聚铭下一代智慧安全运营中心

产品白皮书

聚铭网络科技有限公司

2024 年 04 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

北京总部：北京市海淀区丹棱街 18 号创富大厦 9 层

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

随着新技术应用和新基建发展，网络安全威胁层出不穷，网络安全运营者面临全新挑战。同时由于组织现有安全建设缺乏有效及长远的安全运营规划，导致安全建设效果不理想、安全运维效率低、安全工作价值难体现等问题，也困扰着安全运营者。随着内控与合规的深入，相关政策和标准在安全运营和管理方面都提出了明确的要求。因此，应建设有效的安全运营技术、流程和人员组织体系，以应对各类安全挑战、解决安全运营问题、确保网络及业务系统持续稳定安全运行。

面对新的安全形势，以满足合规为前提的安全建设架构已经无法应对当前安全形势。从场景化角度出发，客户安全运营体系架构中主要面临以下问题：

- 安全分析能力受限：企业购置了不同类型的安全设备，但设备间安全保障工作相对独立，各自为政，需依赖人工进行分析，缺乏体系化管理系统，导致安全事件无法进行综合研判、数据关联分析
- 安全数据噪音过大：在安全运营工作中，安全日志数据收集的越多越广，分析呈现的结果更准确更实时。然而，当采集海量日志数据后，大量无效无关的数据噪音也将产生大量误报，湮没真实威胁信息。
- 安全事件处置效率低：复杂且庞杂的网络环境内各数据间紧密相连，犹如蝴蝶效应般，一个指标的变化可能引发一系列的告警连锁反应。面对不同监控平台的红色标识、不断涌入的告警邮件和短信，安全运维人员往往需要登陆其他系统进行处置，难以快速应对。
- 常态化运维响应慢：企业购买了诸多安全产品，不同安全产品存在壁垒，日常巡检及业务告警往往需人工登陆各个平台主打查看发现，人员投入精力较大，且存在信息获取不及时现象，导致日常安全运维响应速度慢。

1.2. 用户需求

针对上述问题和挑战，亟需建立一套横向贯穿孤立设备，打破数据孤岛的整体安全安全运营中心。通过采集防病毒系统、防火墙、入侵检测系统、漏洞扫描系统、主机、交换机、路由器、数据库、中间件等设备的日志事件、状态事件、网络数据包和状态运行数据，与网络安全事件进行关联分析，实现对来自外部攻击、内部横向扩散以及非法外连的安全审计，为运维人员提供一个监控网络环境下所有软硬件设备运行状况、异常入侵信息、审计业务系统关键数据、告警各类网络安全事件的综合性平台。这其中包括：

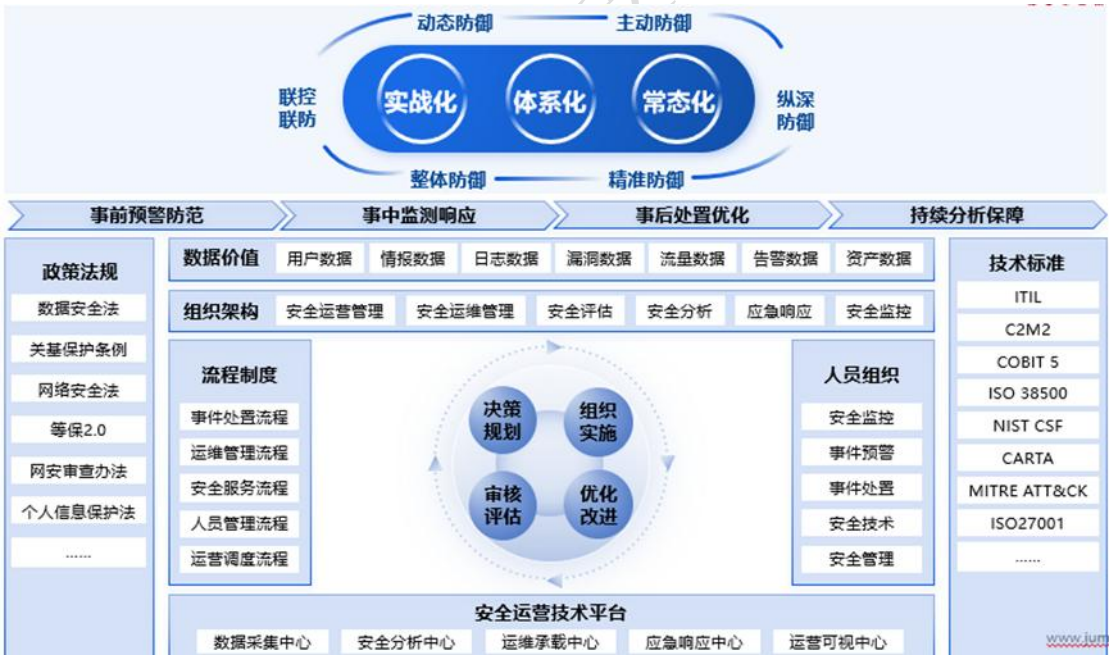
- 整合企业目前部署的各种相对孤立的安全防护资源（主要包括：防火墙、入侵检测系统、漏洞扫描系统、UTM 等），满足海量多源异构日志数据和流量数据的处理需求；以关联分析（知所已知）和行为分析（知所未知）为基础，为运维人员提供智能化分析方法，以应对日益复杂的隐蔽攻击和威胁，从数据中发现价值
- 从海量的安全事件和告警中过滤掉无关紧要、重复、误报或低优先级的信息，具有智能化降噪能力，确保安全运维团队能够高效聚焦于真正需要关注和响应的威胁。例如：同一攻击误报或相似攻击误报产生连续性告警进行智能降噪，减少告警数量。
- 能够通过 API 或无 API 多种方式联动各类异构设备，并且具备自动化响应和工作流编排能力。一旦发生网络安全事件，SOAR 可根据预定义的剧本（playbook）自动触发跨设备的处置动作，如隔离受感染主机、调整防火墙策略、下发终端杀毒指令等。
- 随着企业业务的快速发展，IT 设备数量不断增加，设备类型也日益多样化，需具备集中管理跨品类 IT 设备能力，可以满足设备日常巡检，并且能力针对与关注业务数据（如设备资源状态）随时随地接收告警信息。

2. 解决方案

以大数据分析、异构设备联动、智能编排等技术为基础，结合威胁情报、ATT&CK、攻击链、流量取证等研判技术，协助用户对网络安全工作的常态化运维工作开展，并加强日志收集、流量分析、基线合规、等保合规的管理工作；实现安全风险的集中收集及监控、威胁的集中分析及处置、应急响应集中指挥、常态运营的持续支撑、态势及效能的统一展示。

2.1. 解决方案整体框架

依照等级保护、网络安全法、数据安全法等政策法规，ITIL、ISO27001 等技术标准，整合各行业制度规范、技术平台、管理流程、人员组织，实现信息中心、网络出口的安全风险的集中监控、安全事件的集中处置、安全策略的合规检查、安全态势的统一展示，将信息安全管理和技术有机结合，健全信息安全保障体系。



2.2. 方案组成

■ 数据中心安全集中建设

通过下一代智慧安全运营中心建设，对整体网络的安全状态实时监控分析，同时通过大屏展示可视化的呈现网内资产失陷、网络攻击威胁、脆弱性等模块。

提供一个全面的可视化安全运维平台，方便及时了解整体的网络状况以及安全风险等级。

■ 安全联防联控

以资产为核心，对现有安全基础设备产生的告警，提供充足的研判数据，通过自动编排处置，及时做出处置措施，避免人工参与造成的威胁处置滞后问题。能够自动通知资产所属管理员，让不在信息中心管辖内的资产，能及时通知到二级单位；能够联动边界设备、数通设备，对威胁进行封堵。

■ 三化六防安全运营建设

通过对组织、制度、流程的不断建设，建立符合自己的常态化运维流程、应急响应机制、应急演练机制等，当出现网络安全事件后第一时间响应，保证业务不中断。建设“一个安全管理中心”管理下的“三重防护体系”，逐步建立“实战化、体系化、常态化”的安全防护体系，形成“动态防御、主动防御、纵深防御、精准防御、整体防控、联防联控”的安全防护能力。

2.3. 解决的安全问题

以下就聚铭下一代智慧安全运营中心能够探知和发现的安全问题进行阐述。

■ 异常外连

聚铭下一代智慧安全运营中心收集网络流量进行安全分析，通过聚铭混合精准情报引擎发现异常外连行为；

■ 僵木蠕检测

聚铭下一代智慧安全运营中心提供百万级的各类僵木蠕信息，检测手段多样、内容丰富；

■ 恶意软件检测

聚铭下一代智慧安全运营中心结合特征检测、行为统计以及机器学习等多种方法对恶意软件行为进行分析及检测；

■ 勒索病毒预防

聚铭下一代智慧安全运营中心基于 ATT&CK 知识图谱分析勒索攻击各阶段使用战术方法，及时发现异常情况进行告警通知及查杀处理；

■ 挖矿防通报

通过与情报引擎进行碰撞，精准识别挖矿木马，动态阻断策略仅阻断与挖矿相关请求；还可与实名认证系统联动直接实名溯源及阻断；

■ 网站安全监控

产品从网站攻击情况、网站挂马、访问性能、暗链、篡改、状态码分布等方面对网站进行整体监控；

■ 数据库威胁

产品支持对数据库威胁进行检测，从风险访问、密码爆破、敏感 sql 执行以及会话审计进行全息系统的安全监控和分析；

■ 弱口令检测

产品在 http、ftp、IMAP、pop3、smtp 等协议上支持弱口令检测，从设备、账号、口令维度来进行分析展现，并可支持定义弱口令规则进行检测；

■ 内部违规行为监测

产品内置丰富的场景化关联分析策略，如：堡垒机绕行、违规访问、异常访问等等，对内部运维人员违规操作进行全方位监控；

■ 其他安全问题

通过聚铭下一代智慧安全运营中心可以充分发现南北向以及各类东西向安全问题，包括诸如 SQL 注入、钓鱼邮件、DGA 域名、密码爆破、C&C 节点、隐蔽通道等攻击手段，充分保障内部服务器及用户终端的安全，避免造成各类损失。

3. 主要功能

3.1. 常态化安全运营

3.1.1. 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，形成安全运营中心的工作机制，实现安全运营的自动化。

3.1.2. 资产全生命周期管控

平台采用主被动结合方式，探测网络内存活的设备及系统组件，采集资产通用属性及安全属性信息 ，识别影子资产、无效资产等问题资产。可实现对资产威胁问题处置的闭环流程，集问题发现、通知、整改、验证、归档五位于一体。

结合漏洞与基线对资产进行全方位分析，管理资产的合规情况。

3.1.3. 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。

3.1.4. 数据包归类自动研判

平台可以快速接入各类告警信息，通过人工智能算法结合内置检测规则、专家经验对海量告警风暴自动去重降噪，减少冗余告警，聚焦处理核心安全事件。此外，通过自动化识别技术，对分类标记的噪音数据进行过滤，实现安全事件分类自动研判，加速威胁分类判定及处置效率，降低日常运维过程中安全运营人员处置海量告警数据的工作量。

除了本地平台助力安全威胁事件高速研判，平台还支持“云地协同，专家赋能”模式，本地运营人员可以将告警事件相关数据上送云端，云端安全专家在对攻击事件进行二次研判后下发检测规则至本地平台，本地安全运营中心在深度融合人工智能算法及专家级定制规则后对类似告警信息进行自动研判。

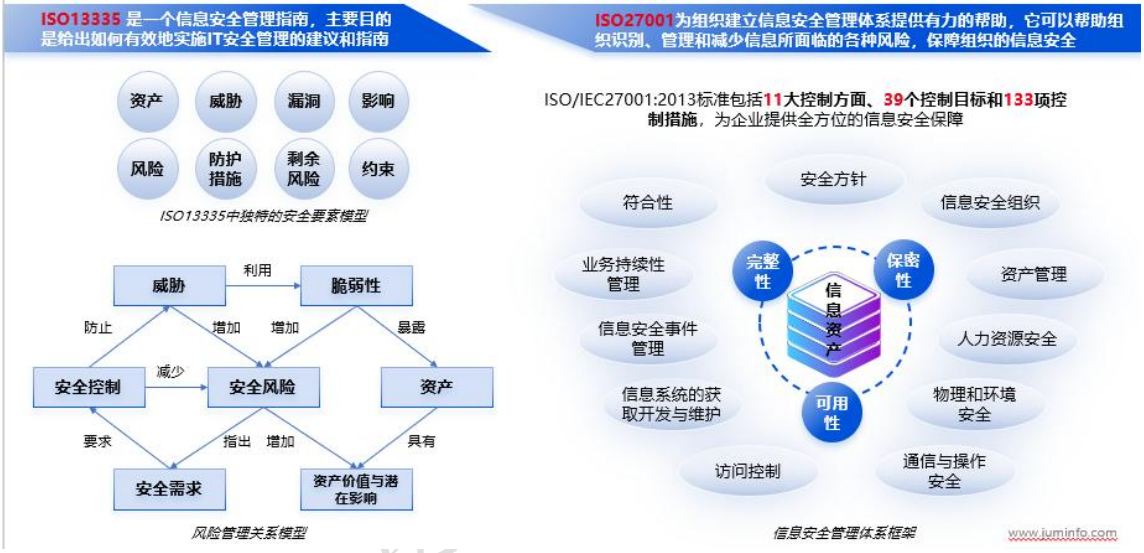
通过以上流程及能力，平台助力用户形成标准的告警事件研判处理流程，提升团队安全事件管理能力，让业务运行更可靠。

3.1.5. 失陷综合研判

产品采用领先的大数据架构设计，数据湖内海量数据经过数据清洗、确认业务场景后，对于异常的访问数据进行降噪处理，围绕研判工作的具体攻击场景对

异常访问 IP 进行提取核实，形成待分析失陷。通过对告警 IP 进行研判信息的补充（行为分析、现有结论等），基于关联分析引擎实时关联多维度数据（包括多数据来源的告警、威胁情报数据、资产管理数据等），结合系统规则、专家经验对主机失陷阶段进行研判，提供高价值研判处置建议，为客户及时掌握情况和决策提供帮助和支持。

3.1.6. 安全风险全流程管控



安全风险管控包含风险管理识别、评估和减轻全流程，旨在降低网络攻击的可能性和影响。这一动态、持续的过程，跟随威胁的发展而相应调整。

网络安全风险评估：遵循 ISO/IE27001：2013 信息安全管理标准，通过识别和评估电子信息和系统的保密性、完整性和可用性的风险，全面评估企业的网络安全风险。

- 识别资产：采集及识别网络环境中的各类资产，包含了对业务运营至关重要的所有设备、数据和应用程序；
- 评估漏洞：评估资产的风险漏洞，包括识别网络攻击者可能利用的各类脆弱性，例如漏洞、违规基线、弱口令等。

网络安全风险管理：在汇总网络环境内所有风险漏洞后，在 GB/T 20984-2022

标准的指导下，综合评估资产受攻击情况的严重程度、频次以及脆弱性情况，给每一受影响资产进行风险赋值，为资产风险处理优先级提供决策依据。

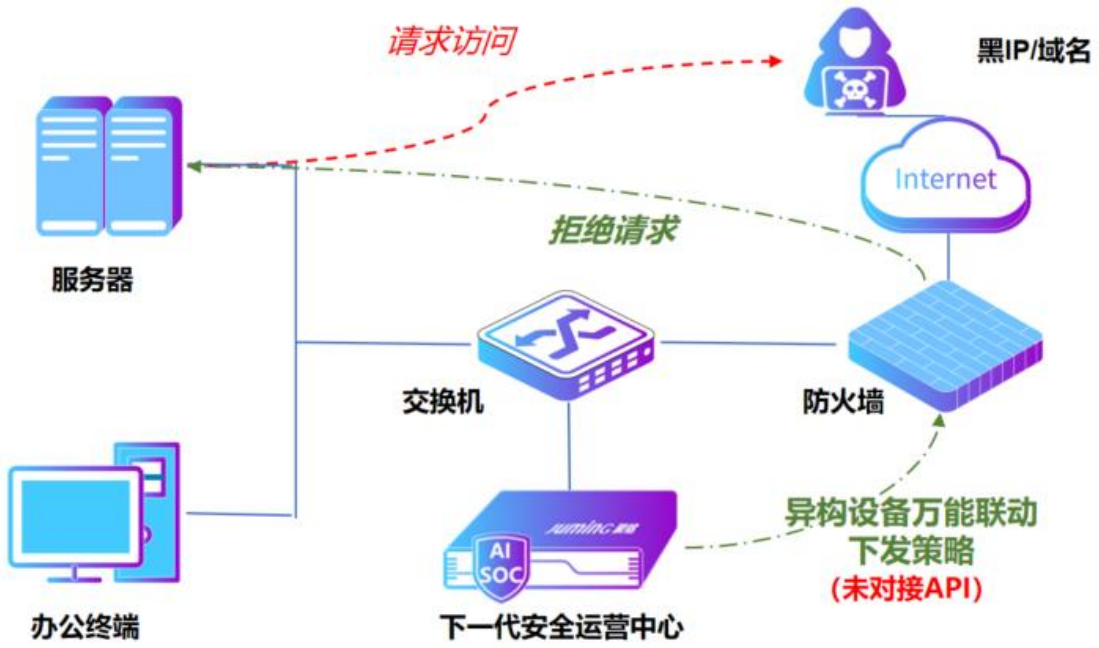
3.1.7. 自动化编排响应处置

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，运营中心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，聚铭安全运营中心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。

3.1.8. 异构设备万能联动



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。

聚铭安全运营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。

3.1.9. 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。

3.1.10. 恶意程序终端猎捕

恶意程序发展迅速且隐蔽性较强，目前市场上大多数病毒防护系统对恶意程序无法准确检测或无法彻底清除，聚铭自研绿色抓捕工具检测速度快，判断准确、使用方便，具备多项核心技术：通过智能行为分析与特征码匹配技术监控系统运行状况，结合病毒行为库检测已知、变种和未知程序；通过独有恶意程序分析技术，以主动和被动方式搜集最新恶意程序特征；通过高效检测引擎技术，根据检测目标主机性能自动调节检测能力，不会对系统造成性能影响。

通过深度分析失陷主机的异常流量行为，无需安装 agent，使用绿色版抓捕工具，即可在失陷主机上对挖矿、木马软件、病毒程序进行精准抓捕，让恶意软件无处遁形。

3.1.11. 安全综合实时监控

从多维数据视角出发，系统的安全态势以高科技动感全息屏方式展示整体安全状况，便于安全团队快速掌控全局安全情况。

安全运营监控中心内汇集平台安全数据分析结果，通过可视化图表展示，包括直方图、折线图、面积图、饼图、表格等多种类型。此外支持对安全事件类型、级别、阶段及状态进行图表展示，支持深度下钻分析，通过界面事件内容直接下钻到详细事件内容，通过事件内容下钻到关联资产和原始事件内容。

安全运营监控中心包含多块全息大屏：

- 安全综合实时监控全息屏：呈现失陷、风险暴露面、脆弱性、安全事件的实时动态；
- 网络攻击实时监控感知屏：呈现网络攻击的实时动态，包括攻击来源 IP、攻击趋势、攻击技术、黑客画像、残余攻击等；
- 违规外连实时监控感知屏：呈现违规外连的实时动态，包括外连趋势、木马家族、僵尸网络、活跃内网主机、回连矿池、攻击技术等；

- 横向威胁实时监控感知屏：呈现横向威胁的实时动态，包括发起攻击主机排行、近 7 天攻击趋势、攻击技术、受害主机排行、恶意程序分布、遭受攻击服务排行等；
- 脆弱性监控感知屏：呈现横向威胁的实时动态，包括发起攻击主机排行、近 7 天攻击趋势、攻击技术、受害主机排行、恶意程序分布、遭受攻击服务排行等。

3.1.12. 汇报式报告

报告集中提供了系统检测到的安全问题，它可以被导出成 HTML 格式，还可以设置相关任务将报表发送到相关用户的邮箱。报表类型包括日报、周报和月报任务，定期生成前一自然天、前一自然周、前一自然月的威胁报告。若要汇报或查看特定时间段内的全网安全态势情况，可自定义时间段生成综合安全分析报告。支持自定义更换报告 logo，对于报告章节可以个性化自由裁剪，因地制宜，便于给不同对象进行汇报。

系统内置多种类型报告，根据不同汇报对象、应用场景、关注内容可直接下载对应报告。

安全综合实时监控报告：适用于安全运维团队监控全网安全态势情况、综合汇报的应用场景，报告内容包括主机失陷整体情况、安全事件整体情况、脆弱性整体情况、运维处置情况。

失陷分析报告：适用于安全运维团队针对失陷主机进行处置的应用场景，报告展示所有失陷主机的风险情况，包括失陷可信度、失陷原因、安全事件举例、风险暴露分析以及终端取证记录，并提供解决方案指导运维人员完成失陷处置。

安全事件分析报告：适用于安全运维团队从外部威胁、外连威胁、内部威胁三个视角，全方位分析安全事件的应用场景，报告在汇总统计的基础上，对各类安全事件进行充分举证。

脆弱性分析报告：适用于安全运维团队对内部资产进行脆弱性分析的场景，从主机漏洞、违规配置、弱口令三个方面全面分析内网的脆弱性情况，辅助运维团队评估脆弱性加固的范围，确定加固范围后，可从系统内导出加固指导建议。

安全运维报告：适用于运维人员针对失陷主机进行处置的应用场景，报告内提供解决方案，指导运维人员完成失陷处置。

3.1.13. 云端专家诊断服务

安全研究院团队密切跟踪全球知名安全组织和软件厂商发布的安全公告，同时和业界专业安全研究厂商合作，对这些威胁进行分析和验证，生成保护各种软件系统（操作系统、应用程序、数据库）漏洞的特征库；

恶意域名签名库通过部署的沙箱环境和自动化的样本培植环境，自动获取C&C 通信恶意域名，生成恶意域名特征库。

3.2. 核心检测能力

3.2.1. 影子资产自动测绘

平台采用主被动结合方式，探测网络内存活的设备及系统组件，采集资产通用属性及安全属性信息，识别影子资产、无效资产等问题资产。可实现对资产问题处置的闭环流程，集问题发现、通知、整改、验证、归档五位于一体。结合漏洞与基线对资产进行全方位分析，管理资产的合规情况。

3.2.2. 风险暴露面梳理

采用主被动结合的风险测绘和自动化学习技术，可以对互联网边界和内网安全域间暴露面进行全面分析。

通过主动和被动方式进行资产信息发现，识别资产基础信息、开放端口和服务运行情况；梳理违规搭建、非法在运、过期未退运、临时发布的系统，以及访问控制不当而泄露的内网管理系统与开发测试环境系统，发现暴露面，可以缩小攻击面；

通过资产、用户流量、动作等行为偏离情况，建立各种场景化模型，构建用户行为基线并进行状态跟踪，能够有效发现非正常时间内的系统访问、违规搭建的内网远程控制通道等行为，并基于场景模型和安全情报发现可疑访问和风险外连行为，可以准确、快速地定位安全事件；

平台在实时更新多种漏洞扫描插件基础上，全面监控暴露在互联网的资产信息，针对用户网络边界暴露面的违规行为进行检测，如私接互联网、私接路由、违规外连、一机两用等，主动检测专网边界状态，预防出现跨网信息交互事件，从而及时发现暴露在外的安全风险。

3.2.3. 脆弱性持续检测

对于资产漏洞，基于已知的漏洞信息采用端口探测等手段对网络中指定主机、网络设备等资产进行漏洞检测，发现网络资产存在的漏洞；采用基线安全配置检测工具，深度获取主机、服务器和网络设备等资产的配置信息，并与配置基线进行比较，发现资产配置的脆弱性。

产品提供定期巡检服务，为企业网络环境提供定期全面体检，通过云端安全运维支撑服务，系统实时更新漏洞插件库及漏洞检测规则，缩短脆弱性风险发现周期，有效应对突发安全事件。

3.2.4. 恶意加密流量检测

基于机器学习方法对恶意加密流量进行检测。主要抽取相关通讯样本的统计和内容两大特征，结合实际情况以及兼顾检测速度需要，对相关恶意软件产生的流量进行训练和检验。经过经验，不仅能够识别隐蔽通道及恶意软件加密流量，此外未授权连接、域名快闪、DGA 域名、异常流量等无法通过规则发现的安全隐患也能精准定位。

异常流量检测中集成了聚铭网络自主研发的智能动态基线、模式信息熵等生成算法，通过一段时间对学习对象的流量特征分析、建模，智能生成该对象多维度的网络特征，实施多维度的纵深检测机制，增加检测的准确性，降低误报概率。

3.2.5. 隐蔽隧道通信检测

由于攻击者将非法数据进行封装，攻击特征不明显，导致隐蔽隧道攻击检测的误报率较高。针对隐蔽隧道攻击，通过收集大量不同协议的隐蔽隧道流量样本进行分析测算，构建出多种隐蔽隧道攻击检测模型。如针对 DNS 隐蔽隧道通过匹配报文中所呈现出的域名信息、域名后缀信息、应答信息等进行综合评估分析；针对 ICMP 隐蔽隧道攻击，通过匹配数据包发送频率、应答信息、payload 大小及内容等进行综合分析，有效提升了隐蔽隧道攻击检测效率。

此外平台支持对各类隧道检测，对协议改写、安全洋葱等存在隐蔽通道的行为进行检测。

3.2.6. 挖矿检测

通过分析异常流量特征，落地形成检测标识，不断提取攻击特征，快速识别终端登录矿池请求、终端与矿池秘钥交互等行为；并且在自动学习历史挖矿流量特征基础上，建立异常流量检测模型，更好的挖掘潜在挖矿信息。在处置程序上，对于挖矿行为、僵尸网络以及 DGA 域名采取动态阻断策略，仅阻断与异常行为相关的请求，在不影响正常业务的前提下，对异常应用流量在客户内网实现阻断。

3.2.7. 社工攻击检测

传统防御体系无法应对高级威胁，比如 0day、社工攻击等。通过机器学习、行为分析、人工智能等技术精准检测绕过防御的攻击行为、内部横向渗透行为与异常外连行为，提前发现潜在安全风险；通过内置场景化异常检测模型，学习正常与异常流量行为基线，识别非法账号登录、数据泄露、违规访问等异常场景，快速定位异常行为。

3.2.8. 僵木蠕恶意软件检测

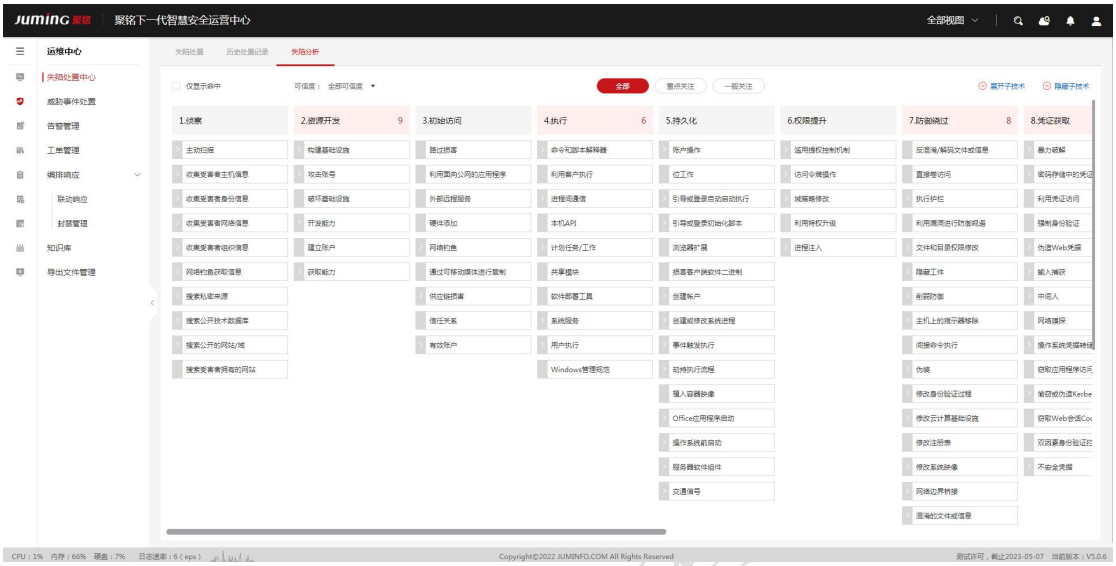
支持僵尸网络、C&C 节点、木马回连、蠕虫、垃圾邮件、钓鱼节点、扫描节点、恶意软件等威胁 IP、URL、文件 HASH 的实时检测。

3.3. 威胁分析能力

3.3.1. ATT&CK 知识图谱分析

在告警事件中安全分析人员可获取相关联的 ATT&CK 攻击技术说明，包括攻击技术的解释说明，攻击技术的数据源等信息辅助分析。ATT&CK 是基于真实观测到的威胁攻击总结出来的全球攻击战术和技术知识库，包括 12 类攻击战术和两百多种攻击技术。产品提供了 ATT&CK 攻击热力图，以图谱展现企业当前遭受

到的威胁攻击，包括攻击利用到的战术和攻击技术，便于安全人员全面详细了解攻击过程及阶段。ATT&CK 攻击热力图支持根据安全设备进行过滤，方便安全团队了解安全资产设备遭受到的攻击。



3.3.2. 场景化关联分析

场景化关联分析，内置多种场景关联分析规则，覆盖违规行为、恶意程序、网络攻击、数据泄露、拒绝服务、运维监控、漏洞利用、网站安全、主机安全、暴力破解、探测扫描等多类场景。支持事件与基线关联分析、事件与漏洞关联分析、事件与事件关联分析。

3.3.3. DNS 穿透分析

利用独有的 DNS 代理穿透技术，从 DNS 解码错误、解析失败、解析超时、威胁情报、DGA 域名、隐蔽通道等维度对 DNS 协议进行全面系统的监测与展现，通过在全流量还原基础上对异常流量特征化，利用 AI 加密流量分析引擎等技术，锁定主机横向渗透与失陷破坏行为，精准定位真实失陷主机，完整还原攻击链条，彻底解决 DNS 代理误报导致的用户溯源定位难问题。

3.3.4. 恶意文件行为分析

实现从 HTTP、邮件、SMB、FTP、QQ 等协议中还原文件，并对文件进行黑名单检测、敏感词检测，不仅能够发现恶意软件，还能够检测客户的核心数据外泄。

除此之外还支持未知威胁文件的识别：基于启发式静态文件扫描技术的恶意文件识别；基于虚拟仿真环境动态文件扫描技术的文件威胁行为检测；基于 AI 的主流恶意家族的恶意软件检测。

4. 系统建设

4.1. 系统平台建设原则

4.1.1. 建设原则

符合性原则：符合国务院下发的《2006—2020 年国家信息化发展战略》中关于加强信息安全保障体系建设的原则；符合国家 27 号文件指出的积极防御、综合防范的方针和等级保护的原则；符合国家《信息安全技术信息系统安全等级保护》标准；符合国家《信息安全事件分类分级指南》标准；遵循 SOX 404 条款要求增强 IT 内部控制的原则；

标准性原则：技术方案的设计与实施应依据国内或国际的相关标准进行；

规范性原则：服务提供商的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制；

可控性原则：项目进度要与时间计划表的安排一致，保证甲方对于项目管理的可控性；

开放性：系统遵循各种 IP 网络国际标准和安全标准，有助于与其他系统的联运与协作；

可扩展性：系统设计时具备良好的扩展性，采用模块化设计，不同模块可以集中和分布部署，中心处理服务器根据规模可以部署多台等不同方式；

互操作性：系统提供与现有系统的接口，包括网管系统、安全系统、流量监控系统，推进和实现“集中管理、集中监控、集中派单、集中配置、集中支援”；

安全性：系统涉及整个 IP 网络的敏感信息，设计时充分考虑了管理数据的保密性、可用性、完整性的要求，对项目过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害甲方网络的行为，否则甲方有权追究乙方的责任；

经济性：在设计方案时，要充分了解甲方现有网络结构及设备状况，再充分考虑利用现有网络和硬件设施的情况之下，考虑购置新设备；

重点部署、分布实施：安全系统工程是融合设备、技术、管理于一体的系统工程，需要全面考虑；同时，尽量考虑到涉及网络安全的重点因素，充分考虑可扩展性和可持续性，从解决眼前问题、夯实基础、建设整个体系等方面作好安全工作；

尽量减少对现有网络应用的影响：部署时要尽量减少对现有网络结构和应用系统的影响。同时也要充分考虑安全产品和现有网络结构、网络产品、网络应用的兼容性，保护网络建设的投资。

4.1.2. 建设目标

通过安全建设项目，建立集中、统一的安全管理平台，实现对全网事件、配置、漏洞、状态的采集、分析和管理，实现安全问题的流程化处理，支持日常安全运维工作的开展。

4.1.3. 预期效果

1. 用户能从系统中查看各类网络流量；
2. 用户能从系统中查看采集到的设备原始事件；
3. 用户能从系统中查看采集到的设备原始配置；
4. 用户能从系统中查看采集到的设备漏洞信息；
5. 用户能从系统中查看采集到的设备状态信息；

6. 通过对原始事件、漏洞的分析，用户能看到需要处理的安全问题；
7. 通过对设备漏洞的管理，用户能看到漏洞修复情况、改善的程度；
8. 通过对设备配置的分析，检查配置是否符合企业策略要求，对违规问题的处理情况、配置改善的程度；
9. 通过对安全问题的流程化处理，落实安全责任；
10. 通过辅以知识，将复杂的安全问题简单化，协助用户处理安全问题；
11. 通过对日常安全维护工作的信息化，实现半自动化、自动化的安全维护，提高安全运维的效率。

4.2. 业务支撑

系统建设完毕之后，能够通过平台功能的组合，有效的支撑用户的诸多安全业务，如下：

4.2.1. 集中监控

支撑组件：安全关联分析、安全事件管理、安全漏洞管理、安全基线管理、接口、系统管理、资产管理、告警管理、风险管理、设备监控

支撑业务：告警监控、风险监控

支撑及实现方式：

1. 通过“安全事件管理、安全漏洞管理、安全基线管理、接口”，能够实时采集各类安全风险，包括安全事件日志、安全漏洞、安全配置。对事件日志采用实时被动方式接收，对设备状态采用实时主动方式采集，对安全漏洞、配置采用主动任务的方式采集；
2. 通过“告警管理”，能够综合分析安全风险，监控风险的发生情况，并予以分级告警；
3. “告警管理”提供多种告警响应方式，如电子邮件、声光效果、短信（需接口）、工单等；
4. “告警管理”结合“资产管理”能够将告警准确定位资产，并予以统计，提供实时的趋势分析；

5. 通过“设备监控”将异构品类设备状态数据采集展示，各类设备日常集中巡检；
6. 接口支持对外数据接入，如网管系统、其他日志系统等（需定制）；
7. 支持定制及功能开发，支撑集中监控的其他需求，如特殊告警、定制的通知方式等。

4.2.2. 安全运维

支撑组件：安全关联分析、安全事件管理、安全漏洞管理、安全基线管理、接口、资产管理、第三方设备告警及智能处置、工单管理、报表管理

支撑业务：事件流程、安全报表

支撑及实现方式：

1. 通过“安全漏洞管理、安全基线管理”能够制定各类采集任务，如漏洞、配置，满足日常运维的工作检查要求；
2. 通过“第三方设备告警及智能处置”提取异构品类数据异常数据，并通过模拟人工操作进行自动化处置；
3. 通过“工单管理”能够将告警自动派发工单，形成流程化的事件处理机制。工单系统可与其他运维系统同步，共享和流转；
4. 通过“报表管理”能够通过定制，形成多种形式、周期性的安全报表，包含告警报表、资产报表、安全事件报表、漏洞报表、安全基线报表、工单报表，满足日常运维的报告要求；
5. 接口支持对外数据共享和通讯，如运维系统等（需定制）；
6. 支持定制及功能开发，支撑安全运维的其他需求，诸如日常运维流程、安全预警、重大事件的处理机制等。

4.2.3. 合规检查

支撑组件：安全漏洞管理、安全基线管理、接口、报表管理

支撑业务：基线合规（任务部分）、内控合规（任务部分）、合规管理（任务和策略）

支撑及实现方式：

1. 通过“安全漏洞管理、安全基线管理”，能够配置安全策略，形成合规检查基线；
2. 通过“安全漏洞管理、安全基线管理”，能够制定各类检查任务，如漏洞、配置，满足日常合规检查的技术手段；
3. 通过“安全漏洞管理、安全基线管理、报表管理”，能够提供安全检查报表，查看合规检查情况；
4. 接口支持对外合规系统的同步，如等保系统等（需定制）；
5. 支持定制及功能开发，支撑安全合规的其他需求，诸如等保合规的处理流程、合规检查流程的定制等。

4.2.4. 策略管理

支撑组件：安全关联分析、安全事件管理、安全漏洞管理、安全基线管理、知识库管理

支撑业务：安全知识管理、专业安全策略

支撑及实现方式：

1. 通过“安全事件管理、安全漏洞管理、安全基线管理 ”，能够实现对专业安全策略的管理控制。专业安全策略包括事件采集策略、事件分析策略、安全基线策略等；
2. 通过“知识库管理”， 能够记录各种安全知识和经验，提供风险发现和处理的支撑服务，包含日之类、安全事件类、漏洞类、安全基线类、安全经验类。可以对内置安全知识类进行展示，又可以扩充安全知识类，以及各种知识的增删改功能；
3. 支持定制及功能开发，支撑策略管理的其他需求，诸如安全体系、安全制度、人员管理等；

4.2.5. 综合展示

支撑组件：个人工作台、安全仪表板、风险管理

支撑业务：风险状况、工作进展、整体安全评价、安全报表

支撑及实现方式：

1. 通过“安全仪表板、风险管理”，能够展示系统内所有风险状况、风险统计，包括系统整体风险、安全事件风险、安全漏洞风险、安全配置风险、资产风险、设备状态风险等；
2. 通过“安全仪表板”，能够展示系统内所有工作任务统计及状态、工单统计及处理情况；
3. 通过“个工作台”，能够展示个人工作待办事项，如待处理工单、检查任务；
4. 通过“个人工作台”，能够展示个人工作的进度情况、检查任务完成情况、所负责工单的处理情况；
5. 支持定制及功能开发，支撑综合展示的其他需求，诸如特定的安全内容展示、安全集中展示、制度上网展示等。

5. 产品优势

5.1. 体系运营：上下联动统一监管，安全运营整体掌控

- 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
- 在“事前安全预防-事中安全监测和威胁检测-事后响应处置”整体方针指导下，通过可视化分析技术，直观呈现安全态势与安全建设成果，达到“事态可评估，趋势可预测，风险可感应，知行可管控”的安全运营目标。

5.2. 全面分析：集群负载全面采集，八大专项分析能力

- 集群负载全面采集：可依据业务需求灵活地扩展资源，从而实现保证平台在高并发、大数据量的情况下仍能保持高效稳定运行。分级分域管控通过权限控制和角色分配，确保不同级别管理员只能访问和操作其负责的域，降低内部误操作和恶意攻击的风险，增强了系统的安全纵深防御能力。
- 八大专项分析能力：攻击威胁特征分析、威胁情报分析、失陷分析、文件还原威胁分析、异常行为分析、网络异常分析、隐蔽外连分析、其他安全分析，全流量立体化威胁检测，多层次、全方位覆盖安全分析的每一个层面。

5.3. 精准溯源：精准失陷分析研判，六层溯源深度定位

- 六层溯源下钻深度挖掘：系统评分、失陷主机、多维威胁数据（情报、资产、日志、安全事件、脆弱性、流量）、事件级、会话级、PCAP 数据包，下钻分析安全事件无需分设备查看，一钻到底溯源取证。
- 基于“多重迭代验证”等专利技术精准研判安全事件和失陷主机，实现每天 10 条以下安全事件降噪能力。

5.4. 异构联动：异构设备万能联动，跨品类集中管控

- 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。
- 集中管控异构品类设备，助力日常安全运维工作，包括异构设备集中巡检、异常状态告警、异常事件处置，减轻日常信息化安全运维工作压力。

5.5. 智能处置：启发式联动响应处置，确凿证据定向抓捕

- 安全运营中心所具备的自动化编排响应能力，不仅能将分散的安全工具和能力通过流程进行可视化组装编排，平台独有的启发式联动响应能力，在不依赖三方安全设备对接的前提下，能自动执行响应剧本进行风险处置，降低对人工的过度依赖。此外编排能力与平台的轻量化集成、移动端与平台协同作战，将团队、工具和流程进行高度融合，极大增强安全运营能力。
- 使用绿色版终端抓捕工具，无需安装 agent，即可在失陷主机上对挖矿、木马软件、病毒程序等进行精准抓捕，让恶意软件无处遁形。