獬豸日志安全审计系统

技术白皮书-V1.0

北京携推信息技术有限公司

2019 年 12 月

声明

本技术白皮书由北京携推信息技术有限公司编制，旨在对獬豸日志安全审计系统进行全面介绍。本文档所载内容的知识产权归北京携推信息技术有限公司所有。未经本公司书面许可，任何单位或个人不得以任何形式复制、转载或传播本文档内容。

本文档内容将不定期更新，最新版本敬请访问官方网站：www.xie-tui.com

公司名称：北京携推信息技术有限公司

目　　录

1 概述

獬豸日志审计安全系统是由北京携推信息技术有限公司自主研发的日志与事件管理分析产品，具备对信息系统中各类日志/事件进行集中采集、集中管理和集中分析的能力。系统支持对操作系统（Windows、Unix、Linux、BSD）、网络设备（路由器、交换机）、安全设备（防火墙、IDS、防病毒系统等）、应用系统（Web、邮件、FTP、中间件等）以及数据库系统等多种 IT 设施产生的日志/事件进行统一采集和存储。

通过獬豸日志安全审计系统，用户不仅能实现日志的集中存储，防止日志被篡改或删除，避免安全事件发生后无据可查，还能借助系统强大的日志分析能力，实现实时监控、高效检索、智能分析等功能，显著提升对安全事件和系统故障的响应与处理能力。

2 用户需求

随着信息化程度的不断加深，政府及企事业单位对信息系统的稳定性和安全性要求日益提高。日志/事件作为保障系统运行的重要手段，在安全事件和系统故障的分析中发挥着关键作用。然而，当前日志/事件普遍存在分散存储、格式不一、保存周期短、易被篡改等问题，导致其在分析时无法有效整合和定位，价值大打折扣。

因此，部署一套统一、高效、全面的日志/事件管理系统，不仅有助于满足政策法规要求，也能切实提升组织对信息系统的整体监控能力。

2.1 政策法规需求

国内外多项法规和标准均对日志管理提出了明确要求，如中国的《信息安全等级保护》、《信息安全风险管理规范》，以及国际上的 SOX 法案、ISO27001 等，均要求企业保留关键日志并进行定期审计。

2.2 安全技术保障体系建设需求

一个完整的信息安全保障体系应由保护（P）、检测（D）、响应（R）三部分组成，而日志/事件正是检测环节的重要基础。当前多数系统依赖入侵检测系统仅能识别部分网络攻击，对运维违规、系统异常等内部威胁缺乏监控能力。獬豸日志审计系统通过分析各类设备、系统、应用的运行日志，能够及时发现内部潜在隐患，提前预警，避免安全事件发生。

2.3 安全建设保障需求

面对日益复杂的安全威胁，企业已部署防火墙、IDS、IPS、漏洞扫描、防病毒系统等多重防线。然而，这些系统相互独立，形成“防御孤岛”，其产生的日志也各自为政，成为“信息孤岛”。安全人员面对海量割裂的日志信息，难以高效发现真实威胁。獬豸日志审计系统通过集中管理、智能分析，帮助企业实现以下目标：

- 集中管理各类设备与应用日志；

- 归一化处理多种日志格式，识别多种安全事件类型，如非授权配置修改、攻击事件、系统异常等；
- 实时监测并告警关键事件；
- 智能过滤无效告警，提升告警准确性；
- 快速定位事件源与目标资产；
- 实现跨设备的安全风险关联分析。

3 系统架构和功能介绍

3.1 体系架构

獬豸日志安全审计系统基于优化加固的嵌入式 Linux 系统开发，包含日志采集、日志分析、系统管理等核心模块。系统采用 B/S 架构，管理员可通过 HTTPS 进行远程管理。

獬豸日志安全审计系统的系统架构如图 3.1 所示。

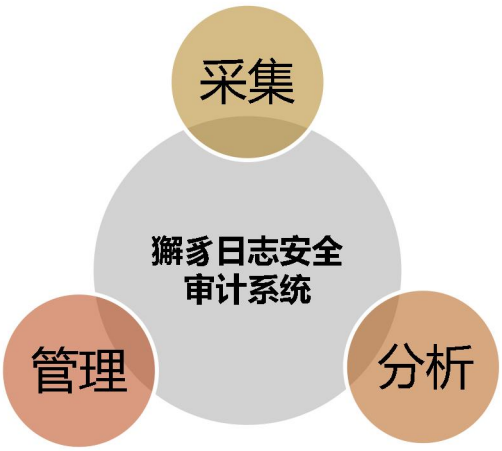


图 3.1 獬豸日志安全审计系统架构示意图

3.2 产品主要功能

3.2.1 日志/事件采集

系统支持广泛的日志采集对象与方式:

- 操作系统: Windows、Unix、Linux、BSD 等
- 网络设备: Cisco、华为、H3C 等
- 安全设备: 防火墙、代理设备、防病毒系统等
- 应用系统: Web (IIS、Apache) 、Mail、FTP 等
- 数据库: Oracle、MSSQL 等

采集方式:

- 专用 Agent 采集
- 日志协议采集 (Syslog、SNMP Trap 等)

3.2.2 日志/事件范式化

- 支持不同原始日志格式的归一化处理
- 支持主流设备与应用的泛化识别，如 Cisco、华为、Juniper、IBM AIX、Windows、Linux、Nessus、McAfee、Exchange、Apache、IIS 等
- 支持 20 大类 240 余种事件类型，包括漏洞利用、认证授权、恶意软件、拒绝服务、系统异常等

3.2.3 实时关联分析

- 基于资产、脆弱性、事件可信度的风险关联模型
- 支持时间、源/目的 IP 的逻辑关联
- 支持多种事件类型的交叉分析
- 内置 8 大类 83 种关联规则，涵盖网络扫描、木马蠕虫、Web 攻击、暴力破解等

3.2.4 资产管理

- 支持主机、主机组、网络域的集中管理
- 支持资产自动发现与属性描述

3.2.5 脆弱性管理

- 支持 CVE 标准的漏洞知识库
- 支持 Nessus、OpenVAS 扫描规则与结果导入

3.2.6 实时监测告警

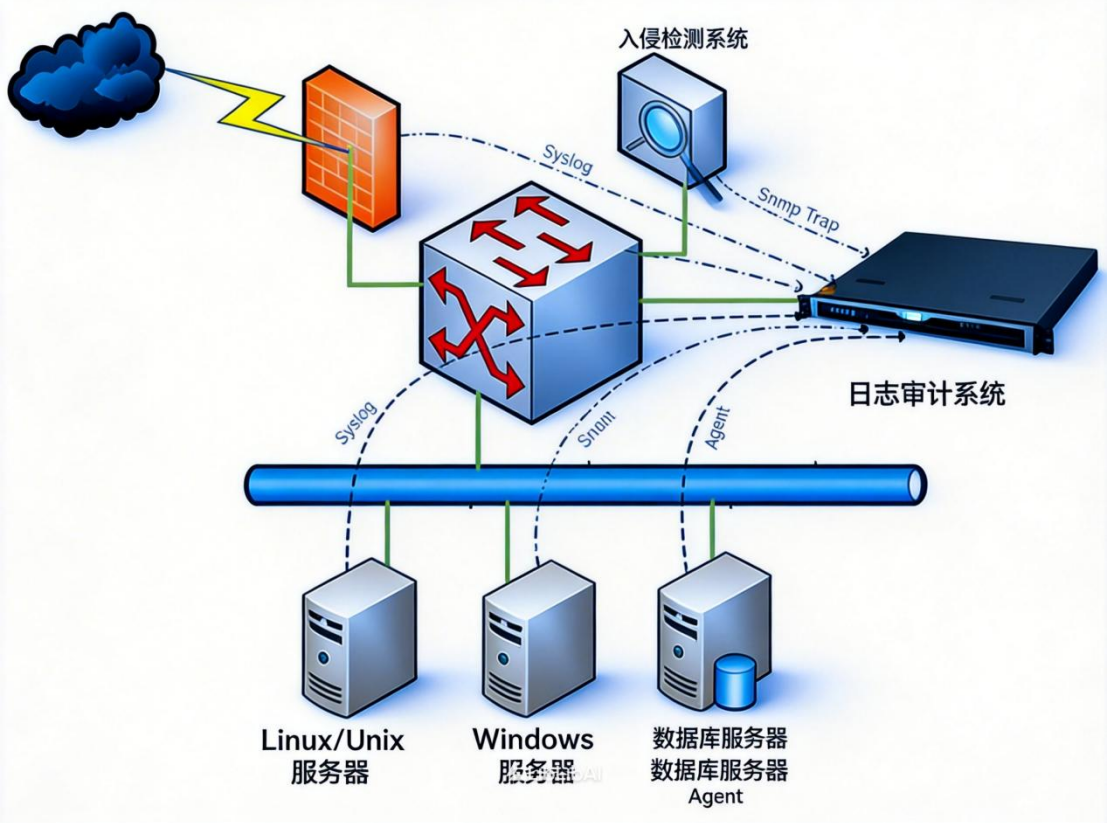
- 基于事件可信度判定告警级别，过滤无效告警
- 支持关键资产监控与多方式告警（界面、Syslog、邮件）
- 支持告警资产定位与日志全文检索

3.2.7 统计报表

- 支持事件统计、告警统计、资产统计、脆弱性统计等
- 支持 TOP 排名、分布分析
- 支持导出为 PDF、Word、Excel、HTML、PPT
- 支持等级保护等合规报表

4 产品部署方式

獬豸日志安全审计系统部署灵活，只需配置独立 IP 即可接入网络。设备可通过 Syslog、SNMP Trap 自动发送日志，或通过 Agent 采集操作系统日志。



5 优势特点

5.1 标准化日志

从安全视角对日志进行标准化描述，涵盖攻击、入侵、内控、漏洞、可用性等多维度信息。

5.2 丰富的日志/事件解析能力

支持按需激活解析规则，采用多级解析与动态规划算法，支持正则、分隔符、MIB 映射等多种解析方式，性能与设备数量无关。

5.3 先进的关联算法

关联分析引擎具备强大的适应性与可定制性，支持基于逻辑表达式的复杂关联与时序宽容处理，有效应对乱序日志。

5.4 高速检索能力

采用自主研发的海量日志检索引擎，摆脱传统关系型数据库的性能瓶颈，实现高速全文检索。

5.5 基于资产、脆弱性、事件可信度模型的风险关联算法。

结合 CVE 漏洞库与 Nessus、OpenVAS 扫描结果，自动生成资产风险报告，实现精准风险评估。

5.6 灵活的查询条件

支持字段级精确匹配与全文检索，用户可根据源 IP、时间等条件快速定位日志。

6 客户价值

- 统一日志管理：实现日志集中采集与多维度关联分析，为决策提供数据支撑；
- 合规审计：满足等级保护、行业法规等审计要求；
- 提升效率：及时发现告警事件与违规行为，提升安全响应能力；
- 完善安全体系：强化安全保障能力，促进安全体系持续优化。