医院数据中心安全基础设施建设

一、项目背景

医院信息系统作为全院的基础设施系统，承载着全院内部办公、门户网站、门诊、HIS 系统、EMR 系统、PACS 系统、电子病历系统等多种应用。信息系统和数据的安全对用户的日常办公和公众服务起到举足轻重的作用。

近几年，随着信息技术的飞速发展，数字时代来临，给各行各业带来了很多便利，特别医疗行业，借助信息技术，在数据和技术驱动下，向数字化转型。但随之而来的诸如隐私泄漏、数据被篡改、数据勒索等信息安全事件频发，给医疗行业造成了很大的损失，再加上等保 2.0 的合规要求，如何通过优化升级现有网络，保障信息安全，使信息系统稳定安全运行，是下一步的工作重点。

二、内容及数量

2.1 本次产品清单

序号	设备名称	要求描述	数量
1	日志审计系统		1 台
2	运维审计与风险控制系统(堡垒机)		1 台
3	安全主机/服务器深度安全防护系统扩容		1 台
4	安全高级威胁网络防护系统 (防毒墙)		1 台
5	磁带库(离线备份)		1 台
6	安全托管服务		1 年
7	数据库运维服务		1 年
8	F5 原厂维保		1 年

9	安全设备扩容及规则库维保		1 年
10	安全设备硬件第三方维保		1 年
11	专人工程师驻点运维服务、系统集成及机房理线		1 年

2.2 产品技术要求

2.2.1 日志审计系统：1 台

指标项	技术参数及要求
性能要求	支持≥750 个日志源； 日志处理能力 EPS：≥20000/秒（峰值：30000/秒）；
	标准 2U 硬件； 网口≥千兆电口*5（包含管理口*1，业务口*4）； 内存≥32G； 磁盘≥6T*6（raid5）； 电源：双电源；
国产化要求	需采用国产化 CPU 和国产化操作系统。
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。
功能扩展	采用解决方案包上传对产品进行功能扩展，无需代码开发。
	支持 kafka 日志接收转发、大数据安全域同步、APT 沙箱报告转发等大数据联调功能。Kafka 收发支持 SSL 加密。
日志收集	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。
	支持使用代理（Agent）方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导。
	支持的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)、安恒信息、珠海伟思、BEA、电信、安氏、帕拉迪、APC、Arbor、Clam、戴尔（Dell）、Digium 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	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。
	具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。
	内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为 6 大类 50+子类的安全分析场景。
	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。
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（APM）	支持监控设备自身 CPU、内存、磁盘等工作运行状况。
	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、磁盘使用率、磁盘使用情况、流量等信息。
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。
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。
	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。
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。

原厂商授权及质保	合同签订前提供五年原厂商软、硬件保修及服务质保函；设备产品序列号对应最终用户：“医院