

宜宾铭星中医医院

网络安全整改及维护服务项目招标文件

一、标的名称

网络安全整改及维护服务项目

二、项目背景

我院为进一步提升医院综合服务能力和医疗质量水平，根据国家卫生健康主管部门的相关规定和医院发展规划，计划申报升级为二级乙等医院。医院升级评审对信息化建设提出了更高要求，尤其是信息系统安全等级保护需达到二级等保标准。

目前，我院现有信息化基础设施和安全防护体系与二级等保要求存在一定差距，为顺利通过等级保护测评，同时也确保医院信息系统安全稳定运行，保护患者隐私和医疗数据安全，亟需按照《信息安全技术网络安全等级保护基本要求》二级标准，对医院信息化建设进行全面整改建设。

三、招标范围

3.1 技术要求

序号	服务名称	技术要求	数量(单位)
1	边界防护服务	1. 配备 1 台深信服 WEB 应用防护系统服务工具，型号：WAF-1000-FH1300A；性能：网络层吞吐量≥4G，HTTP 应用层吞吐量（WAF）≥300M，HTTP 新建连接数≥6 万，HTTP 并发连接数≥150 万；标准机架式设备，配置≥8 千兆电口+2 千兆光口 SFP(含模块)；提供≥3 年特征库升级服务，≥3 年软件	1 项

		升级服务，≥3 年硬件质保服务。 2. 支持防护 SQL 注入、XSS 攻击、网页木马、网站扫描、Webshell、跨站请求伪造（CSRF）、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 漏洞攻击等。 3. 支持 Cookie 攻击防护，支持检测到篡改时将 Cookie 替换为*，支持自定义需要防护的 Cookie 属性范围，包括防护所有 Cookie 属性、防护指定 Cookie 属性、不防护指定 Cookie 属性。 4. 支持伪静态解析；支持 XML、JSON 格式解析。 5. 支持自定义 BOT 防护排除功能，支持通过 IP 地址白名单、User-Agent、URL 前缀的方式排除。 6. 支持主动防护，学习访问 HTTP 的请求参数，总结出参数的路径、变量名、变量类型、长度范围、支持自定义参数防护。 7. 支持识别和拦截中低频、分布式等高级 WEB 口令爆破攻击方。 8. 支持基于地域维度配置访问控制策略，地址库包含中国大陆及海外地区。 9. 支持 HTTP 应用隐藏，支持过滤如 Server、X-powered-by 类型的 HTTP 响应报文头，支持替换服务器出错页面和替换服务器出错页面。 10. 支持对业务详情进行展示，包括业务存在关键的风险，可以提供具体的攻击链过程并对攻击进行举证。	
2	日志审计服务	1. 配备 1 台奇安信网神日志收集与分析系统服务工具，型号：LAS-R11P-QDFX-PA，性能：配置≥6 个千兆电口，预留≥2 个扩展插槽，≥2TB 硬盘存储，至少配置 60 个日志源授权许可，日志采集处理均	1 项

		值≥2600EPS，提供≥3 年硬件保修，≥3 年软件升级服务。 2. 为更好的响应等保合规检查，产品内置等保大屏展示。等保大屏界面须包含（设备运行天数、日志源数量、原始日志数、关联事件数、告警总数、本地最早日志产生时间、已保存日志天数、平均每天日志存储量、存储空间情况）等 9 大界面效果展示。 3. 支持对资产 IP 地址（含内网 IP）的地理信息进行管理，设置单 IP 及 IP 段行政区及经纬度，支持地图显示。 4. 关联规则触发后能够通过多种方式进行告警，支持发邮件、发送 syslog、短信、企业微信、执行命令使设备协同工作、发送 SNMP Trap 等方式发送告警，并能够在动作中引用事件的属性变量。 5. 具备完善的基于规则的分布式关联分析引擎，能够提供逻辑关联、统计关联和递归关联三种关联分析功能。 6. 日志解析字段内置≥150 个字段，属性字段可扩展，用户可根据审计需要自行创建字段，属性类型包括 IP、字符串、整型、IP、布尔等 15 种，可选择映射函数 8 种可选项等。内置及新增的所有字段均可参与事件查询、关联分析和报表数据源统计。 7. 支持正则表达式、JSON、Key-Value、分隔符 4 种解析方案，支持日志自动化辅助范化。 8. 用户点击事件任意属性字段，支持以该字段为条件对事件进行统计分析，并展示 Top 20 排序，排序支持正序和倒序，并可对统计内容进行点击	
--	--	--	--

		下钻溯源审计数据。 9. 支持以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整。 10. 采用机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别(无须范化)，使审计人员清晰了解采集的日志构成。	
3	防病毒服务	1. 配备深信服统一端点安全管理系统服务工具，型号：深信服统一端点安全管理系统 V6.0（aES），性能：至少提供 150 点 PC 端授权，10 点服务器端授权，提供≥3 年特征库升级服务。 2. 采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能。 3. 提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的恶意文件数量、已拦截可疑行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数。 4. 支持勒索可疑行为检测，通过行为 AI 能力对勒索信、命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截。 5. 支持禁止黑客工具启动，包含：xuetr、ProcessHacker、PCHunter、Mimikatz 等工具的自启动，可以防止黑客攻击。 6. 支持跳转链接至云端威胁情报中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析。 7. 支持对系统账号信息进行梳理，了解账号权限	1 项

		分布概况以及风险账号分布情况，可按照隐。藏账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户。 8. 支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示。 9. 可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好设置高、中、低 3 种防护级别。	
4	运维监控服务	1. 提供运维监控服务工具，至少配备 20 个授权点数。 2. 具备大屏展示功能，可将核心流量、告警统计、资产分布等可视化呈现。 3. 支持监控服务器，网络设备，安全设备、云平台、虚拟机、存储、web 网站、数据库、中间件等。系统能够自动化发现设备，并且自动计算设备之间建立连接的链路两端的接口，并计算该链路上下行速率和利用率，链路容量需要支持自定义修改，满足现场不同情况下各个链路实际容量。 4. 具备资产管理全生命周期管理功能，满足资产自动改密。 5. 具备网络拓扑监控及编辑功能。 6. 具备暴露面管理、等保/密码测评自测评工具。 7. 具备拖拽式流程编排管理功能；具备远程运维处置及操作审计追溯功能。 8. 具备 CMDB 功能及业务拓扑监控能力。	1 项

5	网络优化调整 服务	1. 梳理现网资产：合同签订后，对医院的信息化资产进行分类，详细记录每项资产的具体信息，如硬件型号、系统版本等，并建立维护档案库。 2. 梳理现有网络结构，按照医院要求规划网络，包括调整网段、分配资源和绘制拓扑图等。 3. 使用工具对现网终端设备进行入网检查，确保设备入网合规、流程合规、设备自身安全性合规。 4. 服务工具需支持按设备（设备 IP、设备 MAC、设备组、网段、指定设备）、用户（用户、部门、用户组）、操作系统等配置灵活的入网策略及网络权限，并支持对特殊设备 IP、设备 MAC、设备组、用户、用户组进行准入例外，并提供准入例外设备仿冒检查。 5. 服务工具支持 802.1x 准入功能，未经准入的终端不允许接入网络。要求 802.1x 准入能兼容市场上主流网络设备，包括：Cisco、H3C、华为、锐捷、迈普； 802.1x 准入效果包括：端口拒绝/允许、802.1x VLAN 切换、802.1x 动态 ACL 下发等。支持无线 802.1X。 6. 服务工具支持基于设备 GUID、设备实例路径、显示名称、设备服务名等进行某一类设备进行管控，包括审计与禁止。 7. 服务工具提供轻量级面向对象脚本，实现复杂功能调用或是多种检查功能；支持作为辅助脚本执行定时、循环的机械化操作。 8. 服务工具支持用户与计算机 MAC 地址、接入交换机端口号、接入控制点设备、客户端生成的主机码和随机码绑定；终端硬件唯一 ID、认证用户等进行灵活绑定；支持 1 对 1，1 对多绑定，并支	1 项
---	--------------	--	-----

		持设置针对某用户在一定数量范围内的终端自动放行。 9. 服务工具支持打开敏感文件、指定进程、访问指定应用才会触发屏幕水印，且支持将两种及以上水印方案任意组合；支持屏幕水印仅显示在应用窗口，且能够跟随应用程序移动缩放而自适应移动缩放。 10. 服务工具支持终端入网安装检查，可检查是否安装医院内部要求安装的软件；本次至少提供 10 套服务工具授权。	
6	漏洞扫描服务	服务期内使用专用漏洞扫描工具对系统进行漏洞扫描，扫描完成输出漏洞检测报告及漏洞整改建议，并执行安全加强措施。	1 项
7	防火墙质保升级服务	提供防火墙（型号：AF-1000-B1310，品牌：深信服）维保升级服务，包含： 1. 特征库升级：提供≥2 年特征库升级服务，包括 IPS 特征库、僵尸网络防护库、实时漏洞分析识别库和 URL&应用识别库定期更新服务，并进行定期更新。 2. 现场支持服务：服务期内根据采购人要求提供现场产品技术使用支持、策略优化调整、问题处理服务。 3. 软件升级服务：提供同等或优于现有硬件相匹配的软件版本更新、升级、BUG 修复，提供该软件版本配套的文档资料、用户手册，升级后用户将享有新版本软件的使用权利。 4. 因设备生产厂家为深信服科技股份有限公司，投标人需提供深信服科技股份有限公司出具的针对此项服务的有效授权书，并加盖原厂公章。（需	1 套

		提供授权书复印件，并加盖公司鲜章）。	
8	测评服务	提供 HIS、LIS 两套业务系统测评服务	1 套

3.2 其他要求

依据《中华人民共和国网络安全法》《信息安全等级保护管理办法》的要求，“信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评”。投标人必须确保本项目整改完成后我单位的两套二级系统能够顺利通过二级等保测评（实施时间大约为 2026 年底-2027 年初），并获得第三方权威机构出具的测评报告。

四、投标递交截止时间

2026 年 05 月 21 日前递交（邮寄）至宜宾铭星中医医院采购办，逾期未投，视为自动放弃。

五、投标报价

本项目采用综合单价包干，投标人自报增值税普通发票税率。投标人需提供纸质投标书（正副本各一套，密封）。

投标文件中需明确供货及安装周期，并附质保期后维护费。

六、付款方式

1、前期相关设备到场完成签收后付款 50%，软件及设备安装调试完毕结算办理完成后付款 45%，保证金扣留 5%。（投

标人也可根据最优惠报价提出相应付款方式）。

2、测评费用以甲方通知时间为准，第一次资料提交后付款 50%，测评通过后付款 50%。

七、质保金

结算总价的 5%作为质保金（不包含测评费），质保期内无质量问题，待二级等保通过后，经甲方确认后一个月内无息退还。

八、质保期

1. “边界防护服务工具、日志审计服务工具、防病毒服务工具”质保期为自通过甲方验收合格之日起计算 3 年；

2. “防火墙质保升级服务”质保期为自通过甲方验收合格之日起计算 2 年；

3. “网络优化调整服务、漏洞扫描服务”质保期为自通过甲方验收合格之日起计算 1 年。

九、投标有效期

投标有效期 4 天，投标文件递交后均不退还。

十、联系人及电话

信息科：0831-6885787 18990994447

宜宾铭星中医医院

2026 年 5 月 18 日