ThreatBook

聚焦威胁 情报驱动

2018 网络安全分析与情报大会

ThreatBook

企业信息安全体系建设与实践

2018 网络安全分析与情报大会

-- 李强 --

中国农业银行科技与产品管理局
信息安全与风险管理处 副处长

网络安全形势严峻

各类安全事件频发，信息安全事态严峻

- 2017年5月12日晚，一款名为Wannacry的蠕虫勒索软件袭击全球网络，这被认为是迄今为止最巨大的勒索活动，至少150个国家、30万名用户中招，造成数十亿美元损失。
- 2017年10月，台湾远东国际商业银行披露，其电脑系统遭黑客植入恶意程序远端操控转账。据悉，主要受影响范围为少部分PC、伺服器（即“服务器”）及SWIFT系统，客户个人资料没有外泄。台湾警方随后表示，已通过国际刑警组织通报追回部分赃款，预计远东银行损失在50万美元以上，警方已着手进行鉴识比对，追查入侵远东银行电脑系统的黑客团伙。

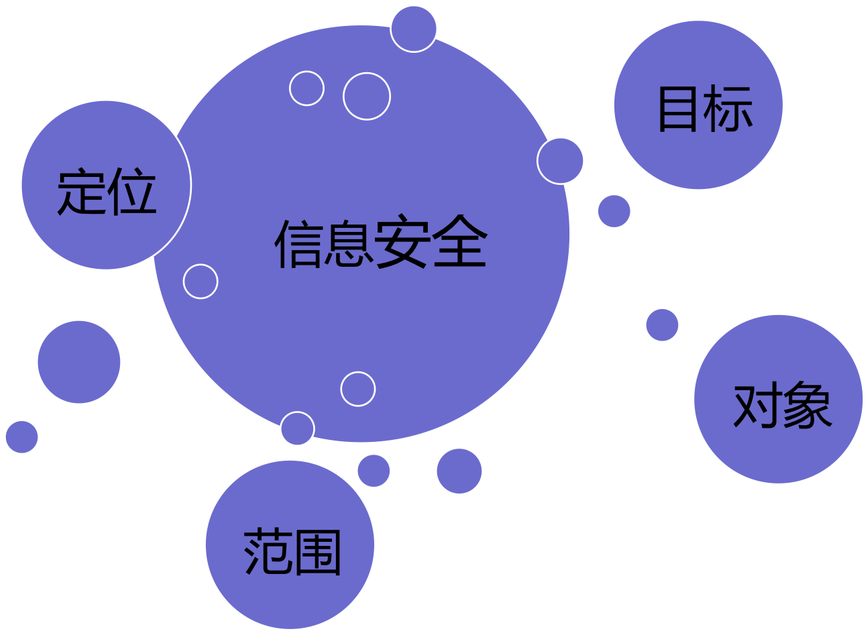
巨大经济利益驱使地下黑色产业链

- 整个黑产链条可划分多达15个不同工种，他们分工明确、协同作案，形成了完整的网络诈骗地下产业链。
- 初步统计，网络诈骗从业者至少有160万人，每年非法获利金额超过1100亿元。

数据泄露事件导致企业出现严重损失

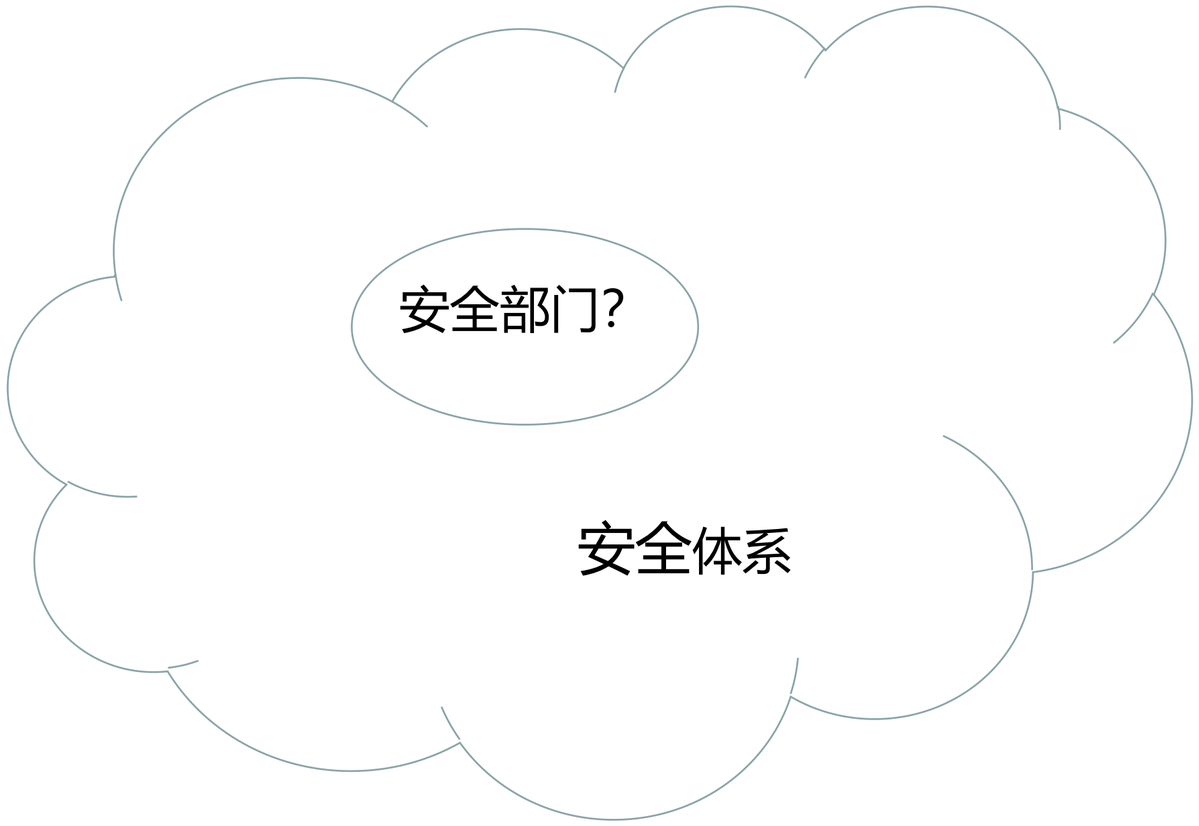
- 2018年3月17日，美国纽约时报和英国观察者报共同发布了深度报道，“ The Cambridge Analytica Files”，称Facebook上超过5000万用户信息数据被一家名为Cambridge Analytica（剑桥分析）的公司不当获取，用于在2016年美国总统大选中对目标受众进行精准信息投放，可能影响到大选结果。
- 几百亿美元市值瞬间蒸发，这个代价足以在地球上养活一支绝对庞大的安全团队，甚至可以直接收购几家规模比较大的安全公司了。

领导层对信息安全的疑问?



实现路径和方法?

领导层对信息安全的疑问?



建设者？运营者？检查监督？

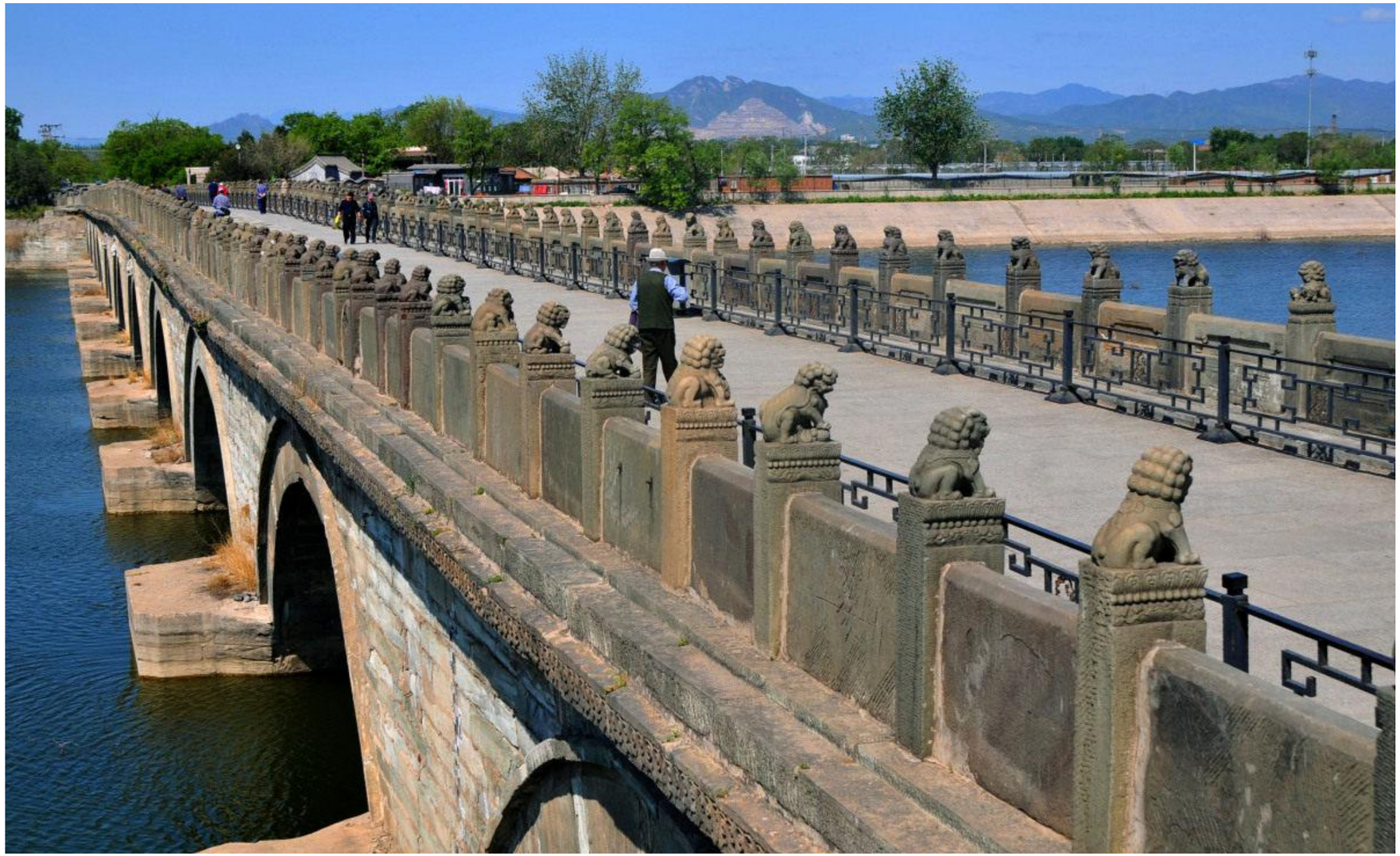
应该管什么?

安全部门和各部门工作关系?

工作边界如何划分?

为什么需要这些资源?

信息安全在企业发展中的定位



信息安全要与企业发展现状相结合

信息安全的基础工作目标

1 进不来-防攻击

2 出不去-防泄露

3 发现早-全面监测

4 处置快-应急响应

信息安全总体工作视图

领域		管理对象	管理和建设活动	监督和检查活动			
一般安全领域	业务管理运行	业务功能和数据	应用系统安全需求分析、应用系统操作手册制订、应用系统日常管理	合规检查 开发、运行、管理等工作过程合规检查和风险评估	技术检查 源代码安全检查、渗透测试、漏洞扫描、等保测评、网页防篡改等	行内其他部门检查或评估 风险评估、尽职监督检查、IT审计	行外检查或评估 公安部、人民银行、银监会、审计署等国家部委发起的信息安全检查
	应用建设运行	应用研发过程	安全需求评审、安全架构设计、安全需求分析、安全功能实现、安全编码、漏洞修复				
		源代码	源代码安全需求分析、源代码安全管理要求制订、源代码日常安全管理				
		开发和测试数据	开发和测试数据安全需求分析、开发和测试数据安全管理要求制订、实施开发和测试数据日常安全管理				
		已投产应用实例	已投产应用安全需求分析、数据访问权限管理、数据变更管理、漏洞修复				
		待提取数据	数据提取安全需求分析、数据提取安全要求制订、数据提取过程安全保护				
	IT基础设施建设运行	系统	系统安全需求分析、系统安全要求制订、系统安全技术研究、系统安全架构设计、系统资产信息统计、系统安全漏洞修复、系统用户权限管理、信息安全事件处置、威胁情报分析				
		网络	网络安全需求分析、网络安全要求制订、网络安全技术研究、网络安全架构设计、网络资产信息统计、网络安全漏洞修复、网络用户权限管理、信息安全事件处置、威胁情报分析				
	实体环境保障	数据中心园区	安全制度制订、值班、巡查、门禁系统建设管理、视频监控系统建设管理、访客管理				
		办公大楼	安全制度制订、值班、巡查、门禁系统建设管理、视频监控系统建设管理、访客管理				
		机房	安全制度制订、值班、巡查、门禁系统建设管理、视频监控系统建设管理、访客管理				
基础安全领域	威胁情报和态势感知		安全威胁情报收集、安全威胁情报分析、安全威胁情报通报、安全态势感知平台需求分析、安全态势感知平台架构设计、安全态势感知平台建设、安全态势感知平台运营				
	防病毒		防病毒系统需求分析、防病毒系统建设、防病毒系统运营				
	钓鱼网站		反钓鱼网站需求分析、钓鱼网站监测、钓鱼网站处置				
	终端	自助终端	终端安全防护需求分析、终端管理制度编制、终端安全新技术研究、终端安全技术架构设计和建设、终端安全相关资产信息统计、网络访问控制、安全补丁管理发、安全策略制订、外设接口和端口安全控制、安全事件应急处置				
		办公终端					
		客服终端					
		柜员终端					

可供选择的实现路径和方法

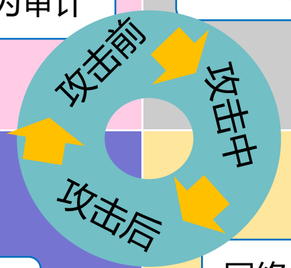
防攻击：攻击进不来

Predict 预测

- 源代码安全检查
- 渗透测试
- 互联网暴露资产监测
- 漏洞扫描
- 子系统安全测评
- 源代码泄露监测
- 等保测评
- 威胁情报管理
- 反钓鱼网站
- 漏洞修复
- 基线配置核查
- 操作行为审计

Prevent 防御

- 网络防火墙
- 网络入侵阻断
- 网络准入控制
- 应用防火墙
- 服务器入侵阻断
- 垃圾邮件拦截
- 身份认证
- 访问控制
- 网页防篡改
- 终端端口管理
- 终端外设管理
- 终端补丁管理
- 终端账户管控
- 病毒查杀



Respond 响应

- 攻击路径展示
- 人工调查和处置
- 攻击者画像
- 智能调查和处置
- 终端威胁响应
- 控制点优化

Detect 监测

- 网络入侵检测
- 服务器入侵检测
- 用户行为分析
- 数据库安全审计
- 集中日志分析
- 异常流量分析
- 威胁情报服务
- 终端威胁监测
- 病毒流量监测
- 蜜罐

可供选择的实现路径和方法

防泄露：信息出不去

Predict 预测

- 用户行为分析

Prevent 防御

- 网络准入控制
- 数据加密
- 数据脱敏
- 用户身份认证
- 移动存储设备管理
- 终端防泄漏
- 邮件防泄漏
- 文件加密
- 打印水印
- 信息访问控制
- 屏幕水印
- 桌面虚拟化

攻击前 → 攻击中 → 攻击后

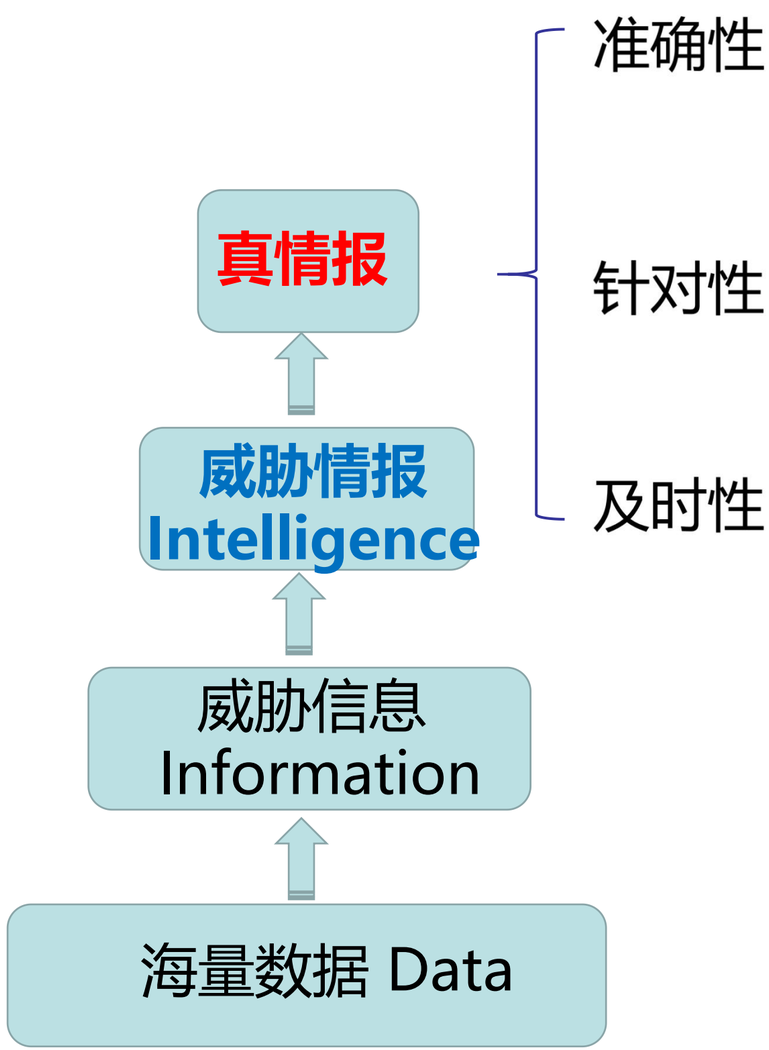
Respond 响应

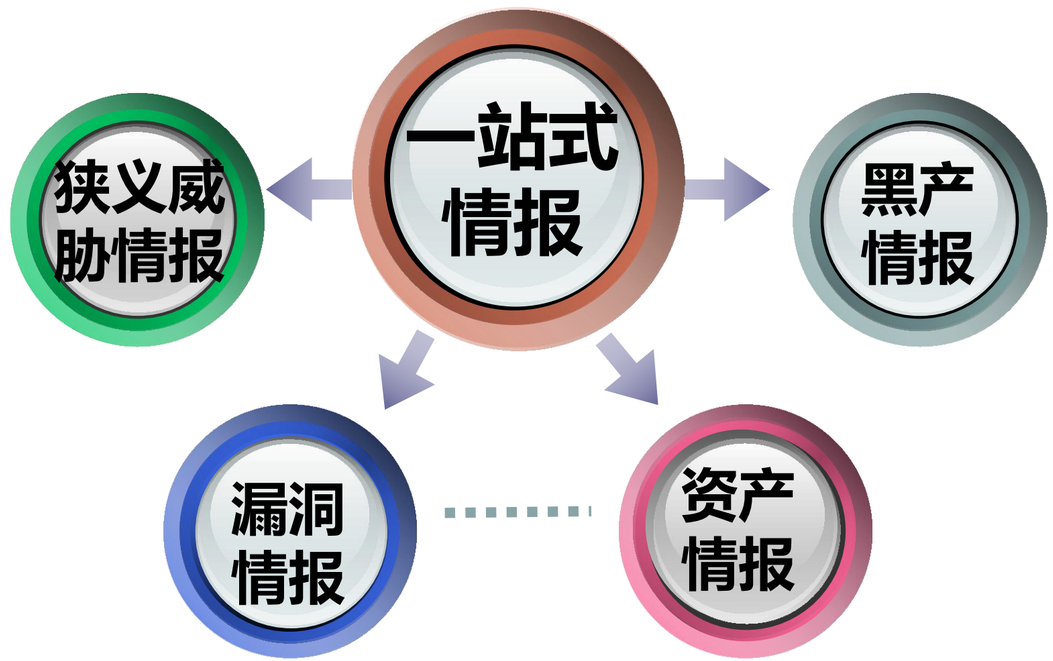
- 泄露源代码删除和修改
- 泄露文档删除
- 操作行为审计
- 调查取证
- 控制点优化
- 终端威胁响应

Detect 监测

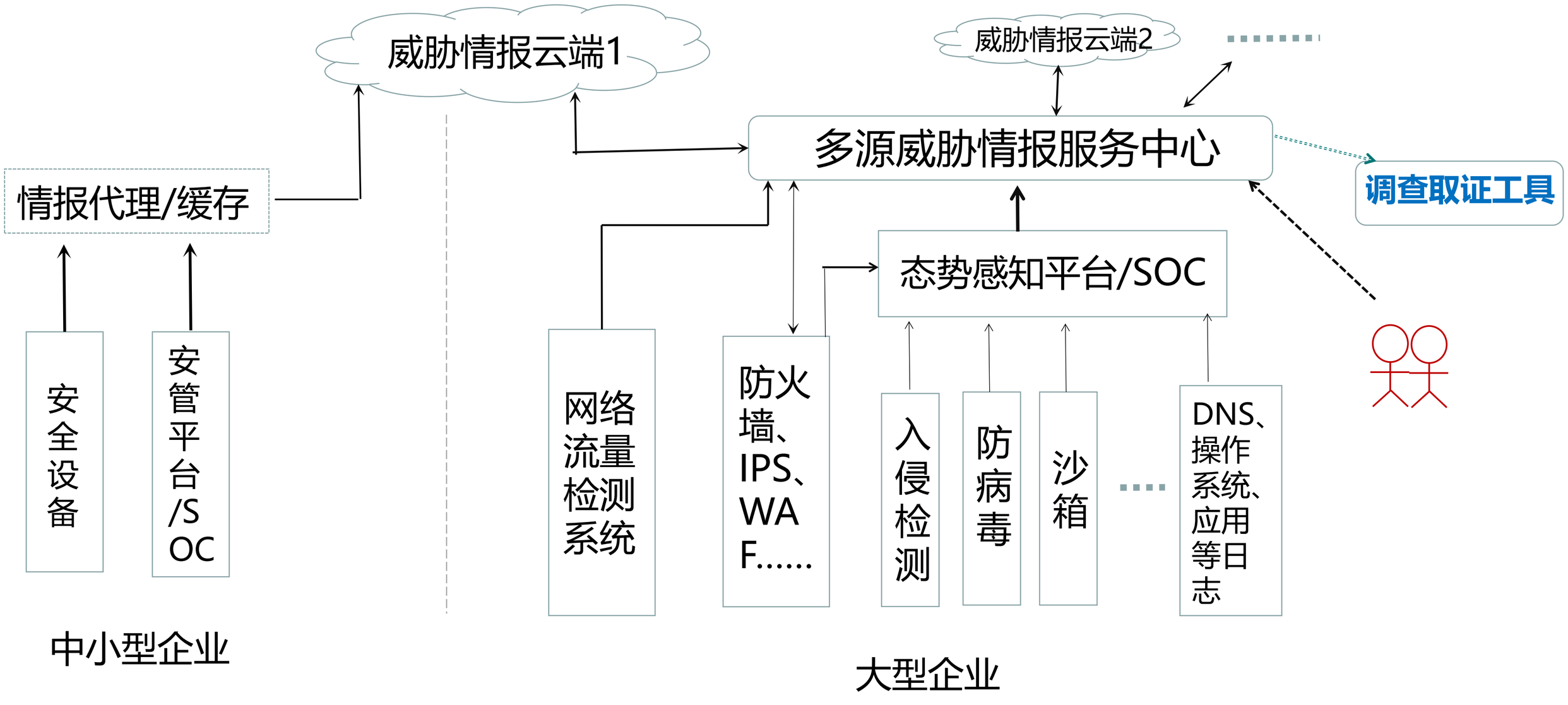
- 数据库安全审计
- 源代码泄露监测
- 文档泄露监测
- 集中日志分析
- 异常流量分析
- 终端威胁监测
- 用户行为分析

以威胁情报为例（用户视角）

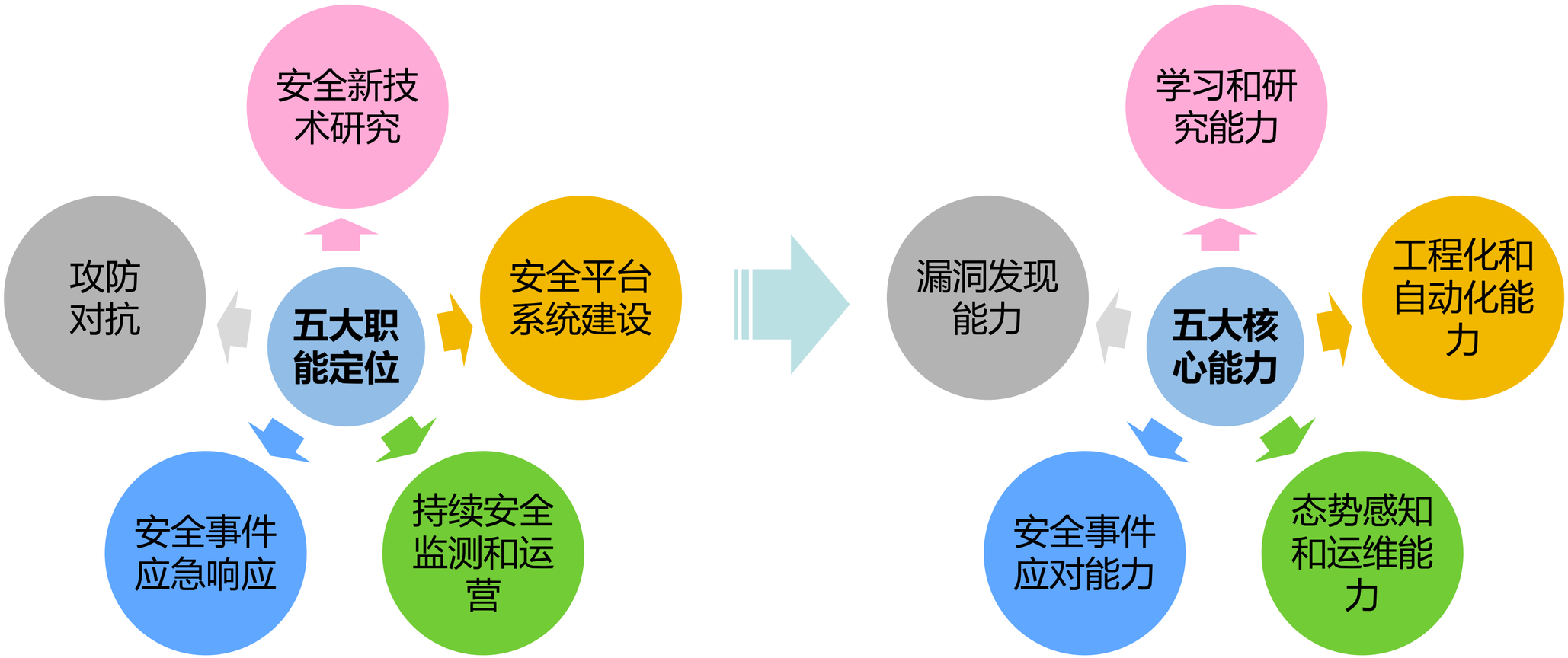




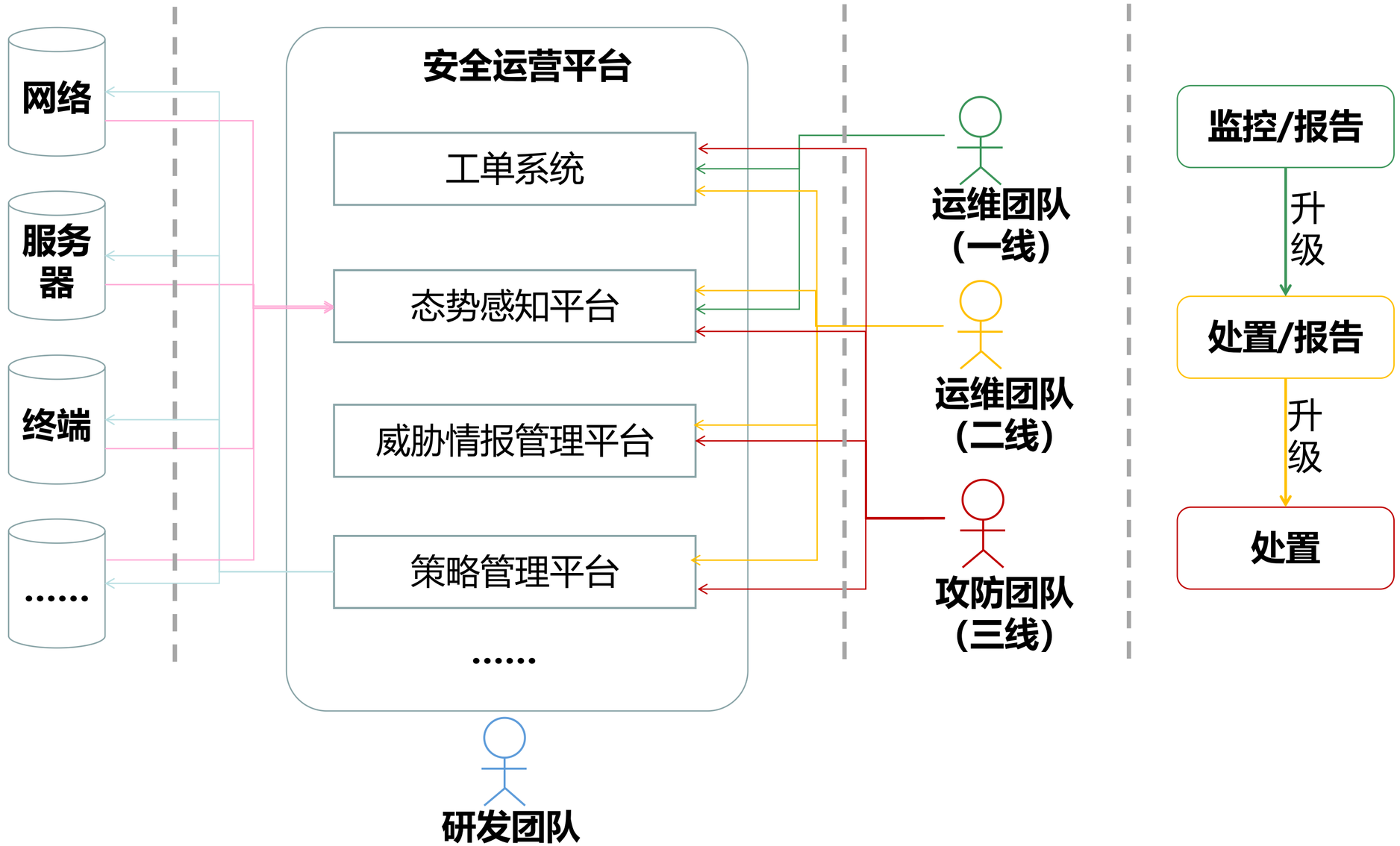
以威胁情报为例（用户视角）



安全团队的五大职能定位与五大核心能力

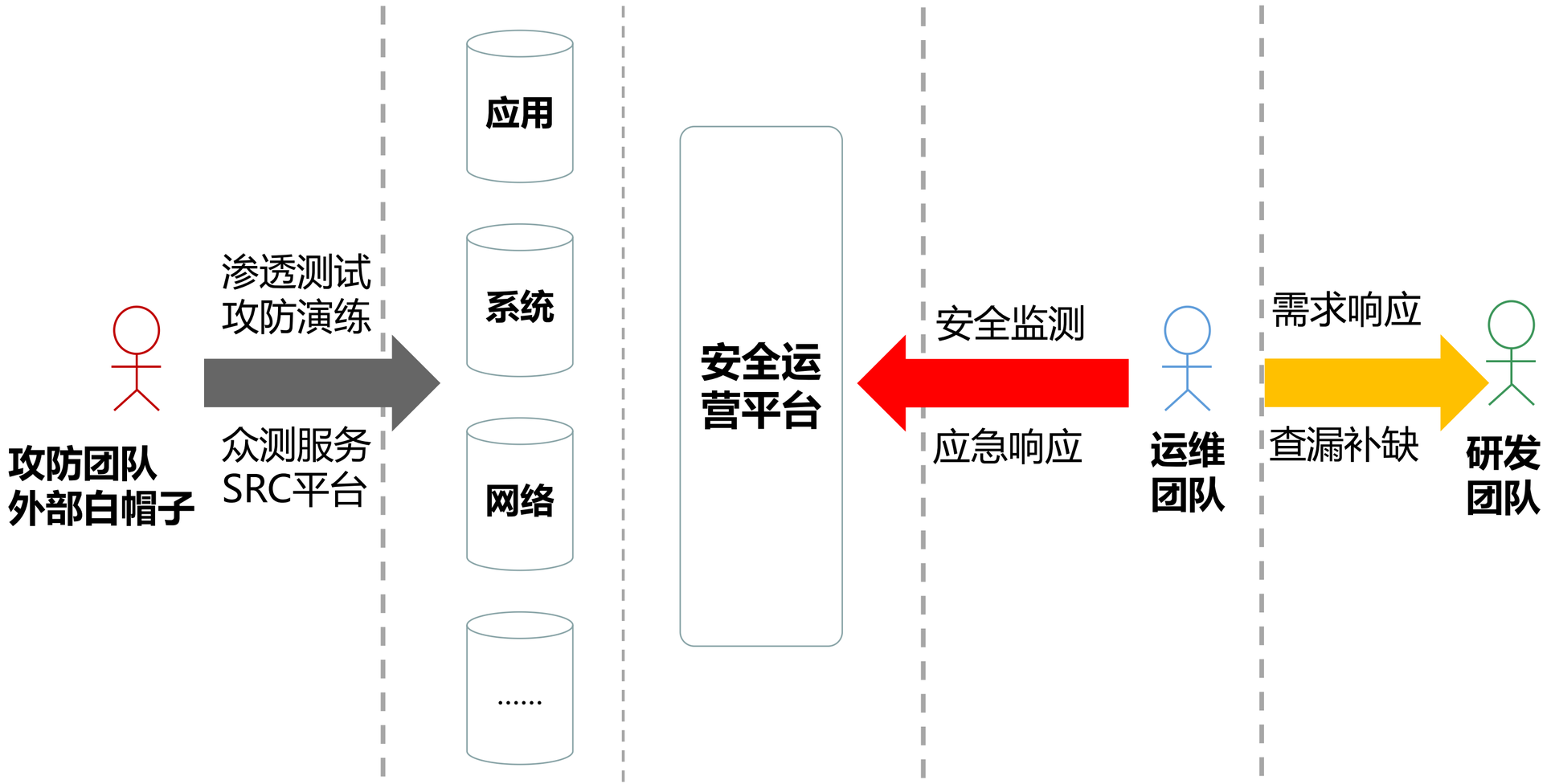


建立安全运营体系


网络
服务器
终端
……
安全运营平台
工单系统
态势感知平台
威胁情报管理平台
策略管理平台
……
研发团队
运维团队
（一线）
运维团队
（二线）
攻防团队
（三线）
监控/报告
升级
处置/报告
升级
处置

建立自我检查完善的机制

以真实红蓝对抗检验信息安全防控效果



企业信息安全体系建设九大要点

1. 向高管层阐明信息安全的作用，摆正安全和业务的关系。
2. 明确信息安全的工作目标。
3. 明确信息安全管理的对象，规划完整的信息安全管理视图。
4. 明确各方的信息安全职责，信息安全不止是安全部门的事情，需要各部门群策群力。
5. 根据面临的风险点，选择构建适合自己的信息安全技术体系。
6. 信息安全不止是技术，而是技术和管理的结合。
7. 信息安全不止是建设，更重要的是运营。
8. 信息安全工作的核心在于人，需要构建内外结合的信息安全队伍。
9. 用PDCA的思想，建立信息安全自我完善机制。

谢 谢！

ThreatBook

感谢您的观看

2018 网络安全分析与情报大会