中国医学科学院肿瘤医院

综合日志审计

技术需求

**信息中心/计算机室**

**2017年8月**

目录

[中国医学科学院肿瘤医院 0](#_Toc491932502)

[综合日志审计 0](#_Toc491932503)

[技术需求 0](#_Toc491932504)

[一、 项目简介 2](#_Toc491932505)

[二、 参数要求（数量1台） 2](#_Toc491932506)

[三、 服务 6](#_Toc491932507)

# 项目简介

为更好的执行《信息安全等级保护基本要求》，不断应对新的安全挑战，我院先后部署了防火墙、IPS、漏洞扫描系统、防病毒系统、终端管理系统、WAF等，构建起了一道道安全防线。

然而，这些安全防线都仅仅抵御来自某个方面的安全威胁，形成了一个个“安全防御孤岛”，无法产生协同效应。更为严重地，这些复杂的IT资源及其安全防御设施在运行过程中不断产生大量的安全日志和事件，形成了大量“信息孤岛”。有限的安全管理人员面对这些数量巨大、彼此割裂的安全信息，操作着各种产品自身的控制台界面和告警窗口，显得束手无策，工作效率极低，难以发现真正的安全隐患。

综合日志审计作为信息资产的综合性管理平台，通过对我院网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理员提供全局的视角，确保业务的不间断运营安全。

# 参数要求（数量1台）

|  |  |
| --- | --- |
| 硬件规格 |    4个工作管理口，1个console口 |
|    内存：16GB，磁盘：2T\*2 raid1 |
|    双电源 |
| 可扩展项：内存可扩展至32GB |
| 单个磁盘可扩展至4T(4个盘位)，支持HBA卡扩展 |
| 网口可扩展（4电4光、8电、8光、2万兆光） |
| 处理性能 |    支持审计200个日志源； |
|    平均处理能力（每秒日志解析能力EPS）：9000EPS； |
|    峰值处理能力（每秒日志解析能力EPS）：12000EPS。 |
| 工作模式 |    独立完成审计日志采集，不依赖于设备或系统自身的日志系统； |
|    审计工作不影响被审计对象的性能、稳定性或日常管理流程； |
|    审计结果存储于独立存储空间； |
|    自身用户管理与设备或主机的管理、使用、权限无关联； |
|    提供全中文WEB管理界面，无需安装任意客户端软件或插件 |
| 功能扩展 |    ★采用解决方案包上传对产品进行功能扩展，无需要代码开发。 |
| 日志收集 |    支持Syslog、SNMP Trap、OPSec、FTP协议日志收集 |
|    支持使用代理(Agent)方式提取日志并收集； |
|    支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等； |
|    设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell），digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS系统日志，Linux/UNIX syslog、IIS、Apache等； |
|    ★支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等 |
| 日志分析 |    可以以日志等级进行过滤； |
|    应该可以通过自定义配置将用户不关心的日志过滤掉； |
|    支持对收集到的重复的日志进行自动的聚合归并，减少日志量； |
|    支持可由用户定义和修改的日志的聚合归并逻辑规则; |
|    支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备； |
|    支持对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展。 |
|    可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息（公网情况） |
|    ★支持基于内存的实时关联分析，跨设备的多事件关联分析； |
|    ★支持自定义条件都事件进行聚合； |
|    ★进行关联分析的规则可定制； |
|    ★支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析（三维关联），所有的三维关联算法和准则以CVE、Bugtraq、OWASP公开协议和标准为为基础。 |
| 日志备份 |    可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比； |
|    ★支持日志备份自动传送到远程服务器； |
| 日志查询 |    支持B/S模式管理，支持SSL加密模式访问； |
|    支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询； |
|    支持用任意关键字对所有事件进行高性能全文检索 |
|    支持可指定多个查询条件进行组合查询 |
|    支持将查询的条件存储为查询模版，方便再次使用 |
|    ★极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。 |
| 应用性能监控 |    支持如下应用的性能监控（Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris）、数据库（mysql、oracle）、应用服务器（weblogic、tomcat）、web服务器（apache）。 |
| （APM） |    支持应用性能历史详情回溯查看 |
|  |    支持如下性能监控参数 |
|  |  支持监控Windows操作系统如下参数：cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数； |
|  |  支持监控Linux操作系统如下参数：一分钟系统负载、5分钟系统负载、15分钟系统负载、cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数 |
|  |  支持监控Mysql如下参数：查询缓存命中率、键缓存命中率、立即获得锁数、连接数、线程数、每秒SQL查询数、每秒发送字节、每秒接收字节； |
|  |  支持监控Oracle如下参数：库缓存命中率、内存排序比率、词典缓存命中率、SGA数据缓存命中率、重做日志缓存命中率； |
|  |  支持监控Apache如下参数：总访问数、写日志次数、每秒发送字节数、长连接数、关闭连接数、空闲活动数、查询DNS数、正在发送数、请求完成数、负载、等待连接数、总数据量、读操作数、工作线程数、空闲线程数、CPU占用率 |
|  |  支持监控应用服务器（tomcat、weblogic）如下参数：活动线程数、堆内存（已用）、守护线程数； |
| 脆弱性管理 |    支持从IBM Rational AppScan导入资产弱点漏洞信息 |
|    支持从安恒明鉴Web应用监测工具导入网站弱点漏洞信息 |
|    支持从安恒明鉴数据库弱点扫描器导入数据库弱点漏洞信息 |
|    支持从NetSparker Web应用扫描器导入网站弱点漏洞信息 |
|    支持从Nessus网络扫描器导入网络弱点漏洞信息 |
|    支持从OpenVAS扫描器导入弱点漏洞信息 |
|    内置73000+条CVE漏洞数据知识库 |
|    内置数十项符合OWASP的Web漏洞数据知识库 |
| 地理安全系统 |    内置GeoSec地理安全子系统，内置世界以及中国安全GIS地图 |
|    支持用地理地图展示来源威胁的趋势 |
|    支持用地理地图展示目的威胁的趋势 |
|    支持在地理地图上标注威胁事件的发生分布 |
|    内置IP地址到经纬度的转换库 |
|    支持以地理信息类进行统计的数据报表 |
|    支持切换Google地图（需要连通互联网） |
| 告警功能 |    可预设置安全告警策略； |
|    支持数据阀值设置，超过阀值将产生告警; |
|    可以通过邮件、短信和屏幕显示进行告警； |
|    支持自动防止报警信息在短时间内大量发送(告警抑制)； |
|    具备报警合并和在一个时间段内抑制报警次数的能力。 |
| 综合查询及报表管理 |    内置合规性报表1000+种； |
|    ★内置SOX、ISO27001、WEB安全等解决方案包 |
|    ★内置完善的等级保护合规报表 |
|    内置综合性自动化审计报告 |
|    支持用户自定义报表； |
|    自定义的报表支持多个统计维度的数据集合。 |
|    支持报表导出为PDF和Word格式文件。 |
| 用户管理 |    根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。 |
|    系统自带自身管理日志 |
|    ★注册用户资产时，提供自动发现识别能力。 |
|    ★提供一键式故障排除功能。 |
|    提供自助式的升级接口，支持对产品升级、规则升级。 |
| 部署方式 |    ★支持分布式部署； |
|    ★支持集中式管理和升级模式； |
|    支持分级管理模式； |
|    采用B/S架构操作方式，无需客户端安装。 |
|    支持监控设备自身CPU、内存、磁盘等工作运行状况 |
| 品牌要求 |    产品获得公安部计算机信息系统安全产品销售许可证以及公安部信息安全产品检测中心出具产品检验报告。所提供的产品检验报告须符合《信息安全技术日志分析产品检验规范》，并提供完整的检测报告复印件（行标三级）； |
|    产品获得国家保密科技测评中心检测并获得涉密信息系统产品检测证书，需符合《涉及国家秘密的信息系统安全监控与审计产品技术要求》，并提供完整的检测报告复印件； |
|    军工资质认证； |
|    产品取得软件著作权登记证书； |
|    原厂商为《国家网络与信息安全信息通报中心》技术支撑单位； |
|    原厂商具有《中国信息安全认证中心》颁发的信息安全应急处理服务资质（一级）； |
|    原厂商获得省级《计算机网络应急技术处理协调中心》颁发的省级网络安全应急响应单位； |
|    原厂商具有信息安全服务资质证书（安全工程类二级）； |
|    原厂商为《中国信息安全测评中心》中国国家信息安全漏洞库共享平台（CNNVD）一级技术支撑单位； |
|    原厂商通过 ISO27001信息安全体系国际认证； |
|    原厂商通过ISO9001 2008质量管理体系认证； |
|    原厂商应具有CMMI3及以上等级资质证书； |
|    原厂商具有云计算安全联盟成员（CSA）证书。 |
| 售后服务支持 |    提供5年免费升级维护； |
|    提供安装调试后1天本地操作培训； |
|    提供24小时支持热线； |
|    本地应急响应时间<=2小时。 |

# 服务

提供原厂三年免费服务，包括软件升级，硬件质保，现场技术支持服务，永久电话支持服务。