聚铭安全管家平台

产品白皮书

聚铭网络科技有限公司

2026 年 02 月

目录

声明

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司和北京聚铭信安科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

南京总部：南京市雨花台区软件大道 180 号南京大数据产业基地 7 栋 4 层

电　　话：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

聚铭网络技术服务以及营销网络覆盖全国，并在各地设有办事处和分支机构，为客户提供无微不至的解决方案和高效的服务支持。聚铭专家团队 7x24 小时全天候在线，确保在安全事件发生时提供分钟级应急响应。

1. 面临问题和挑战

1.1. 面临问题

随着网络安全威胁的日益复杂化，企业安全建设正加速向服务化（Security-as-a-Service）转型，MSS（托管安全服务）成为主流交付模式。然而，安全服务提供商（MSSP）及安服团队在运营过程中仍面临诸多挑战，涵盖技术、管理、商业等多个维度。

1. 安全运营效率低下，人力成本高

- **告警疲劳与误报泛滥：**企业平均每天产生 **10000+安全告警**（SANS 2023 报告），其中 **70%以上为误报或低优先级事件**，导致分析师陷入“告警泥潭”，真正的高危威胁被淹没。
- **手动响应效率低：**传统安全运营依赖人工研判，平均 MTTR（平均修复时间）长达**数天**（IBM X-Force 数据），无法满足实时对抗需求。
- **技能门槛高，人才短缺：**全球网络安全人才缺口达 **340 万**（ISC² 2023），高级威胁分析、逆向工程等核心能力难以快速复制，服务商高度依赖少数专家。

2. 安全服务标准化不足，质量参差不齐

- **缺乏统一的服务框架：**不同 MSSP 的运营流程、SLA（服务等级协议）差异巨大，客户难以横向对比服务质量。
- **工具链碎片化：**多数服务商使用**多套独立工具**（SIEM、SOAR、EDR 等），数据孤岛严重，跨平台分析效率低。
- **经验难以沉淀：**安全运营依赖分析师个人经验，缺乏标准化的**威胁检测规则库、响应剧本（Playbook）**，导致服务交付不稳定。

3. 威胁态势复杂化，传统防护模式失效

- **攻击面持续扩大：**云、IoT、OT 等新环境引入，企业暴露面增长 300%+（Gartner 2024），传统边界防护失效。
- **攻击者自动化程度高：**勒索软件、APT 组织采用 AI 驱动的攻击工具（如自动化漏洞利用、钓鱼生成），传统人工防御难以应对。
- **威胁情报利用不足：**83%的 MSSP 未能有效整合威胁情报(Forrester 2023)，导致检测能力滞后于新型攻击手法。

4. 合规与风险管理压力加剧

- **监管要求升级：**GDPR、等保 2.0、SEC 新规等对安全运营提出更高要求，但人工合规审计效率低下，错误率高。
- **第三方风险传导：**供应链攻击频发，但多数 MSSP 缺乏**供应商安全评估**能力，导致服务链存在盲区。

5. 商业竞争激烈，服务商盈利与拓客困难

- **同质化竞争严重**：基础 MSS 服务（如日志监控、漏洞扫描）进入价格战，利润率持续下降。
- **客户信任度低**：缺乏客观的**服务效果可视化**，客户难以感知安全价值，续约率不足 60%。

6. 数据出网与本地化合规挑战

- **数据出网合规受阻：**大多数 MSS 平台，在客户侧只部署采集探针，需要将客户数据上送至 SaaS 平台，导致数据出网
- **自有客户捆绑严重：**已服务的客户数据沉淀在厂商 SaaS 平台，安全服务提供商无法直接管理自有客户

1.2. 需求

针对前文所述的安全运营服务化趋势及行业痛点，亟需建立一套体系化、合规优先、效率驱动的 MSS 平台工具，通过技术赋能解决服务商与客户的双向需

求。

核心目标

- **对客户**
  - **保障数据主权**：支持本地化安全运营，满足“数据不出网”合规要求
  - **透明化运营**：运营过程可视化，实时查看运营情况
  - **效果可量化**：直观展示整体的安全建设情况、等保合规情况、安全防护情况
- **对安服商**
  - **降低运营成本**：通过自动化及 AI 能力，替代 70%以上重复性人力工作
  - **提升服务标准化**：定义一套标准的 SLA 体系，安服人员按照标准体系运营
  - **提升服务质量化**：通过平台能力，使安全复杂度降低，不因安服人员个体能力参差不一导致的服务有差距。通过自动化能力，提高 MTTR 响应时间，及时保障业务安全
  - **客户自管控，提升复购率**：对已运营的客户进行全生命周期管控，对即将过期的客户资源

2. 解决方案

作为国内最早布局 MSS 托管安全服务的厂商之一，聚铭基于多年实战经验与行业洞察，打造出新一代**体系化、合规优先、效率驱动**的聚铭安全管家平台。该平台采用**三级分层架构**（智能决策层-中枢控制层-本地化防御层），深度融合自动化、AI 与合规设计，系统性解决安服商效率瓶颈与客户数据主权诉求，实现“服务更高效、客户更满意、安全更简单”的核心价值。

方案整体框架

一级平台部署在聚铭云端，提供威胁情报、策略更新、AI 大模型赋能、外部暴露面测绘等服务。

二级平台可以部署在服务商机房，也可以部署在云上，需提供一个公网 IP，用于三级平台的数据上报。主要对服务商自有的客户进行管理、安全运营、安全监控等，运维人员可以登录二级平台，对所负责的客户做远程运营；管理人员可以管理监控已服务的客户，保障服务的质量。

三级平台部署在客户侧，主要纳管客户侧已部署的所有安全设备，将各类告警数据统一收集分析，进行威胁检测及治理、脆弱性检测及治理等安全运营体系工作。

3. 主要功能

3.1. 一级平台

3.1.1. 威胁情报共享

构建多源情报融合分析体系，实现全球主流威胁情报源的自动化采集、标准化处理和智能分发。结合本地资产数据实现精准影响分析，为安全运营提供及时可靠的威胁预测能力。

3.1.2. 基于大模型的智能研判

集成多模态大模型技术，打造智能化的安全分析决策中枢。实现事件的智能分析、数据包的智能研判等核心功能，大幅提升分析效率和准确性。通过可视化的推理和持续优化的专家经验库，使复杂安全事件的分析研判更加高效透明。

3.1.3. 安全垂直大模型赋能安全运营人员

专注安全垂直领域大模型，基于海量真实安全事件训练而成。具备日志智能分析、漏洞影响评估和处置建议等专业能力，通过持续学习机制不断优化模型效果，为安全运营人员提供强大的 AI 辅助工具。

3.1.4. 行业策略库及知识共享

汇聚行业最佳实践的智能知识中枢。包含经过实战运营的检测规则和响应剧本，支持安全经验的沉淀共享和效果评估，通过智能化的策略共享机制确保安全运营的持续优化。

3.2. 二级平台

3.2.1. 客户及项目管理

在传统企业服务模式下，客户管理面临管理流程割裂、服务标准缺失等痛点，导致从签约到交付的执行过程难以规范管控。

为此我们提供客户全生命周期管理解决方案，通过提供客户全生命周期管理能力，实现从服务签约到项目交付、执行的流程化管理。支持多层级客户组织结构管理，可灵活配置项目团队体系，SLA 服务体系等功能，确保服务交付、运营过程规范可控。

3.2.2. SLA 计划编排

当前，不同客户订阅的 SLA 套餐存在差异化要求（如渗透测试、护网服务等），运维人员需同时管理多套服务标准，人工排期易出现疏漏；同时，客户缺

乏透明化监督手段，难以确认 MSS 服务是否按约定执行，导致双方信任成本升高。

对此，平台推出 SLA 智能编排模块—通过根据客户项目，将 SLA 要求拆解为可执行计划（如漏洞修复时限、定期扫描等），并动态下发至三级平台任务队列；客户端通过三级平台实时可视化看板同步更新任务进度，结合自动提醒功能确保运维人员严格履约，最终实现"客户可查、执行可控、风险可预警"的服务闭环。

3.2.3. 远程运营

传统远程运营模式依赖客户部署 VPN 等第三方工具，在多客户同时要运营的场景下需频繁切换连接，严重影响运维效率。

二级平台提供安全可靠的远程运营模块，可以直接连接到各个三级平台运营界面及管理后台，无需借助任何第三方远程工具，即可实现远程运营，SSL 加密隧道护航、动态凭证即时失效、所有操作全程留痕可追溯，实现"效率与安全并重"的远程运营。

3.2.4. 客户情况可视化

客户服务的质量往往会直接影响到客户的复购率，但在传统运营模式下，企业难以实时掌握客户的安全服务状态、设备运行情况、事件处置时效及许可到期等重要信息，导致服务响应滞后，客户体验不佳。

通过提供客户运营全景视图，基于多维度数据分析，实时展示客户许可状态（含到期预警及自动续期提醒）、SLA 套餐分布、团队服务效能等关键指标，并深度集成客户运营健康度评估（风险评分、问题闭环率、等保合规、三级平台运行状态等），帮助运营商精准掌握客户运营态势，优化安全投入产出比，提升服务透明度与客户续购意愿。

3.2.5. 互联网暴露面测绘

构建互联网数字资产实时监测体系，自动化采集域名、IP 、系统服务、信

息系统及邮箱等全量资产数据，同步识别风险资产。通过二级平台智能调度探测任务，实时将资产情报推送至三级平台，形成风险监测-探测-处置的全闭环自动化流程。

3.3.三级平台

3.3.1. 安全运营体系化

以资产为核心，在安全建设基础能力的基础上，提升安全基础设备检测的精准性，打造智能化事件分析、自动化响应及处置能力。通过对事件的深度分析及信息情报共享，建立预测预警机制，并针对性改善安全系统。最终达到有效检测、防御新型攻击威胁之目的，直观呈现安全态势与安全建设成果。

通过网络安全制度、策略、流程的梳理，形成安全管家平台的工作机制，实现安全运营的自动化。

3.3.2.多维数据采集及融合

平台内置的数据采集引擎，支持多源异构设备日志的采集及范式化处理、流量数据的还原及精细化解析、漏洞/弱口令/违规基线/web 应用等脆弱性数据采集。

除此之外，更为重要的是，平台支持抓取及监控各个安全设备页面，实现跨平台和多业务系统的数据汇聚及融合。

日志、流量、脆弱性及安全设备页面数据采集及融合为安全检测分析提供更全面的数据来源。

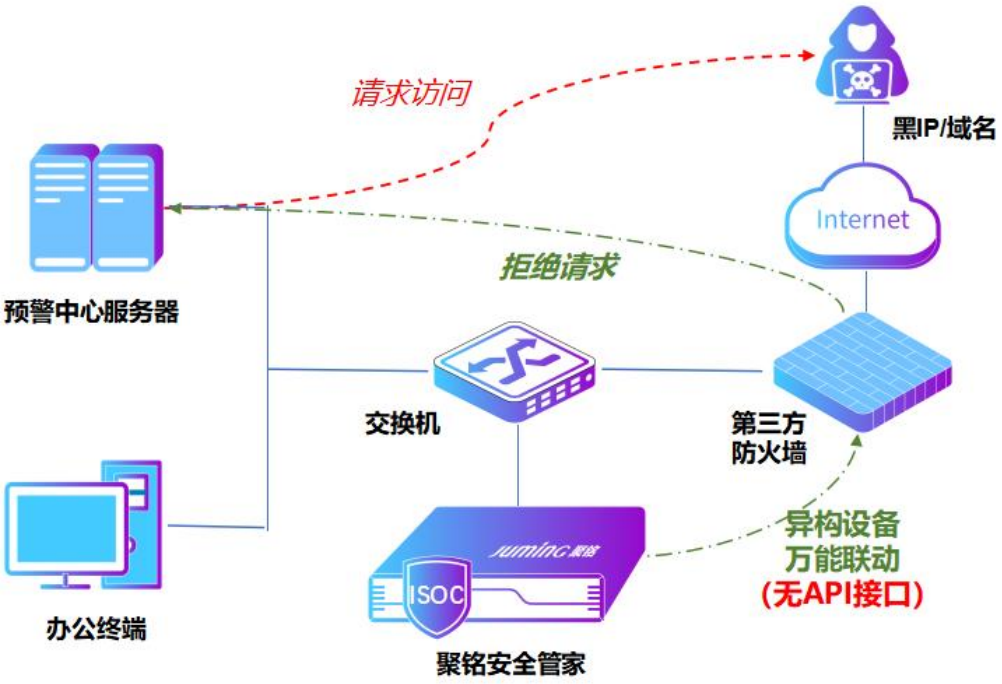
3.3.3.自动化编排响应处置

所有的攻击威胁发现，没有及时的闭环响应处置都是无济于事的，处置响应能力为安全运维人员提供便捷的处置方法和相关的处置建议，安全管家平台具备自动化编排响应能力和安全检测加固能力。

基于 SOAR 技术的自动化应急响应，将原本需要人员参与的安全事件处置流程转变为安全剧本。将事件处置过程中人、安全工具及能力、流程等参与元素和环节进行可视化组装编排，降低对人工参与的过度依赖。有别于单独的 SOAR 产品，聚铭安全管家平台通过能力接入将剧本编排能力与平台进行轻量化集成，编排能力与平台进行深度耦合，通过编排与运营两大体系协同作战增强安全运营合力。

平台支持移动端协同能力，通过平台可将数据通过企业微信、邮件等方式推送至移动端，让安全运维人员不受时间、地点影响参与及响应安全事件处置，确保每一个漏洞能得到及时修复、每一个黑 IP 能得到快速封禁、每一个安全告警能得到有效处理。

3.3.4. 异构设备万能联动



示例：万能联动阻断场景

异构设备联动通常指的是不同品牌、不同协议或架构的设备之间进行协作处置，但由于企业现场大量异构品牌设备各自孤立，对接生产厂家提供往往提供标准接口（如：API）存在障碍，给企业现场异构设备的集中联动响应带来挑战。

聚铭安全管家平台独有的异构设备异构联动能力，无需代理工具，仅需提供联动设备访问地址、用户名、密码即可，基于万能联动的方式进行异构融合联动及智能识别验证码能力，联动设备不限与防火墙、IPS、WAF、交换机等异构品类，实现异构设备联动快速处置能力，进一步降低安全运营人员的工作负担。

异构设备万能联动可实现一次配置长期稳定使用，同时能融入平台自动化编排响应功能，实现自动化响应处置能力，灵活适配多种场景处置方式，提升安全运营人员工作效率。

3.3.5.异构设备集中管控

通过异构设备集中管控功能，企业可从设备分类和业务信息系统视角出发，通过页面对服务器系统、网络、安全产品、操作系统、应用系统、储存设备等异构设备的状态、性能等实时监控巡检。提供统一用户界面，进行集中管理，可自定义自动巡检时间频率，准确反映各类设备运行状态。例如网络管理平台设备状态巡检。

对于关注设备可配置状态告警，并通过企业微信、邮件等方式发送用户移动端，随时随地接收告警信息，减少各类 IT 设备故障影响范围。例如对于虚拟化系统设备资源（cpu、内存）异常表现进行，通过企业微信发送告警至用户移动端。

对于告警可配置自动化处置策略，通过用户行为模拟的方式进行处置，快速响应处置，避免未及时发现告警而产生业务影响。例如日志接收异常时，自动重启接收组件。

3.3.6. 配置保障监测处置

通过智能化的变更管理技术，对已完成安全加固的设备进行自动化持续监测。系统可定期自动扫描设备的配置文件、开放端口、运行进程及启动项等关键安全要素，通过指纹校验和基线比对技术，实时识别任何异常变更。一旦发现配置篡改、后门植入等安全风险，系统将在 1 分钟内自动触发告警并推送给运维团队，大幅提升威胁发现效率。该方案有效解决了传统人工巡检效率低下的问题，可减少 70%以上的日常监测工作量，同时确保安全事件得到及时处置。系统支持自定义监控策略，并具备完整的变更溯源能力，能够详细记录每次变更的内容和时间，为安全分析提供可靠依据，真正实现"自动化监测、智能化预警"的安全运营目标。

3.3.7. AI 智能研判

由于网络安全威胁日益复杂多变，分析人员需要具备丰富的攻防经验，通过人工方式对数据包进行深度解析，在海量告警日志中逐条检索排查，耗费大量时间却往往事倍功半。这种高度依赖人工经验的工作模式不仅效率低下，还容易因疲劳或经验不足导致关键威胁被遗漏，给企业安全带来潜在风险。

智能告警研判系统通过安全大模型技术实现了革命性突破。系统能够自动解析告警数据包内容，结合业务环境上下文，运用先进的语义理解技术精准识别告警性质，智能区分误报、真实威胁或需专家介入的可疑事件。对于确认的威胁，系统可即时生成包含阻断攻击源 IP、隔离感染终端、调整用户权限等在内的个性化处置方案，将传统需要数小时甚至更长时间的人工分析处置流程压缩至分钟级完成，使安全运营效率获得质的飞跃。同时，系统还能持续学习安全专家的处置经验，不断提升研判准确率，实现安全运营能力的持续进化。

3.3.8. AI 安全数智化机器人

借助 AI 安全数智化机器人，赋能安全运维团队，提供精准智能化决策支撑。运维人员仅需通过对话交互，便能高效达成事件辅助研判、逻辑推理、汲取运维

经验、妥善处置事件等操作，大幅提升运维工作的质量与效率。例如，当安全事件发生时，运维人员可直接询问"今天有哪些高危事件？"，机器人将实时汇总并分析告警数据，快速定位关键威胁；或直接发出指令"请联动防火墙封禁攻击者IP"，系统即可自动执行拦截操作，实现从分析到处置的闭环管理。

该机器人深度融合安全知识库与 AI 推理能力，既能快速响应具体操作需求，也能为复杂场景提供决策建议。无论是日常巡检中的漏洞排查，还是应急响应时的处置方案生成，运维人员均可通过对话式交互获取实时支持，大幅降低人工研判成本，推动安全运维向智能化、自动化升级。

4. 产品价值

4.1. 合规建设：智慧运营，数据不出网

- 通过在客户侧部署轻量化的三级平台模式，将核心安全分析能力下沉至客户本地环境，确保所有运营数据（包括日志、流量、事件等）完全在客户侧留存和处理。通过二级平台加密隧道或零信任安全架构与本地三级平台建立通信，实现远程安全运营能力。该架构严格遵循"数据不出网"原则，既满足《数据安全法》等合规要求，又保障了客户对自身数据的完全掌控权，同时不影响安全服务的专业性和时效性。运营人员可通过安全的远程工作模式，在数据不出网的情况下完成威胁分析、事件处置等全流程工作，真正实现"数据本地化、运营云端化"的新型安全服务模式。

4.2. 优质拓客：构建从签约到交付的标准化服务体系

- 通过二级平台建设，提供客户全生命周期管理能力，实现从服务签约到项目交付、执行的流程化管理。支持多层级客户组织结构管理，可灵活配置项目团队体系，SLA 服务体系等功能，确保服务交付、运营过程规范可控。
- 客户运营全景视图，基于多维度数据分析，实时展示客户许可状态（含到期预警及自动续期提醒）、SLA 套餐分布、团队服务效能等关键指标，并深度集成客户运营健康度评估（风险评分、问题闭环率、等保合规、三级平台运行状态等），帮助运营商精准掌握客户运营态势，优化安全投入产出比，提升服务透明度与客户续购意愿。
- 客户侧部署的三级平台，并非只是采集工具，而是根据“三化六防”体系建设的一套安全管家平台，通过提供的安全概览、合规概览、通报防护、SLA 概览等模块，实现对整体安全状况、合规水平及安全运营态势的全面感知。通过运营过程透明化，平台使用户能够直观掌握安全动态，从而增强用户体验，提升用户黏性。

4.3. 高效运营：体系化运营，安全运营更高效

- 三级平台预置安全运营自动化协同流程，覆盖安全问题发现、监控、告警、处置、知识库沉淀全流程，便于安全运维团队成员进行威胁分析和处置。
- 通过智能化的变更管理技术，对已完成安全加固的设备进行自动化持续监测。系统可定期自动扫描设备的配置文件、开放端口、运行进程及启动项等关键安全要素，通过指纹校验和基线比对技术，实时识别任何异常变更。一旦发现配置篡改、后门植入等安全风险，系统将在 1 分钟内自动触发告警并推送给运维团队，大幅提升威胁发现效率。该方案有效解决了传统人工巡检效率低下的问题，可减少 70%以上的日常监测工作量，同时确保安全事件得到及时处置。
- 轻量化联动第三方设备，无需对接 API 等接口，万能联动多种品牌类型设备，不限于网络设备、边界设备、终端设备等。在发现安全事件，可快速处置响应，提升安全运营处置效率。

4.4.智慧运营：AI 智能运营，安全运营更简单

- 依托先进的 AI 大模型技术，三级平台深度赋能安全运营全流程，大幅降低了对专业人才的依赖门槛，让安全运营真正实现了从"经验驱动"到"智能驱动"的转型升级。