聚铭安全态势感知与管控平台

产品白皮书

聚铭网络科技有限公司

2023 年 11 月

目录

声明

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

随着组织信息化建设规模的扩大，安全架构日趋复杂，各种类型的安全设备、安全数据越来越多，组织自身的安全运维压力不断加大。另一方面，以高级可持续威胁攻击（Advanced Persistent Threat，APT）为代表的新型威胁的兴起，随着内控与合规的深入，越来越需要组织充分利用更多的安全数据进行分析检测，对基础架构安全、应用安全、数据安全乃至业务安全中面临的各类高级威胁做出判定和响应，以支撑业务持续稳定、安全运行。

面对新的安全形势，被动防御已经无法应对当前安全形势，只有切实落实好安全监测工作，持续监测、主动发现、及时预警，才能做到“知己知彼，百战不殆”。从场景化角度出发，客户网络环境中主要面临以下风险：

- 网络情况复杂难于监管：因安全监管要求，各组织对网络环境进行分区隔离，业务系统生产环境部署在组织内网，通过互联网出口连接互联网，网络环境复杂、云计算和大数据技术应用广泛，且面临来自互联网和各下级部门的攻击风险，技术监管难度大。
- 安全保障能力参差不齐：某些客户组织层级架构较复杂，各层级的安全保障能力差距较大，有些下级部门的安全保障纯靠传统安全产品的堆砌，呈现的维度较为单一，且存在大量重复报警及误报。
- 业务众多易遭受攻击：各组织的生产网络环境承载着大量的应用，时刻存在着：攻击者用病毒木马或者内部主机漏洞等脆弱面进行的攻击、内部人员违规操作的风险等，各 IT 系统所面临的威胁严峻。
- 内部资产难以摸清：内部到底有多少资产，有多少资产存在漏洞，这些漏洞的风险级别如何，会不会给网络带来危害等，都是用户所关心的，摸清内部资产情况能够提早发现并规避大量风险。

1.2. 当前挑战

1. 客户购置了各种不同类型的安全设备，但设备的安全保障工作相对独立，各自为政，运维难度大；
2. 传统安全设备产生海量安全日志，且误报率高，需要靠人工甄别；
3. 传统安全设备只能分析过去或现在正在发生的问题，但是无法告诉客户未来会发生什么；
4. 传统安全设备不会存储原始数据信息，攻击事件一旦发生，追溯难；
5. 客户购置了很多安全设备，但缺乏专业的运营人员对数据进行分析处理，保障网络安全。

2. 客户需求

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态势感知平台。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

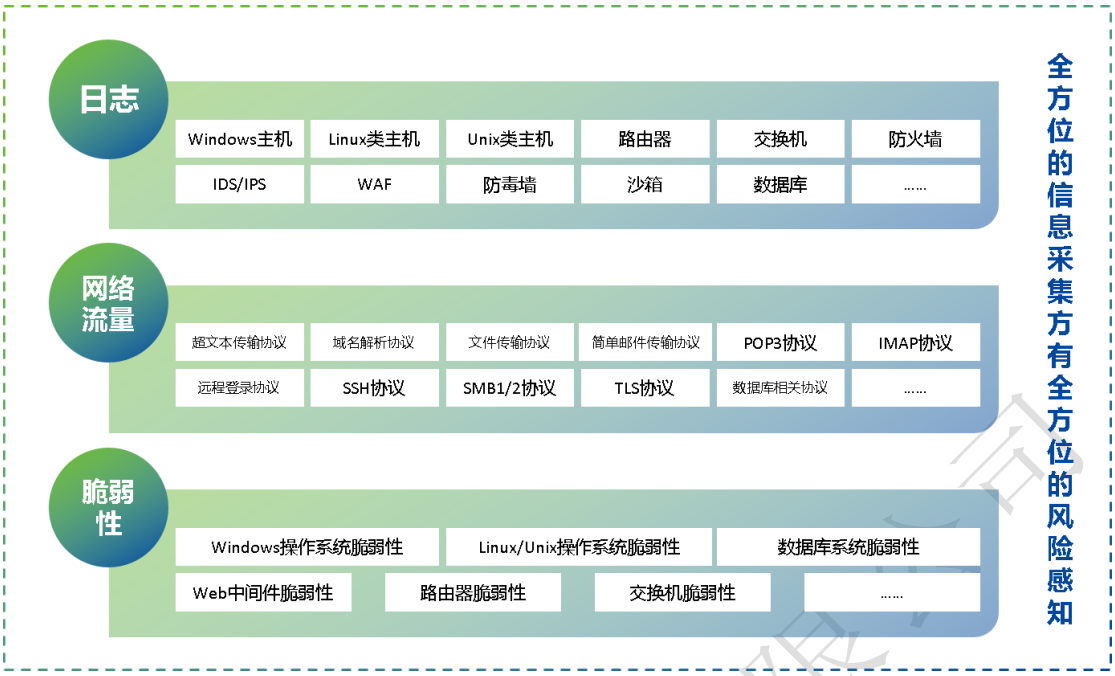
据、告警各类网络安全事件的综合性平台。这其中包括：

- 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），实现对各种网络安全设备信息的综合监控、管理及分析；
- 在大数据时代，以数据为核心，用新技术提供的低成本、高可靠、可弹性扩展的数据处理能力，满足海量多源异构日志数据的处理需求；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；同时，以运维和管理为动力，提供流程辅助、合规管控、安全分析和决策支持等能力；并且通过可视化技术和人机交互为运维人员提供工作接口，展现数据价值；
- 紧密围绕具体业务，采取主动和真正具有安全智能的管理技术，并采用融合大数据技术的软件架构，严格监控各种关键业务系统，防止对重要数据非授权篡改行为的跟踪及审计等。

3. 聚铭安全态势与管控平台解决方案

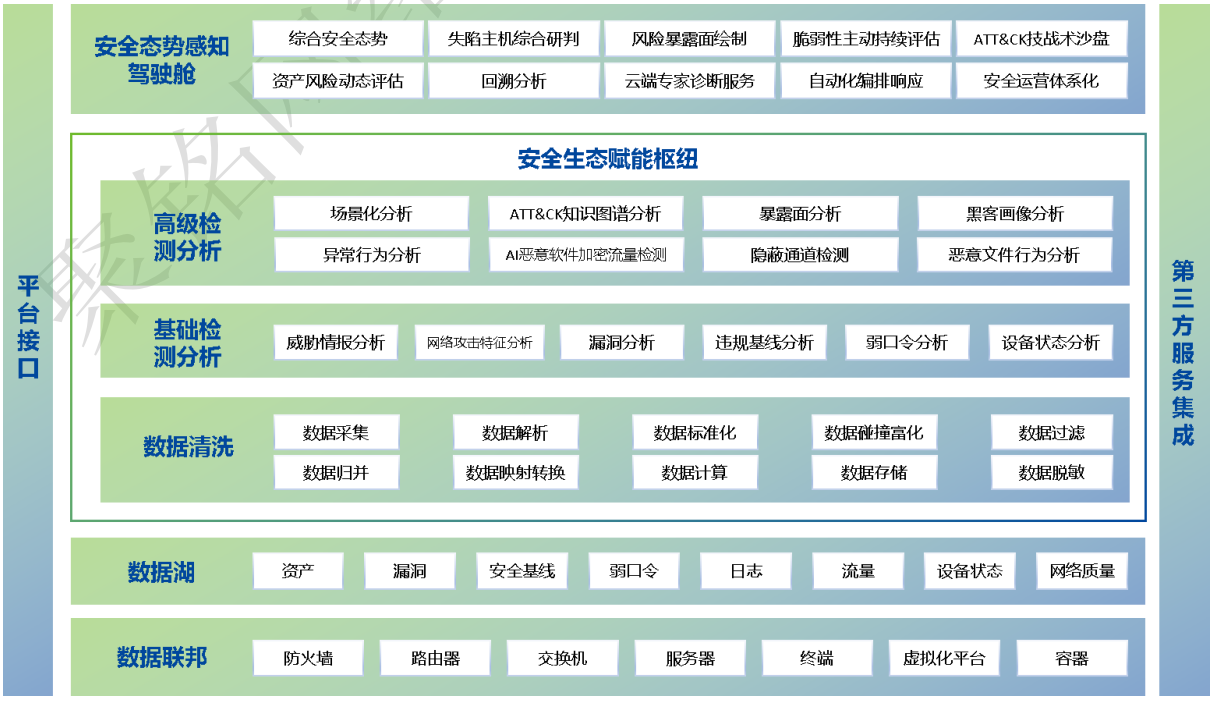
聚铭网络科技自主开发的基于大数据技术的安全态势感知与管控平台，统一采集各类结构化和非结构化的数据，包括各类设备、应用日志以及网络流量和各种脆弱性，通过平台内置的标准风险模型，从实时分析、离线分析、关联分析、统计分析、规则库、专家经验库以及外部安全情报的交换、机器学习等多方位进行风险分析。

聚铭安全态势感知与管控平台，充分收集各类安全相关数据，通过大范围和深度地广泛检查，尽可能发现相关安全问题。



3.1. 解决方案整体框架

聚铭安全态势感知与管控平台，具有完全分布式的数据采集和分析框架，包含了数据湖、数据清洗、基础检测分析、高级检测分析、安全态势感知驾驶舱（含综合安全态势、失陷主机综合研判、风险暴露面绘制、ATT&CK 技战术沙盘、资产风险动态评估等），如下图所示：



3.2. 方案组成

聚铭结合多年信息安全研究和项目实践，基于 IPDRR 能力框架模型构建以安全态势感知驾驶舱为核心的下一代安全能力新框架体系。此架构采用风险识别与安全保护的系统安全加固方法，融合传统网络与安全运营平台优势，联动系统实时检测与响应机制，遵循深度分析技术原则，全面保障网络安全、数据安全、应用安全以及主机安全。

- 数据联邦：指部署在用户环境中大量的安全设备及产品，包括但不限于防火墙、路由器、交换机、服务器、终端、虚拟化平台、容器等一系列设备。

- 数据湖/数据仓库：包括部署在用户环境中数据联邦设备产生的各种日志，经过收集，输送给生态赋能枢纽，为后续的检测分析提供原始数据。数据湖内包含资产、漏洞、安全基线、弱口令、日志、流量、设备状态、网络质量等数据。其内数据归由安全态势感知驾驶舱统一管理调度。

- 数据清洗：安全生态赋能枢纽接收到数据湖输送数据后，进行数据清洗处理。主要包含数据采集、数据解析、数据标准化、数据碰撞富化、数据过滤、数据归并、数据映射转化、数据计算、数据存储、数据脱敏等各种功能。实现全量数据的集中采集、处理、存储、分析，为上层模块打下数据检测与处理的基础。

- 基础检测分析与高级检测分析：检测分析模块是安全生态赋能枢纽的核心模块，模块内拥有众多强大的分析引擎，数据经过治理后，对海量多源异构数据进行实时数据分析、批量数据分析，生成相应的安全告警，确保各类威胁全面可视。

  本模块上承云端威胁情报中心，将云端海量威胁情报数据赋能于本地；下接数据湖，对数据湖内产生的各种数据进行检测分析。

- 安全态势感知驾驶舱：驾驶舱为安全运营工作提供了一站式指挥运营中心，包含安全运营工作相关的各类模块和管理功能，提供集安全态势、

事件分析、溯源分析、响应处置于一体的安全运营全流程工作平台。企业安全态势多维展示当前系统安全运营状况；ATT&CK 技战术沙盘以图谱展现当前环境所遭受威胁攻击，包括攻击利用到的战术和攻击技术；自动化编排响应为防护人员提供便捷的处置方法和相关的处置建议；风险暴露面绘制全面分析互联网边界和内网安全域间暴露面。

3.3.解决的安全问题

以下就聚铭安全态势感知与管控平台能够探知和发现的安全问题进行阐述。

■ 异常外连

聚铭安全态势感知与管控平台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

聚铭安全态势感知与管控平台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

聚铭安全态势感知与管控平台结合特征检测、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

聚铭安全态势感知与管控平台基于 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

通过聚铭安全态势感知与管控平台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。

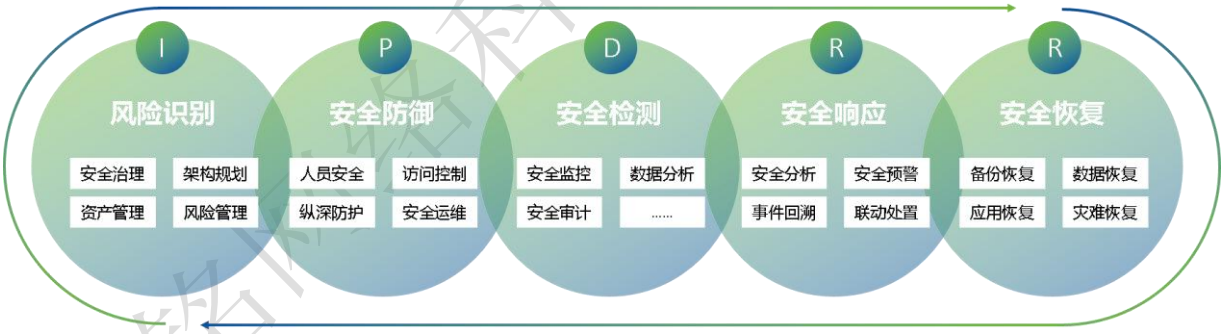
4. 主要功能简介

4.1. 安全态势感知驾驶舱

4.1.1. IPDRR 体系化运营

为应对日益严峻的信息安全形势，结合多年信息安全研究和项目实践，在传统被动防护基础上提出集风险识别（identification）-安全防御（protection）-安全检测（detection）-安全响应（response）-安全恢复（recovery）的 IPDRR 安全技术架构。此架构采用风险识别与安全保护的系统安全加固方法，融合传统网络与安全运营平台优势，联动系统实时检测与响应机制，遵循深度分析技术原则，全面保障网络安全、数据安全、应用安全以及主机安全。

基于 IPDRR 架构的信息安全防御闭环：



风险识别（identification）：对于网络架构、网络流量、资产和数据面临的安全风险进行识别和确认。明确其生产网络中的接入资产类别、网络结构、通信行为、主机行为等，确认其中存在的脆弱性以及可能遭受攻击的可能性，落实切实可行的安全架构，并为防御、检测提供有效的数据支撑；

安全防御（protection）：基于风险识别能力的支撑，构建以行为管控为基础的防御能力。对通信过程中的指令、数据地址、数值内容进行访问

控制，并在必要节点采用加密认证手段，落实数据传输过程中的完整性与保密性。在主机防护层面，以最小化原则落实系统管理、应用程序管理、进程和服务管控以及接口管控。

安全检测（detection）：基于风险识别能力的支撑，采用深度检测技术，实时监测越权操作行为。同时，深度结合业务系统逻辑，在越权、越线检测外，构建基于数据变化的检测能力，有效监控基于合法路径、合法行为的非法攻击过程。

事件响应（response）：面对已经发生的网络安全事件和已知威胁，整合安全识别、安全防御和安全检测三大安全模块，并结合以大数据为核心的安全分析能力，构建安全运营系统。安全运营系统通过三大安全模块的信息收集和资源整合，分析网络安全态势，与其它安全模块策略联动，并具备安全监测、风险评估、事件追踪和响应恢复能力。

安全恢复（recovery）：在安全事件后，为最大限度降低事件对于业务系统的影响，对业务系统数据进行备份恢复，并通过安全服务，消除攻击过程中残留的恶意脚本、僵尸主机，对安全事件处置进行闭环，并有效防范后续的攻击过程。

4.1.2. 综合安全态势

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。

安全运营驾驶舱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。

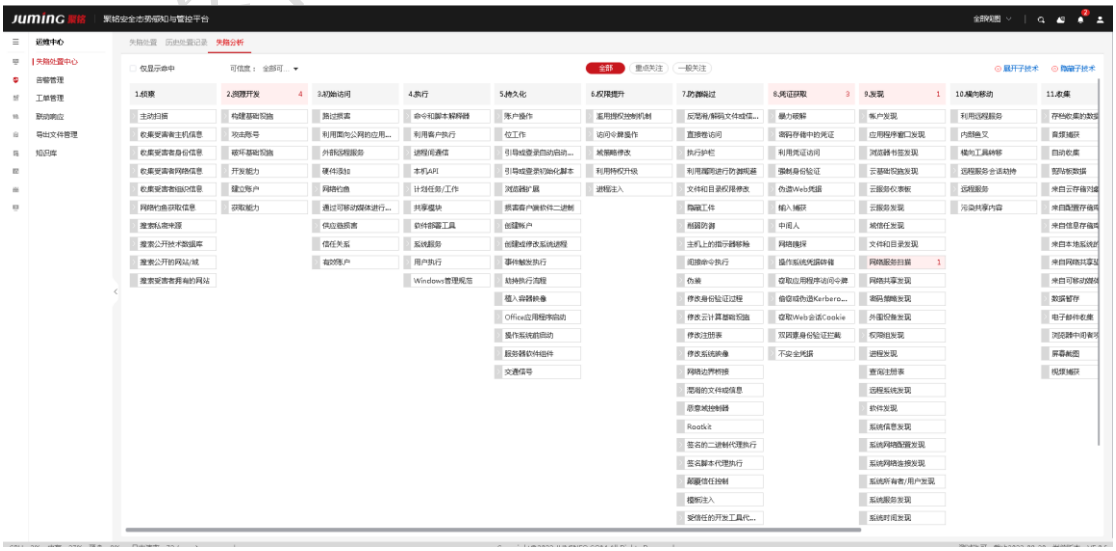
安全运营驾驶舱包含多块全息大屏：

- 综合态势感知全息屏：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：呈现网络环境内脆弱性实时动态，包括各漏洞影响设备排行、漏洞总量、各级漏洞数量分布及占比分析、违规基线类别分布及排行、弱口令账号总数及影响分布等。

4.1.3. ATT&CK 知识图谱

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。



4.1.4. 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。

4.1.5. 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。

4.1.6. 黑客攻击面绘制

基于平台的大数据分析引擎通过关联分析发现网络中的失陷主机、安全威胁，识别业务潜在安全风险和高级 APT 攻击行为，同时实现了基于攻击场景的有效攻击检测和被利用漏洞检测，进而对攻击进行溯源。将黑客的所有信息（IP、Domain、Hack tools、黑客位置、攻击手段、历史攻击记录、入侵过程）关联起来，还原整个攻击场景，形成完整攻击者画像。

基于对攻击者画像分析，将提供联动响应策略建议便于安全运维人员对攻击者进行处置。

4.1.7. 云&端交互式威胁溯源

平台能够基于已发生的网络攻击事件及线索，针对攻击对手、攻击手段、攻击途径、攻击资源、攻击位置、攻击后果等进行追踪溯源和拓展分析，为事前防御、安全防范提供支撑；针对高级威胁攻击、DDoS 攻击、钓鱼攻击、木马病毒等恶意行为通过云端数据进行关联分析、拓展扩线，进行事件溯源，为取证提供技术、数据支撑。

通过云端提供网络空间资产探查、网络安全监测、威胁雷达监控和 APT 预警、威胁情报、漏洞发现、攻击分析以及来自于终端、边界、深度网络威胁检测设备采集的海量数据，与本地流量探针、资产发现等数据的全面融合，提供紧贴客户业务的安全大数据分析与运营服务，帮助客户达成网络安全防范和挖掘取证的成效。

4.1.8. 资产自动测绘与管理

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。

众所周知，对于分支机构众多的集团企业而言，资产风险处置工作并非单一部门可独立完成，需要跨部门协同，对于安全运营人员而言是一项费时费力的常态化运营工作。

产品支持以资产视角对资产和网络进行划分管理，通过对安全管理人员分配权限实现多层级、多维度管理分支机构资产情况。此外，产品还支持自动绘制资产拓扑，以图形化的方式清晰描绘网络架构并进一步处置资产风险。

4.1.9. 脆弱性主动持续评估

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。

4.1.10. 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，产品具备自动化编排响应能力和安全检测加固能力。

自动化编排响应联动了安全事件生命周期的每个环节，包括事件生成、研判、人工处置、策略下发、自动处置和响应报告，来增强安全事件的响应速度。联动设备除了 FW、IPS、WAF、ACG 常见安全设备外，还能实现与交换机等网络设备联动。

产品除了能与设备进行联动进行安全事件响应处置，此外针对 DHCP 场景，能够溯源到具体的人员账号信息，实施基于上网账号的阻断。

4.1.11. 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。

4.1.12. 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态势感知报告。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。

综合态势感知报告：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。

4.1.13. 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。

4.2. 安全运营检测分析组合拳

4.2.1. ATT&CK 战术分析

利用 ATT&CK 知识库可检测识别威胁攻击各阶段中的攻击技术，并可以 ATT&CK 图谱的方式展现，包括攻击利用到的战术和攻击技术，可以让安全人员方便了解攻击过程。

4.2.2. 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。

4.2.3. 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。

4.2.4. 僵木蠕恶意软件分析

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。

4.2.5. 隐蔽隧道通信分析

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。

4.2.6. 挖矿检测分析

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。

4.2.7. 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。

4.2.8. 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。

4.2.9. 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。

5.产品优势

5.1.更全面：主动被动全面采集，八大专项分析能力

- 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
- 全面采集网络安全数据，为态势理解和预测打下数据基础，主动式采集方式支持 WMI、SMB、KAFKA、CONSOLE、Telnet、SSH 等；被动式采集方式支持 Syslog、SNMP Trap、Netflow、Web Service 等

5.2.更精准：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 100 万：10:1 的安全事件降噪能力

5.3.更自动：多维联动响应处置，确凿证据定向抓捕

- 具备自动化编排响应能力，支持防火墙、IDP 安全设备以及二层交换机联动，降低在网关式设备上的性能负荷，且支持与用户认证系统联动对用户账号下发阻断策略
- 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

5.4.更体系：上下联动统一监管，安全运营整体掌控

- 预置安全运营自循环内部协同流程，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