炎凰数据
YANHUANG DATA

YHP 智能安全运营平台技术方案

从海量安全数据到 AI 驱动的研判处置闭环

面向安全运营团队的一体化建设方案

全量数据接入 | 智能研判分析 | 自动化响应处置 | 持续运营优化

炎凰数据
YANHUANG DATA

安全运营面临的新挑战

从看见告警，到理解风险、快速处置、持续复盘

告警量大

重复告警多，
噪声占比高

数据割裂

日志、资产、
身份、终端分散

研判依赖专家

人工筛选耗时，
重保期压力大

响应速度有限

判断慢、联动难、
闭环弱

经验难沉淀

同类事件反复
消耗人力

> 安全运营不缺告警，缺的是把告警变成行动的能力。

炎凰数据
YANHUANG DATA

建设目标：从告警处理到智能安全运营闭环

让平台完成重复劳动，让专家专注关键判断

- 从文件导入数据
- HTTP 通过HTTP采集数据
- Syslog 采集Syslog数据
- 通过连接器导入数据
- 通过DataScale采集数据

- 任务告警
- 输出
- 决策
- 数据可视化
- 告警邮件
- 报表

统一接入多源安全数据
打通孤岛，全面可视

生成高质量安全事件
降噪去重，精准聚焦

形成可控自动化响应
策略驱动，快速处置

建设可持续运营机制
复盘沉淀，持续进化

炎凰数据
YANHUANG DATA

建设原则：自动化不是目的，准确闭环才是目的

没有上下文的自动化，只是更快地犯错

先研判，再处置

基于完整上下文与证据链开展判断

分级响应，可控执行

高危自动执行，中危人工确认，低危观察留痕

过程留痕，便于复盘

每一次分析、调用、执行都可审计可追溯

“平台不是替代专家，而是把专家的方法沉淀下来。”

炎凰数据
YANHUANG DATA

YHP 智能安全运营平台总体方案

一个平台，打通数据接入、智能研判、自动响应和持续运营

多源数据接入

安全设备
防火墙 / IDS / IPS / WAF / EDR / XDR / SIEM / NDR

终端与网络
主机 / 服务器 / 网络流量 / DNS / DHCP / VPN

身份与资产
AD / IAM / 账号 / 权限 / 资产 / 漏洞 / 配置

业务与日志
应用日志 / 数据库 / 中间件 / 业务系统 / 审计日志

外部情报
威胁情报 / 漏洞情报 / 黑名单 / 开源情报 / 行业共享

YHP 智能安全运营平台

统一数据底座
- 多源接入与标准化
- 高性能存储与索引
- 全量留存与可追溯
- 数据质量与血缘管理

AI 智能运营引擎
- 智能检测与告警降噪
- 关联分析与攻击链还原
- 威胁评分与风险优先级
- UEBA 行为分析

编排自动化响应
- 处置 playbook 编排
- 自动化联动处置
- 编排审批与人工协同
- 闭环处置与知识沉淀

开放集成生态
- 丰富 API 与事件订阅
- 标准协议与数据导出
- 第三方工具与平台集成
- 开放插件与扩展能力

智能运营输出

高质量事件
精准告警，降低噪音，聚焦真正威胁

智能分析
深度关联分析，攻击链还原与根因定位

联动处置
自动化联动响应，快速遏制与风险控制

运营复盘
闭环复盘与知识沉淀，持续优化运营能力

为企业带来的核心价值

更全面的数据融合
打通多源数据，资产与风险全景可视

更智能的安全运营
AI 驱动研判，提前发现，精准识别

更高效的响应处置
自动化编排响应，分钟级处置，降低损失

更持续的运营提升
复盘闭环与能力沉淀，持续优化，不断进化

炎凰数据 YANHUANG DATA

智能安全运营中心业务架构

用户交互层

- 多角色 / 多智能体身份控制
- 桌面浏览器 + 手机 APP 交互
- 标准对话 + 深度思考 / 研判
- 企业内网单点登录集成

安全运营能力层

- 50+ 预置智能助理
- 深度研判 & 自主响应智能体
- 经典安全运营平台 SIEM / SOC
  - 告警收集
  - 智能研判
  - 情报收集
  - 事件闭环
  - 漏洞闭环

YHP 智能安全运营引擎

多轮次自主驱动的 ReAct 引擎

- 领域知识检索（可持续优化）
  - RAG 引擎
  - Vector DB
  - 安全运营资料库
- 模型服务平台（支持热插拔）
  - 商业模型
  - 国产模型
  - 大模型动态切换
  - 开源模型

执行管理与数据能力层

- 资源集成与执行能力
  - Restful API / WebHook
  - 资源配置数据库

YHP 平台数据能力

- 数据收集
  - Kafka
  - Syslog
  - HTTP
  - API
  - 文件导入
  - DataScale
- 读时建模
- 关联分析
- 数据查询 / 数据集
- 告警监测
- 数据可视化 / 报表输出

基础应用层

- 异构算力中心
  - CPU
  - GPU
  - 异构加速卡
  - 存储资源
- OpenEuler
  - 高性能
  - 安全可信
  - 开放生态
  - 稳定可靠
- 基础 IT / 安全 / 网络产品
  - 防火墙
  - WAF
  - IPS/IDS
  - 交换机
  - 负载均衡
  - VPN
- 数据库
  - 关系型数据库
  - 时序数据库
  - 对象存储

安全合规保障 · 统一运维管理 · 开放生态集成

炎凰数据
YANHUANG DATA

平台总体架构

数据底座 + 智能研判 + 编排响应

闭环响应层
- 任务告警 实时通知
- 自动工单 闭环处置
- 策略编排 自动响应
- 效果评估 持续优化

工具联动层
- 工具集成 生态对接
- API 编排 灵活编排
- 自动化脚本 批量执行
- 能力扩展 插件市场

智能研判层
- 多维分析 关联洞察
- 风险研判 威胁识别
- 攻击溯源 链路追踪
- 智能决策 高效处置建议

安全数据底座层
- 数维汇聚 多源整合
- 数据治理 标准规范
- 数据存储 高效可靠
- 数据服务 统一供给

数据接入层
- 文件导入 批量上传
- HTTP 采集 协议采集
- Syslog 采集 日志采集
- Kafka 采集 流式接入
- DataScale 采集 大数据接入
- 更多接入 持续扩展

全域数据驱动 | 智能研判决策 | 自动编排响应 | 全流程可视可控 | 持续优化闭环

炎凰数据
YANHUANG DATA

多源数据接入：先把安全现场接进来

看得见现场，才能看得清风险

安全设备
防火墙 / IDS / IPS / WAF / 堡垒机 / 上网行为管理 / 漏洞扫描器 / NDR

终端与网络
终端安全 / EDR / NTA / DHCP / DNS / 交换机 / 路由器 / 无线控制器

身份与账号
AD / LDAP / IAM / 统一认证 / 多因子认证 / 特权账号

资产与CMDB
主机 / 容器 / 云资源 / 中间件 / 应用 / 数据库 / 物联网资产

业务日志
应用日志 / 访问日志 / 审计日志 / 数据库日志 / 交易日志

威胁情报
IOC / 漏洞情报 / 恶意域名 / IP信誉 / 开放源 / 商业情报

YHP
安全数据底座

统一接入
多源数据标准化接入，打通安全现场

统一治理
规范数据模型与质量，保证可信可用

统一使用
数据一次接入，全域场景复用

炎凰数据
YANHUANG DATA

读时建模与高速查询：让数据可查、可联、可解释

不等数据治理完美，也能快速支撑安全运营

1 **原始日志**
多源采集
原始数据

→

2 **查询模型**
读时建模
快速构建视图

→

3 **安全语义**
统一指标与对象
标速化语义层

→

4 **关联分析**
多源数据关联
发现关键线索

→

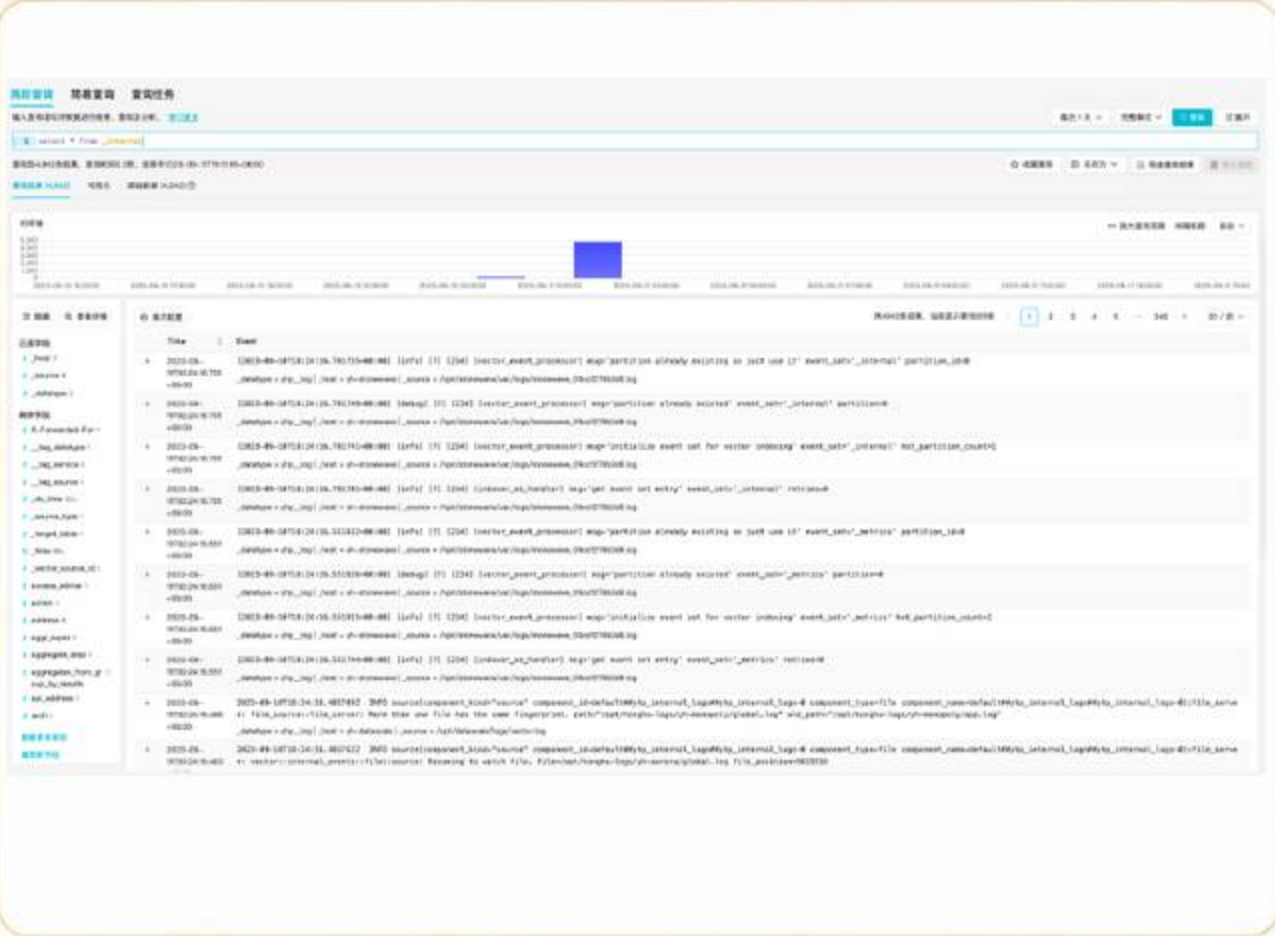
5 **事件上下文**
拼合时间线与上下文
还原事件全貌

快速建立查询视图 | 读时建模，分钟级生成可查视图

支持跨源关联分析 | 打通多源数据，关联实体与行为

支持时间线回溯 | 多维时间线，快速回溯事件脉络

为 AI 提供结构化上下文 | 结构化语义与关系，促进智能分析



炎凰数据
YANHUANG DATA

告警治理：从海量噪声到高质量安全事件

告警越多不代表越安全，能被验证的事件才有价值

合并重复告警

智能去重与规则过滤，消除冗余噪声，让团队专注真正的风险。

补充资产与身份信息

融合资产、身份、脆弱性与威胁情报，补齐上下文，提升告警准确度。

形成证据摘要

自动关联行为链与证据要素，生成可追溯的证据摘要，便于调查与取证。

输出等级与建议

智能评估事件等级与影响，输出处置建议与优先级，驱动高效响应。

让威胁可验证，让处置更精准，让安全运营更智能，实现从“告警洪流”到“安全价值”的转变

炎凰数据
YANHUANG DATA

AI 智能研判：不是聊天机器人，而是安全分析流程自动化

把专家经验沉淀为可复制、可协同的研判能力

炎凰数据
YANHUANG DATA

深度研判机制：多轮任务拆解 + 证据链输出

让安全分析从“人工翻系统”变成“平台自动找证据”

1 **接收事件**
告警、情报、线索统一进入

2 **识别目标**
明确对象、范围与优先级

3 **拆解任务**
生成多步调查任务

4 **调用工具**
联动数据、知识与接口

5 **还原脉络**
拼合时间线与攻击链

6 **输出结论**
形成结论、证据与建议

多轮分析更完整
多源多维，层层递进，覆盖更全面

证据链更清晰
全链路拼合，来源可溯，结论可信

报告输出更高效
结论结构化，证据可追溯，快速输出

炎凰数据
YANHUANG DATA

编排自动化响应：研判之后必须动得起来

从“知道有风险”到“完成可控处置”

研判结论
风险等级、影响范围、处置建议

策略判断
根据策略分级控制执行方式

自动执行
- 封禁恶意 IP
- 隔离终端

人工确认
- 变更关键账号
- 下线高风险接口

观察留痕
- 持续监测
- 保留证据与记录

封禁　隔离　改密　通知　工单　报告

策略可控　执行可审计　闭环可复盘

炎凰数据
YANHUANG DATA

运营工作台：安全团队的一张作战视图

让值班、研判、处置、复盘都在同一张图上发生

统一态势视图
全量数据汇聚，安全态势一目了然

统一事件队列
告警去重聚合，事件优先级清晰可见

统一任务跟踪
任务流转透明，进度状态实时掌握

态势感知

事件研判

任务跟踪

复盘沉淀

MTTA	MTTR	降噪率	闭环率	自动化执行率
–	–	–	–	–

炎凰数据
YANHUANG DATA

场景总览：围绕安全运营闭环建设可落地场景

— 先从高价值场景跑通闭环，再逐步复制扩展 —

1 重保 / 护网攻击告警闭环

2 钓鱼邮件处置闭环

3 失陷主机与异常外联闭环

4 敏感信息泄露风险闭环

从发现问题到形成闭环，持续提升安全运营价值

炎凰数据
YANHUANG DATA

场景一：重保 / 护网攻击告警闭环

从一条高危告警到完整攻击链研判与联动响应

触发

WAF、NDR、EDR、
态势感知产生高危告警

关联

关联资产重要性、
漏洞状态、账号行为、
威胁情报

研判

还原攻击链，识别
攻击阶段、影响范围
与关键证据

处置

封禁攻击源、隔离主机、
通知责任人、
生成事件报告

复盘

沉淀攻击手法、
策略优化建议与
专项整改清单

7×24 快速响应

重点资产优先保护

重保期间高效协同

炎凰数据
YANHUANG DATA

场景二：钓鱼邮件研判与应急处置闭环

从员工举报到全域清理，尽可能压缩攻击窗口

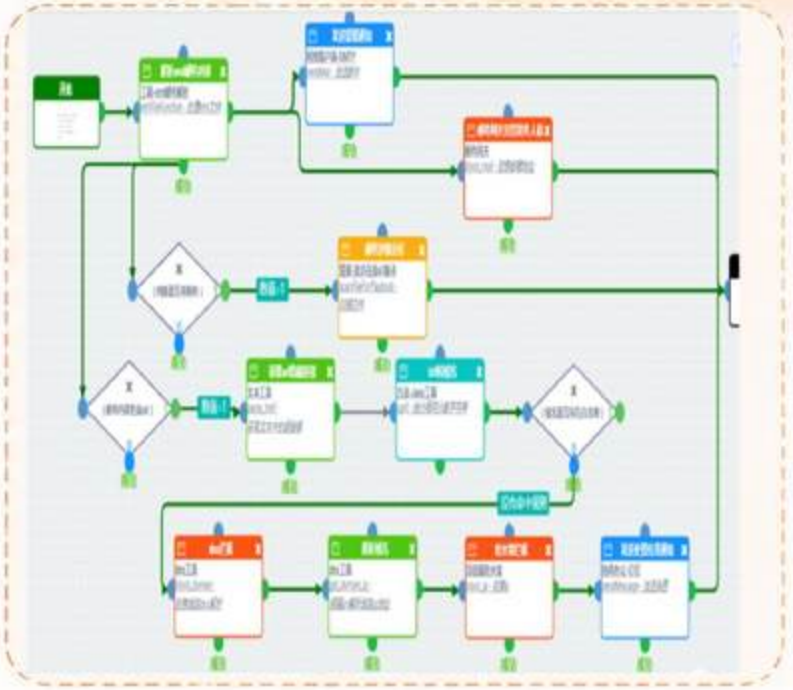
01
触发
邮件网关告警、员工举报、终端发现可疑附件

02
分析
解析发件人、域名、URL、附件、二维码与诱导话术

03
扩散排查
检索同主题邮件，统计点击员工与终端行为

04
处置
批量撤回邮件，封禁域名/IP/URL，通知员工改密

05
输出
自动生成影响范围、处置过程与复盘建议



快速止损 | **自动排查** | **协同处置**

炎凰数据
YANHUANG DATA

场景三：失陷主机、挖矿与异常外联闭环

既要快速响应，也要避免粗放处置带来的业务影响

1 触发

终端发现可疑进程，NDR发现挖矿连接，DNS/代理发现异常外联

2 关联

结合资产归属、业务属性、历史外联、账号登录与进程树

3 研判

区分正常业务、测试行为、误报与真实失陷，输出置信度

4 处置

终端隔离、进程查杀、IOC封禁、账号改密、漏洞修复工单

5 复盘

输出感染路径、暴露原因、同类资产排查与策略优化建议

降低误判 | 缩短处置时间 | 兼顾安全与业务

炎凰数据
YANHUANG DATA

场景四：敏感信息泄露风险闭环

作为安全运营延展场景，承接 DLP、文件、打印与账号等多源线索

1 **提出离职**
员工提交离职申请，
HR 系统产生离职流程

2 **访问敏感目录**
频繁访问研发/财务等
敏感目录及项目资料

3 **文件外发被拦截**
通过邮件/网盘/IM 外发
敏感文件被 DLP 拦截

4 **跨部门打印资料**
短时间内在多部门
打印大量敏感文档

5 **异常拷贝或外传尝试**
尝试使用 U 盘拷贝或通过
第三方工具外传数据

6 **联动处置与证据固化**
多源线索关联确认风险，
联动处置并固化证据

关联线索
DLP、终端、打印、账号、审批、访问日志

研判重点
时间线还原、证据链构建、影响范围识别

联动处置
终端隔离、账号冻结、权限收敛、
通知安全/HR/法务

证据链摘要
多源数据串联，形成完整
证据链路，支撑决策与追溯

离职申请记录 时间：T-14 天 → 敏感目录访问日志 时间：T-10 ~ T-5 天 → DLP 拦截记录 时间：T-5 天 → 打印记录 时间：T-3 天 → 外设/外发尝试日志 时间：T-1 天 → 处置工单与证据归档 时间：T 日

让风险可追溯、证据可核验、处置可闭环

炎凰数据
YANHUANG DATA

扩展能力：从安全运营延伸到运维、数据安全与攻防演练

平台优先服务安全运营主战场，同时具备持续扩展能力

网络运维

- 拓扑识别
- 策略巡检
- 链路诊断

数据安全

- 影子API发现
- 敏感数据访问审计
- 风险追溯

YHP
平台能力

红蓝对抗 / 攻防演练

- 演练编排
- 响应评估
- 报告生成

日常运营

- 安全巡检
- 合规检查
- 知识问答

一个平台能力底座，多类业务场景复用

炎凰数据
YANHUANG DATA

场景五：IOC情报驱动的自动化排查闭环

从外部情报进入，到内部资产排查、影响面确认与处置反馈

1 情报接入
威胁情报、漏洞公告、黑名单

2 资产匹配
匹配CMDB和互联网暴露面

3 历史回溯
检索DNS、代理、终端、流量

4 风险研判
判断是否命中攻击链

5 联动处置
封禁、隔离、通知、报告

主动排查

影响面可见

处置可追踪

炎凰数据
YANHUANG DATA

场景六：漏洞情报与资产风险联动闭环

把漏洞通报转化为可执行的资产整改任务

受影响资产识别

- 基于漏洞特征精准匹配
- 识别受影响的IT/OT资产
- 支持多维度关联（IP/域名/组件）

暴露面确认

- 验证资产是否对外暴露
- 端口/服务/路径探测确认
- 威胁可达性评估

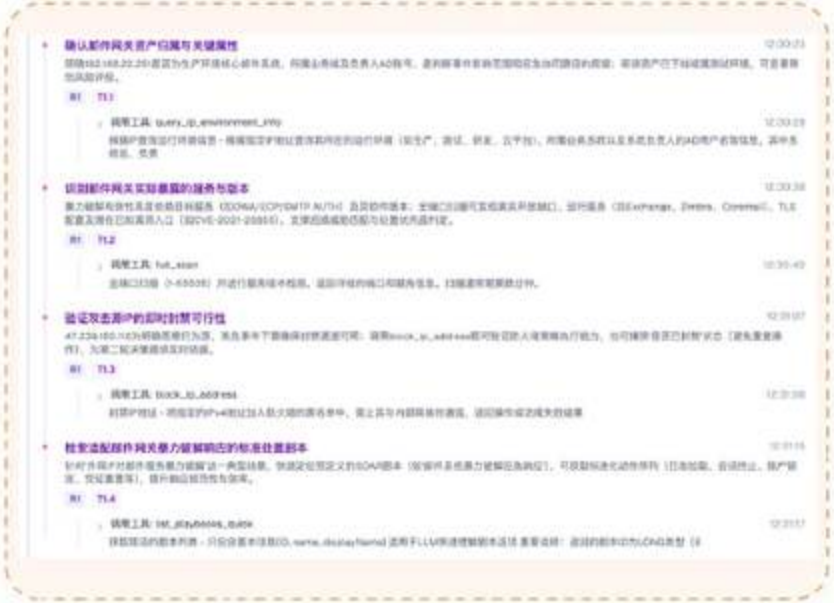
漏洞情报

风险优先级

- 漏洞严重度评分（CVSS）
- 资产重要性加权
- 生成风险优先级（P1/P2/P3）

整改闭环

- 生成整改任务与工单
- 跟踪处理进度与状态
- 复测验证，闭环归档



漏洞公告 → 版本/组件匹配 → 资产责任人 → 修复工单 → 复测验证 → 复盘沉淀

> 漏洞管理的关键，不是知道有漏洞，而是知道谁受影响、谁负责、何时修完。

炎凰数据
YANHUANG DATA

场景七：账号异常登录与权限滥用闭环

围绕身份、资产、行为和权限构建统一研判链路

预留：账号风险详情截图

1 触发

异地登录/异常时间/高频失败

2 关联

身份、岗位、权限、终端、资产

3 研判

识别误报、共享账号、盗用风险

4 处置

强制改密、冻结账号、收敛权限、通知责任人

5 复盘

账号治理、策略优化、权限整改

炎凰数据
YANHUANG DATA

场景八：网络运维辅助与故障诊断

作为安全运营扩展能力，联动网络设备提升排障效率

YHP 平台能力

多源数据融合

自动发现网络设备与链路，
构建实时拓扑视图

智能分析引擎

基于关联分析与模型识别，
快速定位异常根因

策略与配置洞察

配置合规检查与策略分析，
识别风险与变更影响

自然语言助手

支持自然语言问答与操作指引，
降低使用门槛

拓扑识别

自动发现网络设备和链路关系，生成可视化拓扑
支持层级展示、设备状态与链路健康度呈现

链路诊断

链路连通性检测、时延/丢包分析、路径追踪
快速定位故障节点与影响范围

策略巡检

安全策略与配置合规检查，识别高危与冗余策略
变更影响分析与巡检报告输出

平台优先服务安全达营主战场，网络运维可作为扩展场景逐步落地。

炎凰数据
YANHUANG DATA

场景九：红蓝对抗与攻防演练复盘

让演练过程可记录、响应能力可评估、整改任务可追踪

红队攻击路径

01 侦察
信息收集、端口扫描、指纹识别、漏洞探测等

02 利用
漏洞利用、载荷投递、权限获取、建立访问等

03 横移
内网探测、凭证窃取、横向移动、权限维持等

04 外联
数据外传、C2通信、隐蔽隧道、对外控制等

YHP平台

安全运营中枢

数据汇聚 · 统一分析 · 智能编排
联动响应 · 闭环管理

蓝队响应路径

01 发现
多源告警、威胁检测、异常行为、可视化监控等

02 研判
事件分析、威胁研判、影响评估、攻击链还原等

03 处置
策略阻断、主机隔离、溯源取证、应急响应等

04 复盘
演练复盘、效果评估、经验沉淀、改进优化等

发现时间	响应时间	处置准确率	整改闭环率
--	--	-- %	-- %
从攻击开始到首次发现	从发现告警到响应启动	有效处置占处置总数比例	按期完成的整改任务比例

预留：演练报告 / 攻击路径图截图

炎凰数据
YANHUANG DATA

落地路径：以一个闭环场景验证平台价值

先用一个场景跑通闭环，再用闭环复制场景

1
需求调研与场景选择
明确试点范围、数据源与验收目标

2
数据接入与读时建模
接入关键日志、告警、资产与账号数据

3
研判流程与响应策略配置
配置任务、工具联动、审批与剧本

4
POC 验证与效果评估
用真实事件或演练验证闭环能力

5
规模化推广
扩展到更多安全运营场景

建议 POC 周期
- 2–3 周
- 优先选择 1–2 个高价值场景
- 以真实数据验证效果

关键成效指标（KPI）

MTTA | MTTR | 告警降噪率 | 事件闭环率 | 自动化执行率

以可验证结果推动平台建设，以试点成功带动规模推广

炎凰数据
YANHUANG DATA

总结：建设面向未来的智能安全运营体系

从数据底座到智能研判，从自动响应到持续复盘

全域可见

资产、威胁、风险
全域可视，态势可感

智能研判

AI驱动关联分析
精准识别，高效研判

可控响应

自动化编排响应
策略可控，快速处置

持续运营

复盘驱动优化
经验沉淀，能力提升

预留：客户现场建设目标 / 下一步计划

以统一平台承接安全运营主流程，让告警变事件，让事件形成闭环，让经验沉淀为能力。

炎凰数据
YANHUANG DATA

客户建设收益：从安全投入到运营价值

降低重复劳动，提升响应效率，增强风险可解释性

效率提升

- 告警自动聚合
- 研判自动找证据
- 报告自动生成

风险收敛

- 高危事件优先处置
- 关键资产重点保护
- 处置动作可控可审计

能力沉淀

- 知识库持续积累
- 剧本持续优化
- 运营指标持续跟踪

> 平台的价值，不是多展示一张大屏，而是让安全团队少走弯路、快做判断。

炎凰数据
YANHUANG DATA

平台落地方式：不推倒重建，接入现有体系

以开放接口和工具联动，保护既有投入，降低实施成本

低改造
最小改动，快速接入

快接入
标准接口，即接即用

可扩展
模块化对接，灵活扩展

可审计
全程留痕，合规可追溯

炎凰数据
YANHUANG DATA

价值衡量：让安全运营效果可被量化

从响应速度、告警质量、闭环能力和运营沉淀四个维度评估建设成效

01 MTTA 首响时间

从告警触达到开始研判的时间

02 MTTR 处置时间

从确认风险到完成闭环的时间

03 告警降噪率

减少重复、误报、低价值告警

04 闭环率

事件处置、误告、复盘均有记录

能被度量的安全运营，才有可能被持续优化。

炎凰数据
YANHUANG DATA

POC验证建议：用真实场景验证闭环价值

2-3周跑通一个高价值场景，形成可量化评估结果

1 需求调研

- 梳理业务目标
- 识别高价值场景
- 明确评估指标

2 数据接入

- 接入关键日志
- 接入告警与事件
- 数据清洗与关联

3 读时建模

- 构建知识与基线
- 识别模式与异常
- 生成研判线索

4 研判配置

- 配置研判规则
- 定义处置动作
- 设置审批策略

5 闭环验证

- 触发处置并执行
- 人工/自动化协同
- 验证效果与复盘

建议范围

- 选择 1-2 个高价值场景
- 接入关键日志与告警
- 定义处置动作与审批策略
- 输出评估报告形成量化结果

可量化评估指标（KPI）

MTTA	MTTR	降噪率	闭环率	自动化执行率
平均告警确认时间	平均故障恢复时间	无效告警减少比例	闭环事件占比	自动化处置占比

先把一个场景做深，再把闭环能力复制到更多场景。

炎凰数据
YANHUANG DATA

THANKS