AI 驱动的安全告警智能处置与自动化运营实践

一、背景与挑战

随着基金行业数字化转型持续深化，银华基金管理股份有限公司（以下简称我司）的信息系统规模持续扩张，生产环境已部署 NDR 网络流量检测、HIDS 主机入侵检测、WAF 应用防护等多类安全设备，每日产生的原始告警量高达数千条。与此同时，APT 定向攻击、供应链入侵、AI 辅助的鱼叉式钓鱼等攻击手段持续演进，基金公司作为金融数据的汇聚机构，始终是攻击者的重点目标。

然而，传统安全运营模式正面临日益突出的结构性困境。其一，告警海量充斥：扫描类、重复类、误报类低价值告警占比超过 90%，安全分析员深陷「告警疲劳」，极易造成有效威胁遗漏；其二，溯源处置：面对疑似入侵事件，安全人员需在多个平台间反复跳转，完成一次完整研判动辄耗时 30 分钟以上，而攻击者横向移动所需时间往往不超过数分钟；其三，巡检覆盖不足：传统人工巡检无法实现小时级常态化覆盖，设备离线、规则库过期等隐患难以及时发现。

二、技术方案

2025 年底，我司启动 AI 赋能安全运营探索工作，依托主流安全厂商开源平台 Flocks 企业版为技术底座，构建以 AI 原

生智能体（Agent）为核心的告警自动处置体系，系统性重塑安全运营工作流，以最低成本进行最高效率的运营能力提升。

（一）多层降噪工作流：消除 90%以上告警噪音

针对原始告警较多问题，AI 平台构建了五层串行降噪工作流，全程无需人工干预：第一层，黑白名单过滤，自动消除内部合规系统产生的无效告警及已知恶意 IP 告警；第二层，自定义业务规则过滤，结合基金交易系统专属通信行为配置规则，消除与实际业务无关的误报；第三层，扫描类告警自动识别与过滤，通过高频率、顺序端口等特征自动判定端口扫描行为；第四层，短时重复告警合并，同类告警合成一条并携带触发次数；第五层，历史研判去重，对已有明确结论的告警直接跳过。

经过五层过滤，日均原始告警量从数千条压缩至数十条高价值有效告警，告警噪音压缩率超过 92%。

（二）智能告警研判 Agent：压缩研判时长至分钟级

经过降噪筛选的高价值告警自动进入告警研判 Agent 执行链路：并发调用威胁情报 API 核查涉事 IP/域名/文件声誉；调用内部 CMDB 确认目标资产归属及重要性分级；检索历史处置记录排查是否曾出现过。所有信息整合后，Agent 自动生成结构化研判报告，明确标注风险等级及处置建议，同步推送至飞书安全告警群。单条告警平均研判时长：从 30 分钟压缩至 3 分钟以内。

（三）设备巡检 Agent：从日度巡检到小时级主动监测

借助 Flocks 智能体任务调度中心，我司构建了定时巡检 Agent，每小时自动检查 NDR、HIDS、防火墙、WAF 等十余类安全设备的在线状态、日志连续性、规则库更新、性能指标等。一旦设备离线或规则库超过 30 天未更新，立即推送告警至飞书。设备异常平均发现时间：从超过 **4 小时**压缩至 **1 小时**以内。

三、实践成效

关键指标	上线前	上线后
日均需人工处理告警量	数千条	**数十条（下降超 92%）**
单条告警平均研判时长	30 分钟以上	**3 分钟以内**
人工研判工作量（日均）	约 4 小时	**约 1 小时（下降约 75%）**
设备异常平均发现时间	超过 4 小时	**1 小时以内**
低危事件自动闭环率	—	**超过 85%**
高危告警识别准确率	—	**超过 95%**

在多次内部模拟攻防演练及应急响应测试中，AI 研判 Agent 均在人工发现威胁之前完成识别并推送预警，平均响应时间低于 20 分钟，高危告警识别准确率保持在 90%以上。

四、经验启示

本项目的核心体会是：AI 在安全运营中的价值，不在于取代人工，而在于精准切入「规则明确、输入固定、流程稳定」的高频重复任务——告警初判、降噪分类、威胁情报查询、设备巡检均属此类。AI 平台告警降噪、初步研判、设备巡检等重复性工作，人工团队聚焦高难度处置、APT 分析、安全策略优

化等复杂工作，二者边界在制度层面明确划定，才能实现自动化收益与风险可控之间的平衡。

展望未来，我司将在现有成果基础上进一步扩展 AI 安全运营应用场景，探索漏洞全生命周期管理、供应链安全风险评估、安全态势自动生成等能力，推动安全运营从「事件响应」向「主动防控」持续深化。