EISS-2018企业信息安全峰会之上海站

"Face the challenge,Embrace the best practice"

November 30th,2018|SHANGHAI

2018年11月30日|上海

安全加

电商风控体系建设

2018年11月

苏宁易购 suning.com

01 反欺诈面临的挑战

黑灰产业链

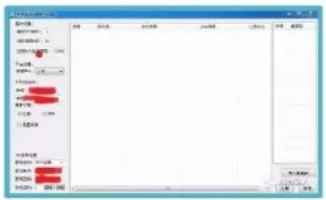
苏宁易购 suning.com

所谓的”网络黑色产业链”，是指以互联网为载体，以盈利为目的的有组织、分工明确的团伙式犯罪行为。一般来说，上游为提供技术支持的黑客或泄露个人隐私数据的内鬼，下游则是实施黑产犯罪行为(如诈骗、洗钱、骗贷)的团伙。

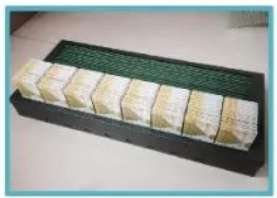
上游 黑灰产工具	中游 黑灰产信息	下游 黑灰产行为实施
破解软件	社工库	欺诈
伪造工具	垃圾注册	刷单
注册工具	信息盗取	黄牛
代理工具	信息爬取	勒索
交流平台	盗号洗号	盗窃

黑产工具

群控设备



注册工具



猫池
（接码平台）

打码平台

电商核心场景风险

苏宁易购 suning.com

客户端	注册登录	营销活动	交易	评论
逆向破解	垃圾注册	薅羊毛	薅羊毛	违规信息
仿冒应用	撞库攻击	秒杀	刷单	评论爬取
漏洞攻击	暴力破解	抢券	虚假交易	
	账户盗用	广告作弊	盗卡盗刷	
			套现	

企业防守弱势

企业防守：全线防护

黑产进攻：单点击破


02
苏宁风控发展历程

苏宁风控发展历程

苏宁易购 suning.com

- 组建风控团队
- 建立风控产品线

- 支持实时决策引擎
- 支持实时计算引擎
- 支持监控及数据分析能力

- 满足业务定制化需求
- 快速分析定位问题
- 满足业务自定义告警
- 满足核心链路的监控能力

- 支撑百万级TPS数据实时精确分析
- 研发滑块验证码
- 支持高并发下流量控制

- 支持多数据中心部署
- 业务风控联动
- 如何主动发现异常请求
- 如何发现未知安全威胁
- 风控与WAF联控

2014	2015	2016	2017	2018
初创	发展	体系化建设	能力提升	智能化
风控决策引擎1.0	风控决策引擎2.0	数据分析监控体系	设备指纹	风险标签体系
		数据化	人机识别	AI模型应用
			行为验证	验证码平台
				一键

03 风控体系建设

风控架构


核心技术
设备指纹
人机识别
验证码平台
人脸识别
IP画像
位置检测
地址校验
手机号校验
专家决策平台
风控规则引擎
指标计算
全局名单服务
大数据建模
风险画像/特征库
行为模型
风险分模型
关联模型
风控机器人
机器/深度学习
系统对接
风控风险实时服务
风控离线计算服务
风控活动运营服务
数据与运营平台
风险情报平台
风险预警监控平台
风险统计分析平台
风控查询跟踪平台

苏宁风险决策引擎

苏宁易购 suning.com

01
- 可视化配置业务策略，无需开发即可配置规则

02
- 与业务分离，修改无需发布，即时生效

03
- 可扩展，通过内外部数据、AI模型不断提升能力

监控体系

- 实时监控大盘：实时监控整体拦截情况
- 异动监控：包括趋势异常、指标异常
- 事件分析：拦截率、漏拦率
- 风险告警：攻击风险、业务风险、刷接口、破解
- 核心场景分析：拦截率、止损金额、风险分布、风险会员特征
- 全网链路风险分析：分析黄牛行为特征，预先预测未知风险，提前防控。
- 会员风险画像：利用模型输出会员风险标签，提升拦截能力

机器请求监控


人机监控
请选择事件
请选择渠道
搜索
19.09%
请求总量
机器请求量
机器占比
正常请求量
正常占比
请求趋势
机器请求量
正常请求量
机器请求占比
请求量
占比
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
50%
40%
30%
20%

账户安全监控


撞库
7442
撞库账号数
0
撞库成功账号数
0%
撞库成功率
16779
防止撞库次数
142
撞库IP数量
326
撞库设备
撞库趋势
占比
次数
800
700
600
500
400
300
200
100
0
2018-11-22 00:00
2018-11-22 06:00
2018-11-22 12:00
2018-11-22 18:00
撞库分布
告警记录
设置
IOS
HTML
ANDROID
设备类型
设备为空
手机-iOS-苏宁易...
手机-Wap
PC-Windows...
手机-Android...
撞库渠道

交易监控


交易概览
全部事业部
全部事件
全部订单
按天
今天
搜索商品编码
搜索券活动编码
查询
重置
风险趋势
60
50
40
30
20
10
0
60%
50%
40%
30%
20%
10%
0%
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00

基础数据服务

苏宁易购 suning.com

IP画像

设备画像

手机黑名单

会员画像

更多

核心技术服务

苏宁易购 suning.com

设备指纹

人机识别

行为验证码

人脸识别

智能验证码平台

苏宁易购 suning.com

整合多种验证码，结合风控决策引擎和人机识别等技术，安全用户只需轻点即可通过验证；可疑用户根据疑似程度弹出不同难度的验证码进行二次验证

智能风控


数据仓库
数据结构化
数据清洗
数据补全
风险特征
会员风险标签
设备风险标签
IP风险标签
手机风险标签
用户行为标签
策略进化
行为链路模型
物理特征模型
风险告警模型
离线分析模型
智能决策
依据风险特征利用无监督学习AI算法智能生成风险标签及策略


苏宁易购
suning.com
谢谢！
安全加