

58同城TEG安全平台研发部负责人

分享主题

安全画像在58同城的落地实践

议题介绍

为有效从资源层面打击黑产、提升黑产攻击成本、有效支撑智能化、跨场景的业务风控平台，58集团安全平台部建设了集标签生产、标签管理、黑产团伙分析、综合风险决策、黑产攻击预警于一体的安全画像体系，本次分享主要围绕如何通过模型/策略有效识别黑产、如何构建闭环打标流程、如何将安全画像能力应用于黑产对抗等方面进行详细阐述

安全画像在58落地实践

目录

01

背景

背景

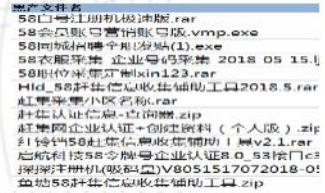
卡商

IP供应商

程控设备

套证

黑产工具



恶意注册 → 爬取信息 → 微信吸粉 → 涉黄 → 诈骗

背景

- 传统风控手段主要是基于行为和内容的拦截，在对抗初期，效果比较明显，但随着黑产攻击行为的不断变化，问题也逐渐显现

- 传统风控系统虽然行之有效，但是没有对黑产资源进行消耗
- **安全画像的目标**：利用现有风控手段的安全治理成果，持续对黑产资源进行多维度消耗，提升黑产攻击成本

解决方案

全栈式的安全画像体系

黑产资源

卡商

IP供应商

号商

套证

黑产软件

防御场景

注册 → 登录 → 发布 → 活动 → 投诉

挖掘方式

规则策略　分类　关联　统计　文本识别　图片识别

画像数据

账号	是否恶意注册	设备指纹	是否越狱	黑卡	是否猫池	IP	代理	企业	虚假注册
	是否盗号		是否模拟器		是否小号		秒拨		欺诈
	是否养号		设备农场		是否虚拟号		机器行为		信息虚假
	……		……		……		……		……

02

整体架构

系统架构


能力域
门户
画像查询服务
综合风险分
关联分析服务
查询服务
标签库
名单库
统一数据接入服务
运营域
标签管理平台
策略管理后台
综合风险分平台
自动化评估平台
关联分析平台
监控预警平台
权限管理
生产域
实时标签备注系统
离线任务调度系统
基础平台域
数据流转平台
规则计算引擎
特征库平台
基础数据域
用户行为数据
风控审核数据
算法模型数据
第三方数据

技术选型

维度结构不固定

T级数据存储

存储横向扩容

高并发低延迟

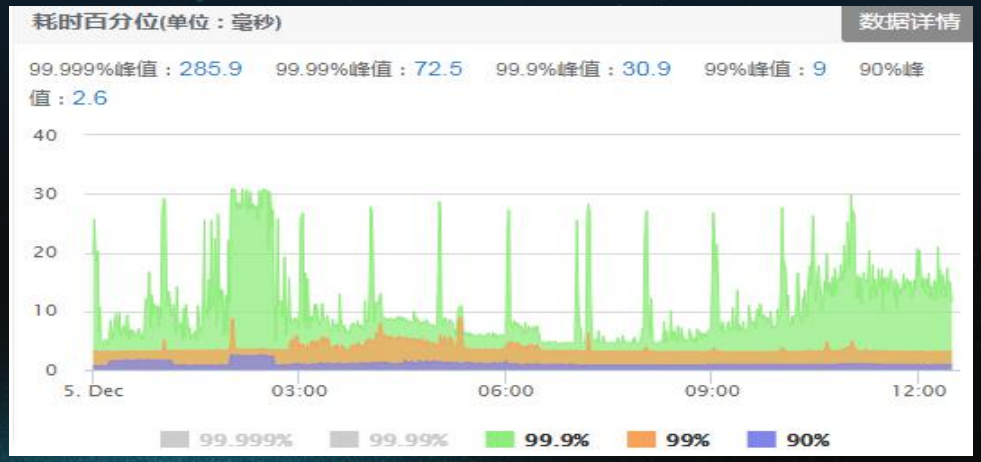
标签数据可视化管理

实时复杂标签聚合查询

离线分析

算法模型支撑

高可用



03

标签生产

多种标签生产方式

- 丰富的标签生产方式

01 行为特征分析

02 黑产情报

03 黑产工具分析

04 群体聚类模型

05 历史违规数据积累

06 第三方数据校验能力

标准化流程


原始数据接入
业务离线数据
业务实时数据
风控审核数据
第三方数据
标签生产
实时标签
离线标签
策略模型
算法模型
评估
准确率评估
召回率评估
数据存储
实时库
高频缓存库
统计引擎
离线库
提供实时数据
标签查询
关联查询
综合风险分
巡检

打标引擎

实时打标引擎	离线打标引擎	算法打标引擎
数据源配置 特征配置 策略配置 策略监控	标签任务配置 任务调度 任务监控	特征配置 样本训练 准招率评估

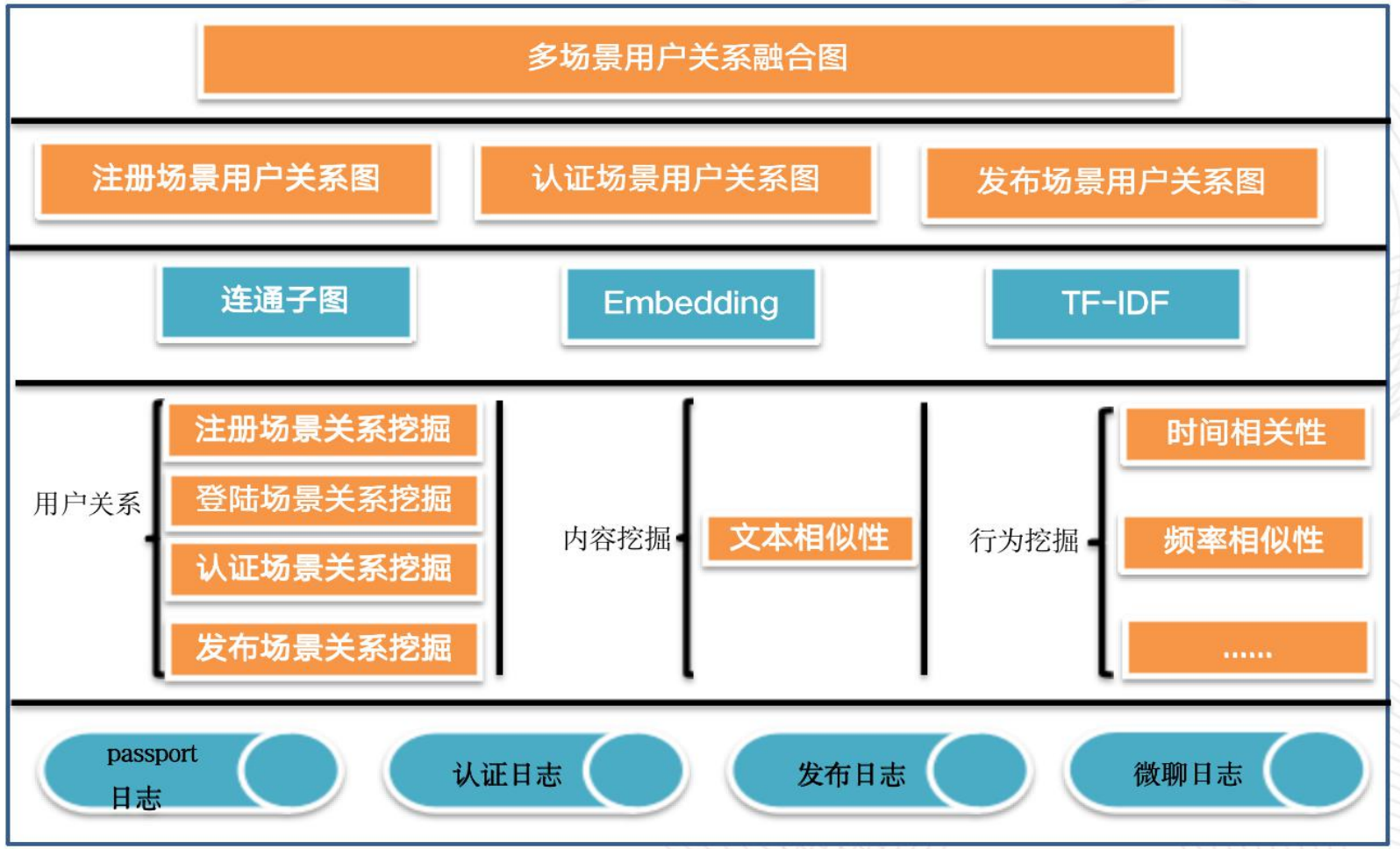
特征库


应用层
算法模型
策略模型
黑产特征分析平台
监控预警平台
特征管理
特征查询
特征配置
计算引擎
实时计算平台
PV计算能力
UV计算能力
滑动窗口能力
流式计算平台
PV计算能力
UV计算能力
原生特征
复合特征
滚动窗口能力
离线计算平台
PV计算能力
UV计算能力
超长窗口计算能力
通用过滤组件
数据层
业务离线数据
业务实时数据

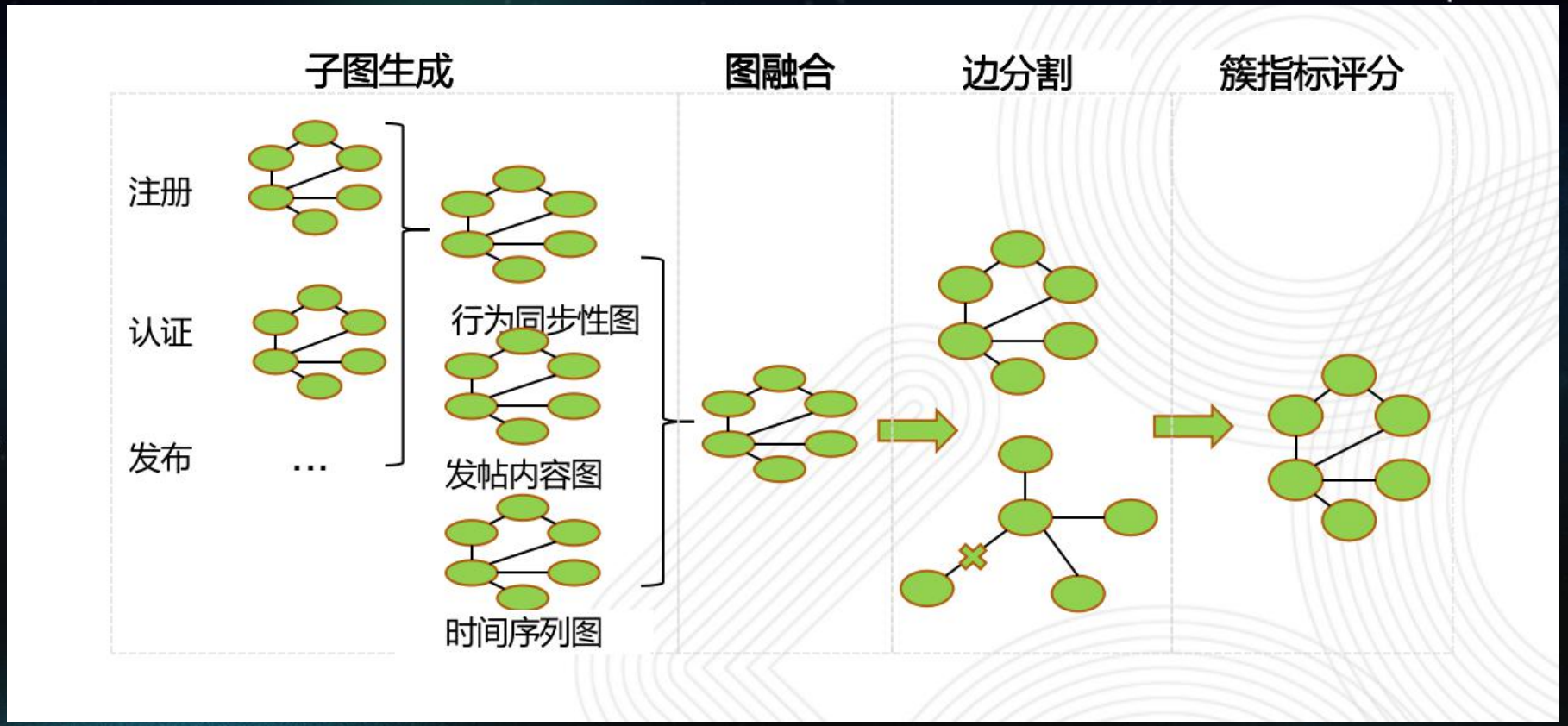
图算法模型

- 传统策略分析、分类算法模型
  - 标签策略繁多，难于维护
  - 准确率、召回率衰减较快
  - 人工投入成本高
- 黑产批量控制账号进行各种违规行为，存在资源聚集性以及行为一致性

图算法模型


多场景用户关系融合图
注册场景用户关系图
认证场景用户关系图
发布场景用户关系图
连通子图
Embedding
TF-IDF
用户关系
注册场景关系挖掘
登陆场景关系挖掘
认证场景关系挖掘
发布场景关系挖掘
内容挖掘
文本相似性
行为挖掘
时间相关性
频率相似性
.....
passport 日志
认证日志
发布日志
微聊日志

图算法模型



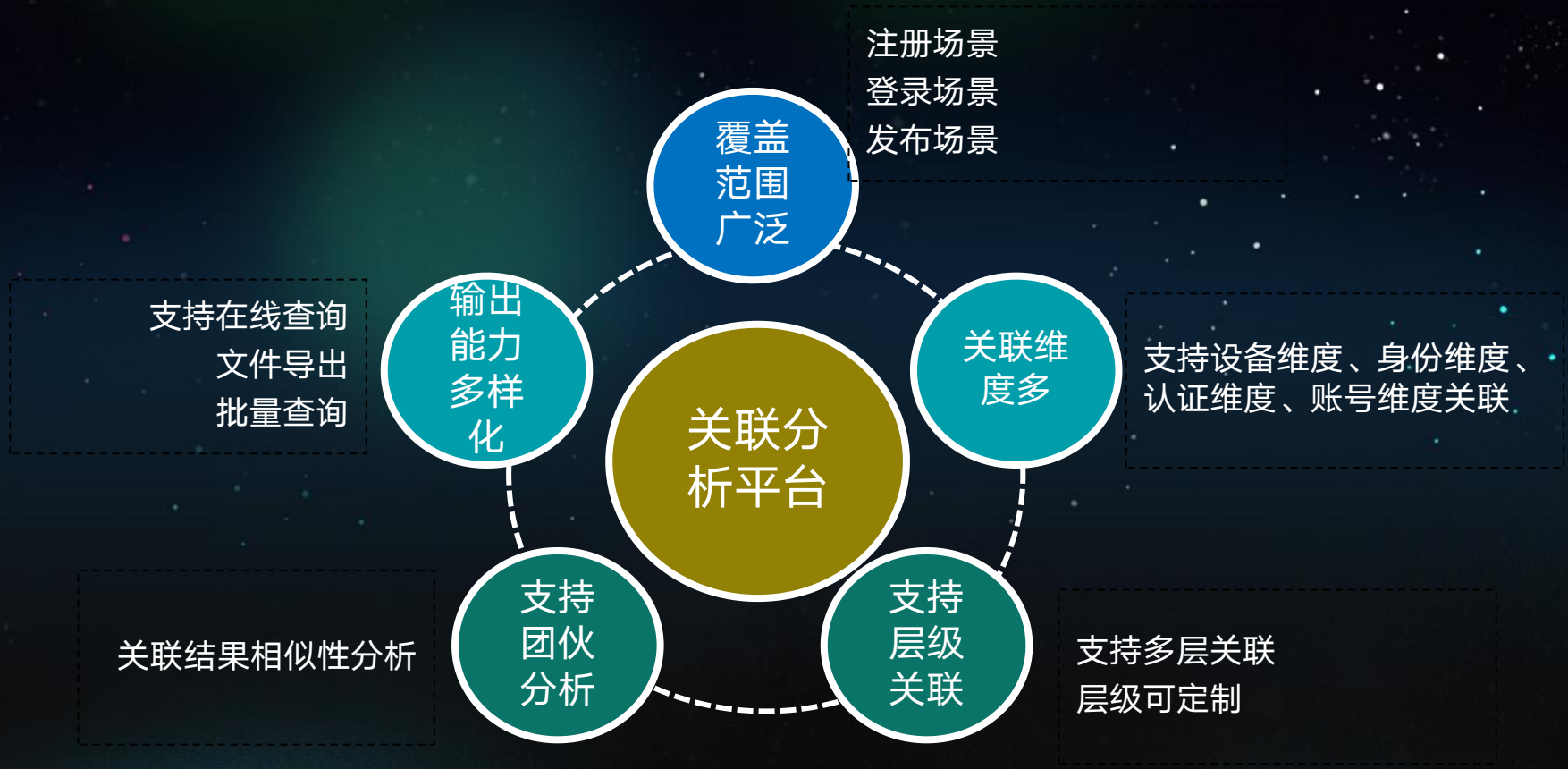
04

标签管理

标签管理平台

维度	标签名称	标签代码	优先级类型	状态	是否恶意	查询频率	创建人	修改时间	备注	操作
安居客账号	机器登录	[redacted]	取最高分	上线	恶意	低频	[redacted]	2021-07-19 14:52:47		修改 存量
58账号	黑产工具	[redacted]	取最高分	上线	恶意	低频	[redacted]	2021-06-24 10:54:12	使用黑产工具或具有...	修改 存量
device指纹	欺诈	[redacted]	取最高分	下线	恶意	低频	[redacted]	2021-05-25 14:32:40	待下线标签，请不要...	修改 存量
device指纹	盗号	[redacted]	取最高分	下线	恶意	低频	[redacted]	2021-05-25 14:32:26	待下线标签，请不要...	修改 存量
device指纹	操作系统	[redacted]	策略优先级	下线	非恶意	低频	[redacted]	2021-05-25 14:32:17	待下线标签，请不要...	修改 存量 优先级配置

关联分析平台


关联分析平台
覆盖范围广泛
注册场景
登录场景
发布场景
关联维度多
支持设备维度、身份维度、认证维度、账号维度关联
支持层级关联
支持多层关联
层级可定制
支持团伙分析
关联结果相似性分析
输出能力多样化
支持在线查询
文件导出
批量查询

自动化评估平台

- 自动化评估平台

05

落地实践

落地数据

26亿+

画像数据存量

16亿+

恶意数据存量

99%+

准确率

120+

接入业务场景

300亿+

日调用量

20亿+

日识别风险请求

服务场景

01 房产

02 招聘

03 二手车

04 黄页

05 passport

06 认证

恶意注册/登陆 → 虚假认证 → 爬虫 → 吸粉 → 涉黄.....

蜜罐


黑样本
白样本
样本投放
全路径追踪
/ 2, 度特征提取
轨迹跟踪
行为轨迹对比
黑白行为分析
差异化分析
风险行为判定
风险实体打标
行为锁定
处置
惩罚
精准打击

THANKS