网络安全创新大会
Cyber Security Innovation Summit

攻防常态化下的企业安全运营体系实践分享

姓名　马军 斗象科技企业事业部技术总监

我们的关注点

- 中华人民共和国公安部
- 国家互联网应急中心
- 中国人民银行
- 中国银行保险监督管理委员会
- 中国证券监督管理委员会

- 黑客攻击
- 黑产
- 内部人员信息贩卖
- IT厂商产品漏洞

信息安全面临的威胁与挑战

互联网经济犯罪活动数量居高不下

- 网络攻击和网络犯罪现象日益突出，呈现**攻击工具专业化、目的商业化、行为组织化、手段多样化**的特点
- 此类威胁特点在于利益驱使高、受害主体广、攻击方式多、社会危害大

行业面临的高级威胁不断加剧

- 黑客攻击手段不断升级，新兴**APT攻击**威胁层出不穷，**恶意木马病毒**持续泛滥，**0DAY漏洞**精准突袭
- 网络安全的主要威胁从黑客攻击模式转化成为犯罪分子规模化敛财模式，呈现出明显**规模化、产业化、精准化**趋势

基础设施、通用软件安全不可控

- 基础设施并不完全可靠，也不是完全可控，近几年频发的**通用软件漏洞**导致全球服务器、**网络设备**、**Web应用**遭受影响就是典型的案例
- 金融业自身**IT资产庞大**，高危漏洞修复工作量巨大，面临的风险敞口加大

移动设备和支付安全问题凸显

- 金融业在互联网上的**业务模式越来越丰富**，但是安全建设仍有待提高
- 随着**移动支付方式的普及**，我们24小时都暴露在互联网攻击之下，安全威胁在不断升高

泄露窃密性攻击步入“高发期”

- 网站系统安全漏洞，以及**内外部勾结买卖客户信息**的事件不断发生
- 除了要防范攻击外，更需防范数据的丢失及有组织的窃取，这关系到金融企业的声誉和品牌形象

安全运营体系建设

安全组织

- 组织架构
- 岗位职责
- 技术培训
- 宣传教育
- 绩效考核

安全运营分析平台

态势感知	安全分析	事件响应	溯源审计	预警通报	GRC系统
风险态势	漏洞预警跟踪	事件任务分析	安全审计	威胁预警通报	合规管理
安全态势	威胁情报整合	自动化任务编排	攻击溯源	突发事件通报	评估检查
攻击态势	安全分析告警	处置执行反馈	攻击链分析	安全分析通报	等级保护

基础平台：大数据智能安全分析 （大数据平台、规则分析、机器学习、智能分析、可视化 ）

动态防御深度分析实时检测

资产与脆弱性检测	威胁分析检测		业务/行为异常分析	安全事件分析
资产自发现	网络流量分析	病毒木马检测	用户行为异常分析	安全信息收集
脆弱性检测	数据泄露检测	潜伏威胁检测	内部违规行为检测	安全事件分析
资产风险分析	威胁画像分析	威胁行为分析		安全事件报告

基础单点安全防护技术体系

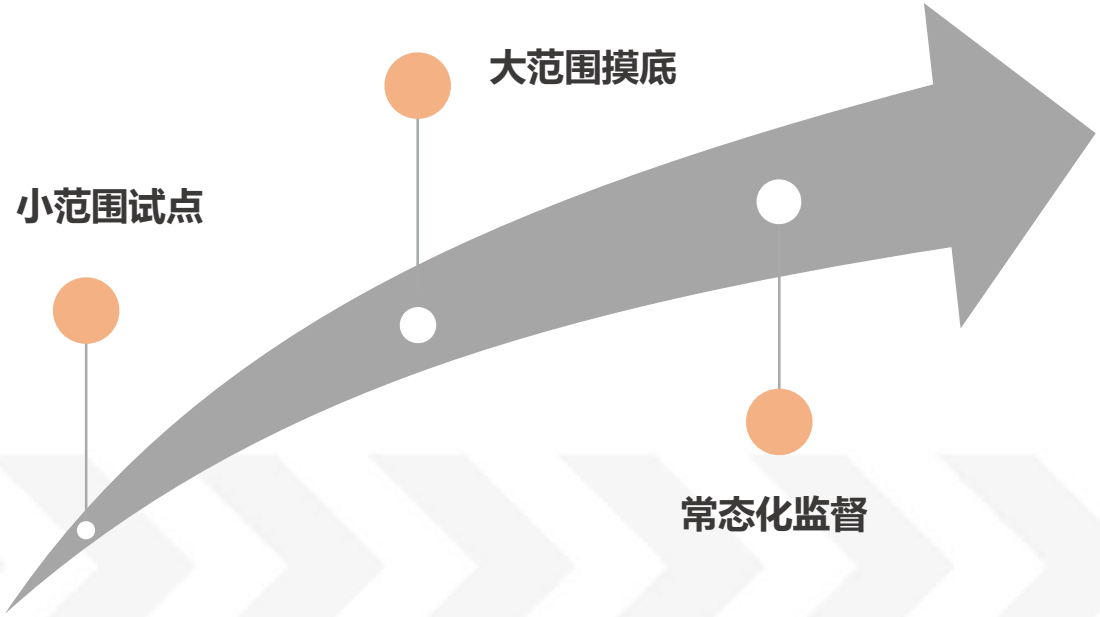
身份认证	访问控制	内容安全	监控审计	备份恢复
物理安全	终端安全	网络安全	系统安全	应用安全

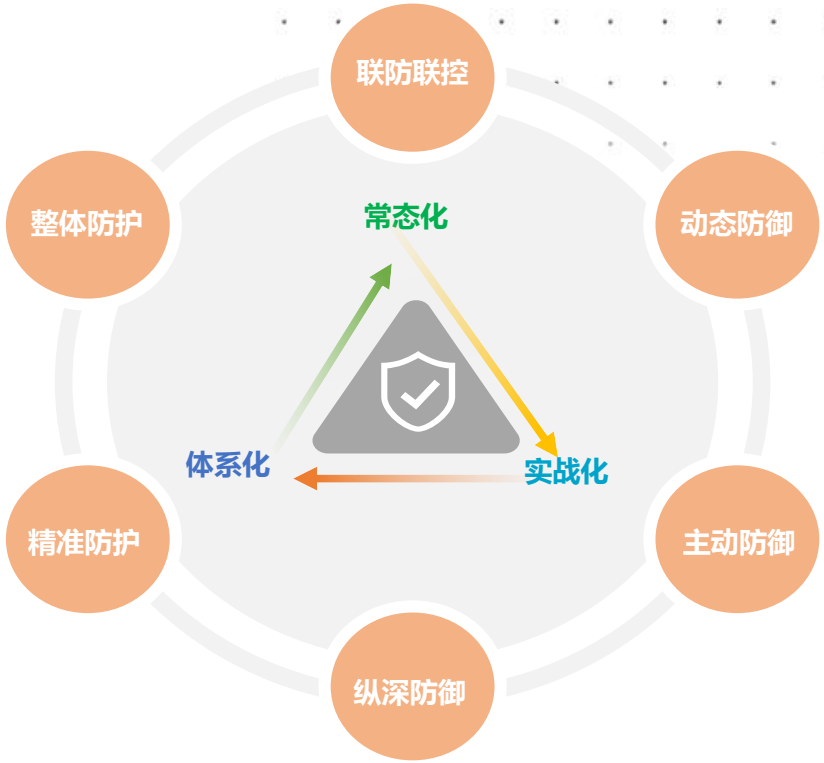
安全管理

- 风险管理
- 流程管理
- 合规管理
- 制度管理
- 知识管理

攻防常态化提出的要求

公安部《**认真落实网络安全等级保护制度 构建新时代国家网络安全综合防控体系**》主题报告中，提出了“三化六防”新思想，以”**实战化，体系化，常态化**“为新理念，以”**动态防御，主动防御，纵深防御，精准防护，整体防护，联防联控**”为新举措，构建国家网络安全综合防控系统，深入推进等保和关保的积极实践。





有效强化网络安全风险意识

检验和提高网络安全应急响应能力

培养和提升网络安全人才实战能力

构建网络安全整体联动能力

攻防常态化下的攻击趋势

趋势一：供应链攻击

- 研发层面：开发环境、依赖仓库、第三方开源库...
- 服务提供商：集成商、硬件设备、软件开发、安全设备

趋势二：自动化、体系化作战

- 预攻准备：计划、分工、数据储备、工具、漏洞
- 攻击阶段：自动化套件、间接渗透、高隐蔽性、干扰、反溯源
- 长期监控新上线业务、自动化服务识别

趋势三：深入了解业务

- 企业组织架构梳理（供应商、三方、渠道）
- 网络结构、组成、技术（SDN、VPS）
- 业务系统、互联关系、私有协议

趋势四：近源攻击

- 物联网办公设备：打印机、咖啡机、门禁设备、考勤设备、IPTV
- WiFi安全

攻防常态化安全运营提升的方向

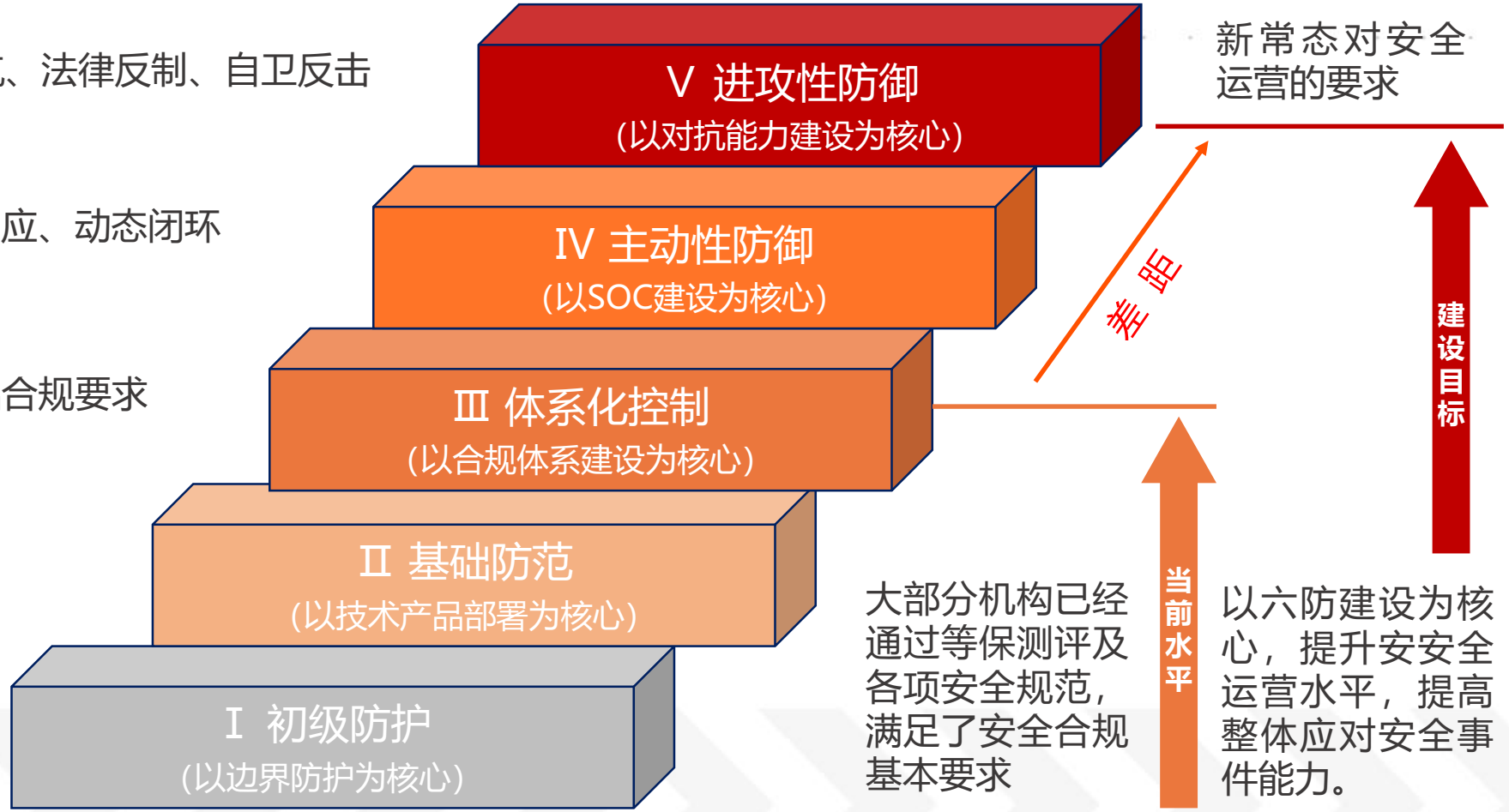
业务安全、漏洞挖掘、红蓝对抗、法律反制、自卫反击

多维度分析、实时检测、快速响应、动态闭环

组织、技术、管理体系满足基础合规要求

偏重单点安全产品，不成体系

只有边界、病毒安全防护



攻防常态化对安全运营的思考

网络安全创新大会
Cyber Security Innovation Summit

攻防实战对抗安全运营调研

- 安全问题发现滞后
- 数据分散、易丢失、易疏漏
- 无验证过程，盲目处置
- 告警噪声过大，失误、失分频发
- 处置流程不完善、事件追踪不及时
- 重复事件重复响应，增加处置时间
- 缺乏协同处置能力，效率低下
- 安全事件无法闭环

事前

无应急预案，无有效组织，权责混乱	统筹组织能力
资产管控梳理不清	资产管理能力
漏洞处置得不到闭环管理	漏洞管理能力

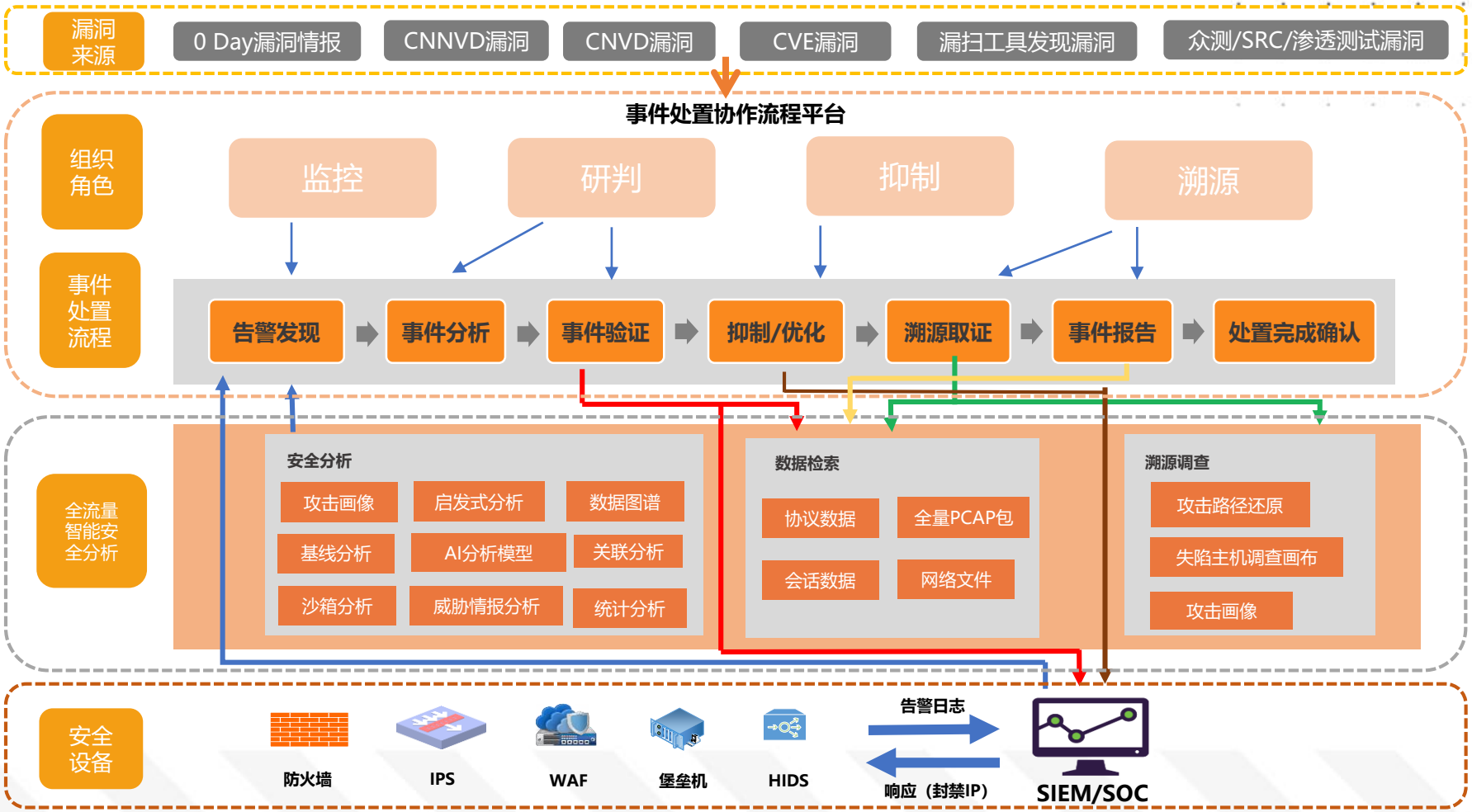
事中

无法第一时间发现未知攻击	攻击检测能力
无统一分析核心平台，孤岛式防护模式	分析研判能力
缺乏溯源分析和调查取证能力	溯源取证能力
安全事件漏跟踪和遗漏处置，导致失分	事件管理能力
无自动化可编排事件处置流程平台	协作处置能力

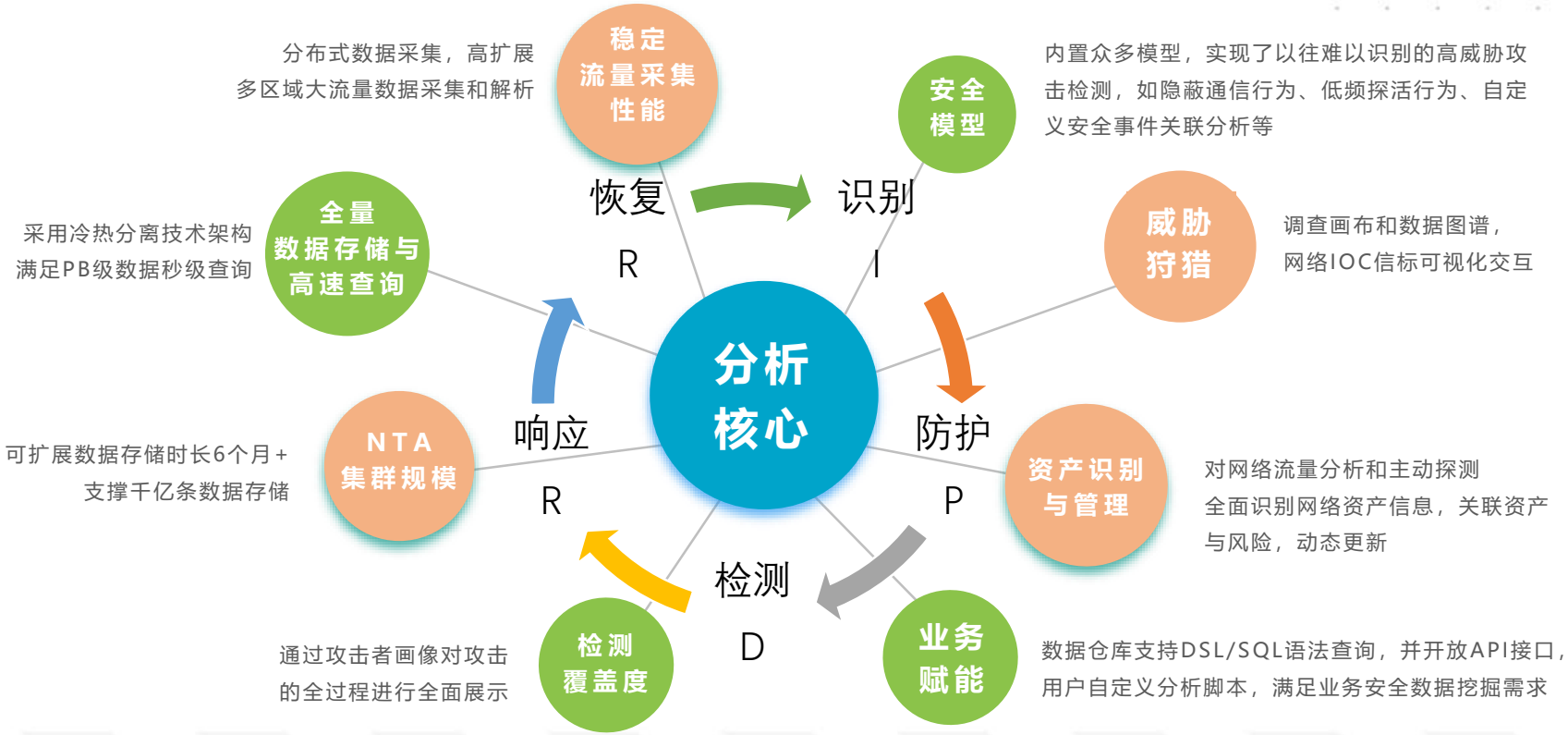
事后

电子证据缺失，无复盘依据	数据留存能力
事件处置经验得不到有效积累	经验积累能力

斗象科技攻防常态化安全运营实践



全流量智能分析特点


稳定流量采集性能
分布式数据采集，高扩展
多区域大流量数据采集和解析
安全模型
内置众多模型，实现了以往难以识别的高威胁攻击检测，如隐蔽通信行为、低频探活行为、自定义安全事件关联分析等
恢复
R
识别
I
全量数据存储与高速查询
采用冷热分离技术架构
满足PB级数据秒级查询
威胁狩猎
调查画布和数据图谱，
网络IOC信标可视化交互
分析核心
NTA集群规模
可扩展数据存储时长6个月+
支撑千亿条数据存储
响应
R
防护
P
资产识别与管理
对网络流量分析和主动探测
全面识别网络资产信息，关联资产与风险，动态更新
检测
D
检测覆盖度
通过攻击者画像对攻击的全过程进行全面展示
业务赋能
数据仓库支持DSL/SQL语法查询，并开放API接口，
用户自定义分析脚本，满足业务安全数据挖掘需求

事件处理流程特点

安全事件

- 安全设备
- 分析平台
- 人员测试
- 监管通报
- 威胁情报

灵活的事件处置流程引擎

表单自定义

资产 漏洞 情报 风险 证据 建议

流程节点绑定表单

流程自定义

事件录入 → 分析研判 → 主防鉴定 / 溯源取证 → 抑制优化 → 事件关闭

工单系统

升级常态化的安全攻防运营体系

网络安全创新大会
Cyber Security Innovation Summit

组织团队

- 提升统筹组织能力
- 安全意识优化
- 人力资源优化
- 团队经验、技术沉淀

检测分析

- 核心分析平台提升风险识别、分析能力
- 历史流量回溯分析、事件调查取证
- 数据再利用与深度挖掘

升级运营

- 实战经验赋能平时安全保障
- 资产管理，漏洞管理系统化
- 安全防护体系建设策略优化
- 安全事件处置电子数据沉淀赋能平时安全运营

流程处置

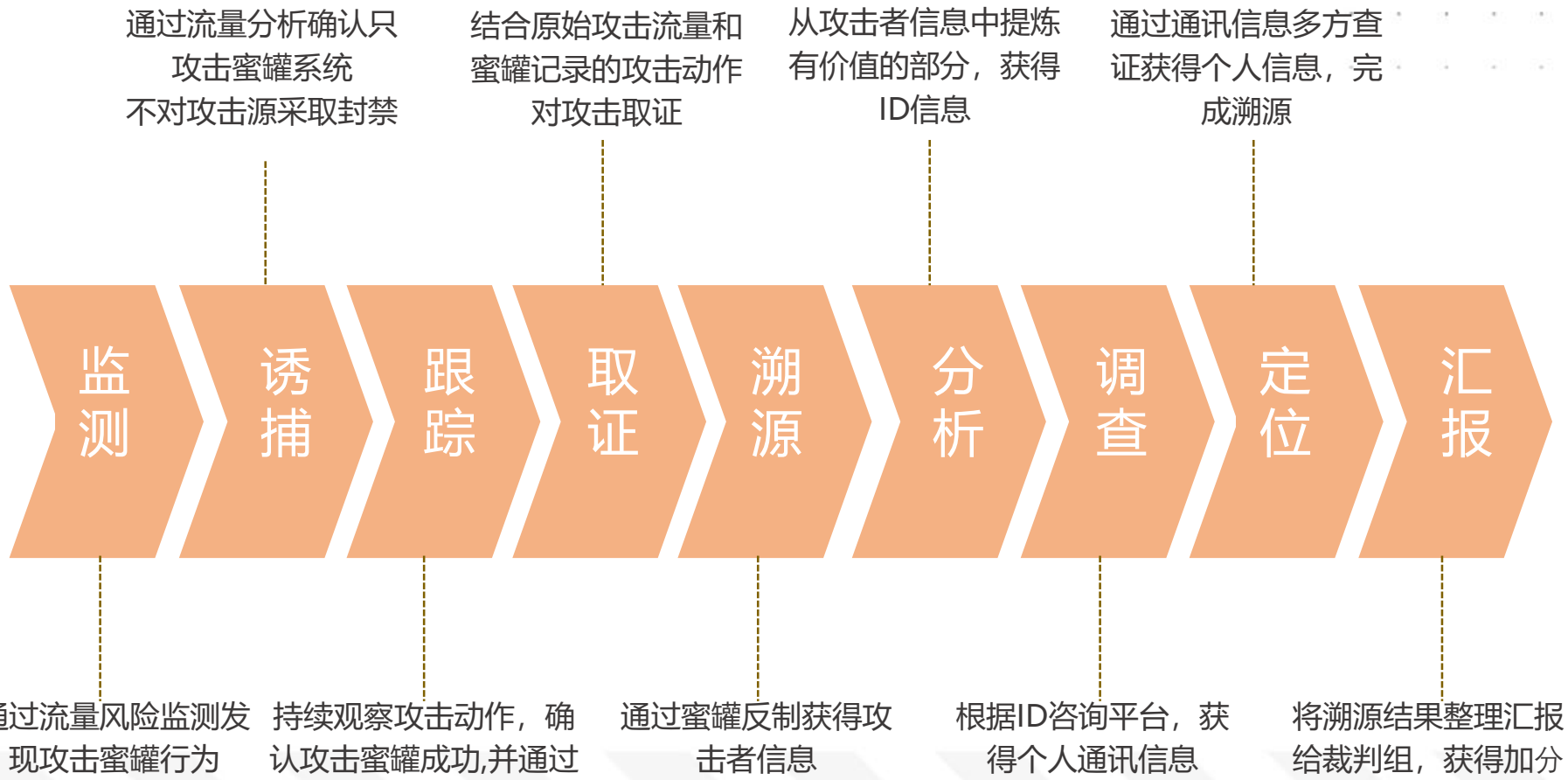
- 事件响应流程标准化，流程引擎驱动事件处置闭环
- 自定义协同处置流、提高处置质量和效率
- 提升应急响应处置能力

某攻防演练活动分析及溯源

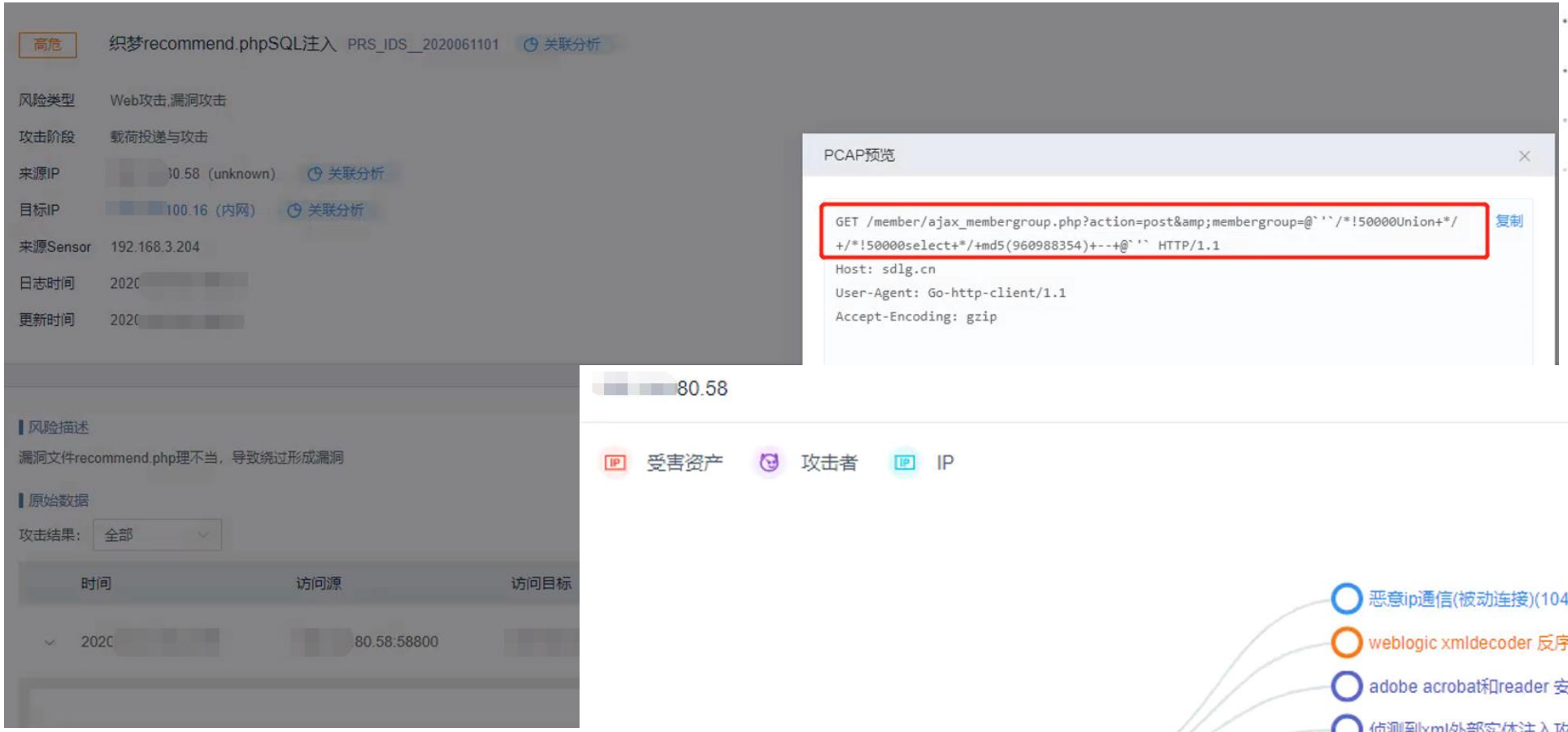
某日常运维钓鱼邮件事件处理

某攻防演练活动分析及溯源

网络安全创新大会
Cyber Security Innovation Summit



某攻防演练活动分析及溯源



某日常运维钓鱼邮件事件处理

网络安全创新大会
Cyber Security Innovation Summit

钓鱼邮件事件通告

某用户内部出现钓鱼邮件事件，需要对事件进行分析，并且给出钓鱼邮件账号及恶意文件名

事件确认

通过流量分析对恶意文件进行搜索，确认流量中检出该恶意文件，并通过恶意文件分析功能确认危害程度

影响面排查

通过流量分析调查画布功能对该邮箱关联邮箱进行定位、对相关主机互访关系进行定位。

文件逆向分析

通过对钓鱼邮件的恶意文件进行人工逆向分析，对恶意文件进行定性

确认恶意文件影响

结合逆向分析结果定位外部恶意访问地址，通过流量对所有外部地址流量进行筛查

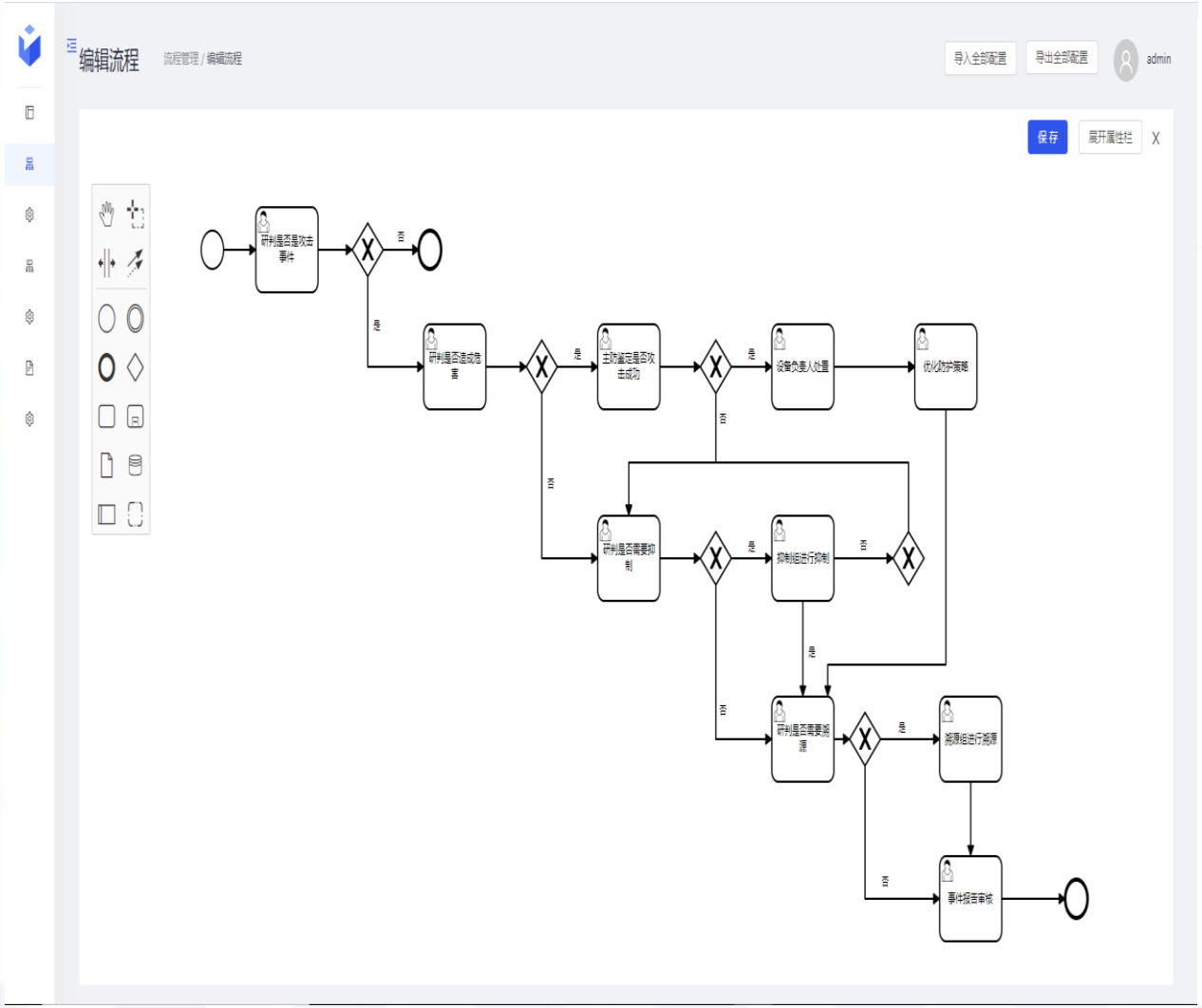
事件处理

对恶意文件外联地址进行封禁、相关邮件账号清理、影响范围内主机查杀，全员告警

编写事件报告

搜集整个过程数据及截图，形成安全事件报告

安全事件处理流程



钓鱼邮件事件

事件编号	事件类型	事件来源	是否启动应急	设备类型
XXXX-钓鱼邮件事件-001	钓鱼邮件	手动提交	否	—

事件状态	事件等级（预判/判定）	事件时间	上报人
待处理	低危 - –	2020-02-02 12:12:12	Admin

攻击IP

153.149.96.119	153.149.96.119	153.149.96.119

审核处理

已超时 60天24小时38分42秒

攻击方式

钓鱼邮件攻击

受攻击资产系统名称

电子邮箱系统

受攻击资产IP

182.1.56.59

事件描述

该类钓鱼邮件从6月17日至6月19日一共发送了8封,来自3个不同的源IP,均已经被邮件沙箱隔离。

事件原因

是欺骗性钓鱼网页，模仿合法网站收集用户的密码。

影响范围

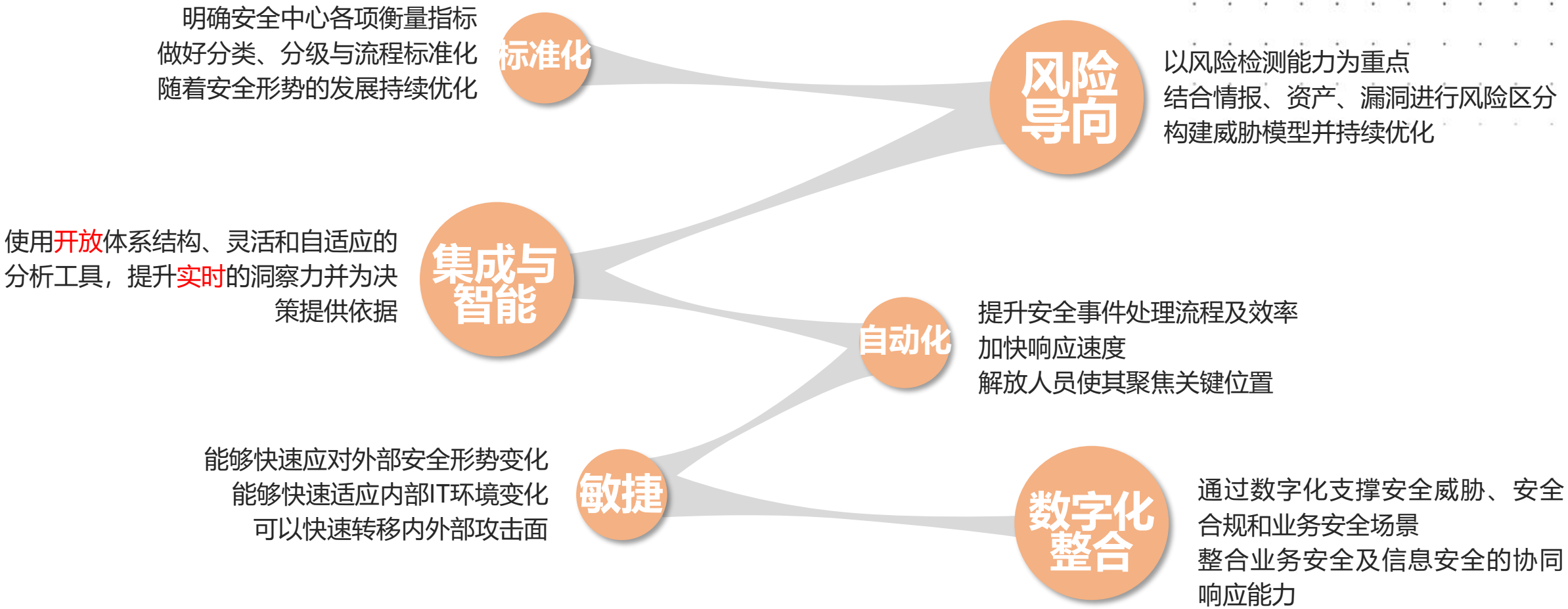
钓鱼邮件的收件邮箱
cheng.yuan@bankcomm.com
hanxing@bankcomm.com
chenmaohao@bankcomm.com

截图

攻防常态化运营特点


数据驱动
安全
深度检测
能力
PRS-NTA
安全分析平台
事件分析
研判能力
溯源取证
能力
提升实战安全
分析与协助效率
VMS
协作流程平台
自定义
流程编排
应急响
应能力
全周期
全流程
支持多源
数据对接

未来安全运营关键能力



“兵者，国之大事，死生之地，存亡之道，不可不察也”

“将听吾计，用之必胜，留之；将不听吾计，用之必败，去之”

网络安全创新大会
Cyber Security Innovation Summit

THANKS