**建德市中西医结合医院**

**日志审计系统采购**

一、项目概述

为满足我院信息安全等级保护需求，需采购一台日志审计系统。

二、招标技术要求

1、项目清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 品牌型号 | 规格简述 | 数量 |
| 1 | 日志审计系统 | 明御综合日志审计分析平台 安恒 DAS-LOG-500 | 授权资产数100个；日志处理能力4000-5000EPS；标准2U硬件，CPU：4核4线程/4GHZ 6MB，内存：8G，硬盘：4T\*2（支持raid）， 电源：双电源， 网口：6个千兆工作管理口(1管理口+1HA口+4审计口) ，1个console口，五年硬件维保服务和五年软件升级服务 | 1台 |
| 2 | 漏洞扫描 | 漏扫服务 | 提供安全服务工程师，进行漏洞扫描：使用系统漏洞扫描工具对数据库、操作系统、中间件等进行漏洞、端口、弱口令扫描，扫描完成后由技术人员对漏洞进行确认，提出整改建议，协助开发人员整改。利用专业级WEB应用扫描工具对被评估对象进行应用检测，以发现网站应用层面可能存在的技术漏洞；包括WEB容器识别，如：Apache、tomcat、Weblogic、WebSphere和Ngix等；支持多种服务端语言探测，如：PHP、JSP、ASP、ASPX和.NET等；支持WEB前端框架探测，如：jQuery、Bootstrap、HTML5等；支持WEB后端开发框架探测，如：Django、Rails、ThinkPHP、Struts等； 支持WEB业务应用探测，如：BBS、CMS和BLOG等（备注：逻辑类漏洞主要通过人工渗透测试完成）支持扫描对象包括：B/S架构类应用漏洞，主要包括：SQL注入、XSS跨站脚本攻击、应用系统弱口令、敏感文件下载、后台用户枚举等。 | 2次/年 |

2、技术要求

2.1、日志审计系统

|  |  |
| --- | --- |
| **产品要求** | **详细说明** |
| 硬件要求 | 标准2U硬件，CPU:4核4线程，硬盘≥4T\*2（支持raid），内存≥8G，USB口： USB2.0≥2，网口：管理口≥1，HA口≥1，千兆电口≥4，Console口≥1个， 1+1冗余电源； |
| 性能要求 | 支持100个日志源，可扩展到180个日志处理能力EPS：4000条/秒（峰值：5000条/秒） |
| 日志收集 | 支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。 |
| 支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持阿里云SLS日志的采集。 |
| 日志分析 | 对日志样例可进行划词辅助解析，一键生成正则表达式。 |
| 支持解析规则性能以界面列表形式显示，可了解解析耗时、解析成功或失败次数等信息。 |
| 支持关联规则性能以界面列表形式显示，可了解触发次数、最近一周监控状态等信息 |
| ★三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件（提供产品功能截图与第三方权威机构检测报告）。 |
| 日志查询 | 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。 |
| 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B/S模式管理，支持SSL加密模式访问。 |
| 应用性能监控 | ★通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、硬盘使用率、硬盘使用情况、流量等信息（提供产品功能截图与第三方权威机构检测报告）。 |
| 支持监控Windows操作系统以下参数：CPU使用率、内存使用率、硬盘使用率、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、硬盘总使用率、进程数、线程数。 |
| 告警功能 | 支持硬盘空间阈值告警，当硬盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警； |
| 支持数据阀值设置，超过阀值将产生告警。 |
| 报表管理 | 内置SOX、ISO27001、WEB安全等解决方案包。 |
| 自定义的报表支持多个统计维度的数据集合。 |
| 用户管理 | ★用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户（提供产品功能截图并盖投标人公章） |
| 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。 |
| 资产管理 | 注册用户资产时，提供自动发现识别能力。 |
| ★资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息（提供第三方检测报告）。 |
| 产品能力与资质 | ★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 日志分析产品安全技术要求 GA/T 911-2019》(增强级)，并提供完整的检测报告复印件。 |
| 售后服务要求 | 本项目提供7\*24小时原厂商400支持热线；提供不少于五年质保服务，包含但不限于硬件保修、系统升级等服务内容。最终用户方为建德市中西医结合医院，可以通过设备序列号在生产厂商官方网站或生产厂商400/800电话中进行验证，并可查询维保期限。 |