聚铭综合日志分析系统产品白皮书

聚铭网络科技有限公司

2026 年 3 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

1. 背景

对于一般的组织或企业，信息安全防护不可避免地从防毒/杀毒、防火墙等基础系统或设备开始的，但是随着信息技术的发展和国内外网络安全形势的日益严峻，信息安全防护已经不再仅仅是单一的防病毒、防火墙。

随着各类组织、企业对信息系统的应用不断深入。为了在复杂网络环境下应付各类安全情况（如黑客的攻击、内部员工的有意或无意地进行越权或违规操作），企业部署了大量的、不同种类、形态各异的信息安全产品：

为了监控黑客的攻击控制，部署了各种入侵检测或入侵防御设备；

为了防范内部员工的非法接入行为，部署了终端管理、网络准入等系统；

为了防止数据的非法泄露或重要数据被修改，部署了防泄漏系统等系统；

除了这些专用安全设备或系统每日会产生各种日志，组织或企业日常业务系统、主机系统、网络设备等也会产生很多和安全相关的日志，这引起了如下的问题：

它们格式差异巨大，没有统一标准；

它们数量巨大，用户无法进行重点分析；

难以挖掘各类日志之间的关联关系。

2.客户需求

由于日志审计工作难于开展，所以企业必然需要部署集中的综合日志分析系统。通过建设综合日志分析系统，企业能够集中采集各类系统中的安全事件、用户访问记录、系统运行日志、系统运行状态、网络存取日志等各类信息，经过规范化、过滤、归并和分析等处理流程后，以统一格式的日志形式进行集中存储和管理。

在此基础上，对日志进行实时的事件分析和审计分析、从而进行实时的事件

监控和异常事件告警，最终实现对各类网络设备、安全设备、操作系统、服务器、数据库和其它应用进行全面的日志安全审计。

综上所述，各级组织或机构部署集中综合日志分析系统的意义在于：

信息安全管理的需要：因为日志审计是日常信息安全管理中最为重要的环节之一；能从纷繁复杂的日志中萃取出具有价值的部分是各类信息安全管理者、参与者、相关者最大的诉求，故选择一款高可靠、高性能、具备强大功能的日志集中审计系统就成为必须。

系统运维使用的需要：传统日志审计系统日常运维使用，通常在会遇到日志源设备逐一配置接入困难，操作一学就会，时间一长就忘，运维无法脱离厂家技术支撑。各类设备日志信息五花八门，无法解读日志数据含义，导致数据价值无法挖掘，因此需要一款简单易用的日志审计系统。

安全技术保障体系建设要求的需要：一个完整的信息安全技术保障体系应由检测、保护和响应三部分组成，而日志审计是检测安全事件的不可或缺重要手段之一。大部分信息系统的所依赖的 IDS/IPS 系统只能检测部分来自网络的攻击事件，对运维人员的违规操作、系统运行异常、设备故障等安全事件缺乏监控能力，而这些异常事件恰恰是内部信息系统主要安全威胁之一。综合日志分析系统通过分析各设备、系统、应用、数据库产生的运行日志，能够及时发现入侵检测系统检测不到的各类安全隐患，并及时给予告警，从而避免安全事件的发生。

各种规范符合性要求的需要：《信息安全等级保护》（几乎各级均要求提供审计功能）、《信息安全风险管理规范》、《基于互联网电子政务信息安全指南》、《银行业金融机构信息系统管理指引》等等。此外，国际上的相关标准、规范也均明确提出信息综合日志分析系统的重要性，如萨班斯法案、ISO27001 等均要求企业对重要系统、设备的运行日志进行保留，并且周期性地进行第三方审计。

3.产品定位

南京聚铭网络科技有限公司（以下简称聚铭）为企业建设综合日志分析系统

提供了一套综合解决方案。

综合日志分析系统是为了能满足企业的日志集中审计需求，针对信息安全事件的“可发现”、“可处理”、“可审计”、“可度量”四大目标进行规划和设计的。

“可发现”：具备对海量安全事件的采集、分析、处理报告能力，可以实时动态展现当前安全事件态势，实时获知异常安全事件或审计违规告警。按需展现各类关注事件的分布状况，可集中管理各类安全事件和安全资产，能够智能化分析安全事件对业务系统可能产生的实际影响和危害，减轻通过人工甄别大量事件的工作难度，提高管理工作效率，降低运维工作负担。

“可处理”：发现安全事件风险是为了更好更快的处理。综合日志分析系统具备安全告警功能，可通过技术手段将发现的安全事件告警纳入到日常安全运维流程中，与第三方设备进行告警联动，建立安全事件处理的自动化体系，提供安全问题处理的效率。

“可审计”：具备针对各类信息安全管理标准或要求的日志审计能力，提供针对诸如等级保护要求、SOX 信息安全审计要求、企业内部下发的信息安全工作要求的审计策略，支持通过技术手段实现日志审计工作的自动执行、自动核查、自动报告功能。

“可度量”：针对信息安全事件日志的采集、分析、处理情况，结合信息安全资产的 IT 属性，能够实现对企业信息安全情况的分析和审计。综合日志分析系统可度量企业信息安全的安全水平，给出企业对各种审计要求的符合性程度，指导企业的信息安全管理和建设工作。

融合安全垂直领域先进 AI 大模型，有效降低运维成本和管理的复杂度，显著提升采集、分析、审计、处理的智能化水平，实现日志自动采集、一键解读、人机交互，让日志运维使用简单便捷。

因此它是全面支持企业综合日志分析系统需求的一个技术平台，是企业日常信息安全工作的重要载体。

4. 聚铭综合日志分析系统解决方案

4.1. 总体架构

聚铭综合日志分析系统的主要功能包括如下模块：

■ 采集层：采集各种设备的事件日志，标准化为统一的格式，然后进行过滤、归并、关联和审计，从海量日志中分析潜在的安全问题，同时进行相关数据的存储和管理；

■ 分析层：系统通过分析引擎，对日志进行关联分析、审计分析和统计分析，并对异常事件告警策略进行管理；

■ 展现层：综合展现层是综合日志分析系统的展示层。该层通过个人工作台和安全概览，将整个系统收集、分析、管理的安全事件、告警概况等信息多维度的展现在用户面前。

4.2. 主要功能

聚铭综合日志分析系统能够实时、不间断地采集并整合各类设备的日志信息，借助先进的关联分析与机器学习技术，助力用户从庞杂的日志数据中快速识别异常安全事件，全面满足合规审计、分析调查及数据留存等日志多场景使用需求。

4.2.1. 采集管理

采集是综合日志分析系统的重要功能模块，它承载了日志或事件采集标准化、过滤、归并功能。采集管理是系统进行分析的第一步，用户通过指定需要采集的目标、相关采集参数（Syslog、SNMP Trap 等被动方式无需指定）、相关的过滤策略和归并策略等创建日志采集器，以收集相关设备或系统的日志。

4.2.2. AI 智能分析

4.2.2.1. AI 智能解读

AI 智能解读原始日志信息的功能，为用户提供高效、便捷的方式来理解和处理日志数据，减少对第三方工具的依赖。这一功能主要三个部分，分别是日志总结、日志内容详细解读、行动建议。

日志总结：日志总结部分为用户提供日志的简短概述，帮助用户快速了解日志的主要内容。

日志内容详细解读：日志内容详细解读为用户提供日志的详细解读，帮助用户深入理解日志中的每一个细节。

行动建议：行动建议会根据日志内容，为用户提供针对性的解决方案或建议，帮助用户快速解决问题。

4.2.2.2. AI 智能解析

用户将日志发送到日志审计平台后，平台能够自动根据采集到的日志信息关联对应的范式化解析策略，极大地提升了日志运维的效率和准确性。日志审计平

台将能够更智能、高效地处理不同类型的日志数据，为客户提供更加便捷、优质的日志审计服务。

4.2.2.3. AI 智能助手

结合人机交互模式和 AI 安全大模型，让系统能够智能地理解用户的问题，并解答用户的安全日志问题，从安全大模型中提取相关信息，并给出准确的解答或建议，从而显著提升运维体验。

4.2.3. 数据识别（标准化）

不同的系统或设备所产生的日志格式是不尽相同的，这给分析和统计带了巨大的麻烦，所以在综合日志分析系统中内置了 1000+种标准化脚本以处理这种情形；即便对于某些特殊的设备，您没有发现相关的解析脚本，综合日志分析系统也提供了相应的定制方法以解决这些问题。

4.2.4. 过滤和归并

为了对接收的日志数量进行压缩，综合日志分析系统还提供了过滤和归并功能；其中，过滤功能不仅仅是丢弃无用的日志，而且也可以将它们转发到外部系统或对部分事件字段进行重新填充。

4.2.5. 告警监控

所谓告警是指用户特别需要关注的安全问题，这些问题来源于事件分析、审计分析的结果。告警监控中包括了如下功能：

- 告警监控：用户可以通过定义过滤器以监控需要特别关注的告警信息，用户也可以根据个人需求，设置告警的提示音、界面显示方式等；
- 告警处理：处理监控列表中相关告警；针对告警，用户可以清除（不予关注）、确认（已知告警可后续处理）。

4.2.6. 实时监控

所谓实时监控是指对当前接入的事件日志的逐条、实时显示，显示的日志内容是可以根据用户的需求进行设置过滤条件来定制的。实时监控中包括了如下功能：

- 设置监控过滤规则：根据用户需要或分析过程的需要设定显示过滤条件，便于观察日志实时接收情况；
- 开始或暂停监控：根据过滤条件开始监控或暂停监控；
- 导出当前监控显示的内容：当暂停监控时，用户可以导出当前显示的日志内容，便于后续分析、挖掘或追溯异常安全事件日志。

4.2.7. 网站监控

基于用户关注网站域名进行监控，通过网站访问量、攻击数、告警数进行综合评分安全等级，采用统计方式进行趋势图动态展示。

网站支持 IPv4、IPv6 地址，可通过手动录取及域名发现进行网站添加。

4.2.8. 日志转发

依据用户需求可将接受日志进行转发，转发方式支持 syslog、kafka 等方式，并支持筛选条件后的日志转发，如转发某个资产的告警日志。转发的日志不仅可提供范化式后的字段，同时可提供详细信息字段。

4.2.9. 会话审计

综合日志审计系统利用独有的智能协议识别技术，可高速、准确地识别上千种应用，在解析五元组（源 IP、目的 IP、源端口、目的端口、协议）、会话发生时间外，根据不同应用协议进行了更加深度的解析，满足客户会话审计的需求。

4.2.9.1. HTTP 会话审计

从流量中还原 HTTP 会话数据，并根据会话特征进一步深度解析 HTTP BBS

访问、HTTP 网页标题、HTTP 威胁情报、HTTP DGA 域名、搜索关键词及其他 HTTP 会话等，数据中至少包含请求方法、返回值、主机名、网页地址、用户代理、语言、服务器类型等数据。

4.2.9.2. DNS 会话审计

从流量中还原 DNS 会话数据，并根据会话特征进一步深度解析 DNS 威胁情报、DNS DGA 域名、DNS 解码错误、DNS 解析错误、DNS 解析超时，数据中至少包含请求域名（FQDN）、DNS 服务器地址、DNS 服务器端口、请求返回解析地址等信息。

4.2.9.3. FTP 会话审计

从流量中还原 FTP 会话数据，数据中至少包含登录用户、传输文件名以及操作命令等信息。

4.2.9.4. Telnet 会话审计

从流量中还原 Telnet 会话数据，数据中至少包含登录用户以及操作命令等信息。

4.2.9.5. 数据库会话审计

从流量中还原主流数据库会话数据，如 Mysql、SQLServer、Oracle 等主流数据库，数据中至少应包含登录用户名、操作命令（SQL）等信息。

4.2.9.6. 邮件会话审计

从流量中还原邮件会话数据，包括 POP3，SMTP、IMAP 协议，数据中至少包含收件人、发件人、主题、附件名称等信息。

4.2.9.7. TLS 会话审计

从流量中还原 TLS 会话数据，数据中至少包含服务器及客户端证书、服务器

名称等信息。

4.2.10. 威胁检测

通过对网络流量进行非入侵性的侦听检测，在威胁发生全生命周期的多个阶段识别攻击者的攻击负荷、恶意行为和网络通信。

4.2.10.1. 基于流量的攻击检测

内置多种网络攻击检测策略，支持对一般网络攻击、明文传输、过期系统或软件、木马检测、隐蔽通道、电子加密货币活动、勒索软件进行检测，支持检测的类型可达 34 种。

- 网络攻击检测：支持对一般的网络攻击进行检测，检测的类型包括端口扫描、拒绝服务攻击、漏洞利用攻击、SQL 注入攻击、缓冲区溢出攻击、Webshell 及其它类型的注入攻击；
- 明文传输检测：对网络传输中存在的明文传输行为进行检测；
- 过期系统或软件检测：支持对可能存在过期的系统或软件进行检测；
- 木马检测：支持对各类木马活动进行检测，包括但不限于木马软件下载、木马登录/回连以及其他木马通讯行为；
- 隐蔽通道检测：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检测；
- 电子加密货币活动检测：支持对主流电子加密货币活动进行检测，包括但不限于比特币、莱特币、门罗币等；
- 勒索软件检测：支持对各类勒索软件进行检测，包括其登录行为、横向扩散行为等，检测的类型包括但不限于永恒之蓝、GandCrab、Satan 等。

4.2.10.2. 恶意动态域名检测

动态算法生成域名，简称 DGA，是黑客常用的回连通讯手段，可以轻易绕开基于特征库的检测手段。主要应用于 HTTP、DNS 等多种协议分析，利用超过千万级别的白域名及黑域名数据进行训练，准确度超过 95%。

4.2.10.3. 威胁情报检测

整合威胁情报库，支持对各类恶意 IP、恶意域名、恶意 URL 以及恶意邮箱进行检测；检测的类型包括僵尸网络、木马回连、隐蔽通道、电子加密货币矿池等。

4.2.11. 事件分析

综合日志分析系统的事件分析功能是系统中的核心功能之一；其中关联分析策略主要侧重于各类日志之间可能存在的逻辑关联关系。

综合日志分析系统不仅支持以预定义规则的方式进行事件关联，还支持基于模式发现方式的关联。

综合日志分析系统支持如下不同类型日志或事件（需结合相关设备，如防火墙、IPS 等）：网络攻击、有害代码、漏洞、用户访问存取、系统运行、设备故障、配置状态、网络连接、数据库操作等。

对于事件关联分析所产生的结果将在关联事件中呈现，如果符合关联策略，将以告警的形式在实时监控模块呈现给用户，用户可以对告警进行相关的处理。

4.2.12. 审计管理

综合日志分析系统的审计管理功能是系统的核心功能之一，其中审计策略主要侧重于发现日志中相关要素是否和预定的策略相符，如时间、地点、人员、方式等。

综合日志分析系统支持以预定义规则的方式进行审计；支持基于模式发现方式的关联；支持短时间内的序列审计；支持长时间的审计（最长可达 30 天）。

审计管理能够方便的自定义审计人员、行为对象、审计类型、审计策略等基本配置；并能够自定义审计策略模板，审计管理内置了大量审计策略模板，涵盖了常见的、对企业非常实用的审计策略模板，如主机、防火墙、数据库、萨班斯审计策略、等级保护策略模板等。

对于根据审计策路所产生的审计违规结果，系统将在审计事件中呈现给用户，如果符合定制的审计策略，也会在实时监控模块以告警形式展现给用户。

4.2.13. 资产管理

安全资产是系统基础的管理对象，是风险分析的依据，与 ISO27001 的关于资产的定义略有不同，综合日志分析系统中的资产是特指具有 IP 地址的 IT 类设备及其之上运行的、可管理的服务、应用。

一般而言，资产具备如下两类属性：

- 基本属性：名称、编号、系统类型（产品类型、操作系统类型、版本等）、IP 地址（支持 IPv4 和 IPv6 格式）、响应人（出现安全问题应由何人处理）、上架信息等；
- 安全属性：完整性、可用性、保密性、风险信息、开放端口、告警、安全事件等。

系统的资产管理支持用户录入、导入或自动发现资产。

为了处理不同网络的资产同 IP 问题，系统还支持对于网络和 IP 地址段的管理。为了用户便于集中、灵活地管理所辖范围内的资产，综合日志分析系统支持用户自定义资产管理视图。

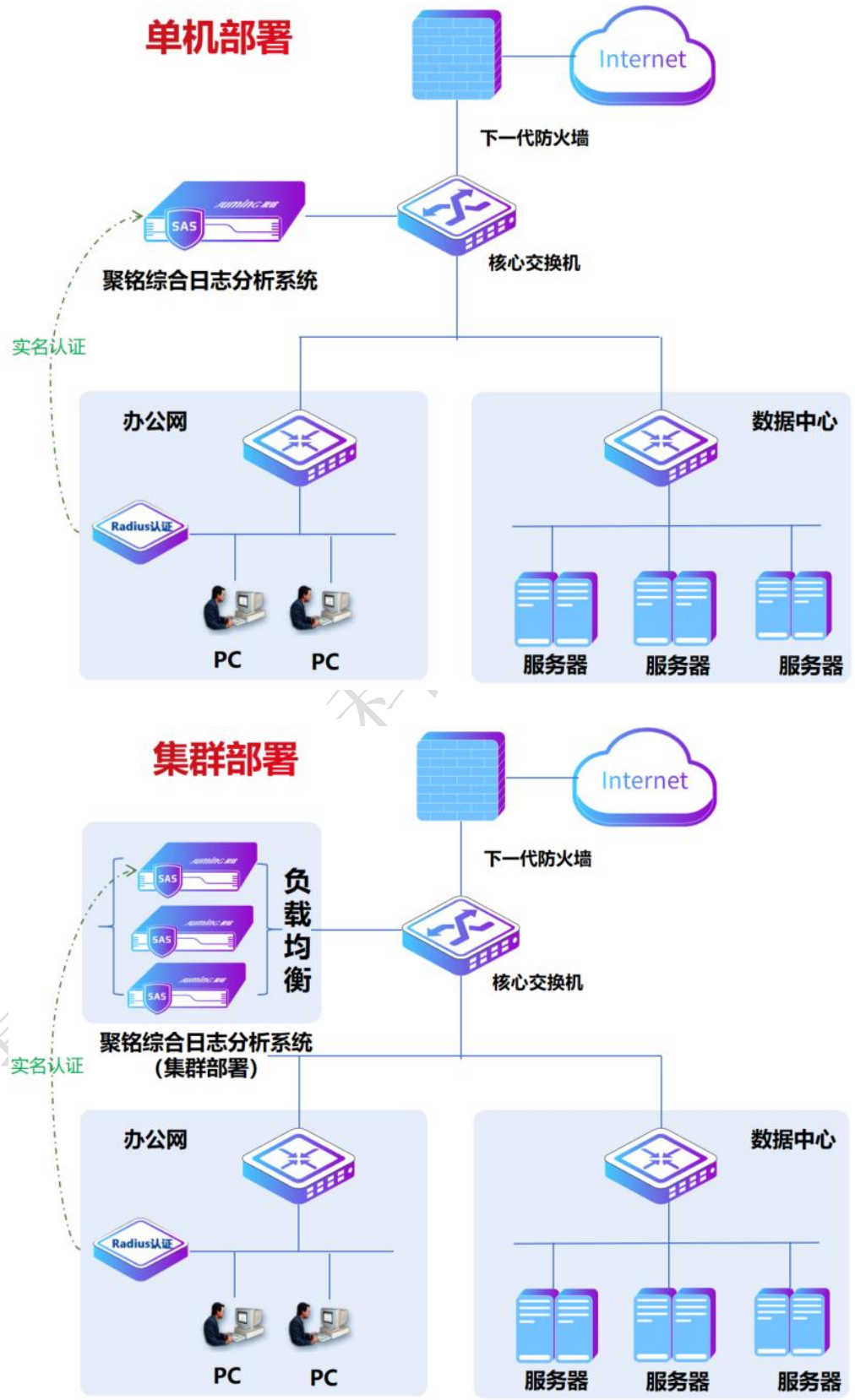
4.2.14. 组织管理

为了集中管理总部与分支不同网络与 IP 地址段日志数据及告警信息，系统支持创建多组织管理不同 IP 地址段/IP 地址。告警监控菜单支持从组织视角展示告警信息，便于管理者掌控及分析不同组织安全威胁态势，弹性制定及采取多样化的安全管理策略。

4.3. 部署方案

聚铭综合日志分析系统支持单机部署、集群部署。

企业网络较为简单，日志量偏少可以采用单机部署；当企业日志量较大时，可以采用集群部署方式进行负载。



5.产品价值

5.1.AI 赋能日志审计

- AI 赋能数据采集：依托 Ai 大模型能力，实现自动化日志采集与解析，无需人工介入操作
- AI 赋能解析：融合安全垂直领域先进大模型，实现日志一键解读，让小白变专家
- 人机交互答疑：AI 小助理随叫随到，及时解答您的安全疑问，让运维工作得心应手。

5.2.全面的日志收集

- 多源支持：支持从各种设备、系统和应用中收集日志，包括但不限于防火墙、交换机、服务器、数据库、安全设备等。
- 实时采集：实时采集日志信息，确保数据的及时性和准确性。
- 灵活配置：支持多种日志采集方式，如 Syslog、SNMP、文件传输等，满足不同环境下的需求。

5.3.强大的日志分析

- 多维分析：支持多维度的日志分析，如按时间、设备、事件类型等进行分类和统计。
- 异常检测：通过机器学习和规则引擎，自动检测异常日志，及时发现潜在的安全威胁。
- 威胁情报：集成威胁情报库，实时分析安全威胁信息，提高业务系统的防护能力。

5.4.高效的日志管理

- 集中存储：提供集中化的日志存储解决方案，确保日志数据的安全性和可靠性。

- 灵活检索：支持快速检索和查询日志，帮助管理员快速定位问题。
- 报表生成：自动生成各类日志报表，方便管理层进行决策和合规审计。

5.5. 安全合规

- 法规遵从：帮助企业和组织满足各种法规和标准的要求，如 ISO 27001、GDPR、HIPAA 等。
- 权限管理：细粒度的权限管理，确保只有授权人员可以访问敏感日志信息。

6. 产品应用场景

6.1. 访问控制审计

项目案例：某运营商

需求：非工作时间对资源的访问和异常访问的主机进行记录审计。

解决方案：全网设备的日志收集，包括网络设备，服务器，安全设备等，集中管理、统计监控。

预期效果：收集全网出口、安全、交换、服务器等设备日志，对海量日志实现高速存储、查询，实现集中日志审计，发现非工作时间访问、堡垒机绕行、异常登录等行为。

6.2. 网络安全检查

项目案例：某高校

需求：安全分析实现精准定位安全风险，学校全网日志收集和高速查询。

解决方案：收集服务器、安全设备等日志实现安全分析，定位关键安全风险，发现安全事件及时告警。

预期效果：对内网日志收集满足日志审计，通过对日志分析实现对内网安全运维。