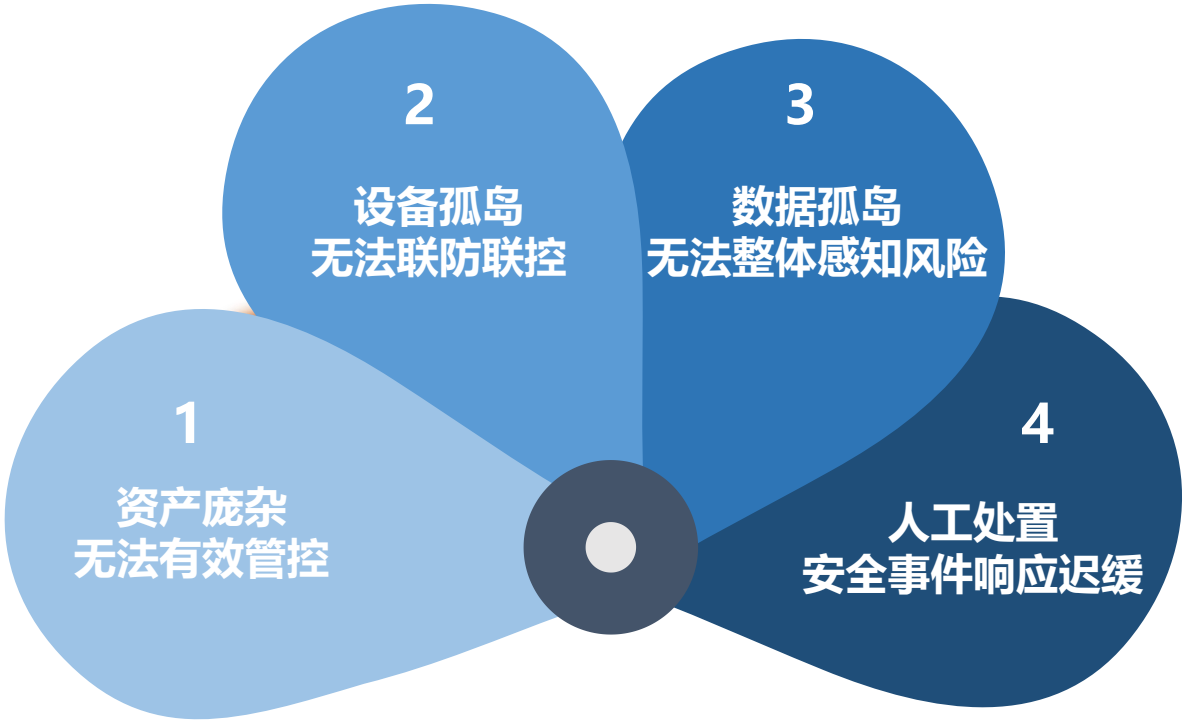
网络空间安全深度防御方案

云思天御-网络安全运营平台

01 防御现状

网络现状 | 防御现状 | 能力现状 | 风险现状 | 整体现状

护网防御现状-防御现状



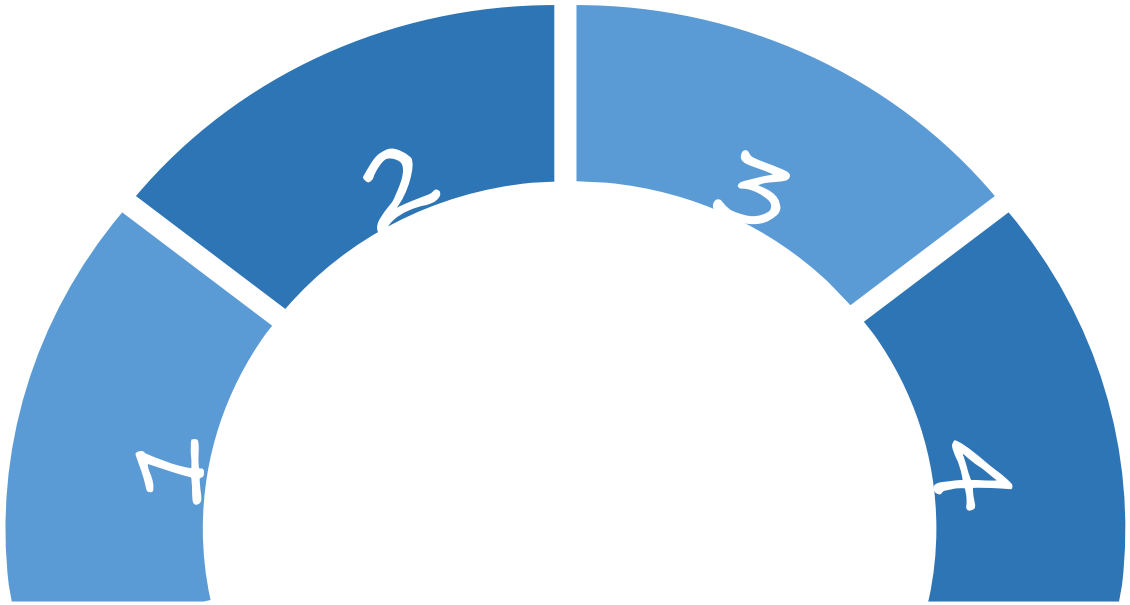
护网防御现状-安全能力现状

缺乏安全协作处置能力

现有网络安全防御能力碎片化，协同联动能力不足，缺乏各级公司、部门联防联控的网络安全事件应急处置手段

缺乏海量数据分析能力

海量日志、海量告警，无法分析、聚合，发现真正的威胁。



缺乏安全攻防对抗能力

普遍缺乏安全运营管理、专业技术人员和或人员经验不足，难以应对安 全事件。

缺乏安全整体运营能力

未形成体系化的、制度化、流程化的网络安全运营能力，缺乏后续运行防护策略持续调优。

护网防御现状-整体安全现状

随着护网越来越常态化、实战化，现有的

人工设备管控+**人工**分析+**人工**处置的方式

已完全不能满足企业安全防护的需要。

1

初级防护

- 有意识无手段

2

被动防护

- 堆人
- 堆设备

3

合规防护

- 人工监测
- 人工设备管控
- 人工分析
- 人工处置
- 多点不协调

4

安全运营

- 整体安全运营
- 安全能力统筹
- 自动化监测预警
- 智能化二次预警分析
- 自动化处置
- 完整的安全制度、流程体系

5

智能防护

- AI分析
- AI预防
- AI决策

大多数企业处于第3阶段

02

整体防御方案

介绍 | 对比 | 设计理念 | 整体架构 | 各模块介绍

运营方案-介绍

透过网络安全整体视角，通过加大防御面（边界防御、内网防御），对安全设备进行统管统控，对安全数据进行汇聚，发现安全问题、验证问题、 分析问题、可视化展示问题、自动化响应处置，联动工单及通讯系统的整套护网解决方案。

运维

可用

传统防御 **整体防御**

运营

实用

传统防御&整体防御

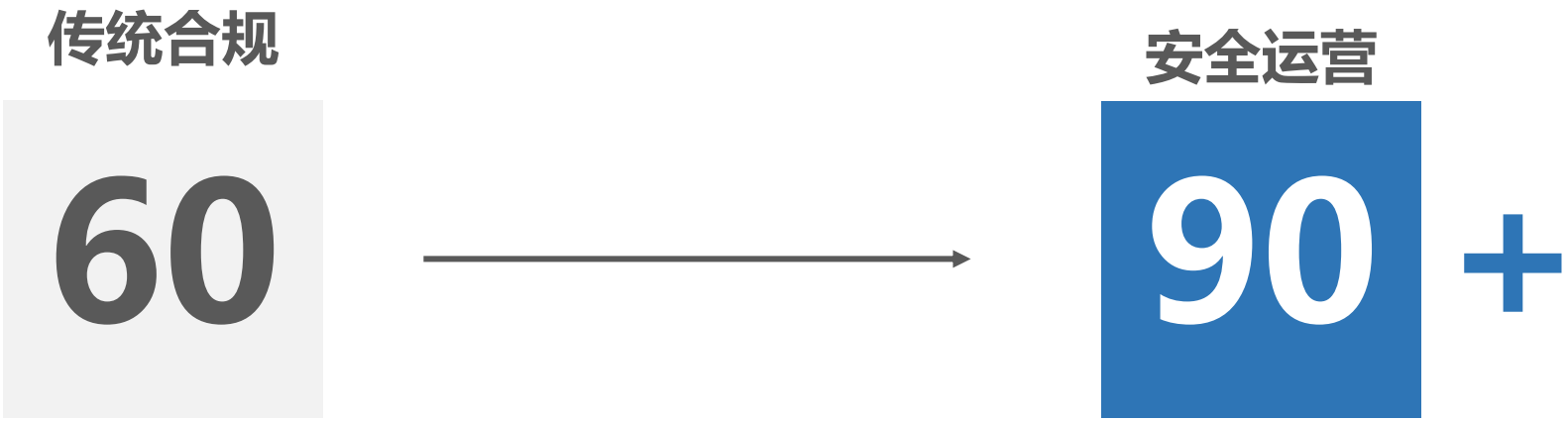
传统防御		整体防御
单纯依赖安全设备 安全孤岛，没有互联互通，各自为战	平台工具	**大数据平台支持** 整体防御，基于大数据分析发现**复杂隐蔽**攻击
单一安全设备告警 会产生大量漏报、误报	数据支持	**多来源数据碰撞** 发现**长链条**攻击行为
单人作战安全运维 专业安全技术知识缺乏	专家团队	**专家团队支持** 通过人与人的对抗，**以动制动**
被动式响应 发生安全事件临时寻求第三方支持	流程机制	**主动式防范** 常态化监测分析，防范有**组织**性的高级别攻击
人工处置 人工登录设备，设置安全策略	响应方式	**自动响应** 通过安全编排进行自动化响应

立体防御方案-目标

安全运营

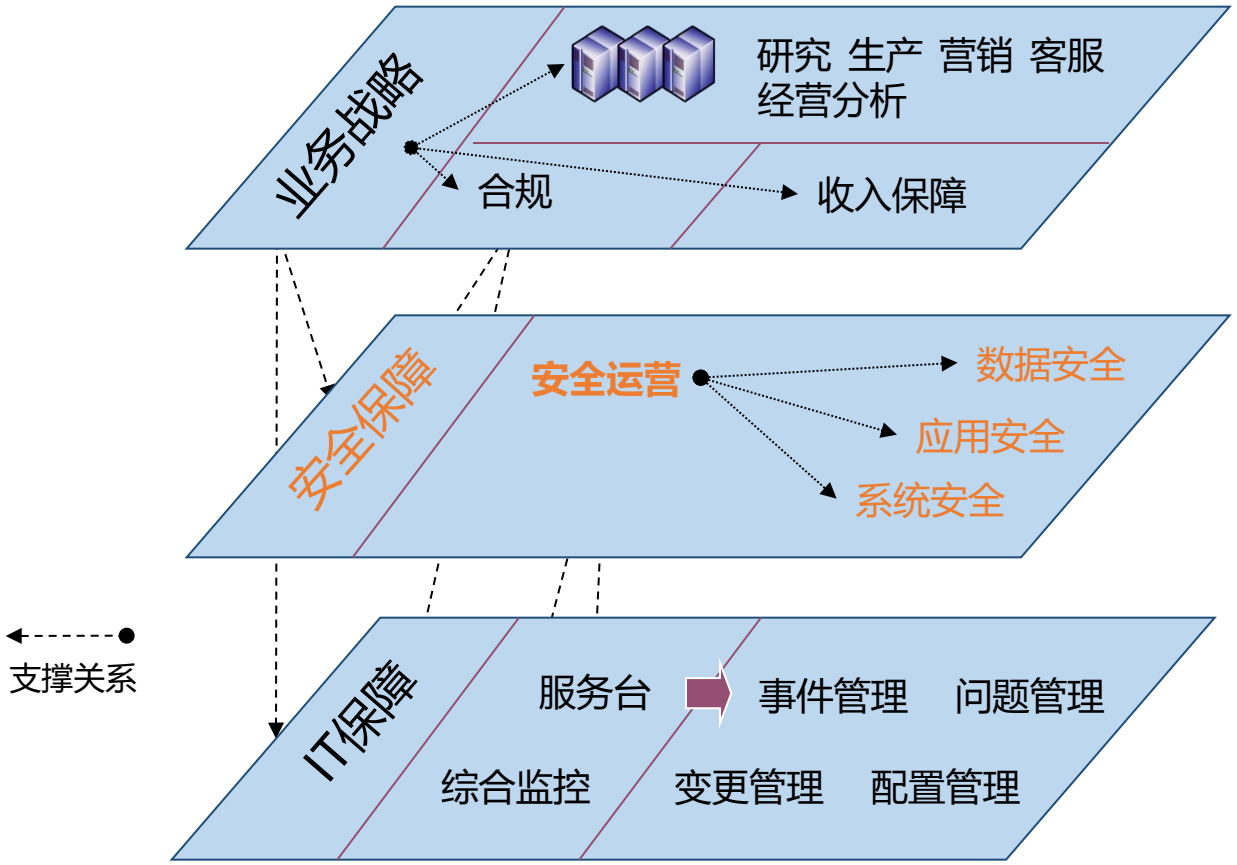
核心：安全防御能力的持续提升和持续输出

目标：在不额外增加安全设备的情况下，将企业的安全防御得分从合规的及格分提高到90+

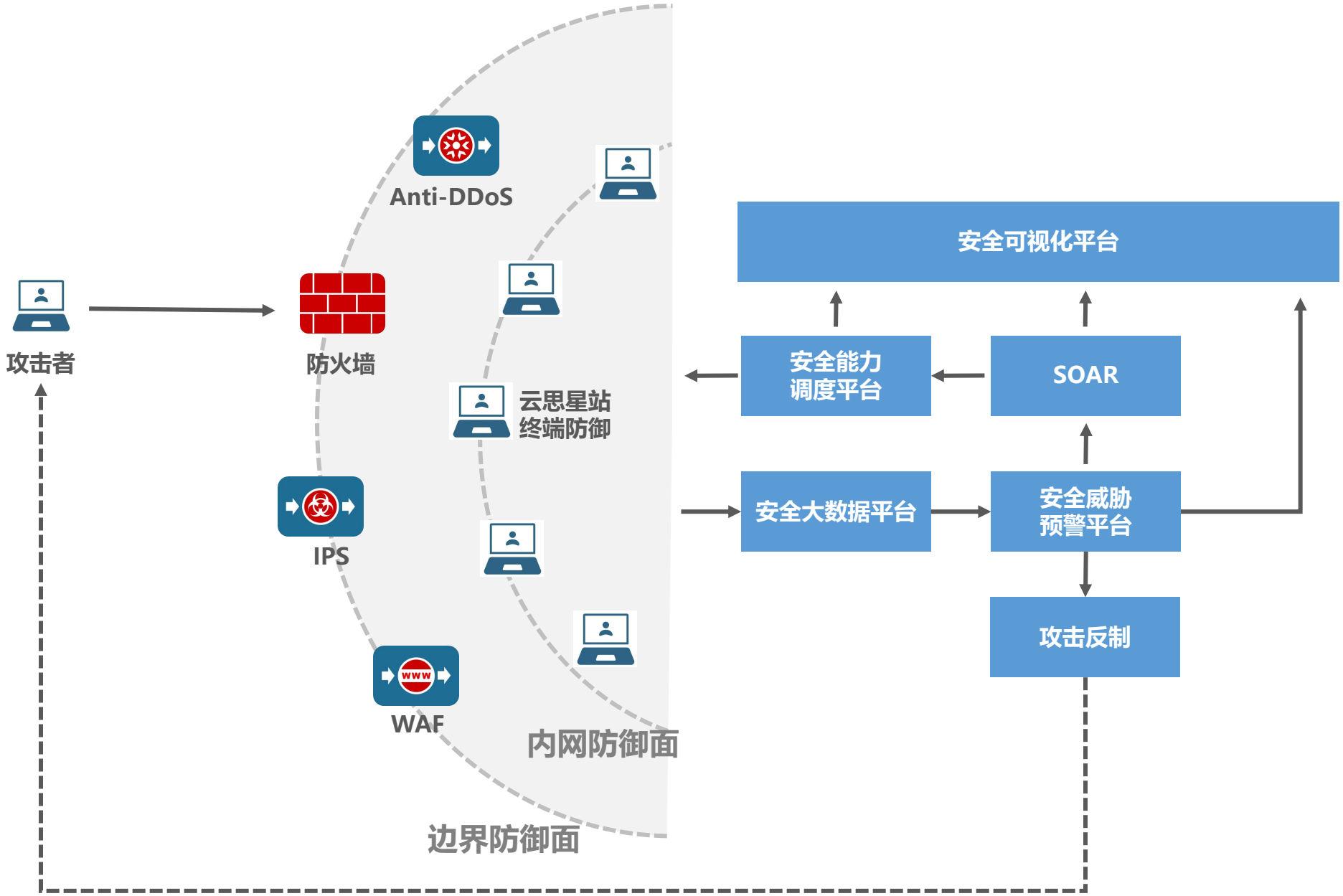


安全运营是IT 治理的重要保障环节

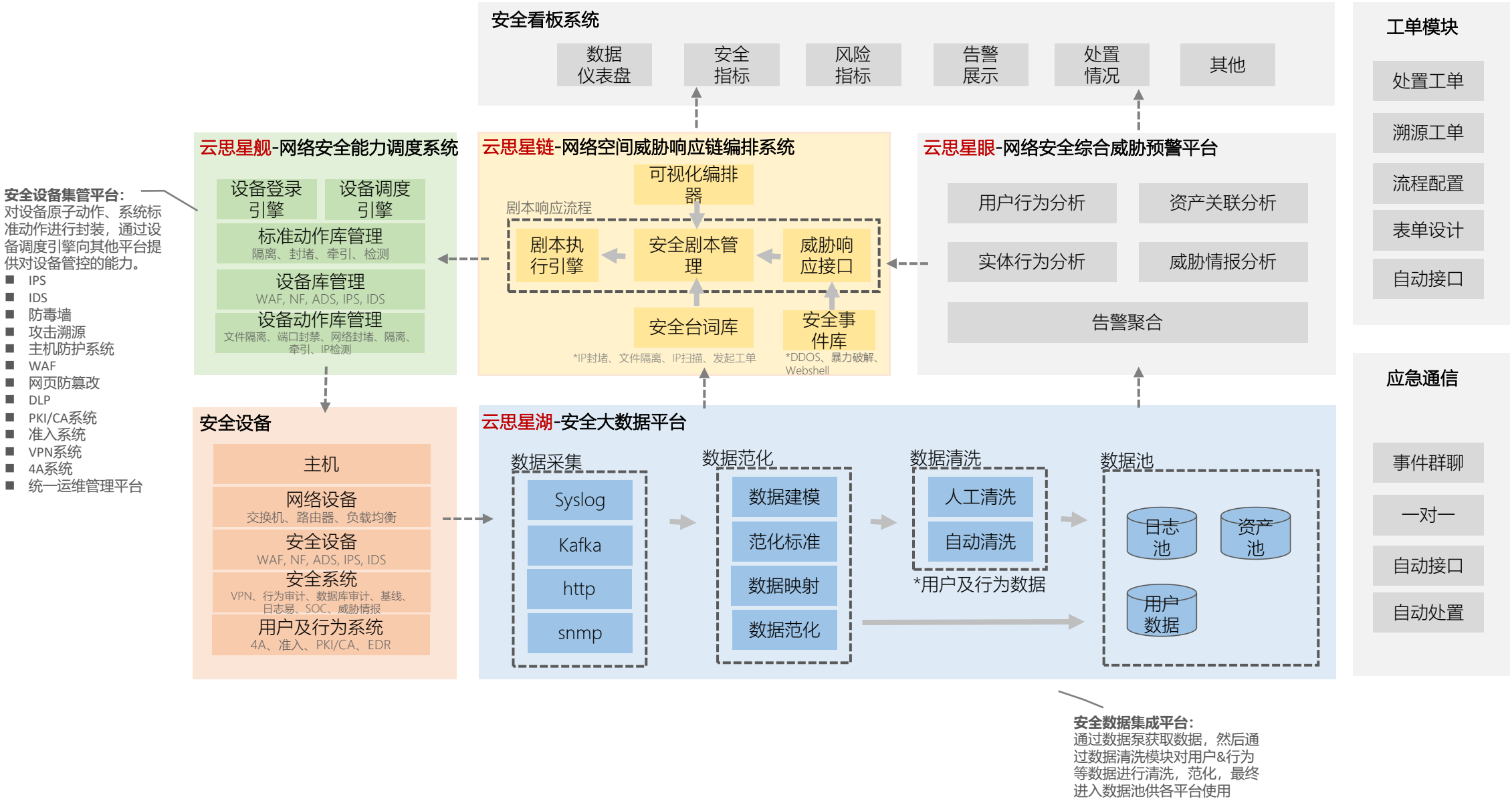
建立并完善安全运营管理体系，是提高安全保障能力的重要步骤。其中包含了人员组织、流程服务以及技术工具等多方面的建设要求！



整体防御方案-防御流程图



整体防御方案-整体防御框架



整体业务架构

态势可视化层

外部攻击态势 | 告警态势 | 漏洞分析 | 综合态势 | 流量态势

内网攻击态势 | 攻防总览 | 系统运行态势 | 资产态势 | 租户安全运营 | ...

业务模块层

资产	漏洞	告警与事件	行为分析	安全专题	朔源调查	响应处置	仪表板	报表
● 资产发现 ● 资产注册管理 ● 资产分组 ● 资产风险	● 漏洞管理 ● 扫描器对接 ● 扫描任务	● 事件管理 ● 告警管理 ● 告警策略 ● 策略引用集	● 用户风险概览 ● 用户实体动态评分 ● 风险行为追溯 ● 安全事件智能分析 ● 行为策略配置 ● 用户发现	● 域名安全 ● 邮件安全 ● 账号安全 ● 数据泄露 ● 攻击IP分析	● 检索溯源 ● 调查任务	● 自动处置工单 ● 人工处置工单 ● 通知策略 ● 联动处置	● 态势总览 ● 系统监控 ● 自定义仪表板	● 报表管理 ● 自定义模板 ● 周期任务

安全引擎层

流量感知 | 多源关联 | 可视分析 | 规则引擎 | AI引擎 | 画像引擎 | 动态评分

大数据层

归一化接入 | 数据范化 | 流式计算 | 离线回溯 | CK存储 | OSS

分布式消息总线

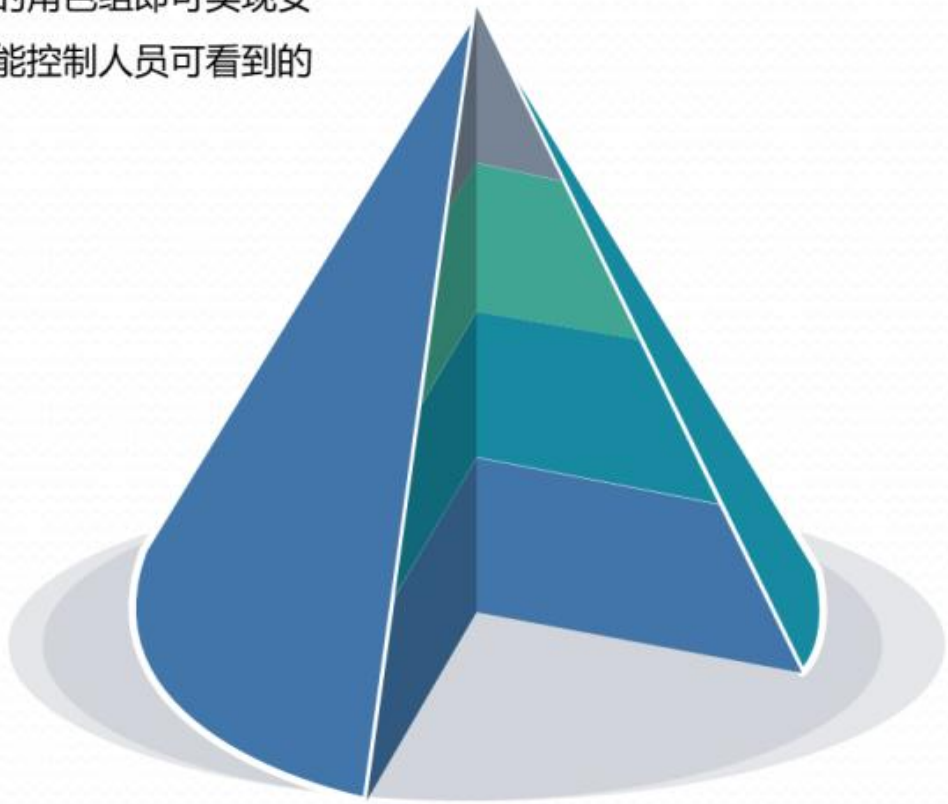
采集执行层

TCP、UDP、HTTP...	威胁情报	主机防护	WAF、FW	Nginx日志...	威胁阻断	漏洞复检
流量数据	情报数据、资产管理系统信息		安全日志、系统/中间件日志		响应执行	

整体防御方案-多层次视图

多层次视图

依据人员职位或级别来创建不同的角色组。使用者只需将对应的账号划分至指定的角色组即可实现安全视图的定制化展示，同时还能控制人员可看到的具体内容…



01

高层管理领导

- ✓ 掌握内部整体安全态势；
- ✓ 评估整体安全机制的有效性；
- ✓ 提供安全管理决策支持…

02

业务部门经理

- ✓ 掌握业务系统安全态势；
- ✓ 查阅业务系统安全报告；
- ✓ 协调业务安全事件的处理…

03

安全部门经理

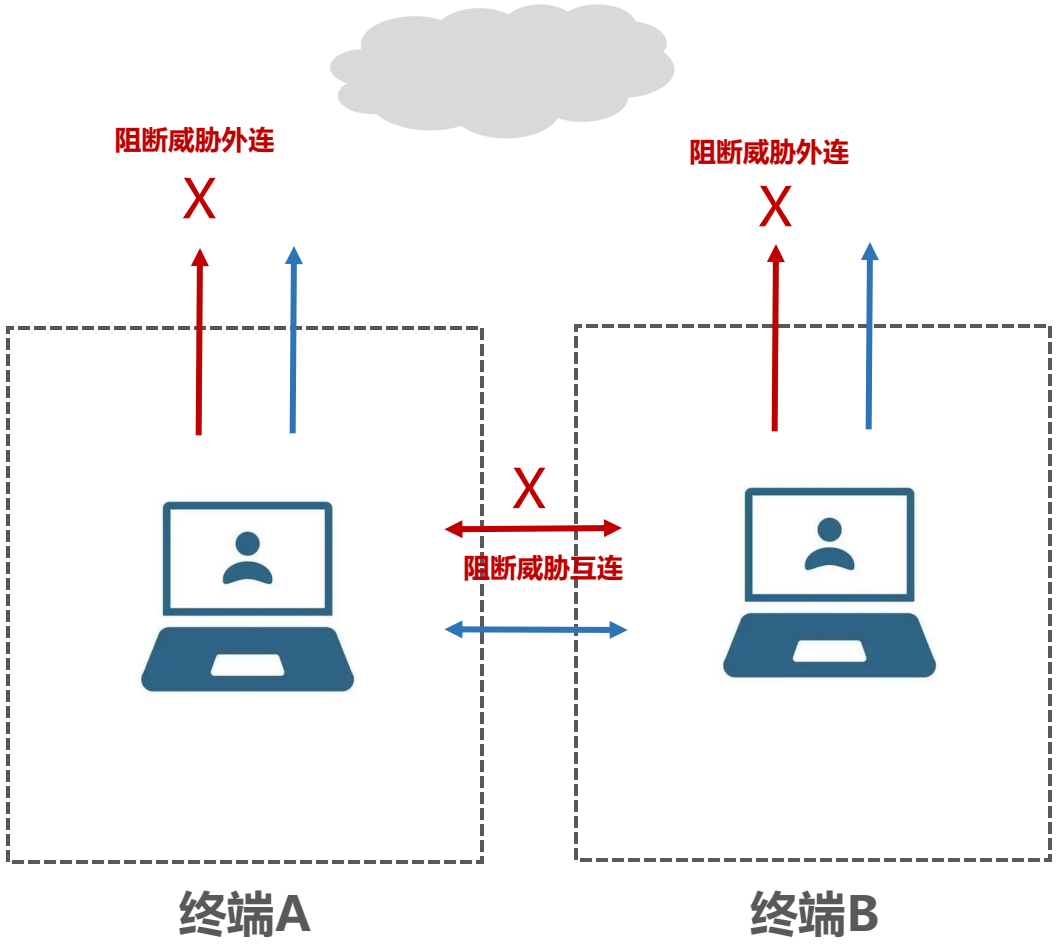
- ✓ 辅助高层领导落实安全策略；
- ✓ 制定安全运维计划；
- ✓ 出具运维安全分析报告…

04

安全运维人员

- ✓ 监测网络具体运行状态；
- ✓ 统计分析具体安全事件；
- ✓ 辅助指定任务处理与应急响应…

整体防御方案-终端防御系统（云思星站）



云思星站实现了如下终端防御能力：

- 发现终端威胁（如横向渗透威胁）
- 阻断威胁外连、互连
- 阻断恶意进程
- 阻断恶意安装包
- 终端行为数据采集
- 终端移动存储设备管控

整体防御方案-安全大数据平台（云思星湖）

通过采集、接收两种方式汇聚安全设备、安全系统的日志数据，并能通过可视化编排的形式对日志数据进行范化、清洗、入库。支持10+采集协议、百亿级日数据采集范化能力。

支持协议采集、RPA、爬虫等方式，解决数据采集难的问题。

高吞吐低时延

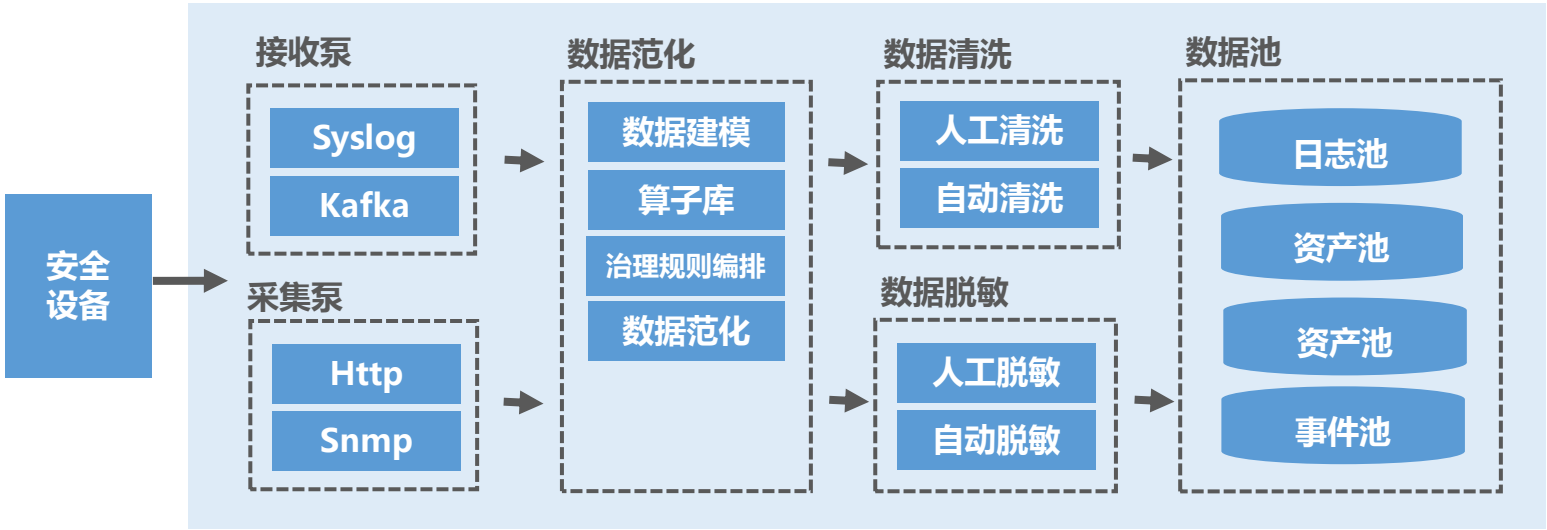
采用分布式集群架构，具有容错性、稳定性和可用性，满足高吞吐、大数据量和低时延实时处理等多方面的数据处理要求；支持百亿级日采集处理能力。

多元数据接入

可支持结构化、半结构化、非结构化数据的统一接入；具备范化规则的可视化编排能力；

多源数据采集

支持设备及系统日志数据（包括不限于：防火墙、ADS、IPS、IDS、WAF、FW）；用户行为数据（包括不限于：VPN系统、准入系统、4A系统等）



整体防御方案-安全大数据平台（云思星湖）

目前业界唯一具备范化规则可视化编排能力的平台，大大降低人员能力要求，提高接入效率。

数据提取

针对非结构化文本数据的日志进行字段分割、提取，获取结构化数据以支持后续的流处理、数据仓库计算。

数据处理

对数据进行处理形成新的数据，如：字段融合、数据提取等；

数据映射

对字典类数据按照映射表进行自动映射，如：1映射成男；

数据脱敏

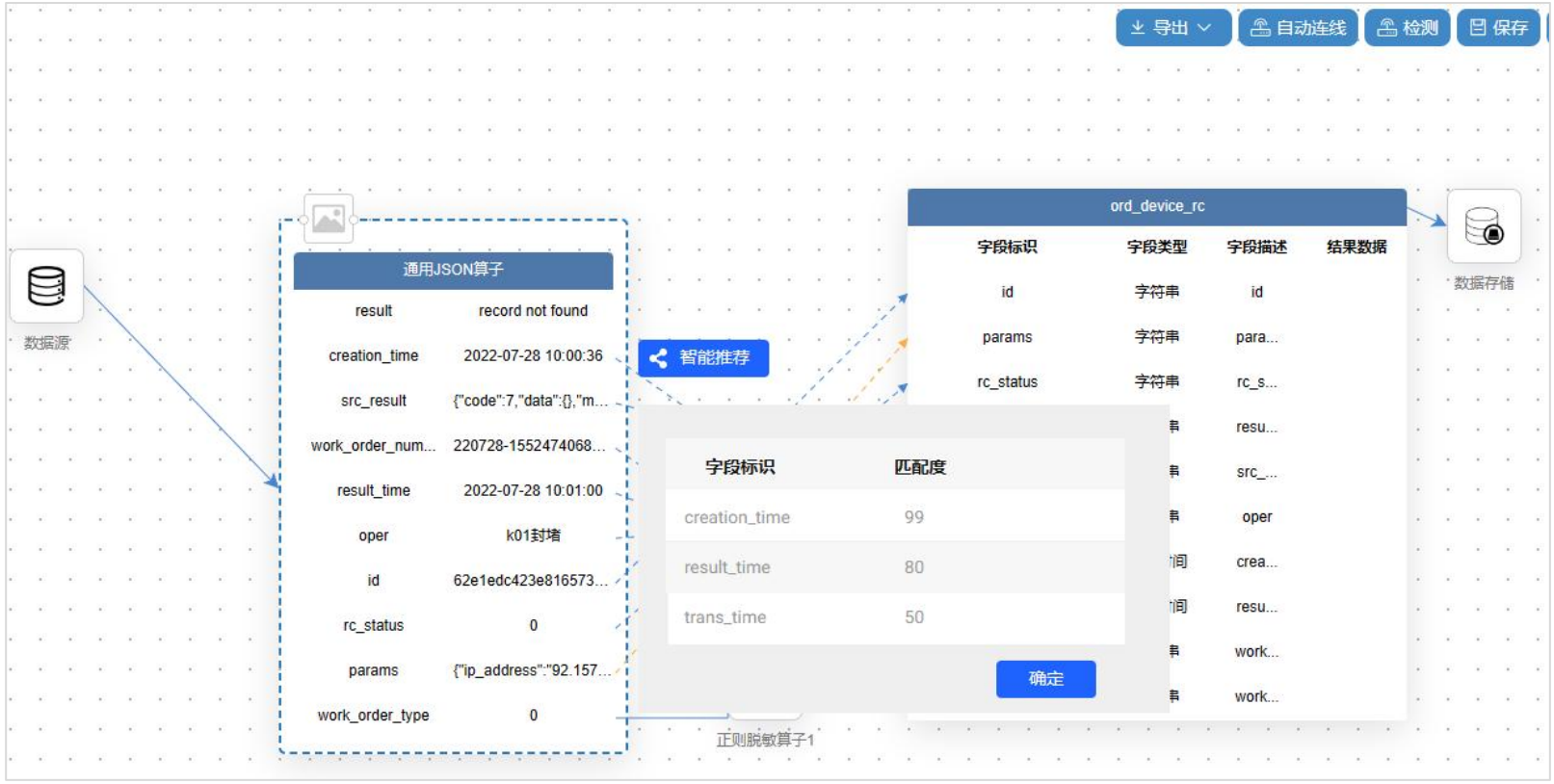
对数据中包含的密码、手机号、地址等敏感信息进行脱敏；

数据流转

支持将采集到的未经过清洗与范化的原始日志数据等进行跨平台转发。

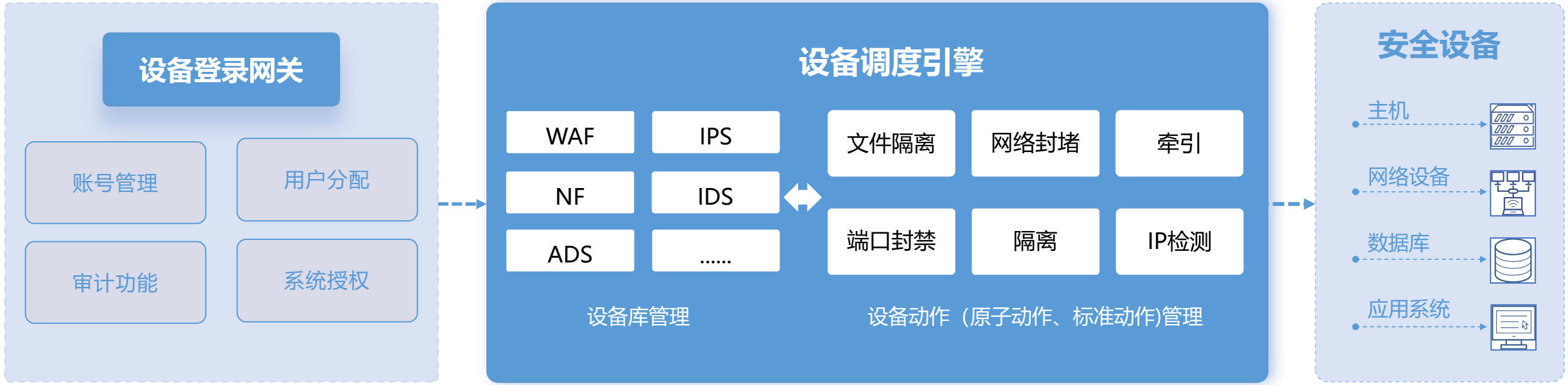
可视化规则编排

通过可视化形式完成安全数据范化规则编排、清洗、入库等操作，大大降低数据治理的难度。



整体防御方案-网络安全能力调度系统（云思星舰）

实现异构、无API、无SDK安全设备的统一登录、统一管控、统一策略下发等能力，并能将这些能够通过接口对外赋能。目前已支持200+安全设备统管



整体防御方案-网络安全能力调度系统（云思星舰）

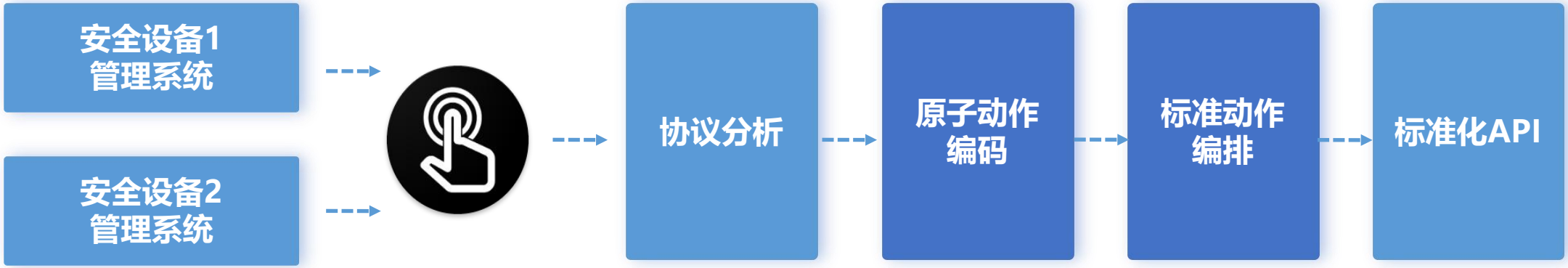
已适配主流厂商设备

已适配主要设备类型

1. 防火墙（华为、天融信、K01等）
2. 防病毒网关（深信服、H3C等）
3. 堡垒机（奇安信、安恒、天融信、启明星辰等）
4. IPS（迪普、绿盟等）
5. IDS（迪普、绿盟等）
6. EDR（天擎、G01、青藤云等）
7. WAF（长亭、迪普、瑞数等）
8. 僵木蠕（天融信、绿盟等）
9. 蜜罐系统（长亭、安恒等）
10. 漏扫系统（深信服、绿盟、Nessus等）
11. 引流设备（迪普等）
12. 主机加固（青藤云等）
13. CA系统（三未信安等）

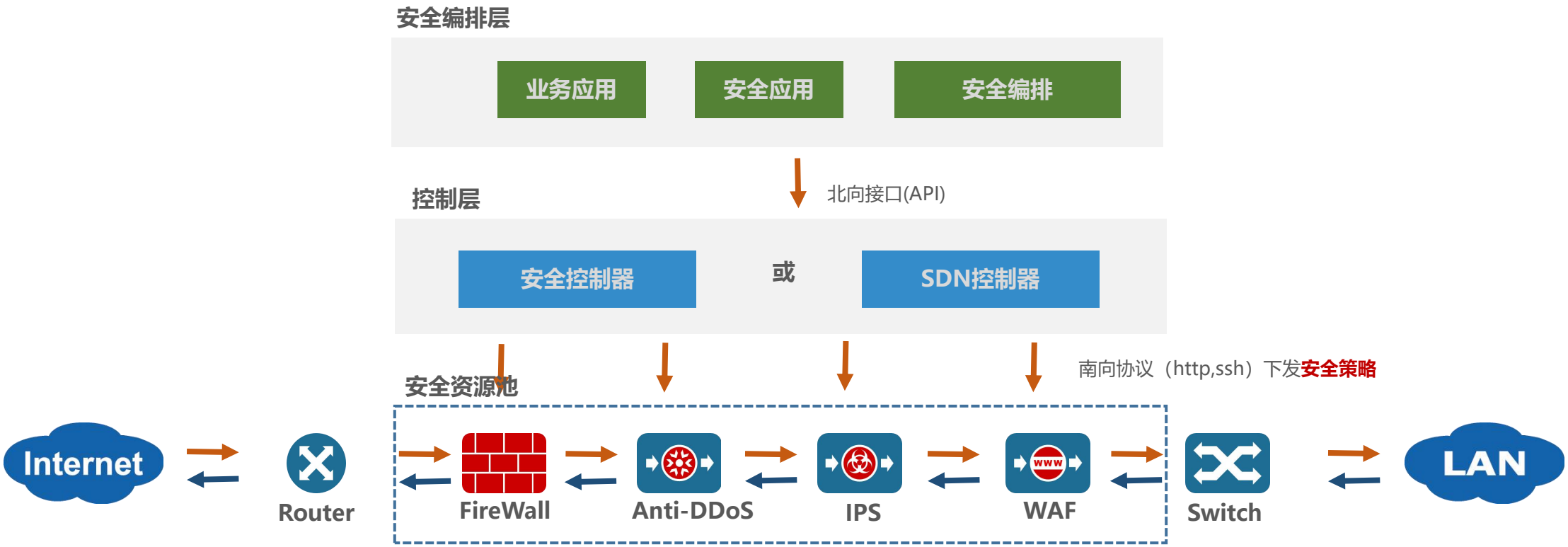
整体防御方案-网络安全能力调度系统（云思星舰）

未适配设备，通过协议分析等手段，可确保2天接入一个



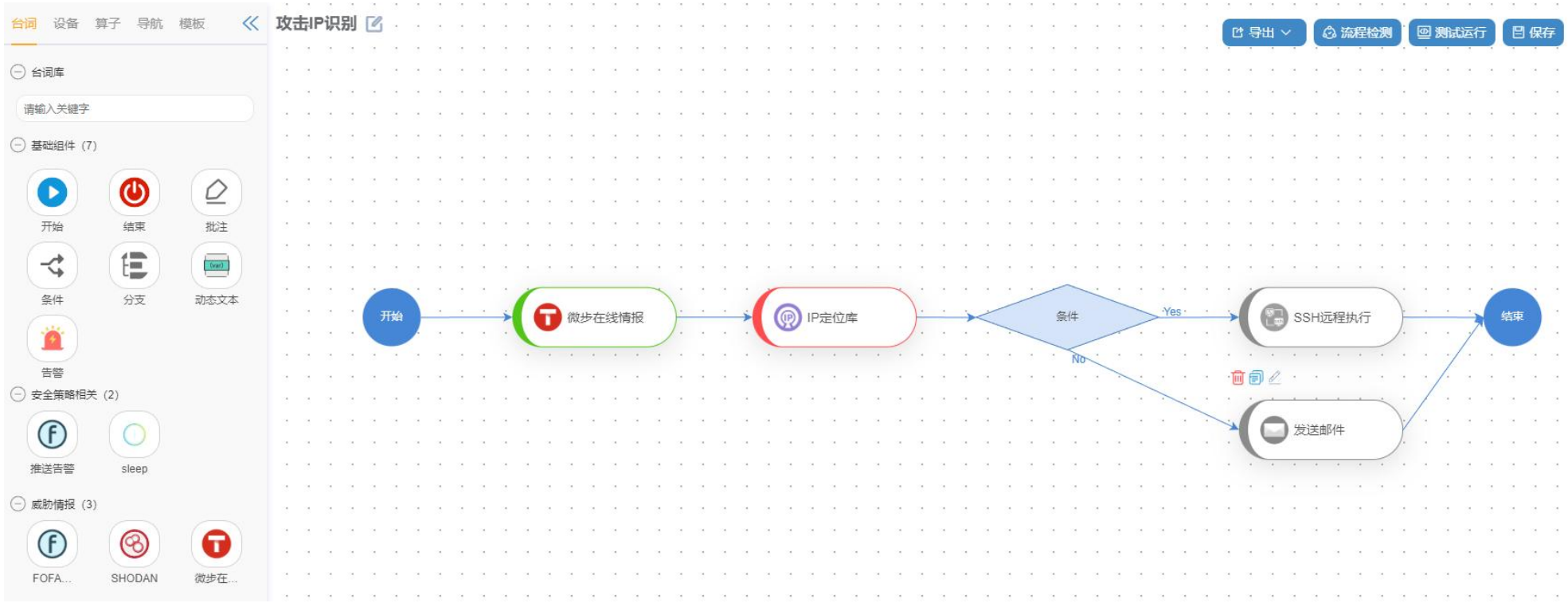
整体防御方案-网络空间威胁响应链编排系统（云思星链）

对安全事件响应（响应链）或日常运维工作流程进行可视化建模，生成剧本，并由安全事件或调度计划驱动剧本的执行，**实现安全事件的自动化响应**，大大减少MTTR时间。

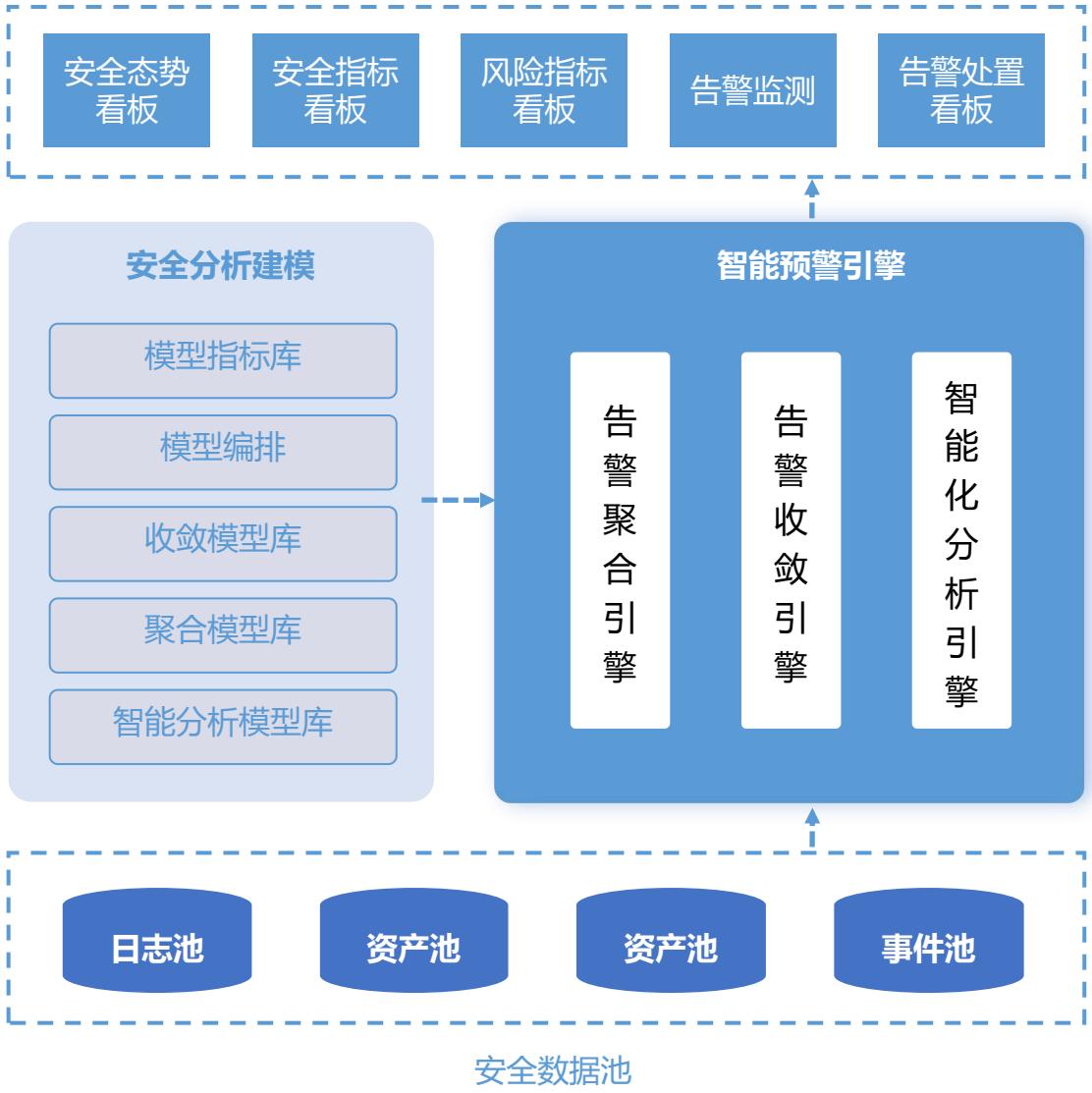


整体防御方案-网络空间威胁响应链编排系统（云思星链）

实现剧本的可视化编排能力、台词的Python插件化扩展能力，并能通过可视化形式展示剧本的执行情况。



整体防御方案-综合威胁预警系统（云思星眼）



- **告警聚合：**通过将告警按照IP、端口、类型、名称等维度化，并将不同维度进行组合，实现安全告警的聚合，大大降低告警的数量；
- **告警收敛：**通过统计分析模型，对低危、垃圾告警进行过滤，解决告警泛滥的问题；
- **告警智能分析：**通过对现有安全告警数据，构建横向移动聚合，内置权限维持聚合，病毒扩散聚合，多维数据关联分析，非时序关联分析，互斥关联分析等智能化分析模型，发现高级可持续威胁，并产生新的告警。

03 应用场景

护网（平、战） | 安全设备统管 | 事件自动化响应

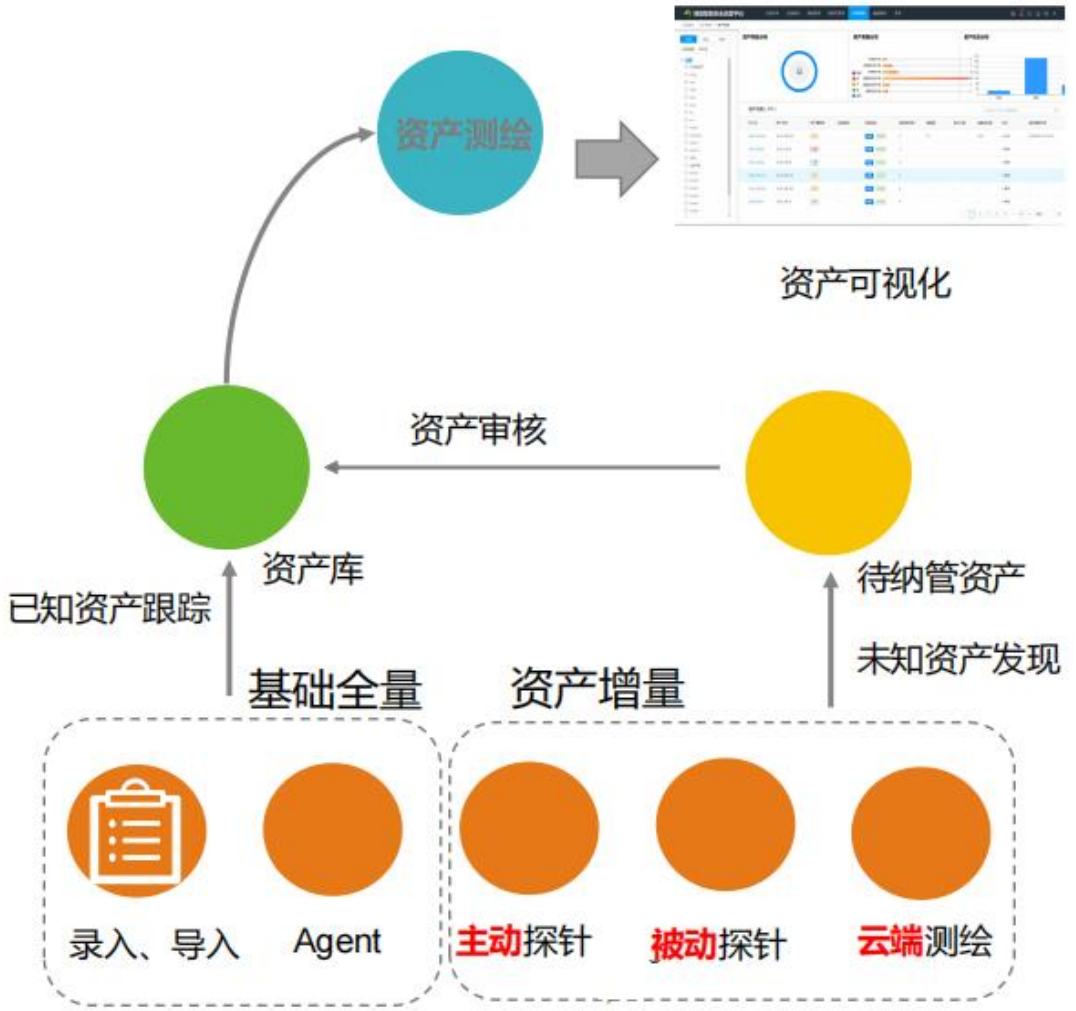
资产测绘发现

优势：

- ✓ 已建资产无缝对接
- ✓ 主动、被动、云端多维度测绘
- ✓ 资产库属性补全
- ✓ 资产信息可视化

过程：

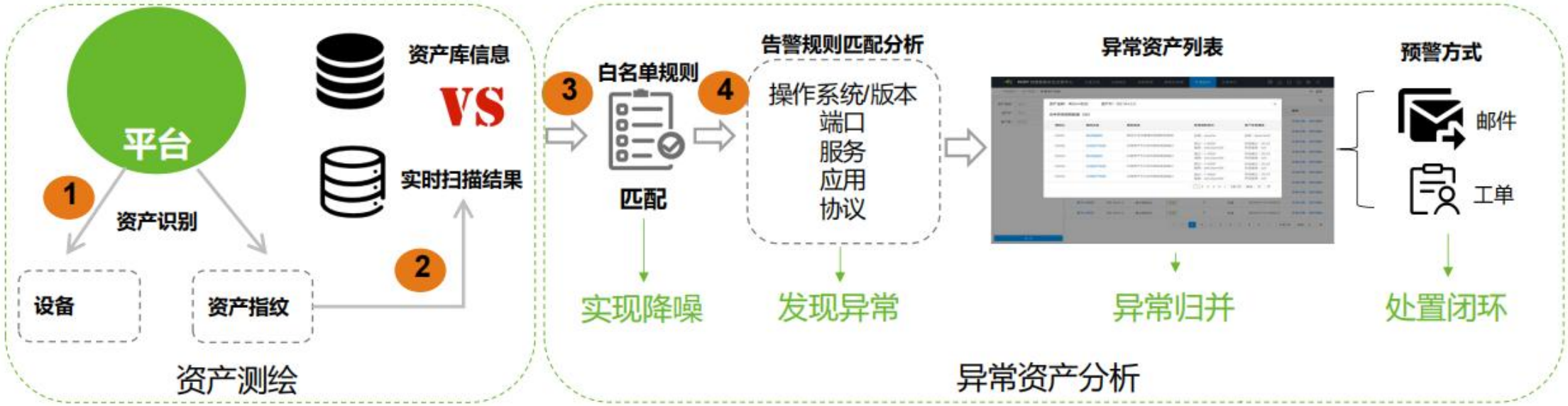
- 支持全量资产导入，与原有资产建设无缝对接
- 基于扫描、爬虫、Agent采集、流量分析等技术自动采集
- 补充关联属性，完成资产备案融合
- 完成测绘，实现资产可视化呈现
- 异常资产发现，最终风险量化



异常资产分析

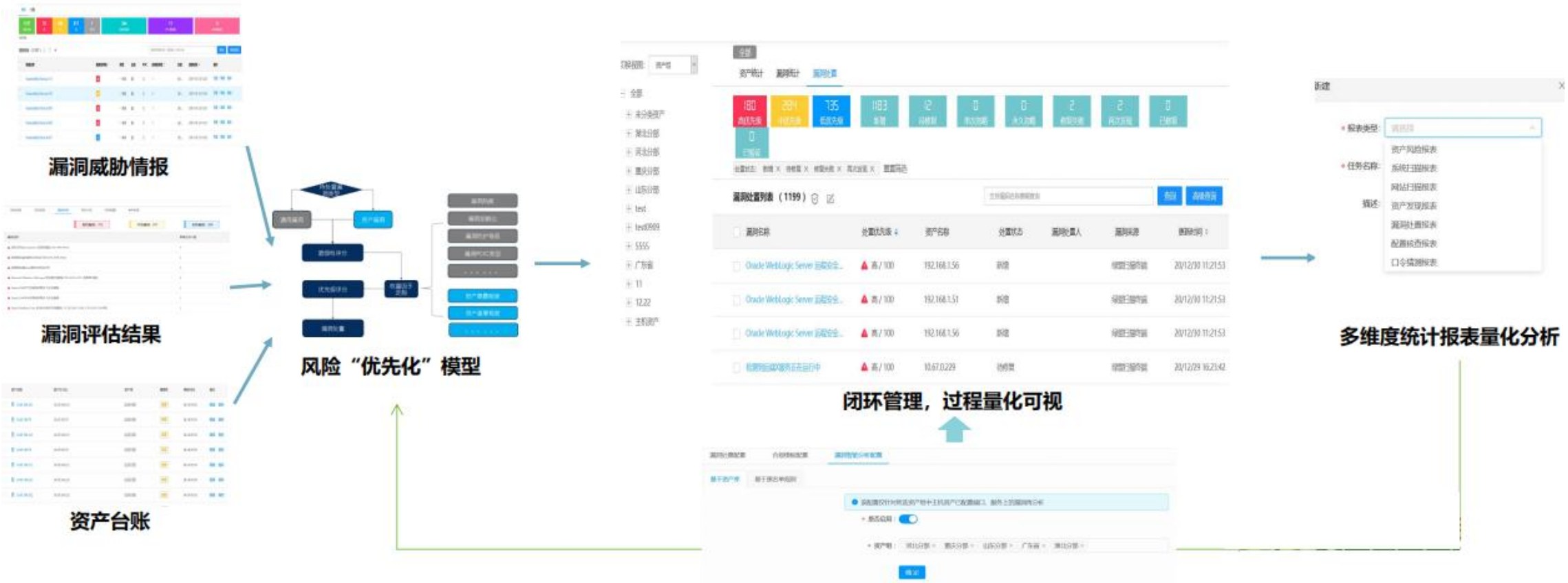
针对上线后资产结合安全基线进行常态化检测，确保资产安全管控满足安全管理制度和规范要求

- 安全基线自定义，设置资产安全基线（端口、协议、操作系统和应用等属性）
- 属性变化检测，发现IP和资产指纹信息与历史数据发生重大变化的资产
- 新增资产和僵尸资产发现
- 配置白名单，应对测试环境中资产频繁变化



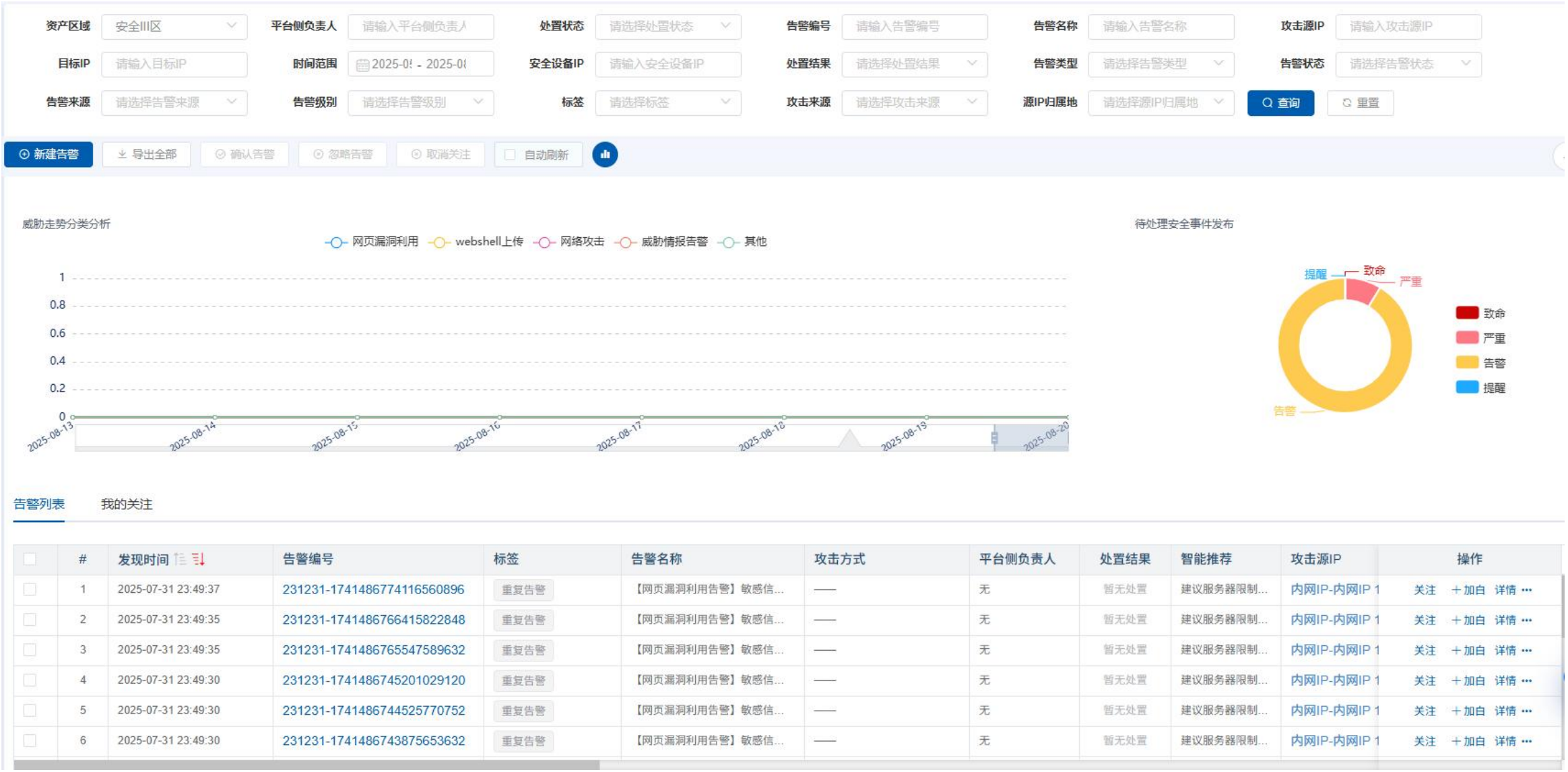
脆弱性闭环

通过自动漏洞扫描，结合隐患消缺流程，有序进行脆弱性闭环

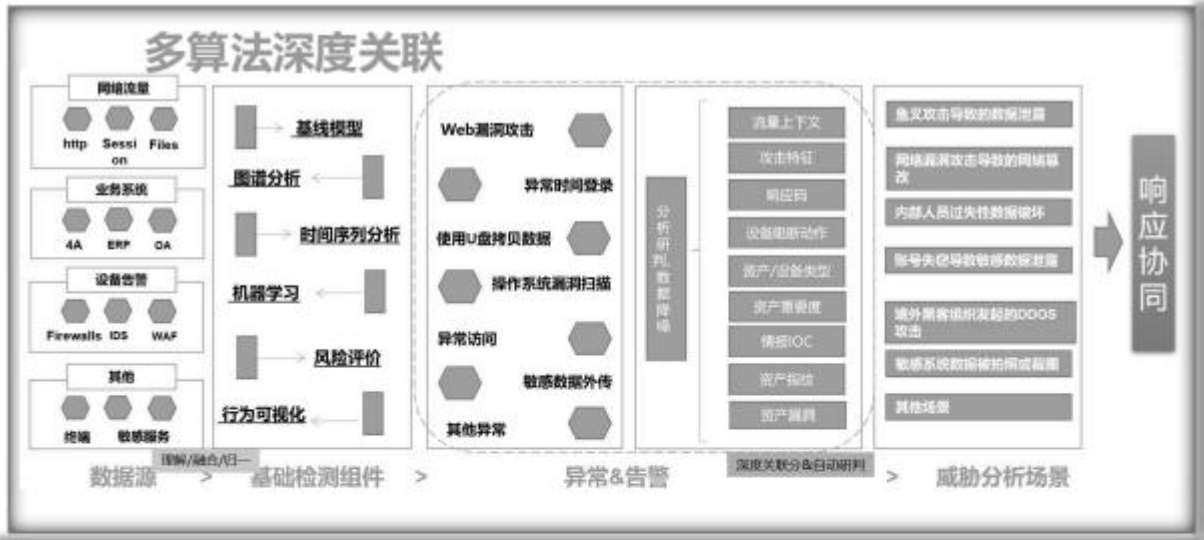


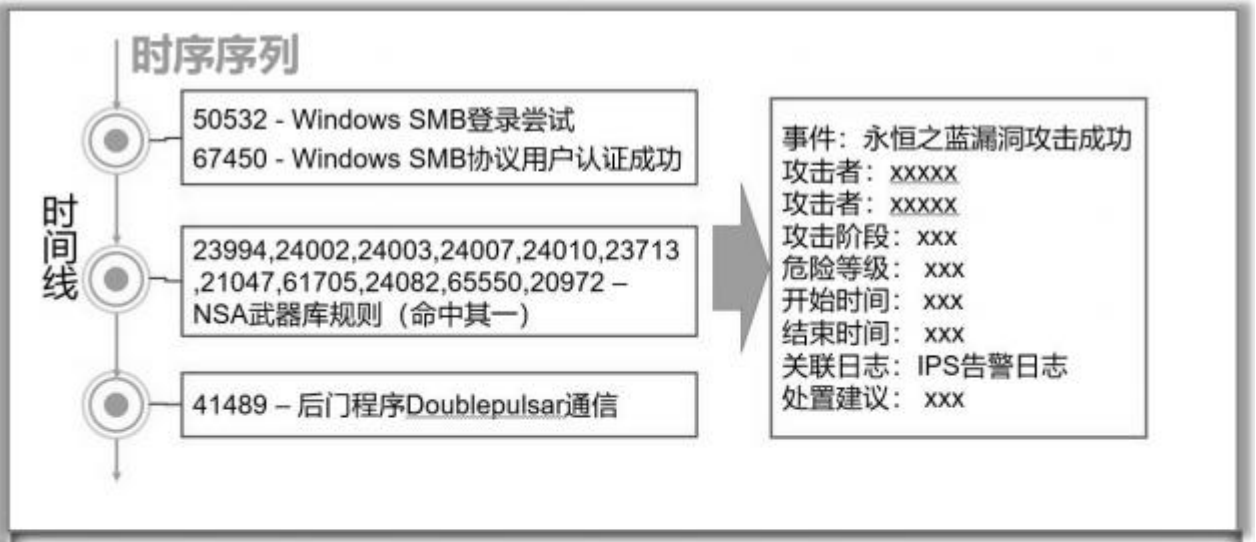
安全风险集中监测

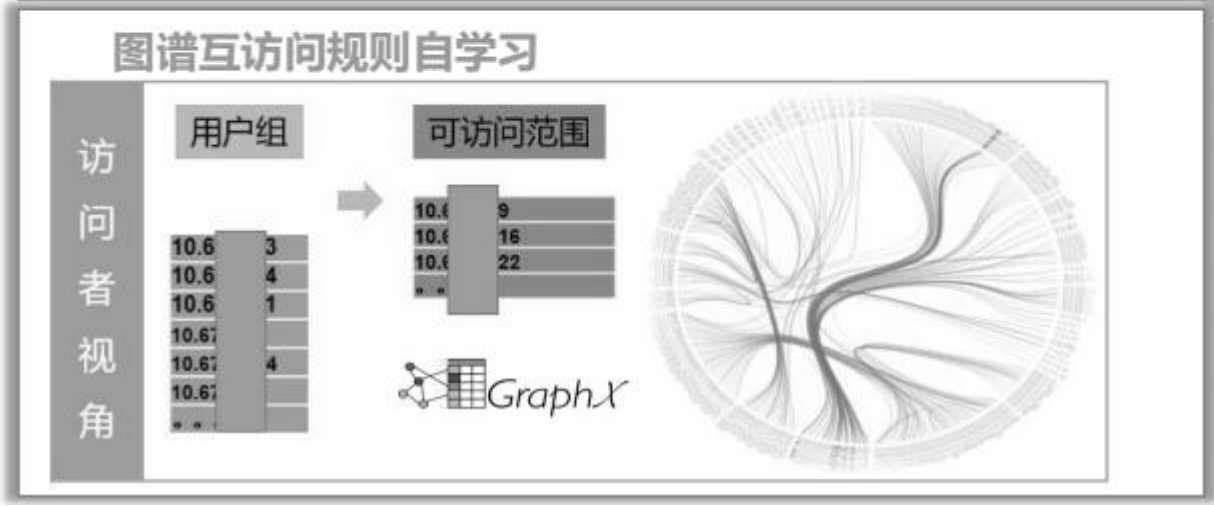
对多源告警数据进行集中监测，自动标注，并通过工单流程进行闭环

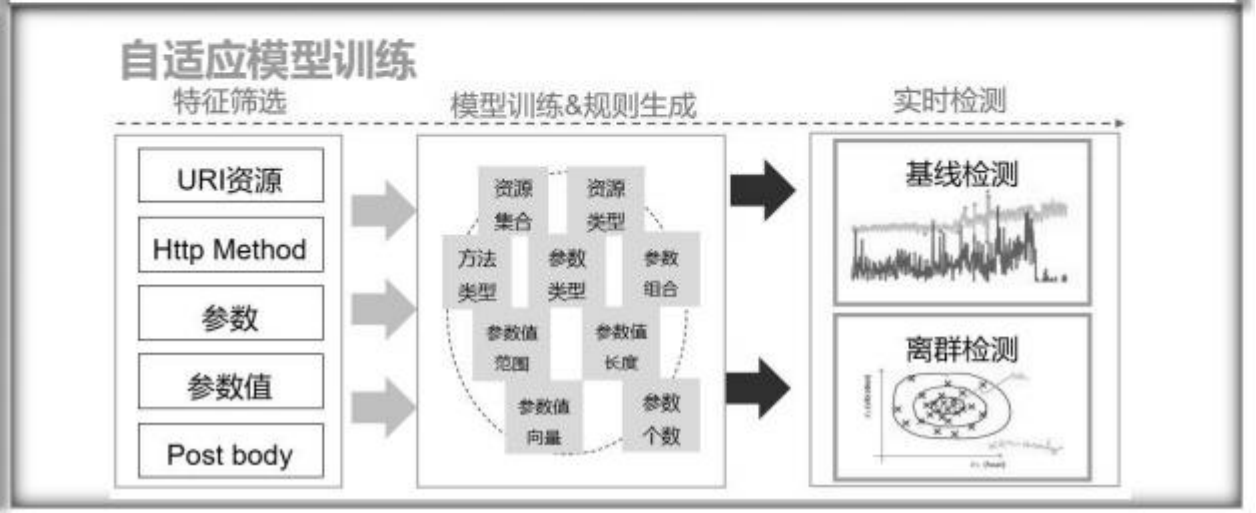


多手段安全风险二次分析



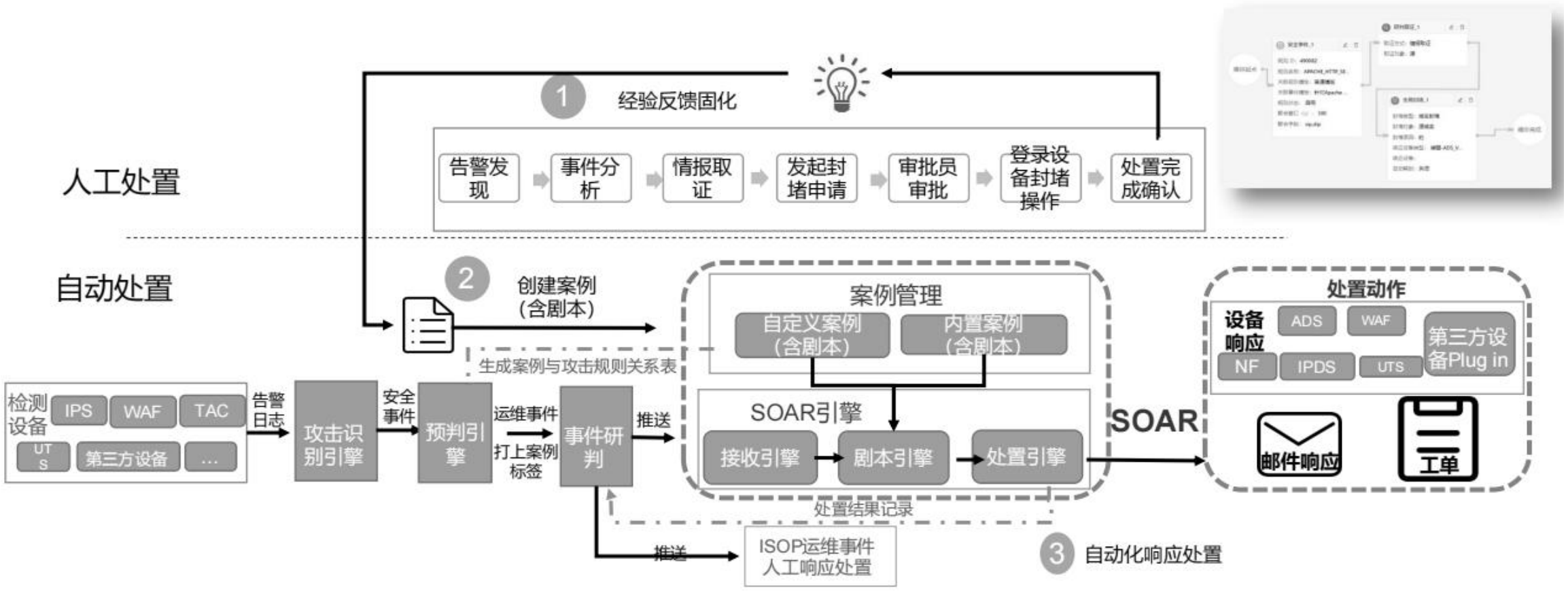




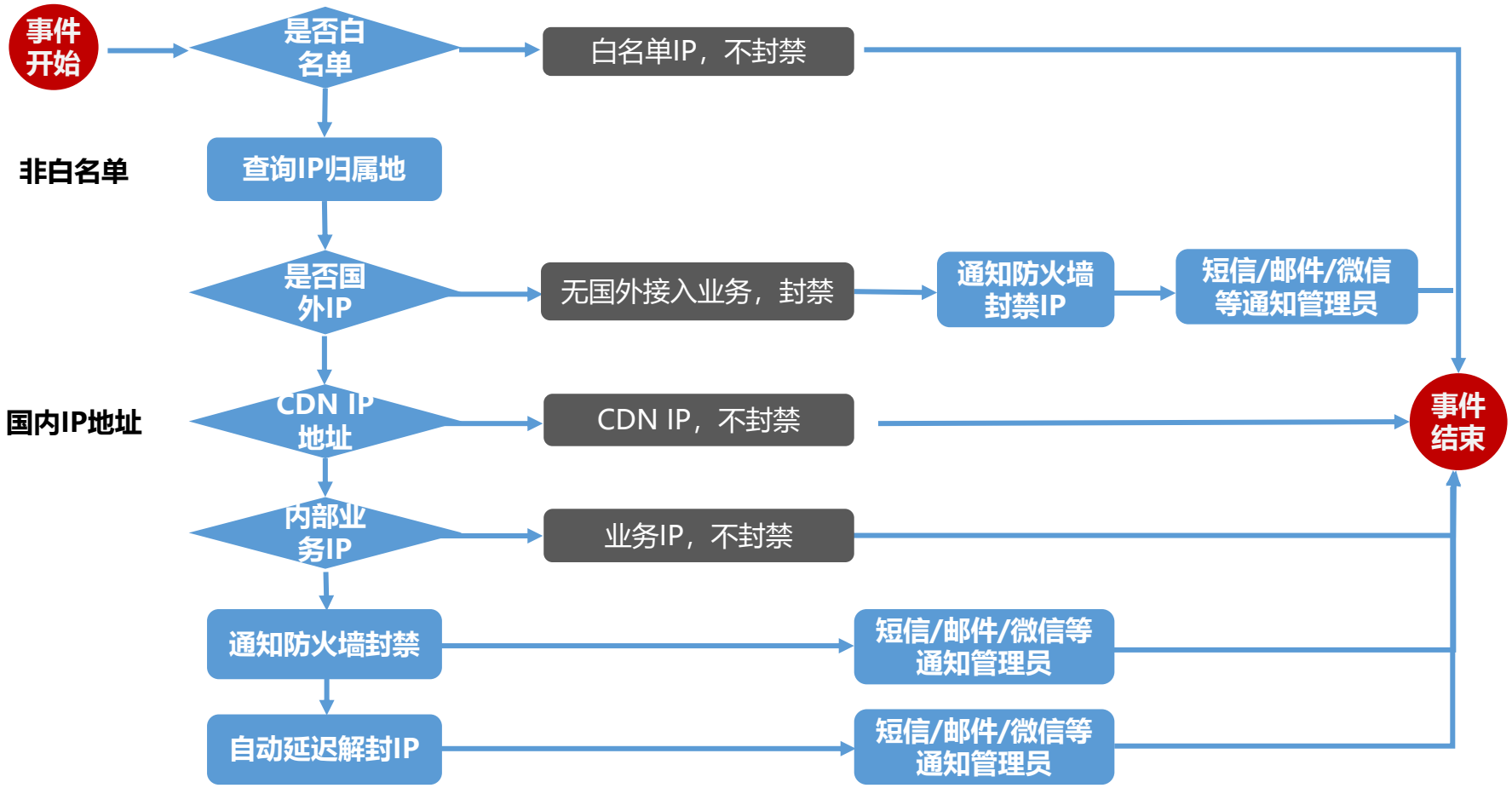


风险自动化处置

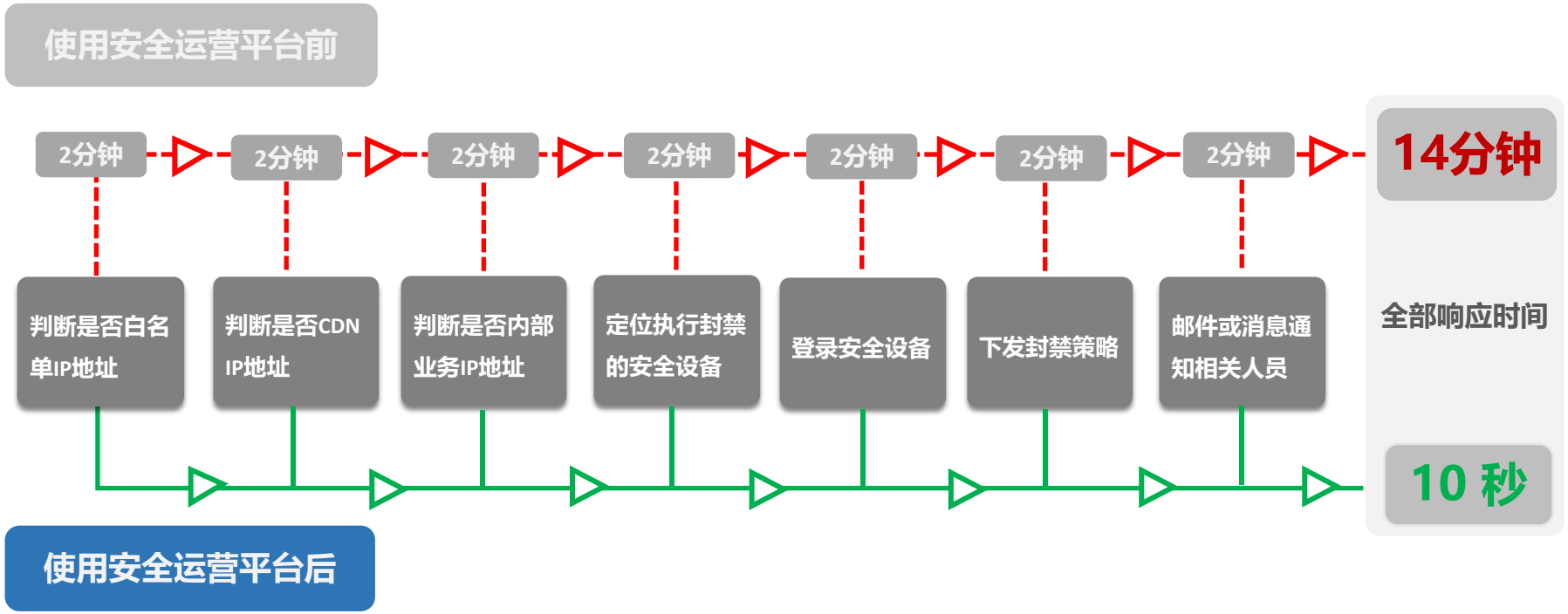
- 内置20+案例，覆盖挖矿、入侵、拒绝服务、勒索、钓鱼等，简化安全运营应急响应处置流程，解放人力，提升效能



应用场景-事件自动化响应-剧本案例



应用场景-事件自动化响应-人工&自动对比



效率提升约84倍（某客户实战数据）

应用场景-事件自动化响应-价值

HW真实场景	人工操作耗时	安全运营平台	类别	增效
一键封禁IP	5～10分钟	10秒	响应	30～60倍
钓鱼邮件分析	30~180分钟	5~10分钟	分析	6～18倍
入侵调查/攻击溯源	60~300分钟	20分钟	分析	3～15倍
网络故障诊断	30~60分钟	5分钟	诊断	6～12倍
快速找人/找资产	15～60分钟	3分钟	协同	5～20倍
一键攻击事件总结	60～120分钟	1分钟	报告	60～120倍

省时、省力、省钱、极速、增效

应用场景2-阶梯式自动化响应

场景：

企业的信息泄露、重要业务受到影响、网络崩溃等安全问题通过阶梯式自动化响应，可以大大提高安全事件应对的速度和准确性，从而快速部署防御措施，最大程度保障信息系统的安全和稳定。

接入日志源：

1. WAF/FW
2. IP归属地数据库/威胁情报系统

应用场景3-恶意软件事件预处置

场景：

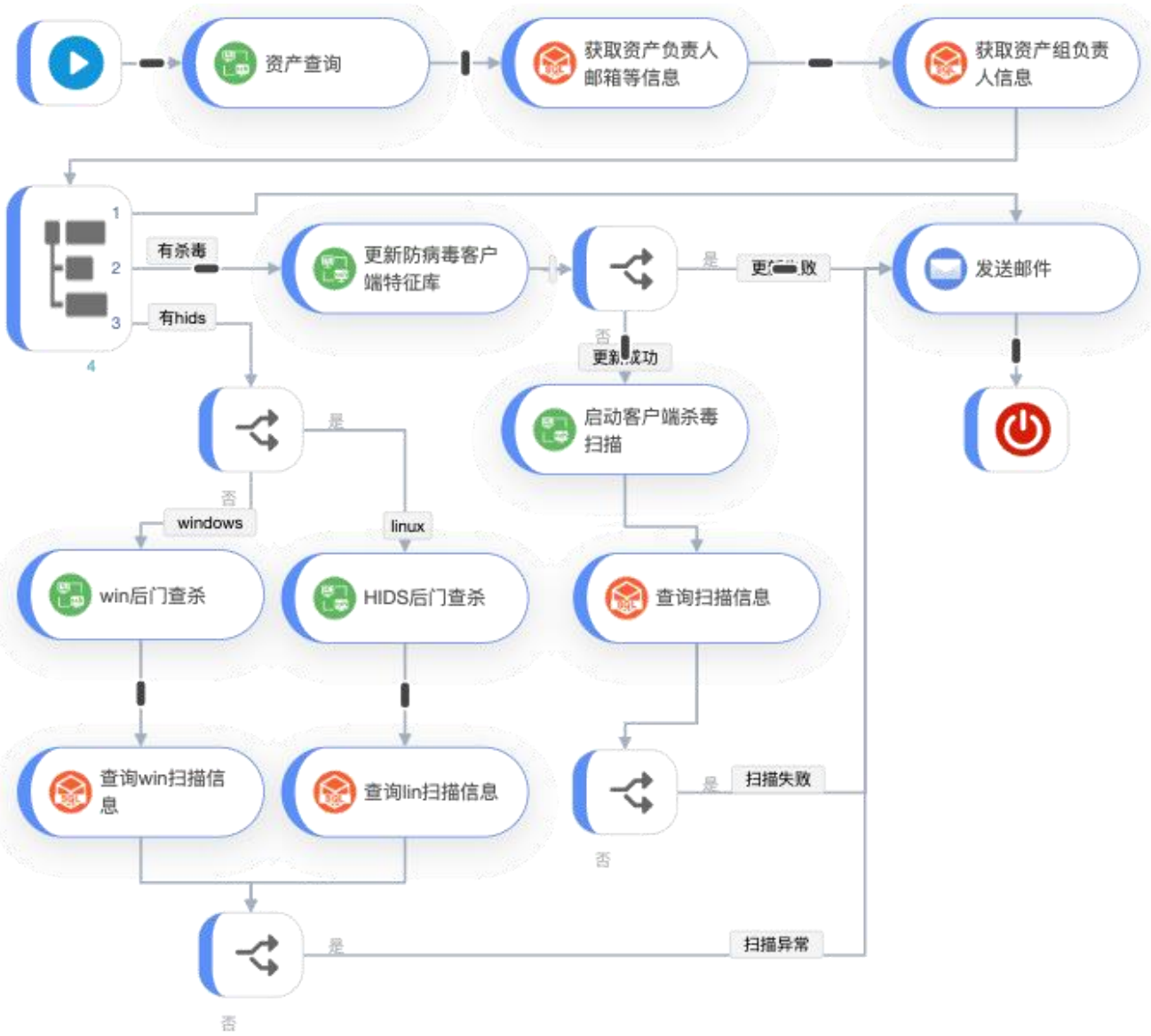
企业在遭受病毒、木马、间谍软件、广告软件等威胁时，安全团队可使用预处置剧本针对不同类型的恶意软件攻击构建响应策略，以缩短恶意软件攻击事件的响应时间。

接入日志源：

1. HIDS服务器、防病毒服务器
2. 资产管理系统

处置响应：

通过HIDS服务器/防病毒服务器主动将客户端更新、发起扫描等任务推送给客户端；并通过内部的资产管理系统查找对应的资产负责人，并将结果通过邮件反馈给资产负责人。



应用场景4-外对内攻击成功事件处置

场景：

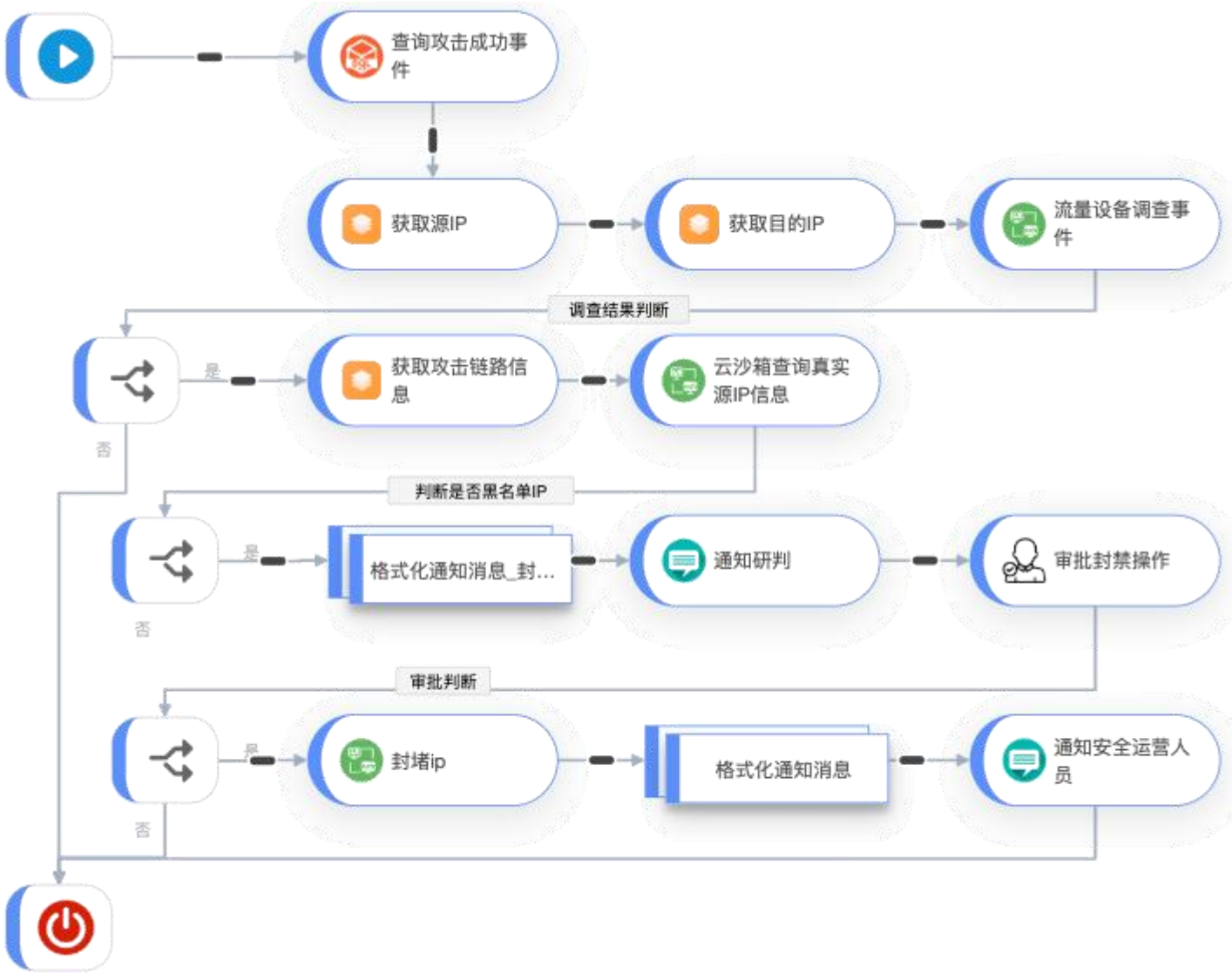
企业通过对已发生的外对内攻击事件的处置，可以更好地了解攻击者的手段和策略，并采取相应的安全措施来防范未来类似的攻击。

接入日志源：

1. HIDS服务、WAF/FW
2. 工单系统（OA等）

处置响应：

通过HIDS服务器确认外对内攻击的源IP目的IP，并通过流量设备获取事件链路信息，联动云沙箱获取真实IP，发起封禁研判并通知安全运营人员。



应用场景5-设备授权到期巡检

场景：

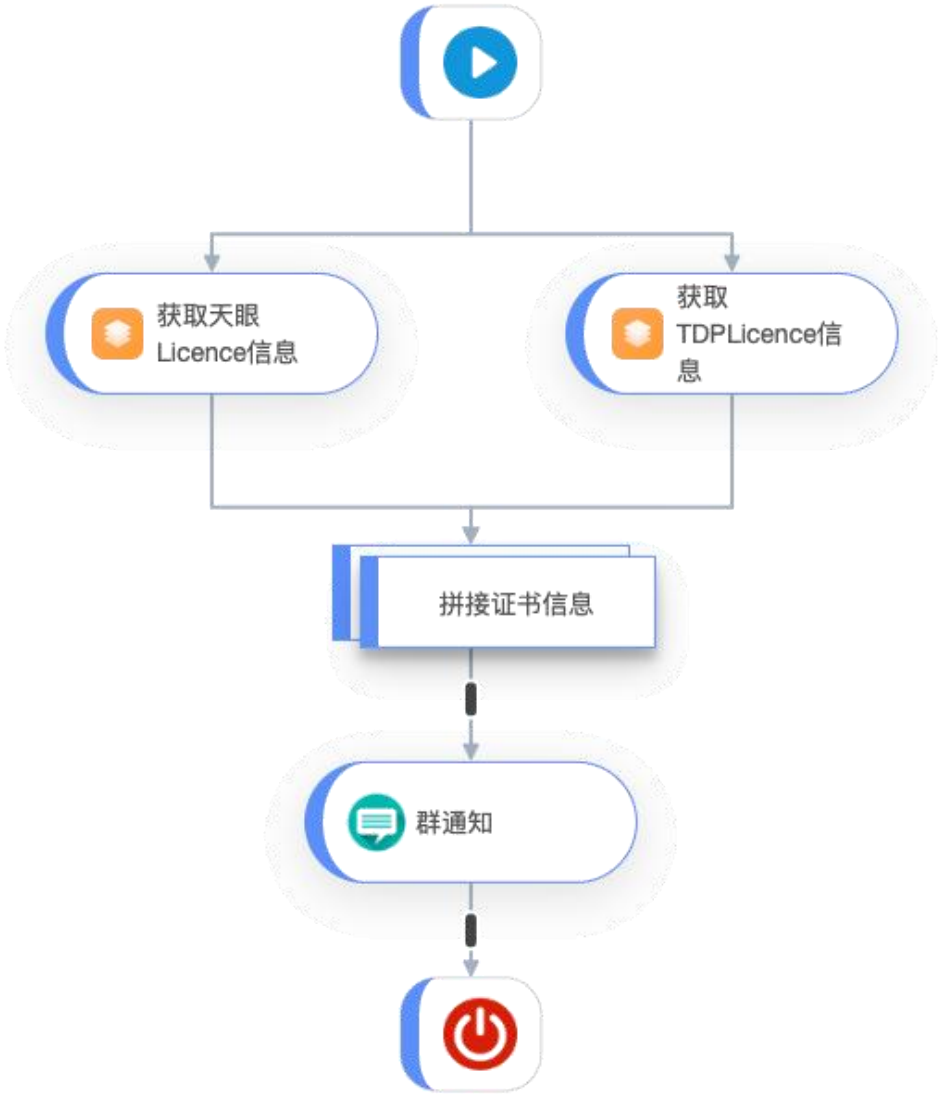
大型企业内部的信息技术管理工作，帮助定期检查所有已安装的软件的证书到期情况，降低人工管理的负担同时极大的提高效率，避免出现潜在的安全问题和业务中断。

接入日志源：

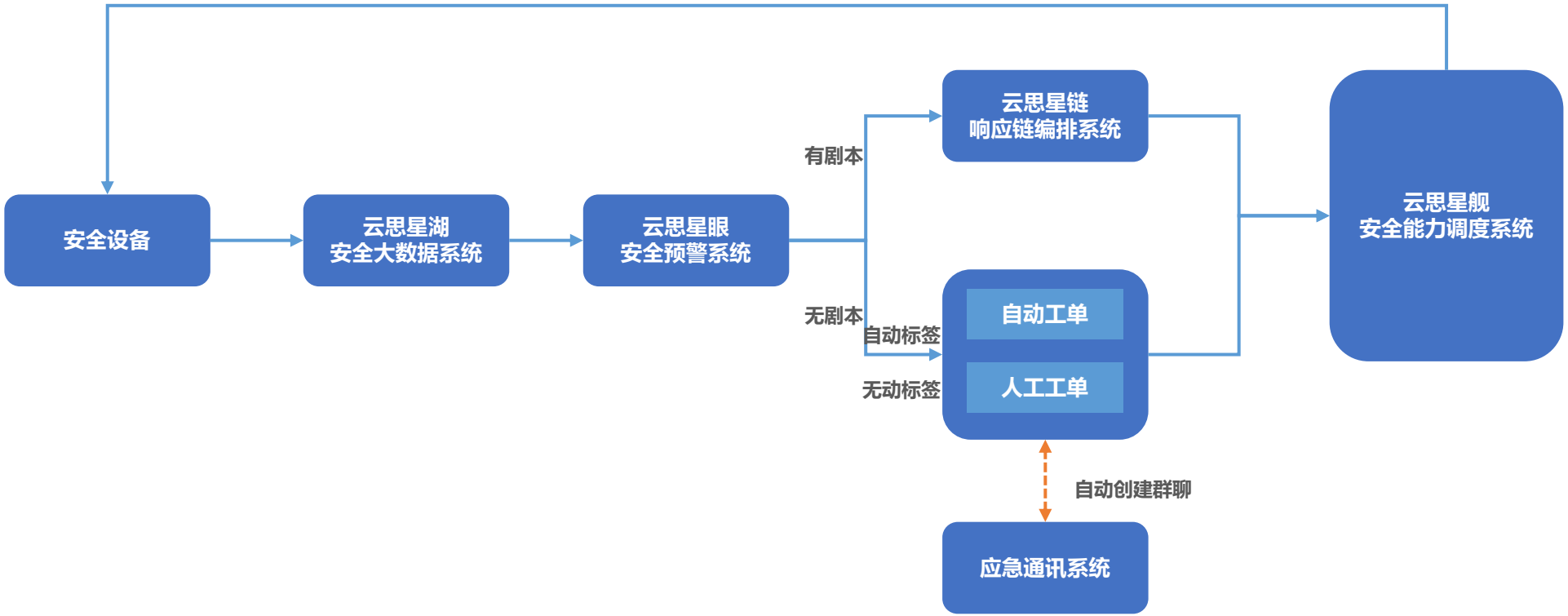
1. 天眼全流量威胁感知系统
2. 工单系统（OA等）

处置响应：

自动获取软件的Licence信息，检查每个软件的相关证书的过期日期以确定证书是否已经过期，如果证书已经过期，则剧本会将该软件标记为需要更新，并向管理员发送警报以通知他们处理该问题



应用场景6-安全事件联动处置



04 客户案例

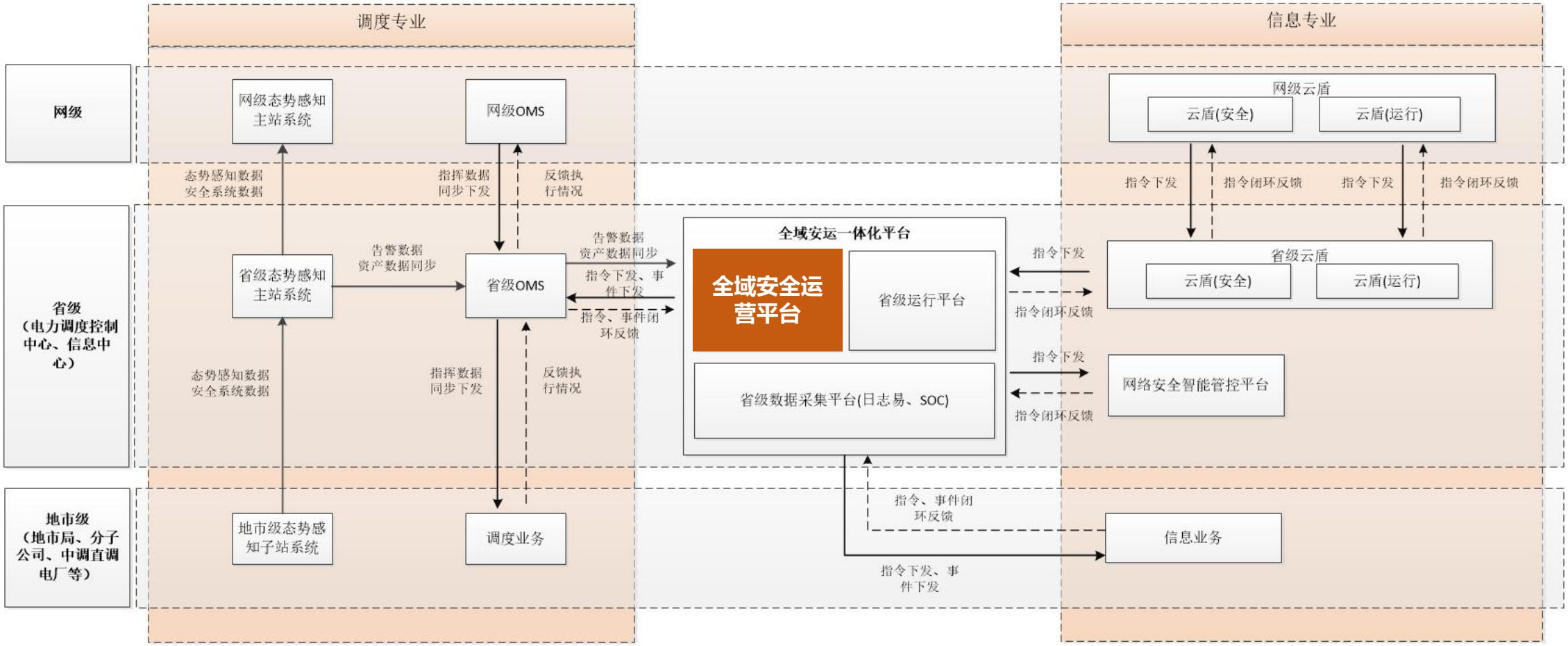
某省级电网公司 | 某央企能源集团 | 某省大数据局

客户案例-某省级电网公司

通过对云思天幕整套方案进行实施，形成了如下成果：

- 汇聚所有安全数据后，形成了统一的安全大数据中台，并实现了为其他系统赋能，大大降低新安全系统开发、上线的时间，节约了成本。
- 实现了3,4区300+网络安全设备的统管、统控，提高了运维效率，安全专责可专注于新技术，新防护手段的研究中。
- 通过近2年的梳理，形成了50+安全剧本，实现了80%安全事件的自动响应和处置，大大提高了安全突发事件的响应速度。特别是在护网中表现良好。
- 通过对云思星站（终端防御）的实施，完成了几万台终端的安全健康画像、威胁外联阻断，很好的限制了安全事件的外延。

客户案例-某省级电网公司-全域网络安全运营平台



客户案例-某央企能源集团

通过对云思天幕中星舰模块（网络安全能力调度系统）的实施，取得了如下成效：

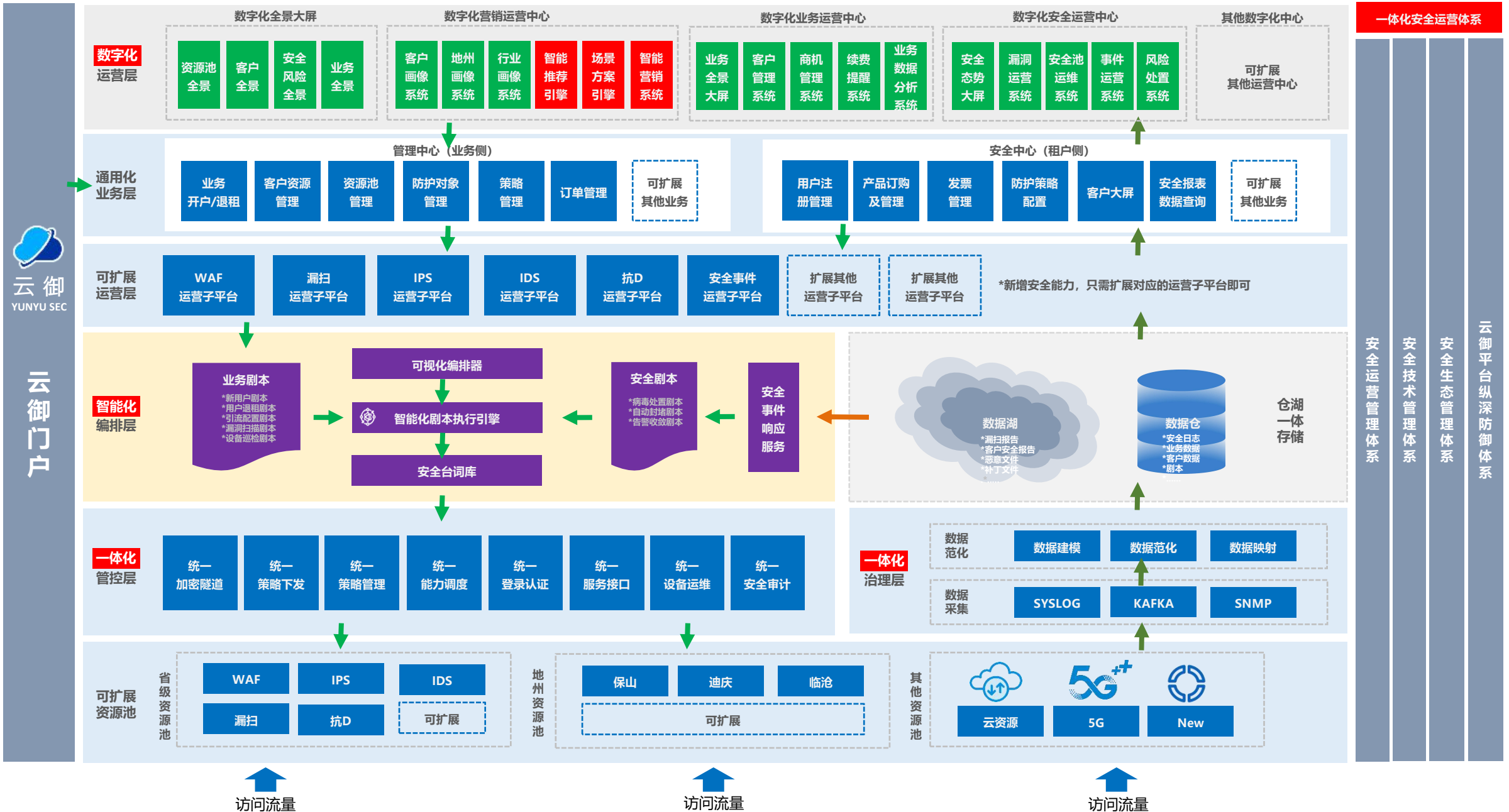
- 基于横向隔离、纵向加密原则，实现了1,2,3,4区网络的分开部署，并对各自区域内安全设备进行统一管控，提高了设备运维的效率，降低了账户密码丢失的风险
- 通过对各区安全设备数据的采集、风险识别，并对安全态势进行可视化，让集控中心实现了对安全态势全局的掌控。
- 通过可视化拓扑图的自动绘制，在检测到威胁时，能快速定位风险点，及时处置。
- 目前正在启动云思天幕整套方案建设的规划。

客户案例-某央企能源集团-智能网络安全运营平台

客户案例-某省移动公司

通过对安全能力池化，为移动的政企客户提供动态的安全能力及服务。整体系统涉及从安全门户->下单->内部业务流程->自动化部署->租户安全运营->安全服务全安全业务流程。

某省级移动公司 打造数智化、场景化、一体化的“战略级”安全运营平台



感谢聆听！

同时请各位领导及专家就以下问题发表意见：

- 贵单位目前的网络安全防御现状如何？
- 贵单位是否已有平台进行安全设备集管及安全事件自动化响应处置？
- 其他问题