**简阳市中医医院**

**信息技术咨询服务（安全运营服务）采购技术参数及商务要求**

一、项目概况

当前我院已部署了安全态势感知、下一代防火墙、终端安全防护软件等安全设备，因此此次安全运营服务团队可选择利用我院当前的网络安全设备接入云端进行服务，也可不采用我院现有网络安全设备，自行提供同等性能指标要求的网络安全设备进行服务。

二、商务要求

1、供应商应对医院≥50个核心信息化资产提供7\*24小时实时网络安全威胁监测预警、事件闭环管理服务、脆弱性分析闭环服务，服务期限1年。实时监测招标方信息化资产的网络安全状态，对安全事件自动化生成工单，及时进行分析与预警，并进行主动闭环。

2、服务方式：提供安全服务团队服务人数不少于5人，其中包含专属安服服务经理1人，服务形式为组建微信群，线下团队配合线上云端7\*24小时值守，遇突发事件必要时，线下团队上门处置。

二、技术服务要求

1、针对医院进行初步安全现状评估，全面梳理漏洞、弱口令、潜伏威胁、安全事件、攻击行为、失陷主机、互联网暴露面等安全现状要求：供应商具备互联网暴露面梳理的服务工具，该工具支持全资产和精确资产两种模式暴露资产收集模式，收集到的暴露面信息至少包括域名、域名标题、IP地址、开放端口、资产指纹、网站截图、移动端暴露面、暴露资产的访问截图、对应暴露资产存在的漏洞等。

2、提供全年不少于12次针对服务内资产进行系统脆弱性和Web漏洞全量扫描，并验证漏洞发生的风险、分析发生后可造成的危害，提供详细的举证信息及可落地建议。针对高危可利用漏洞，要求供应商对服务范围内发现的每一个高危可利用漏洞进行自动化匹配防护规则，且防护率不低于99%。

3、提供全年7\*24h威胁检测和分析，结合医院现有安全设备和工具的告警及日志，对脆弱性、异常流量、攻击日志、病毒日志等数据进行采集和实时分析研判，分析判断受影响范围及是否攻击成功，将分析结果通过服务群或邮件等方式告知用户，同时将各类安全事件自动生成工单，并在工单中展示告警事件的基本信息，涉及用户的业务信息、威胁举证、攻击趋势等内容。

4、供应商应当实时抓取互联网最新漏洞威胁情报和事件情报与医院服务资产信息进行匹配后向医院进行精准推送，及时协助进行安全加固。

5、供应商安全专家每月对医院的安全设备策略进行统一检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。

9、安全专家提供7\*24H在线服务，针对主机发生的安全事件开展调查分析和影响面分析，对发生的安全事件进行人工鉴定和举证分析。对医院网络内服务资产爆发勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，对恶意文件、代码进行根除，辅助采购人快速恢复业务，消除或减轻影响，闭环事件工单。

10、为降低医院因网络安全事件造成的损失和影响，按照国家标准对安全事件的分类分级指南，供应商需按照以下服务指标和要求为医院提供服务：

（1）从安全日志产生到事件通告，重大安全事件通告时间少于30分钟，一般事件的通告时间少于1小时；

（2）高级威胁的处置完成时间少于1小时，一般威胁的处置完成时间少于4小时；

（3）安全事件经过服务人员的确认后，通告给采购人的各类安全事件的准确率不低于99%；

（4）服务范围内的所有安全事件的闭环处置比例达到100%；

（5）满足重大事故启动应急响应机制，工作时间15分钟之内云端专家进行响应，非工作时间30分钟之内云端专家进行响应，2小时上门处置；

（6）对服务范围内发现的每一个高危可利用漏洞提供防护规则，防护率不低于99%。

11、服务交付物要求包括但不限于：

《漏洞清单》&《漏洞举证报告》，报告频率：每月一次

《威胁情报通告》，报告频率：按需触发，不限次数

《安全运营周报》，报告频率：每周一次

《安全运营月报》，报告频率：每月一次

《安全运营季度报告》，报告频率：每季度一次

《安全运营年度报告》，报告频率：每年一次

1. 供应商需为采购人提供服务成果展示门户，具备服务质量可视化展示，采购人能通过可视化的数据，清晰的了解安全专家的服务水平，至少包括：
2. 脆弱性的闭环率、平均响应时长及平均闭环时长；
3. 威胁闭环率、平均响应时长及威胁平均闭环时长；
4. 事件闭环率、平均闭环时长；以验证投标方所承诺的服务指标。

13、供应商云端服务平台应当做好严格的安全防护，并严格按照《信息安全技术—网络安全等级保护基本要求》完成等级保护测评工作，服务平台至少通过等级保护三级测评。

14、为保障服务期内医院对勒索病毒的防护效果，本次服务所依托的服务工具需提供勒索病毒的专项防护能力，能够直观展示勒索病毒防护效果，如已拦截阻止的勒索行为，已成功处置的勒索病毒事件等。

15、为保障服务期内采购人对服务器漏洞恶意利用的防护效果，本次服务所依托的服务工具需具备服务器漏洞防护的能力，云端服务平台针对漏洞的扫描攻击可联动服务组件进行IP记录和封锁。

16、服务需保障采购人业务不受安全事件干扰，覆盖范围包括系统性能问题、数据泄露、病毒攻击及外部侵袭等。响应措施包括：

（1) 快速调配专业工具、设备及人力；

（2）事件发生2小时内专家到场支持；

（3）协同医院定位故障、划定影响范围并实施解决方案以迅速恢复运行；

（4）记录处置全过程，编制应急响应报告，实现安全事件的迅捷管控，保障医院业务连续性。

17、为保证供应商投标响应真实性，医院有权要求供应商在中标后逐条参数进行验证。