
Architect
SACC
2022 中国系统架构师大会
SYSTEM ARCHITECT CONFERENCE CHINA 2022
激发架构性能 点亮业务活力
云上会议 网络直播 | 2022年10月27-29日
IT168.com
ChinaUnix.net
ITPUB

企业业务安全进阶之路

掌数 联合创始人 黄乐

我是谁

新晋创业者

创业

北京掌数信息技术有限公司联合创始人、CTO，专注业务安全解决方案。

多年从业者

打工

曾任央视网网络安全部副总监。负责网站整体安全建设、安全运营、产品研发等工作。

圈子组织者

输出

清流派企业安全沙龙创始人之一
曾任“诸子云”安全社群北京站站长
《企业信息安全建设之道》作者

攻击者的画像

攻击者的
擅长与不擅长

技术层面

漏洞利用、远程控制
隐藏自身、编写病毒

社工层面

收集情报、设计剧本
信息挖掘、扩大战果

实战层面

绕过防御、横向移动
固话收益、协同作战

业务逻辑

关联关系、逻辑顺序
时间特性、关键操作

行为习惯

行为分布、频率习惯
工作时间、偶发事件

场景特点

交班时间、特殊活动
沟通方式、通信模型

思考方式

企业安全团队每天都会面临大量技术性和事物性工作，有限的精力非常容易被分散。

所以防守方应该有独立的思考方式，来应对复杂的安全环境。

Subtitle

01 **思维框架：**善守者应该有自己的思维框架，不能被外界纷繁的攻击行为所左右。

02 **现实情况：**水无法至清，要做到每战愈强，兵形象水。

03 **建议：**在完成合规建设的基础上，对重点业务进行重点保护。

痛点

残余风险

所有信息系统都会面对残留风险治理的问题。如何让残留风险对信息系统的影响最小？

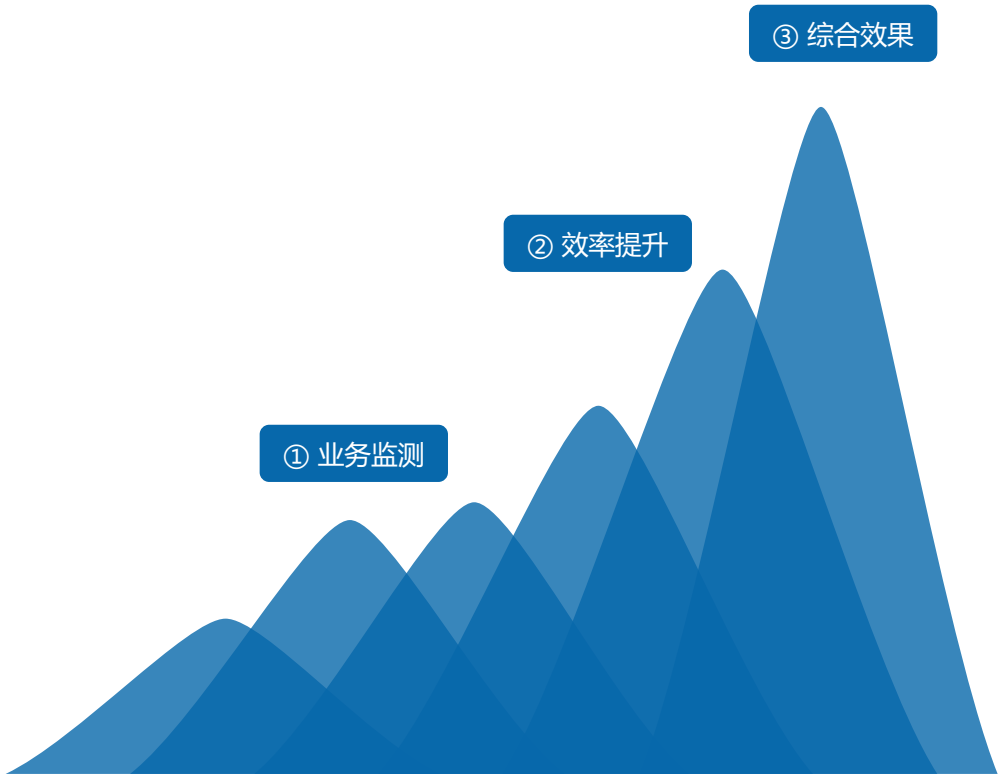
投入产出

市场上有大量安全产品供用户选择，怎样才能实现最佳的投入产出比？

安全产能

经过多年的安全建设，各企业都积累了大量的安全能力。如何将安全产品的能力发挥到最大，实现保护企业业务的目标？

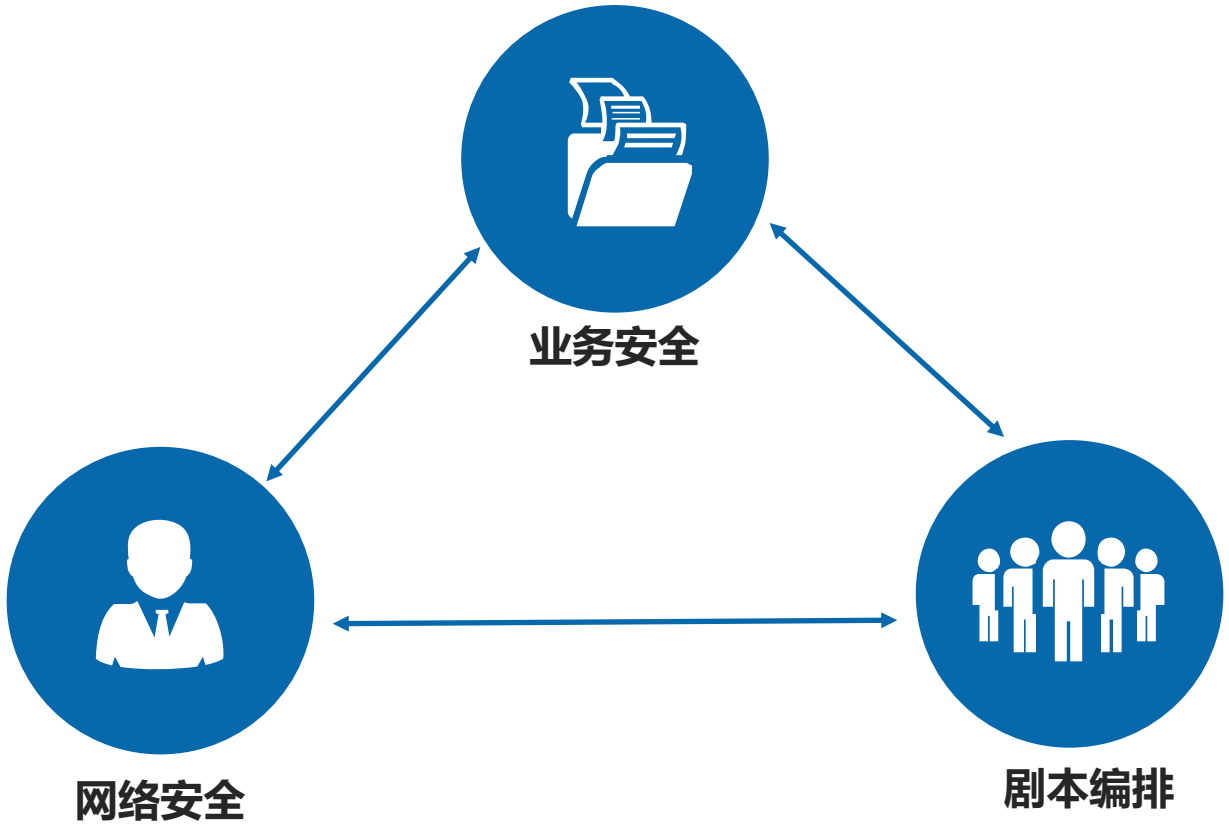
阶梯



① **业务监测** 解决业务安全异常监测的问题

② **效率提升** 解决告警效率提升的问题

③ **综合效果** 解决安全能力综合使用的问题



以业务安全监测为核心，整合网络安全分析能力和安全联动能力的整体安全监测体系。

阶段 1

阶段 2

阶段 3

阶段 4

一个关于对抗的故事

第一阶段

入侵无感知
业务线发现

第二阶段

安全手段有限
业务逻辑防御

第三阶段

业务层面对抗
多轮博弈胜利

第四阶段

临时手段固化
业务安全雏形

业务安全对团队意味什么

A 更有效的安全策略

B 更方便申请预算

C 更大的话语权

D 更广阔的升职空间

用业务数据实现对攻击者的降维打击

将业务数据和业务逻辑加入安全分析中，将安全分析效果提升到一个新的高度。对于擅长绕过各类安全产品的攻击者来说是一种降维打击。

AI技术加持提升异常行为判断效果

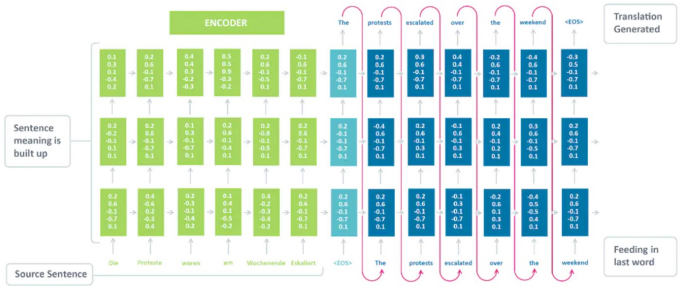
以明确的威胁特征为基础，用AI加持，从寻找已知安全事件，升级为寻找异常行为。机器学习技术的加持让异常行为判断变得更加高效、准确。

从静态防御到动态运营

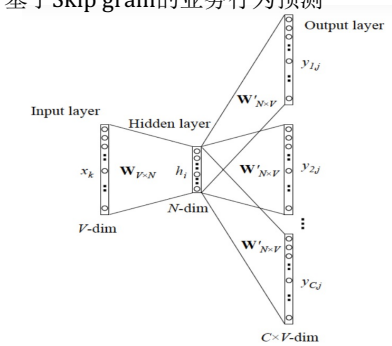
通过落地安全运营的理念，让静态的防御体系“动”起来。实现动态学习、动态分析、动态阻断的防御效果。

业务安全—能力积累

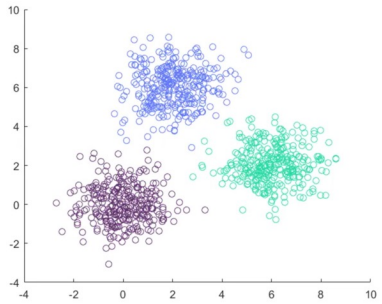
基于马尔科夫链的业务流程分析



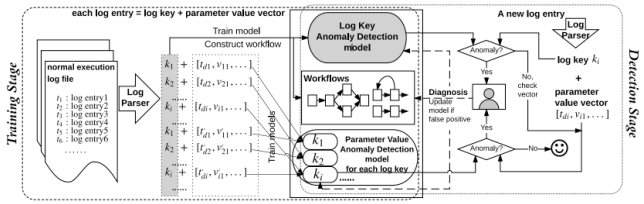
基于Skip gram的业务行为预测



基于高斯混合模型的内容发布行为分析



基于深度学习的日志异常分析

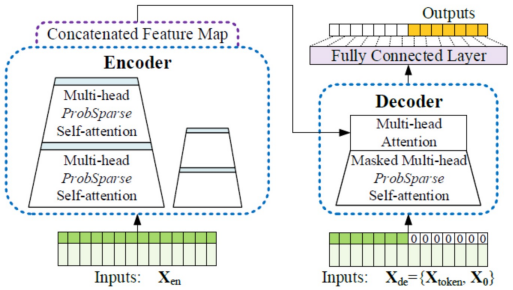


基于TF-IDF&余弦相似性的操作行为分布分析

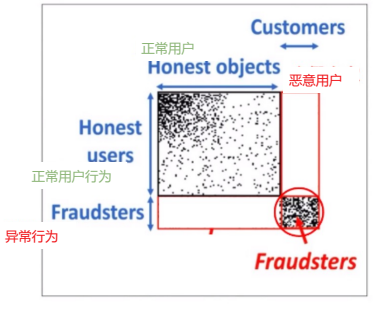
$$w_{i,j} = tf_{i,j} \times \log\left(\frac{N}{df_i}\right)$$

$$\cos\theta = \frac{\sum_{i=1}^{n}(X_i * Y_i)}{\sqrt{\sum_{i=1}^{n}(X_i)^2} * \sqrt{\sum_{i=1}^{n}(Y_i)^2}}$$

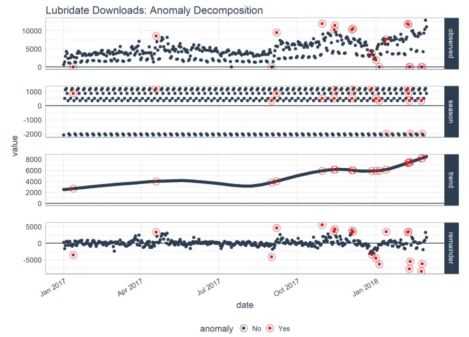
基于transformer长时间系列模型的操作分析



基于Fraudar的恶意用户行为分析

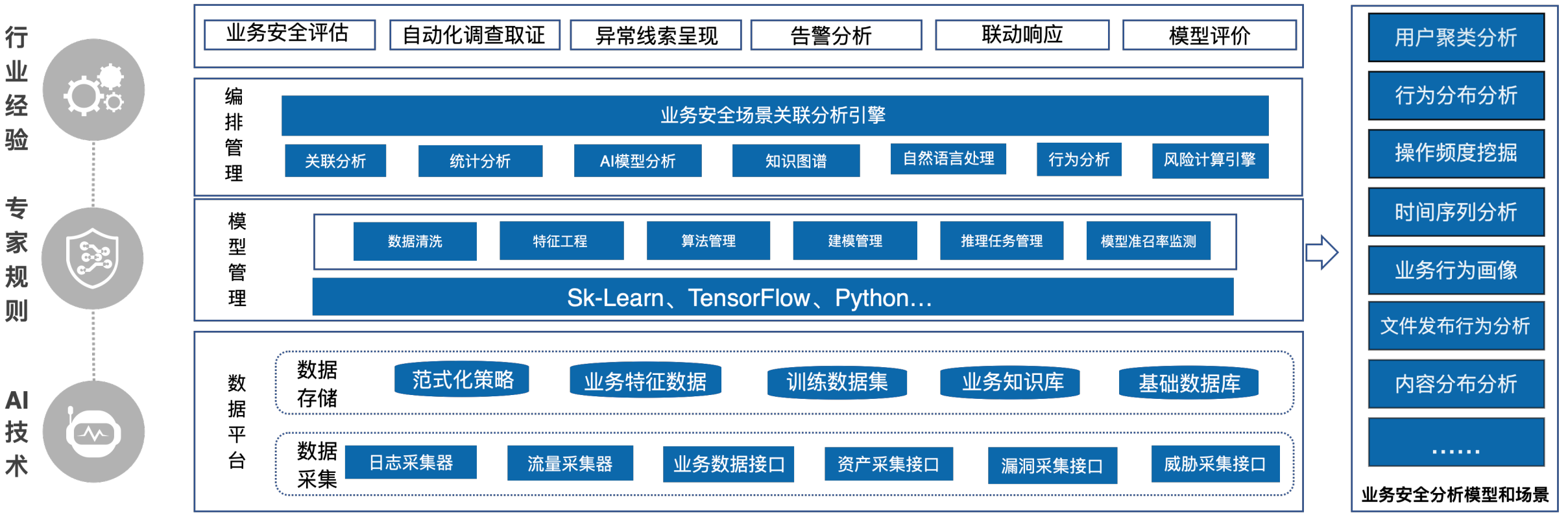


基于时间序列的频率异常检测



快速构建业务监测体系 | 解决日常运维难题 | 用数据进化算法 | 形成高度定制化方案

业务安全—平台架构


行业经验
专家规则
AI技术
业务安全评估
自动化调查取证
异常线索呈现
告警分析
联动响应
模型评价
编排管理
业务安全场景关联分析引擎
关联分析
统计分析
AI模型分析
知识图谱
自然语言处理
行为分析
风险计算引擎
模型管理
数据清洗
特征工程
算法管理
建模管理
推理任务管理
模型准召率监测
Sk-Learn、TensorFlow、Python…
数据平台
数据存储
范式化策略
业务特征数据
训练数据集
业务知识库
基础数据库
数据采集
日志采集器
流量采集器
业务数据接口
资产采集接口
漏洞采集接口
威胁采集接口
用户聚类分析
行为分布分析
操作频度挖掘
时间序列分析
业务行为画像
文件发布行为分析
内容分布分析
.....
业务安全分析模型和场景

业务安全—分析样例

训练数据 (用户ID、操作时间、菜单) —特征工程 文本化→ 训练数据 (用户ID、操作时间、菜单、每人每N分钟对菜单i的点击次数)

ETL 工程

行为分布异常算法 → 行为分布异常模型

训练过程

推理过程

监测数据 (用户ID、操作时间、菜单、每人每N分钟对菜单i的点击次数)

模型 —模型输出→ 用户ID=436异常 —算法解释→

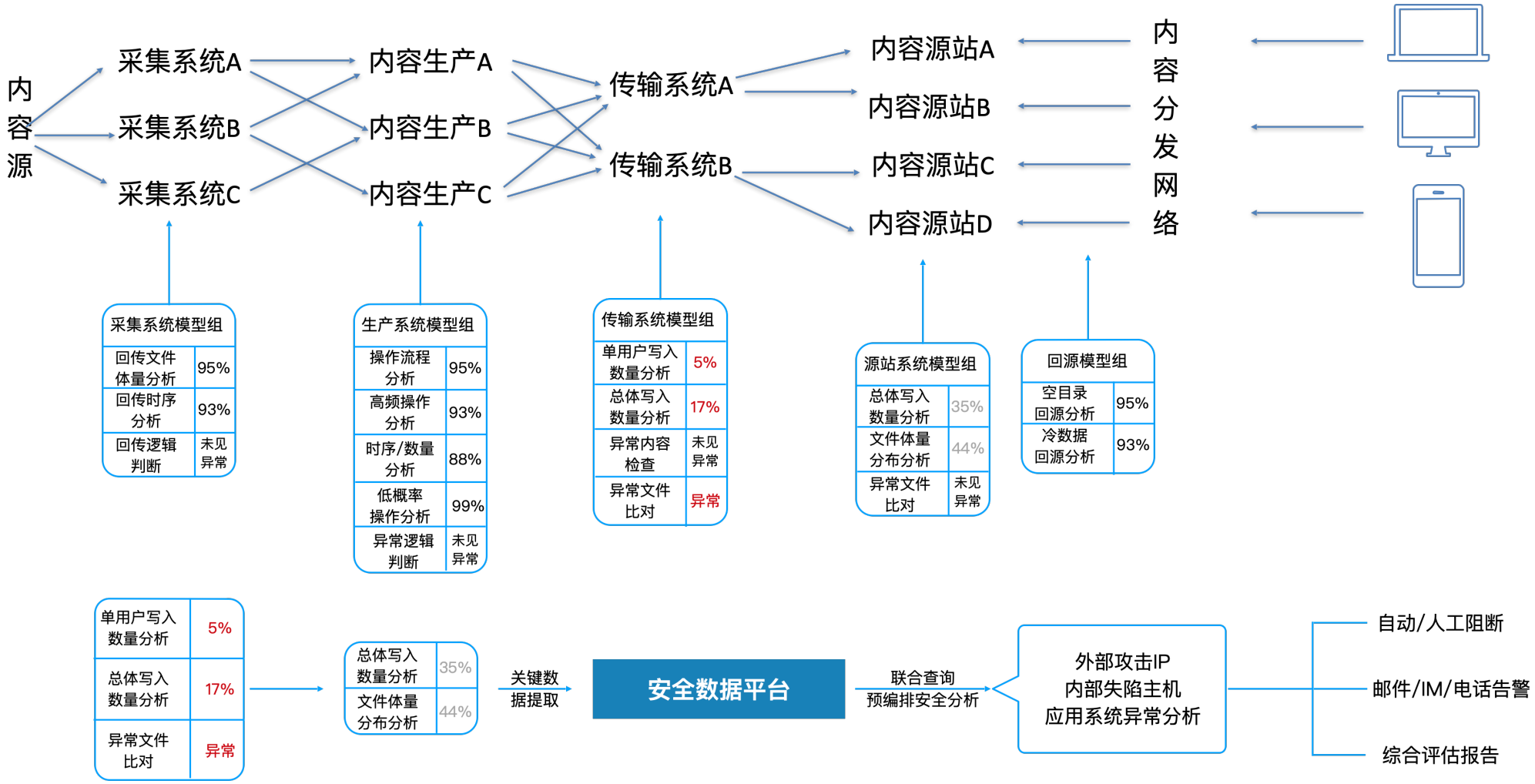
用户ID=436操作行为：

操作行为	操作数量	行为偏离度
用户名查询次数：	38	0.012
用户缴费次数：	30	0.081
用户注销次数：	19	24.95
新装用户次数：	9	0.125
电话号码查询次数：	6	0.274

……

—账号停用→ 用户ID436停用

业务安全+网络安全+编排能力



业务安全

我们认为，所有安全事件的本质都是业务安全事件。
所以，安全团队应该充分了解业务需求，甚至公司战略。
这样才能真正保护企业的核心价值，也能让安全团队的
工作更加有的放矢。

THANKS