
2020 CTIC
网络安全分析与情报大会
共生
Symbiosis
共进
Success
共享
Sharing

威胁情报在银行业的建设方案与实践

牟健君

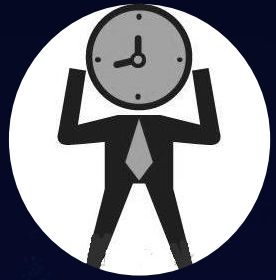
光大银行信息科技部安全处处长

背景

外部网络攻击 愈演愈烈

内部安全运营 困难重重

海量告警筛查

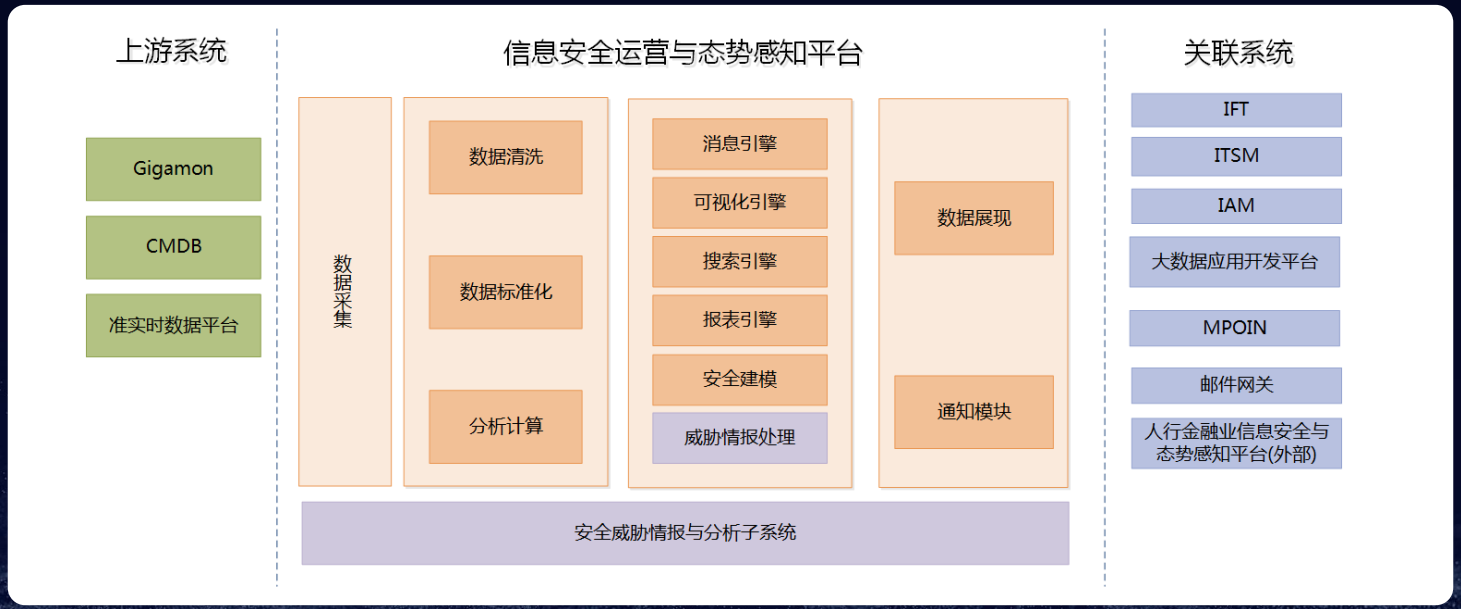


告警处置时效

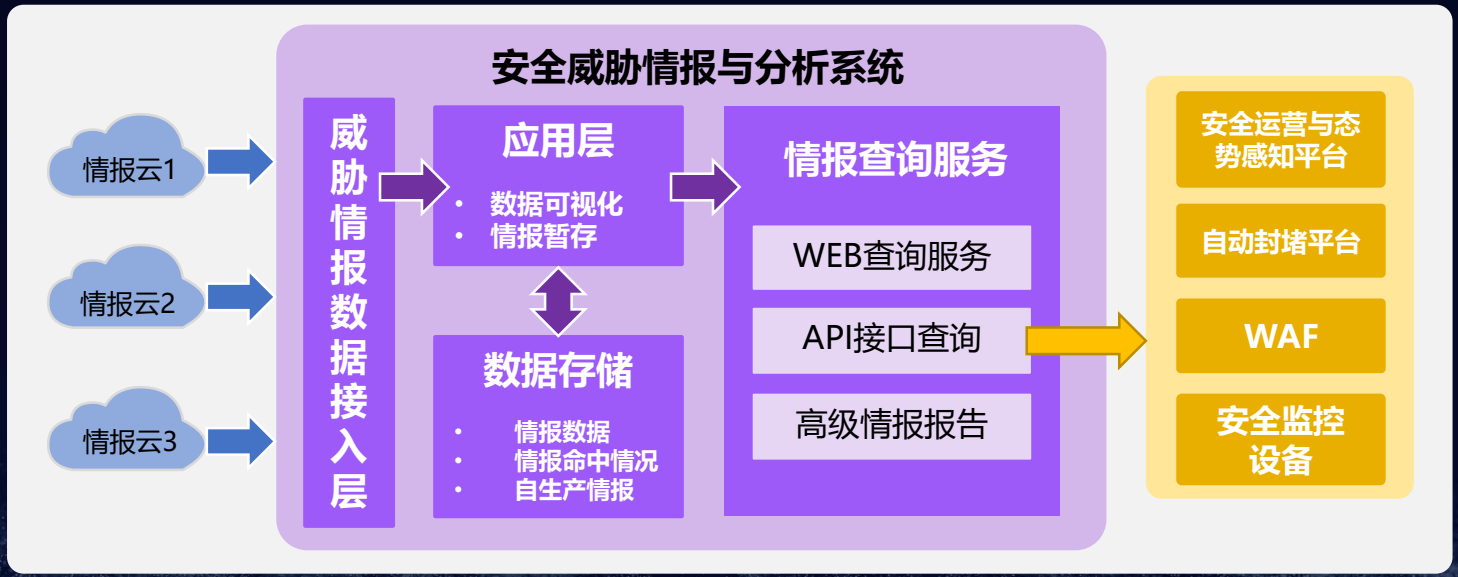
告警研判准确度

目录

威胁情报系统定位


上游系统
Gigamon
CMDB
准实时数据平台
信息安全运营与态势感知平台
数据采集
数据清洗
数据标准化
分析计算
消息引擎
可视化引擎
搜索引擎
报表引擎
安全建模
威胁情报处理
数据展现
通知模块
安全威胁情报与分析子系统
关联系统
IFT
ITSM
IAM
大数据应用开发平台
MPOIN
邮件网关
人行金融业信息安全与态势感知平台(外部)

威胁情报系统整体框架


情报云1
情报云2
情报云3
安全威胁情报与分析系统
威胁情报数据接入层
应用层
数据可视化
情报暂存
数据存储
情报数据
情报命中情况
自生产情报
情报查询服务
WEB查询服务
API接口查询
高级情报报告
安全运营与态势感知平台
自动封堵平台
WAF
安全监控设备

威胁情报系统功能结构


安全威胁情报与分析系统
情报管理
情报可视化
高级情报
情报共享
自定义情报
情报处理
数据接入
数据收集与标准化
关联分析
引擎模块
情报生产
情报存储
原始情报存储
告警事件存储
标准化情报存储
用于评估的历史情报存储
自有情报存储

银行业威胁情报系统部署方案

多源威胁情报种类

网络攻击类威胁情报

网络攻击类威胁情报主要指网络攻击、恶意邮件等网络安全威胁情报。

- 黑IP情报
- 黑域名情报
- 黑URL
- .....

业务安全类威胁情报

业务安全类威胁情报主要指黑灰产对电子银行、支付业务攻击情报，如恶意批量注册、薅羊毛等场景。

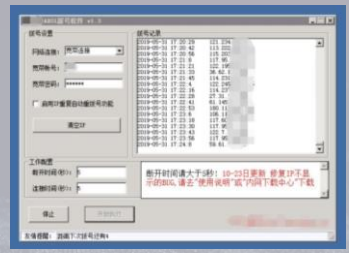
- 黑ip
- 黑手机号（黑卡）

手机号资源

卡商——拥有大量获取到手机号的渠道，并通过接码平台将手机号的短信使用权提供给下游

设备资源

群控、箱控供应商提供大批量的真手机或模拟手机的资源



IP资源

秒拨IP供应商、代理IP供应商——提供大量可用的，在黑名单外的IP，例如混在真实用户中的家庭宽带IP；或利用劫持正常用户流量的IP资源

多源威胁情报与态势感知结合

攻击者威胁行为
- 攻击时间
- 攻击动作
- 威胁等级
- 历史攻击特征钻取

攻击者处置方案
- 威胁等级评定
- 自动化处置手段

攻击者基本信息
- 地理位置信息
- whois、ip、域名、URL、ASN编号

攻击者威胁情报信息
- IP信誉标签
- 风险等级
- 可信度

目录

实践1：基于大数据建模和威胁情报的自动封堵平台建设

1、打造多源监测能力，让威胁“看得见”
2、建设网络智能化平台，让威胁“可处置”
3、依托运营大数据平台，实现威胁“精准研判”

打造眼、手、脑一体化防护的自动化封堵能力

多源监测能力建设

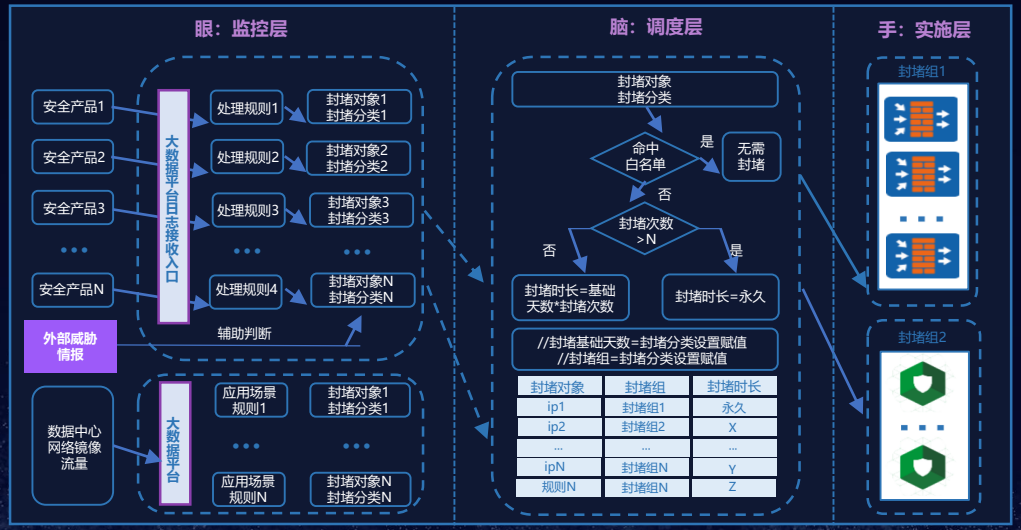
- **多源监测**：以多家厂商检测设备为基础进行异构，互补长短，并结合攻击判断技术、全流量分析技术、WEB深度检测技术开展网络攻击的监测和研判，对互联网边界、DMZ、三方接入等重点区域重点布防

告警时间	受攻击者	攻击者	Host	XFF	威胁页面	威胁类型	威胁名称	威胁等级	攻击结果	详情
2020-08-20 15:5...		192.168.3.146		202.170.14...	/ent/login.do?_logC...	弱口令	Web弱口令登录	高危	企图	查看
2020-08-20 15:5...		58.243.254.1...	e.cebbank.c...		e.cebbank.com/per/...	弱口令	Web弱口令登录	高危	失败	查看
2020-08-20 15:5...		58.243.254.1...	e.cebbank.c...		e.cebbank.com/per/...	弱口令	Web弱口令登录	高危	失败	查看
2020-08-20 15:5...		58.243.254.1...	e.cebbank.c...		e.cebbank.com/per/...	弱口令	Web弱口令登录	高危	失败	查看
2020-08-20 15:5...		58.243.254.1...	e.cebbank.c...		e.cebbank.com/per/...	弱口令	Web弱口令登录	高危	失败	查看
2020-08-20 15:5...		58.243.254.1...	e.cebbank.c...		e.cebbank.com/per/...	其他	发现明文口令传输	中危	失败	查看
2020-08-20 15:5...		58.243.254.1...	e.cebbank.c...		e.cebbank.com/per/...	其他	发现明文口令传输	中危	失败	查看
2020-08-20 15:5...		58.243.254.1...	e.cebbank.c...		e.cebbank.com/per/...	其他	发现明文口令传输	中危	失败	查看
2020-08-20 15:5...		58.243.254.1...	e.cebbank.c...		e.cebbank.com/per/...	其他	发现明文口令传输	中危	失败	查看

详细...	状态	时间戳	源主机	目标主机	感兴趣的主机	威胁描述	检测名称	协议	检测严重性	攻击阶段	显著对象	网络验伤结果	主机验伤结果
		2020-08-20 16:0...	157.55.39.240		192.168.7.61	possible Director...		HTTP	低	进入点	URL: http://xyk.c...	高度可疑	未验伤
		2020-08-20 16:0...			10.1.108.53	Executable file - ...		SMTP	低	进入点	Subject: pinginfo...	尝试	未验伤
		2020-08-20 15:5...	192.168.1.32		192.168.1.32	Possible DOWN...		TCP	中	C&C 通信	IP address: 36.62...	尝试	未验伤
		2020-08-20 15:5...			10.1.108.52	HEUR_PDFEXP....	HEUR_PDFEXP.A	SMTP	中	进入点	Subject: [illegible] ...	尝试	未验伤
		2020-08-20 15:5...	115.53.110.127		192.168.5.199	possible Director...		HTTP	低	进入点	URL: http://ebank...	高度可疑	未验伤
		2020-08-20 15:5...	115.53.110.127		192.168.5.162	possible Director...		HTTP	低	进入点	URL: http://ebank...	高度可疑	未验伤
		2020-08-20 15:5...	115.53.110.127		192.168.1.246	possible Director...		HTTP	低	进入点	URL: http://ebank...	高度可疑	未验伤
		2020-08-20 15:4...	125.93.228.32		125.93.228.32	MINER - TCP (R...		TCP	中	未知的攻击阶段	IP address: 192.1...	尝试	未验伤
		2020-08-20 15:4...	125.93.228.32		125.93.228.32	MINER - TCP (R...		TCP	中	未知的攻击阶段	IP address: 192.1...	尝试	未验伤
		2020-08-20 15:4...			10.1.188.120	Executable file - ...		SMTP	低	进入点	Subject: 光大对...	尝试	未验伤
		2020-08-20 15:4...	45.14.224.143		10.1.3.204	CVE-2018-10562...		HTTP	中	进入点	IP address: 45.14...	高度可疑	未验伤
		2020-08-20 15:4...			10.1.108.53	Executable file - ...		SMTP	低	进入点	Subject: 32343, ...	尝试	未验伤
		2020-08-20 15:3...			10.1.188.120	Executable file - ...		SMTP	低	进入点	Subject: 光大对...	尝试	未验伤
		2020-08-20 15:3...			10.1.108.54	Executable file - ...		SMTP	低	进入点	Subject: RE: [RE...	尝试	未验伤

网络智能化平台建设

基于大数据建模和威胁情报的自动封堵平台建设



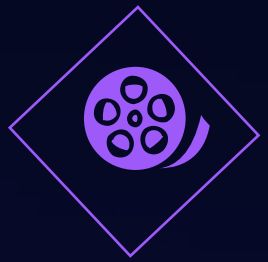
- 依托运营大数据平台，**调度外部威胁情报辅助判断实现精准识别**，调用网络智能化平台接口，实现对多源监控告警攻击IP的实时自动封堵，形成攻击IP自动化筛选、研判、拦截封堵能力

当前自动封堵占比

达到**95%**

基于大数据建模和威胁情报的自动封禁平台建设

——威胁检测模型设计



威胁情报

- IP信誉
- 远控类情报
- 黑客组织类情报
- ...

多元告警

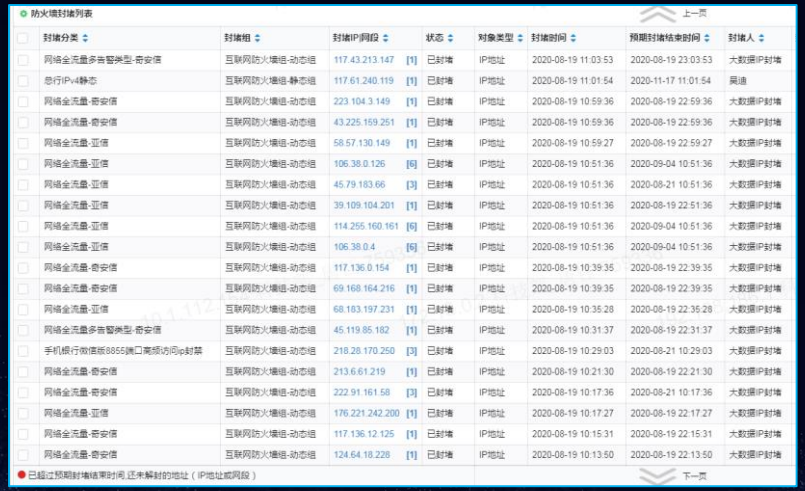
- 同IP触发多设备告警
- 同IP触发同设备多重告警
- ...

高频访问

- 同IP短时高频访问相同业务接口
- ...

基于大数据建模和威胁情报的自动封禁平台建设

——数字化展示



防火墙封堵列表

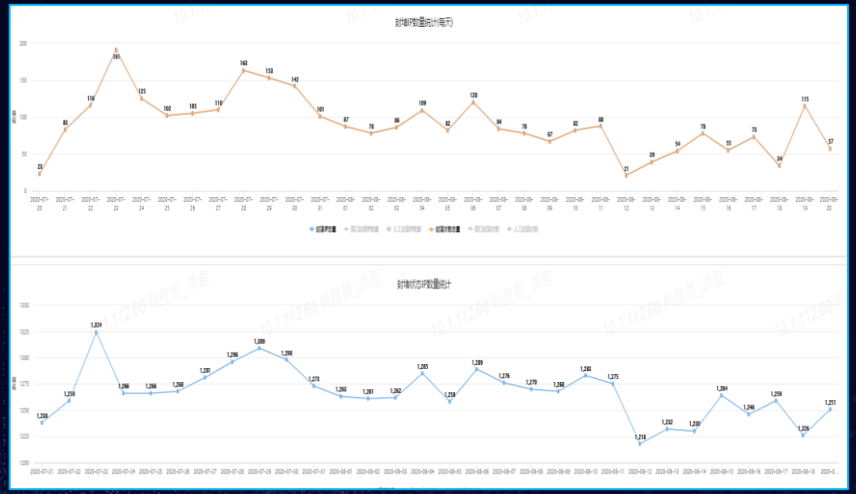
上一页

封堵分类	封堵组	封堵IP/网段	状态	对象类型	封堵时间	预期封堵结束时间	封堵人
网络全流量多告警类型-奇安信	互联网防火墙组-动态组	117.43.213.147 [1]	已封堵	IP地址	2020-08-19 11:03:53	2020-08-19 23:03:53	大数据IP封堵
总行IPv4静态	互联网防火墙组-静态组	117.61.240.119 [1]	已封堵	IP地址	2020-08-19 11:01:54	2020-11-17 11:01:54	吴通
网络全流量-奇安信	互联网防火墙组-动态组	223.104.3.149 [1]	已封堵	IP地址	2020-08-19 10:59:36	2020-08-19 22:59:36	大数据IP封堵
网络全流量-奇安信	互联网防火墙组-动态组	43.225.159.251 [1]	已封堵	IP地址	2020-08-19 10:59:36	2020-08-19 22:59:36	大数据IP封堵
网络全流量-亚信	互联网防火墙组-动态组	58.57.130.149 [1]	已封堵	IP地址	2020-08-19 10:59:27	2020-08-19 22:59:27	大数据IP封堵
网络全流量-亚信	互联网防火墙组-动态组	106.38.0.126 [6]	已封堵	IP地址	2020-08-19 10:51:36	2020-09-04 10:51:36	大数据IP封堵
网络全流量-亚信	互联网防火墙组-动态组	45.79.183.66 [3]	已封堵	IP地址	2020-08-19 10:51:36	2020-08-21 10:51:36	大数据IP封堵
网络全流量-亚信	互联网防火墙组-动态组	39.109.104.201 [1]	已封堵	IP地址	2020-08-19 10:51:36	2020-08-19 22:51:36	大数据IP封堵
网络全流量-亚信	互联网防火墙组-动态组	114.255.160.161 [6]	已封堵	IP地址	2020-08-19 10:51:36	2020-09-04 10:51:36	大数据IP封堵
网络全流量-亚信	互联网防火墙组-动态组	106.38.0.4 [6]	已封堵	IP地址	2020-08-19 10:51:36	2020-09-04 10:51:36	大数据IP封堵
网络全流量-奇安信	互联网防火墙组-动态组	117.136.0.154 [1]	已封堵	IP地址	2020-08-19 10:39:35	2020-08-19 22:39:35	大数据IP封堵
网络全流量-奇安信	互联网防火墙组-动态组	69.168.164.216 [1]	已封堵	IP地址	2020-08-19 10:39:35	2020-08-19 22:39:35	大数据IP封堵
网络全流量-亚信	互联网防火墙组-动态组	68.183.197.231 [1]	已封堵	IP地址	2020-08-19 10:35:28	2020-08-19 22:35:28	大数据IP封堵
网络全流量多告警类型-奇安信	互联网防火墙组-动态组	45.119.85.182 [1]	已封堵	IP地址	2020-08-19 10:31:37	2020-08-19 22:31:37	大数据IP封堵
手机银行微信版8855端口高频访问ip封禁	互联网防火墙组-动态组	218.28.170.250 [3]	已封堵	IP地址	2020-08-19 10:29:03	2020-08-21 10:29:03	大数据IP封堵
网络全流量-奇安信	互联网防火墙组-动态组	213.6.61.219 [1]	已封堵	IP地址	2020-08-19 10:21:30	2020-08-19 22:21:30	大数据IP封堵
网络全流量-奇安信	互联网防火墙组-动态组	222.91.161.58 [3]	已封堵	IP地址	2020-08-19 10:17:36	2020-08-21 10:17:36	大数据IP封堵
网络全流量-亚信	互联网防火墙组-动态组	176.221.242.200 [1]	已封堵	IP地址	2020-08-19 10:17:27	2020-08-19 22:17:27	大数据IP封堵
网络全流量-奇安信	互联网防火墙组-动态组	117.136.12.125 [1]	已封堵	IP地址	2020-08-19 10:15:31	2020-08-19 22:15:31	大数据IP封堵
网络全流量-奇安信	互联网防火墙组-动态组	124.64.18.228 [1]	已封堵	IP地址	2020-08-19 10:13:50	2020-08-19 22:13:50	大数据IP封堵

已超过预期封堵结束时间,还未解封的地址（IP地址或网段）

下一页

实时封堵展示



封禁解封实战效果

基于大数据建模和威胁情报的自动封禁平台建设

——自动化封堵大屏

- 攻击源IP的自动化封堵解封情况，主要包括封堵IP的数量变化趋势，设备封堵的变化趋势，实时封堵列表。

- 数据来源以WAF、防火墙的封堵数据为主，辅以情报、威胁和告警数据进行关联。

其他自动化封堵能力建设

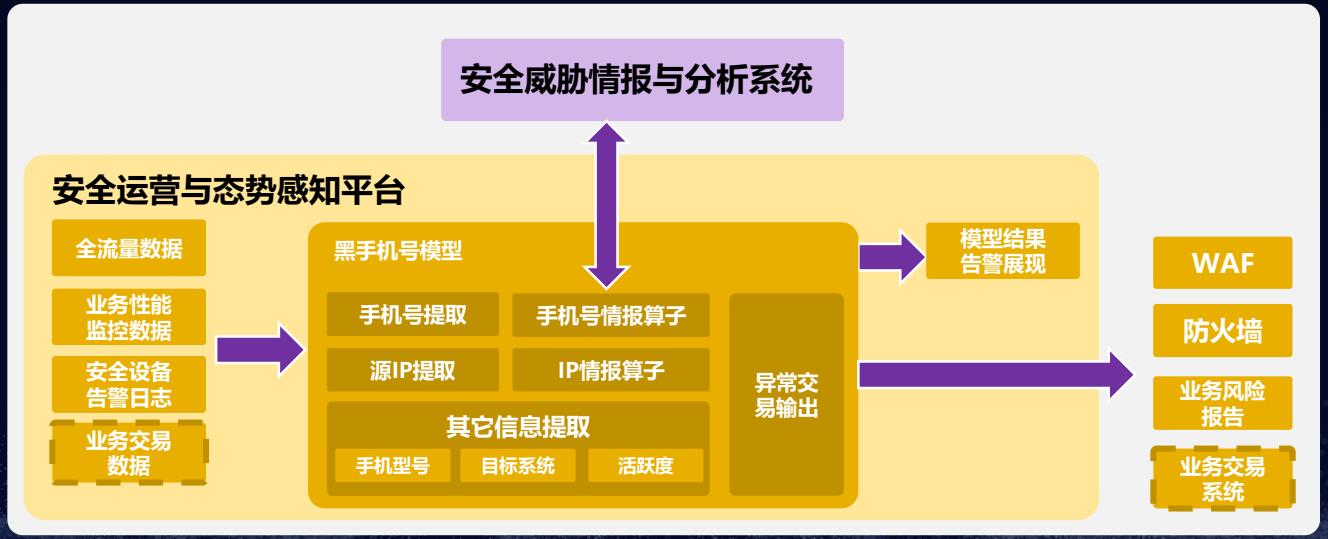
- 互联网防火墙升级为NGFW：引入IP信誉自动封堵等；
- DDoS防护升级，针对网银机器人及慢速攻击的防护；
- 网络攻击阻断系统：引入威胁情报进行异常IP自动封堵；
- 防火墙Deny日志监控：基于防火墙Deny日志，主动发现外部扫描、内部异常外联等特定场景，定义模型实现自动封堵；

实践2：黑手机号情报在黑灰产防护中的运用

通过在分析模型中，引入黑手机号情报算子，增加模型输出准确度。

常见异常场景如下：

- 同一IP地址/同一手机型号/同一UserAgent等，连续利用N个高风险黑手机号注册/登录/交易；
- 仅在业务营销活动阶段活跃手机号，活跃度达到阈值N，且情报匹配为中高风险等。
- ……



目录

下一步计划

多源情报整合

外部多厂商威胁情报整合，交叉验证，建立威胁综合评分机制，实现精准封禁

情报赋能

情报赋能，提升未知威胁/高级威胁的发现能力，提升威胁溯源能力

情报共享

同业协同作战，共建威胁情报共享安全生态圈

Thank you