面向常态化对抗的安全运营

万京平
奇安信集团安服子公司

目录

01 企业如何面对有组织有针对性的“实战”对抗

“实战”背景下的安全新常态

政企面临威胁升级

攻击目标转变：

重要单位都是国家级网空对抗中的分子。

攻击体系提升：

人员向有组织化，专业化提升。

攻击手段升级：

成建制攻击，对互联网暴露攻击面的梳理。外围情报共享，攻击具有更快的攻击速度，打击更精准。

“实战”对抗趋于常态化

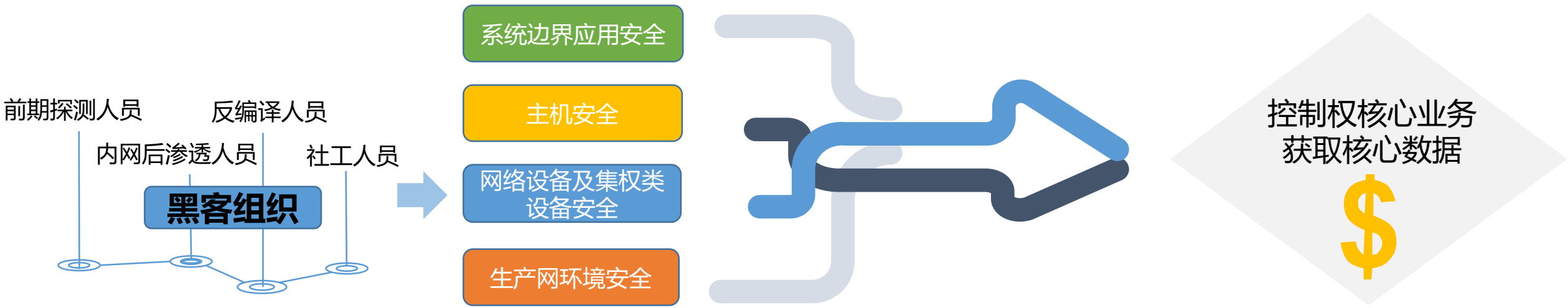
“实战”是检验安全的唯一标准：

各类法律法规标准，网络安全法，等保2.0，各类网络安全管理规定，数据安全管理办法等等，加深了对企业的管理粒度，传统监督检查手段也在由沙盘推演向攻防演习转变。

2006—2018年，美军先后举行的大规模“网络风暴”演习共6次。近几年我国由主管单位牵头的红蓝对抗演习也常态化开展，政企安全建设都面临新的挑战。

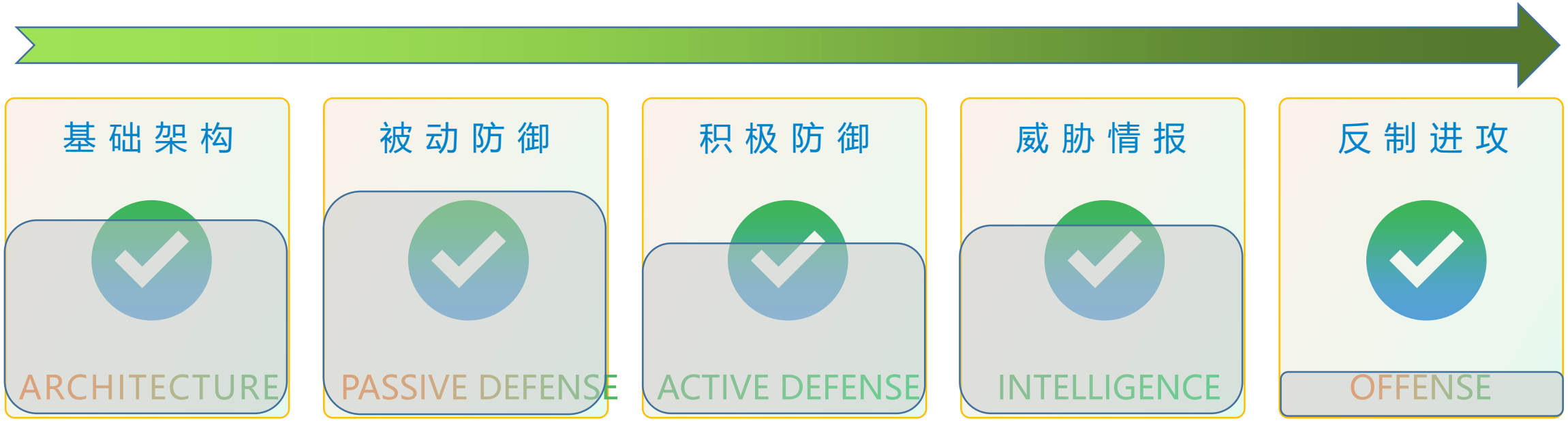
实战的专业化趋势

信息收集	漏洞分析	渗透测试	后渗透
资产发现	漏洞测试	WAF绕过	获取内网敏感信息
端口扫描	供应链研究	反病毒检测	横向渗透
指纹识别	公开资源研究	监测机制回避	中间人劫持
敏感路径探测	扫描结果关联分析	常用WEB攻击	建立隧道
关联域名探测	创建攻击树	逆向、流量分析	提权、权限维持与长期控制
社工、钓鱼、水坑	可利用效果验证	模糊测试	清理痕迹



安全核心能力发展参差不齐

如同我国基本国情一样，安全核心能力亦是贫富不均



加强自身 强身健体
- 安全管理体系
- 安全域划分
- 安全加固
- 安全评估
- 应用内建安全

构建工事 纵深防御
- 传统安全防护
- 纵深防御体系
- 缩小攻击面
- 消耗攻击资源
- 迟滞攻击

全面监测 快速响应
- 持续检测响应
  - 安全分析
  - 追踪溯源
  - 响应处置
- 完善防御体系

获取情报 准确预警
- 信息收集
- 情报生产
- 情报分析验证
- 狩猎

进攻反制 先发制人
- 法律手段
- 对抗措施
- 自我防卫行为

新挑战与老难题

资产边界，攻击面扩大

移动端，虚拟化，物联网，急剧扩张的业务及资产。让企业无法准确判断其攻击面。

攻防之间理解层面的差异

企业大多不了解攻击手段，更不会投入到攻击手段的研究分析。看似“风平浪静”实则“暗流涌动”。

网络安全观的偏差

建设思路很多还停留在合规即免责的基础上，“目的性”很明确，没有切实的上升到安全生产的高度。

网络安全依然还是纸面工作

很多单位报告的水平远比技术水平高，网络安全工作更多停留在口头喊重视，人财物投入严重不足。

无法选择的大背景

可用性

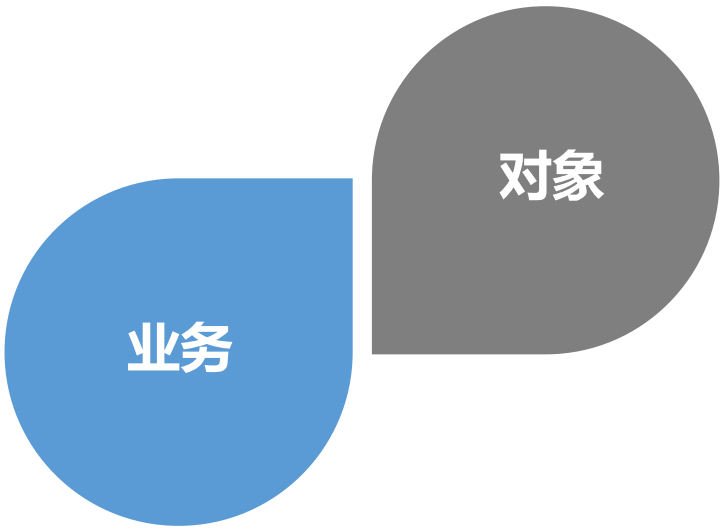
涉及持续性生产、持续性服务的业务

互联网+

大量依托互联网+的业务

社会影响

重要关键基础设施



TO C

直接面向大规模用户提供服务

用户数据

大规模用户的敏感数据

价值

关键敏感重要用户的关系延伸

即使这些因素都不存在，那也还有一个因素—运气

“战时“情况

外部力量

全民动员

突击上设备

突击改口令

互联网服务关停

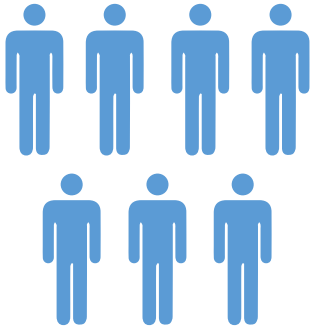
7x24值守

情报共享联盟

互联网出口缩减

自身要硬，内外结合

战术大师也得有必要的人力资源



国家队打法

俱乐部打法

“平战结合”时刻准备打仗

战时较量始于平时准备，“有备则制人，无备则制于人。

长期准备

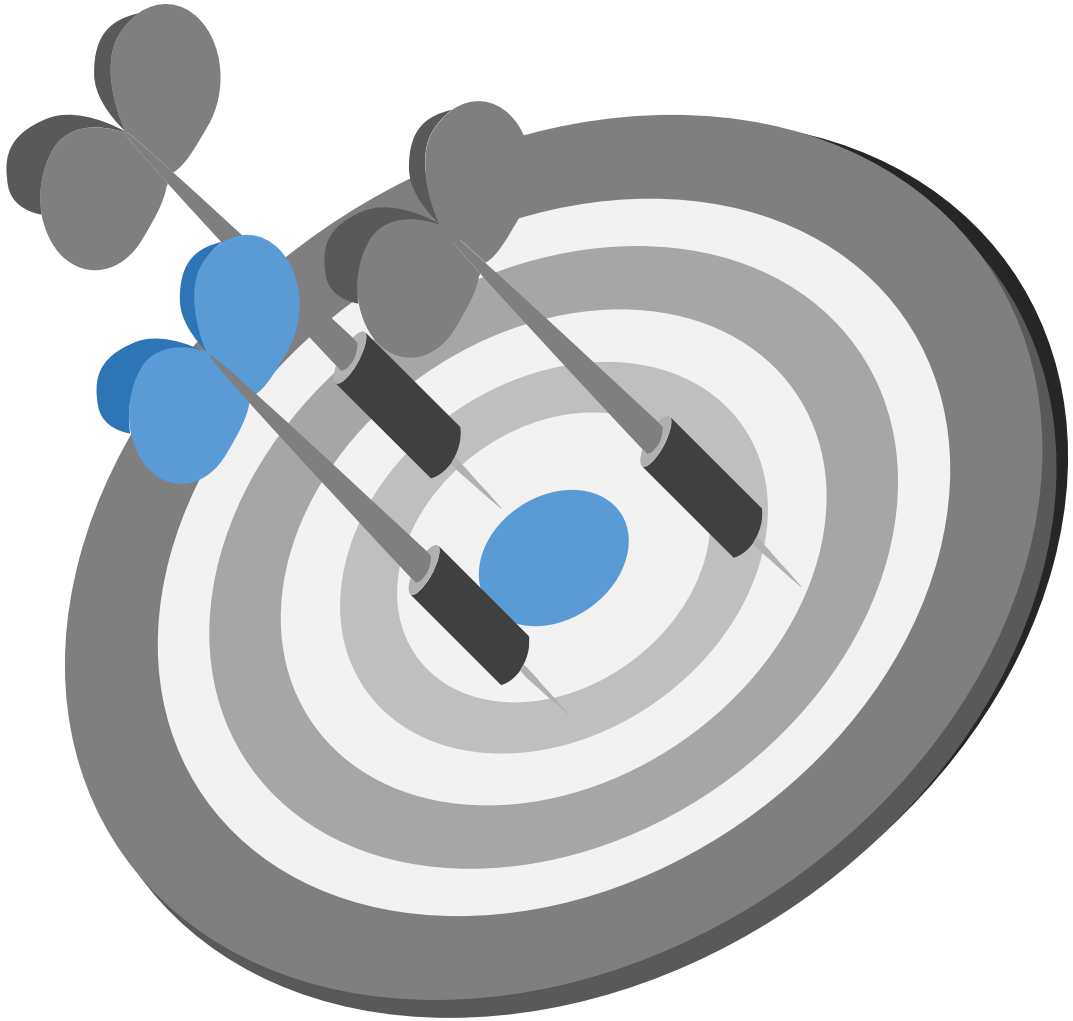
长期准备，就是居安思危，有计划、有步骤地实行网络安全建设。平时组织网络安全建设，做好网络安全各项准备，是战时保护关键信息系统安全的基础和前提。因此，在日常工作中，必须结合体系建设、基础设施建设，有计划、有步骤地做好网络安全的各项准备，只要存在安全威胁，这项工作就不能停止。

重点建设

重点建设，就是在服从整体建设大局的前提下，区分轻重缓急，有重点、分层次地实施网络安全建设。这体现了网络安全建设与信息化建设的依赖关系，是和平时期统筹安排网络安全建设的要求。根据单位情况和国家安全监管要求需要，网络安全建设以关键基础设施为重点，特别以核心数据中心、互联网服务以及关系核心生产数据的重要目标为重点。

平战结合

平战结合，就是在确保战备效益的前提下，兼顾社会效益、投资效益。这充分反映了具有中国特色的网络安全特点，是网络安全发展的必由之路，也是信息化发展对网络安全的客观要求。实践证明，网络安全平战结合，有利于网络安全长期准备，提高网络安全整体防护能力；有利于信息化发展，为企业做贡献；有利于增强网络安全自身发展能力。



02 从普适性的安全运维转向专业性常态化的安全运营

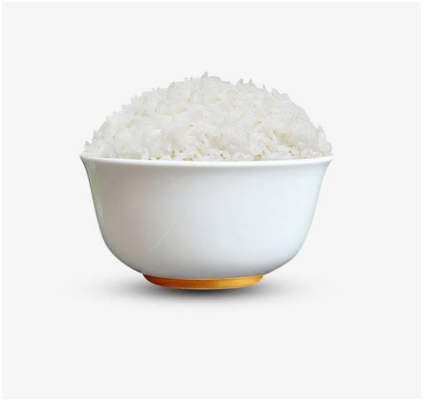
由运维至运营——理念的变化

通过人、工具（平台、设备）、发现安全问题、验证问题、分析问题、响应处置、解决问题并持续迭代优化的过程，通常可以称之为安全运营。

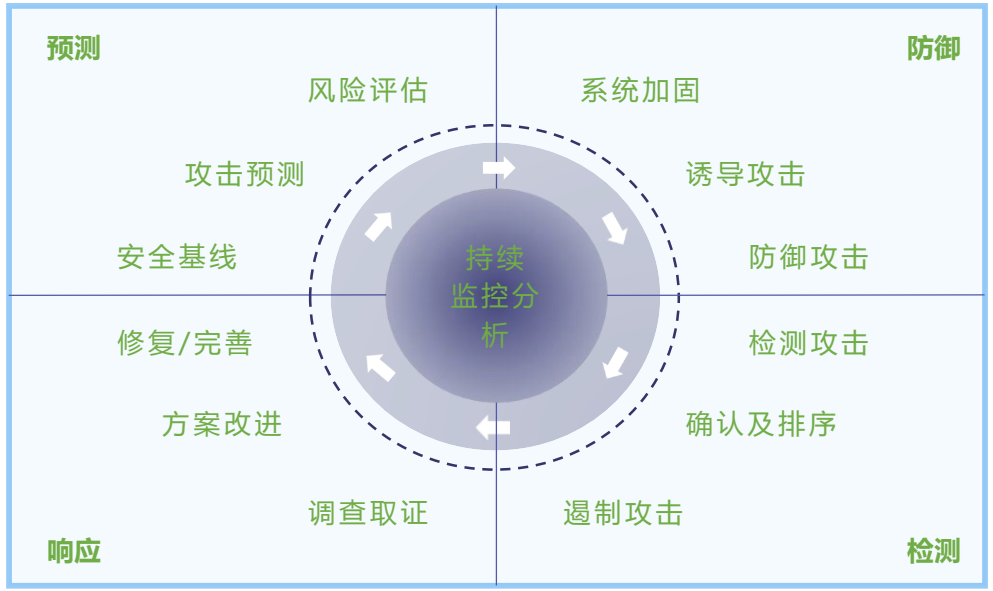
可用

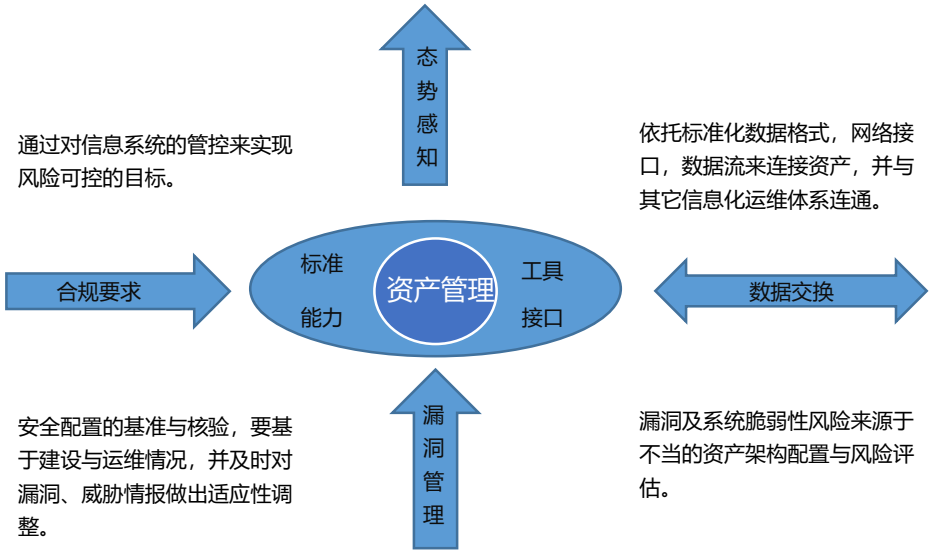
运维 运营

价值



常态化运营的构成





安全管理

以自身单位体制机制为出发，结合合规化体系，形成完整的管理通路.

基础设施（工具平台）

- 以合理的架构方式选择设备布防，实现控制与感知
- 保持所有安全设备的高可用性，确保监控是有效的

安全运营

- 以资产、漏洞、补丁、策略等基础配置工作为基石。
- 以检测与响应为核心驱动力，形成闭环体系。

安全运营需要持续投入与迭代

01

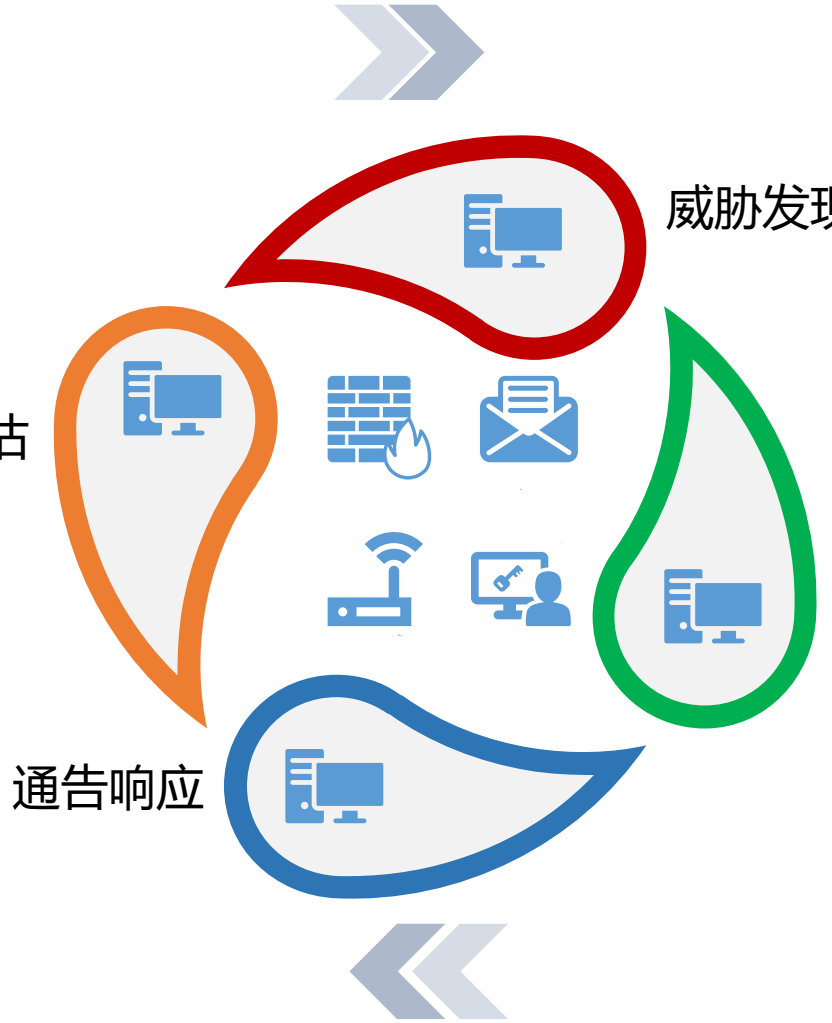
安全研究（Plan）

做好安全工作的整体设计、规划、研究工作，设计各类安全体系。

02

安全建设(Do)

安全基础设施建设，根据业务需要进行的项目建设。



03

安全服务(Check)

安全审计、渗透测试、安全评测、应急响应、安全检测、预警通报等服务。

04

安全优化(Action)

逐步完善安全管理体系、安全防护体系、安全评价体系。

运营不是一朝一夕，不是一蹴而就，需要一路前行

运营要尽可能是高效的

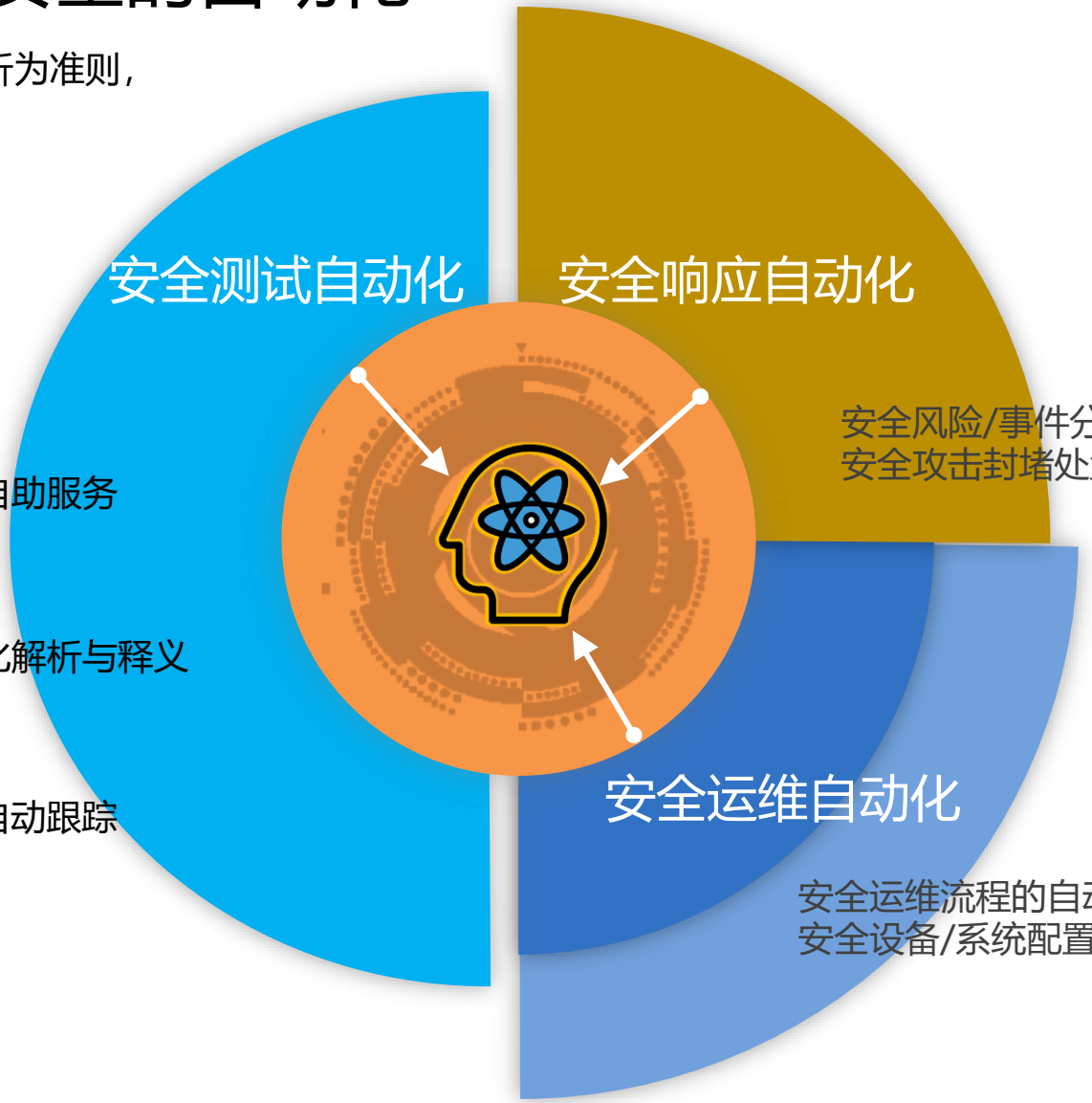
以运营的理念，实现安全的自动化

改变传统，以一切可管理、可量化、可分析为准则，
实现自动化管理和持续的安全响应。

安全检测平台资源自助服务

安全检测结果自动化解析与释义

安全漏洞管理流程自动跟踪



数据是运营量化评估的基础

安全管理

风险评估	安全检查
日常审计	合规要求
通知通报	审核授权

风险源辨识	资产数据
合规数据	事件事态
考核数据	审计数据

安全技术

安全资产管理	安全事件响应
用户身份管理	安全漏洞管理
策略基线管理	安全知识管理

资产数据	事件数据
漏洞数据	策略数据
身份数据	知识数据

安全设施

防御平台	采集平台
监测平台	分析平台

日志数据	网络流量
威胁情报	规则数据

- 态势感知展示
- 威胁检测分析
- 漏洞管理联动
- 合规管理检查
- 资产管理控制

安全可见 上能汇报

安全可控 下能通报

核心——落到实处

- 不同的单位有不同的组织模式
- 不同的单位有不同的业务类型
- 不同的单位有不同的协同困境
- 不同的单位有不同的现实情况

因地制宜，稳扎稳打

人员组织

1-3个人

基础运营（检测与分析、响应与处置、资产维护与配置管理）

5-10个人

进阶运营（资产管理（终端及主机安全管理）、漏洞检测与管理、配置管理、安全监控、溯源分析、应急响应、规则建模、事件挖掘、常态化演练、常态化考核）

……

基础平台

流量分析平台

日志收集与分析平台

终端安全管理系统

主机安全管理系统

边界安全统一管理平台

自动化扫描与监测平台

……

USECASE

异常行为类

（VPN短时异地登录、敏感账号可疑时段登录…）

异常访问类

（绕堡垒机访问、内网高危端口访问…）

猜测破解类

（多次登录失败再成功…）

安全审计类

（高危操作、非变更时段操作…）

资产异常类

（台账外资产、台账外端口…）

……

体系与流程

工单流转

通报处置

考核评价

常态演练

知识维护

……

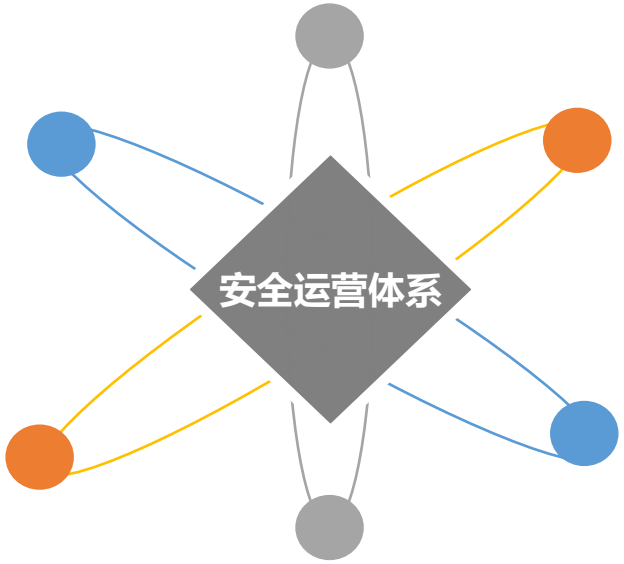
03 以安全运营的视角构建面向对抗的安全体系

通过安全运营驱动整体安全

安全基础设施

防御平台　监测平台　采集平台　分析平台

工具



人员

安全管理

风险评估　安全检查

日常审计　合规管理

通知通报　审核授权

流程

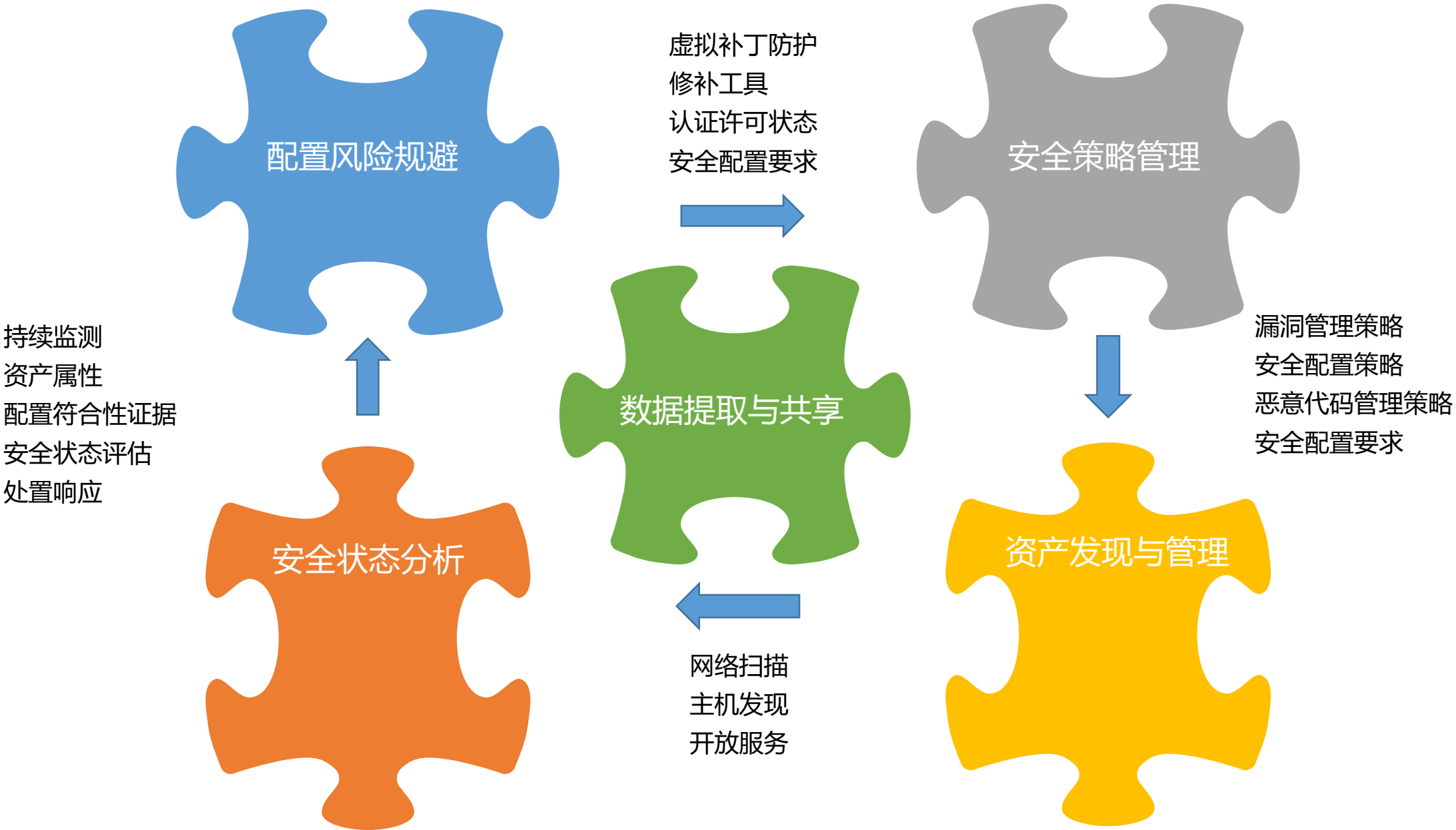
安全技术

安全资产管理　安全事件响应

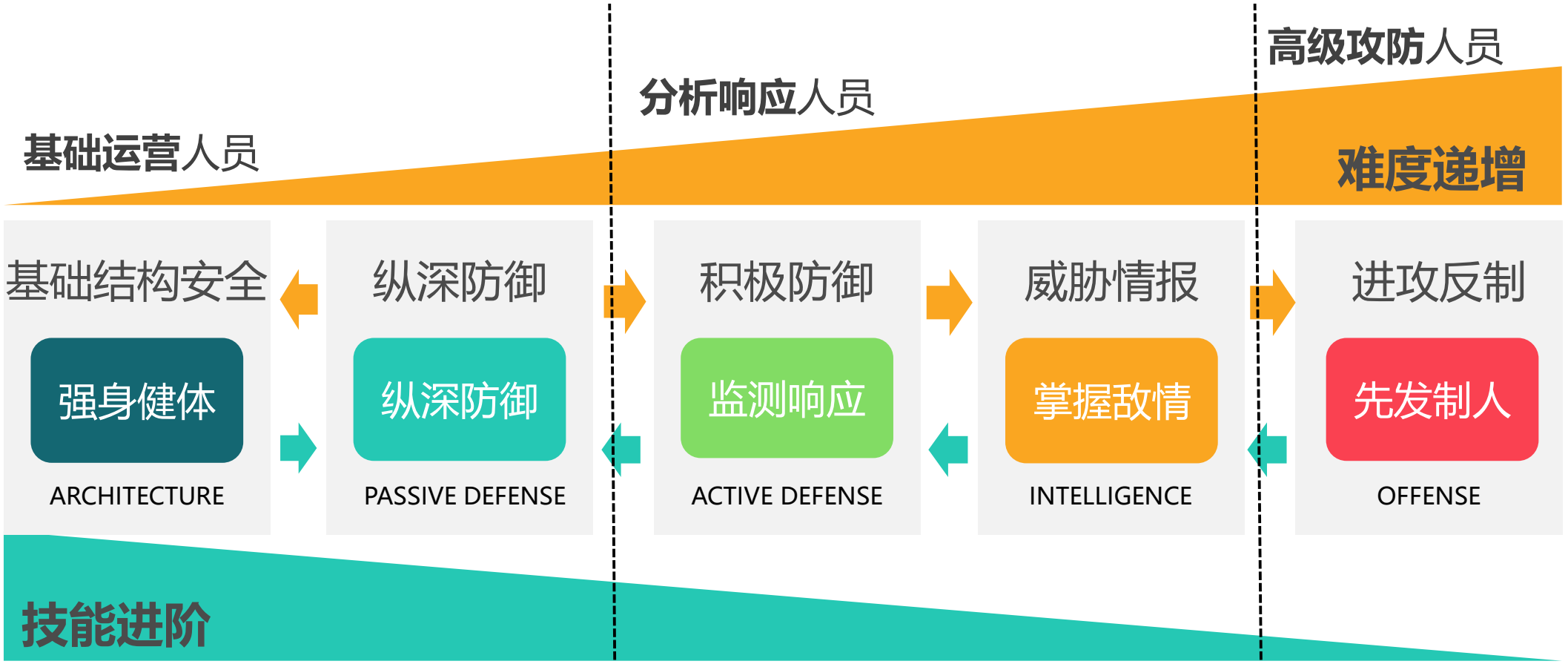
用户身份管理　安全漏洞管理

策略基线管理　安全知识管理

核心——安全运营基础为先


配置风险规避
虚拟补丁防护
修补工具
认证许可状态
安全配置要求
安全策略管理
持续监测
资产属性
配置符合性证据
安全状态评估
处置响应
数据提取与共享
漏洞管理策略
安全配置策略
恶意代码管理策略
安全配置要求
安全状态分析
资产发现与管理
网络扫描
主机发现
开放服务

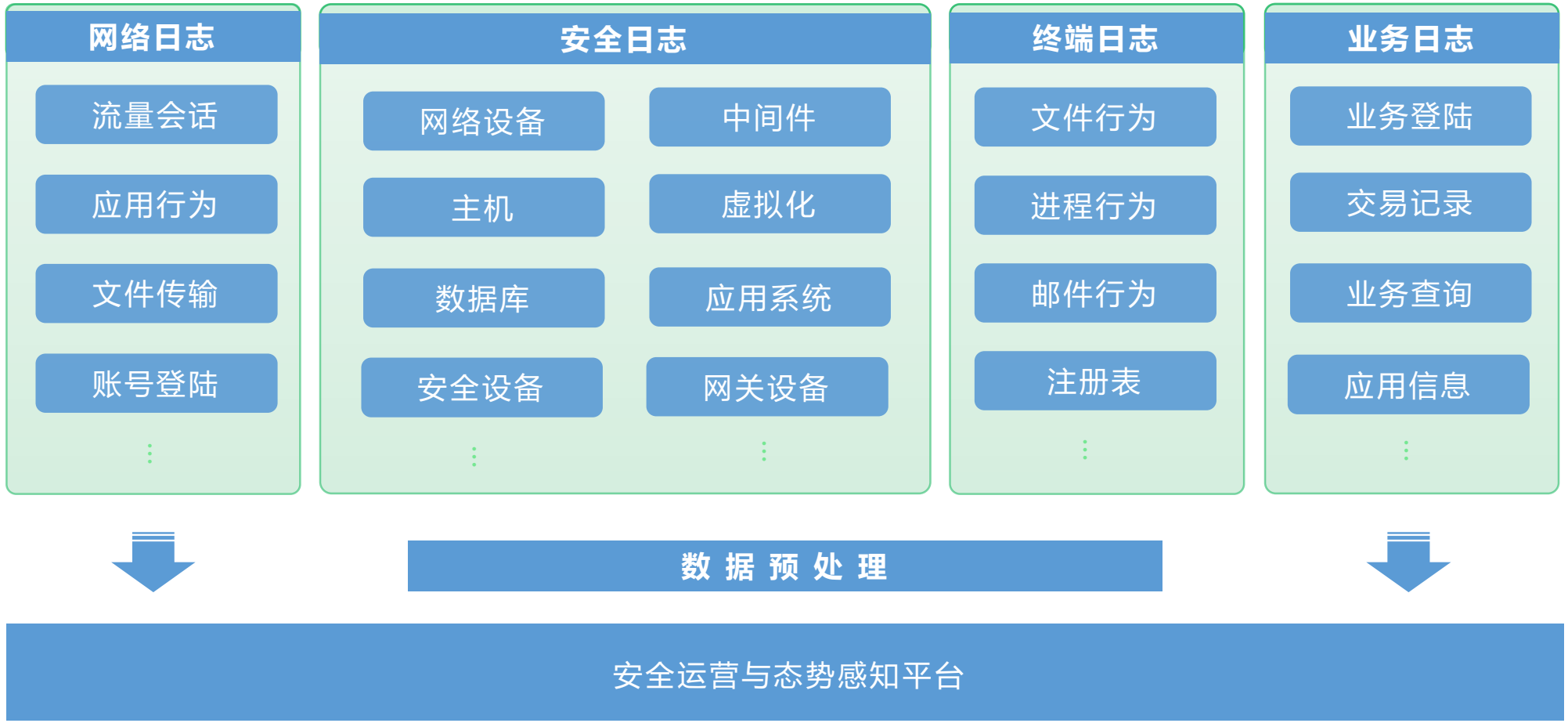
人-安全运营体系构建以人为主导



物-构筑核心平台

常见设备的自动解析、过滤、富化、内容转译、归一化

通过**Syslog、DB、SNMP、Netflow、API**接口、镜像流量、文件等多种采集方式采集、过滤，处置海量数据

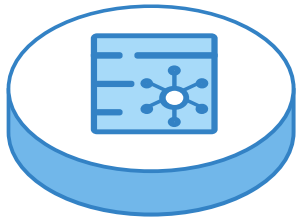


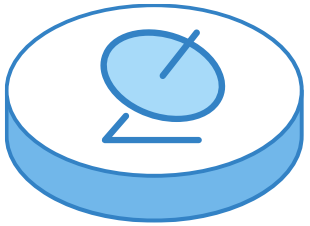
物-垂直体系化构建

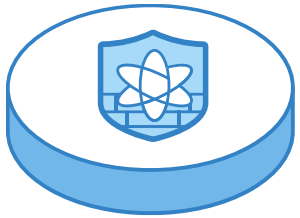
数据共享

Tier1 总部

安全策略管理
安全系统管理
安全测量管理


安全策略管理


总部SOC平台

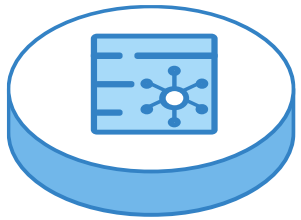

安全态势分析

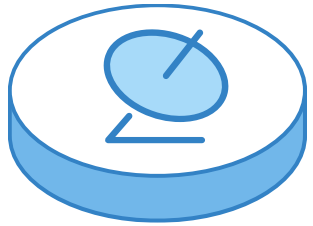
态势感知
审核监控
风险评估

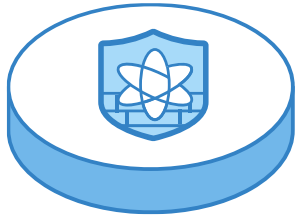
业务主管
运维团队
安全建设团队
安全运营团队
安全管理团队

Tier2 分支

安全策略管理
安全系统管理
安全测量管理

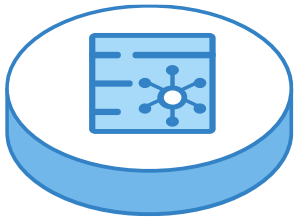

安全策略管理


二级SOC平台


安全态势分析

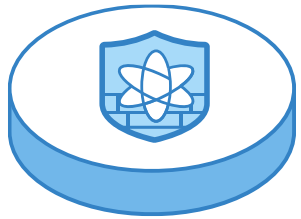
上级主管机构
业务分支主管
网络评估团队
外部服务支撑

Tier3 基层


安全策略管理


资产发现与管理


配置风险规避


安全状态分析

桌面支持
网络管理员
系统管理员
上级策略落实

配置策略 → 发布推行 → 追踪配置状态 → 威胁情报 → 漏洞修补 → 确认修改 → 发布更新 → 持续监测 形成初步态势感知

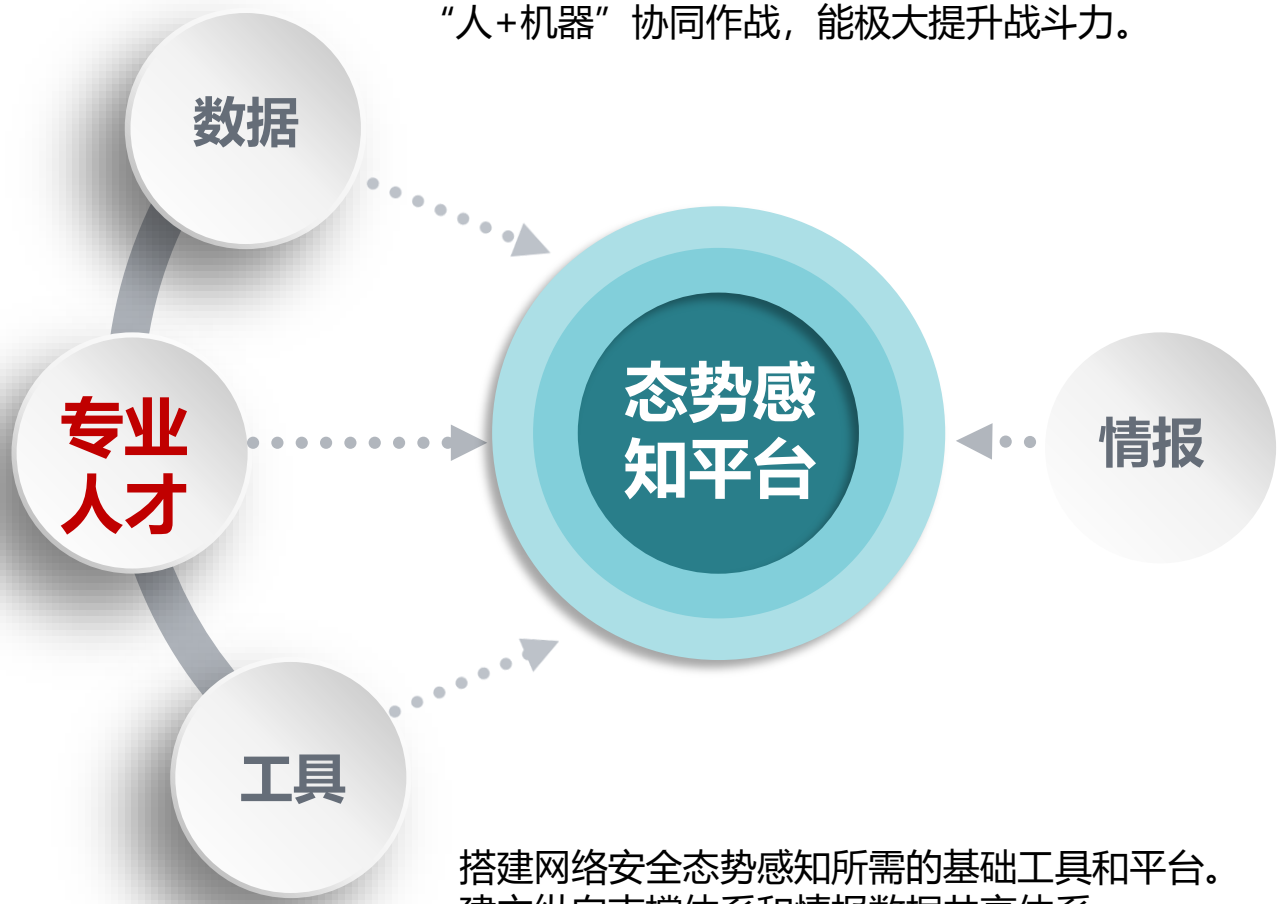
技-培养核心技术能力

日常运营工作梳理

- 资产运营
- 基础信息维护
- 安全事件分析
- 安全模型构建
- 事件追踪溯源
- 攻击者刻画
- 日常通报预警
- 应急预案编排
- 应急演练

人与人的对抗、人与机器的对抗、人与人工智能的对抗。

“人+机器”协同作战，能极大提升战斗力。



搭建网络安全态势感知所需的基础工具和平台。
建立纵向支撑体系和情报数据共享体系。
建立自动化、体系化的主动动态防御能力。

- ✓ **监控岗：**
  实时监控、预警通报
- ✓ **分析岗：**
  数据分析、验证
- ✓ **追溯岗：**
  情报分析、威胁追溯
- ✓ **处置岗：**
  安全事件技术处置
- ✓ **通报岗：**
  安全事件预警通报

战-战术战法演练

预测

- 靶场
- 渗透测试
- 风险评估
- 仿真
- 威胁情报
- 安全基线
- 漏洞管理
- 对抗演练

防御

- 安全加固
- 动态授权
- 访问控制
- 加密脱敏
- 入侵防御
- 安全隔离

响应

- 事件处置
- 应急响应
- 调查取证
- 安全运维
- 安全审计

监测

- 威胁检测
- 资产检测
- 行为分析
- 态势呈现
- 流量分析

THANKS

2019北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE