四川省第四人民医院网络安全服务项目采购需求文件

1. 项目申请理由

根据《中华人民共和国网络安全法》明确网络运营者安全保护义务（第21条），要求采取技术措施保障网络安全。保障业务连续性，7×24小时威胁监测与自动化响应，降低勒索病毒导致业务中断风险，避免因系统瘫痪延误诊疗。提升数据安全防护，敏感患者数据（如电子健康档案）加密存储与访问控制，减少数据泄露事件。漏洞修复率提升至98%以上（托管服务指标），降低黑客入侵风险。强化应急响应能力，攻防演练实战化支持（如红蓝对抗），缩短安全事件响应时间至分钟级。驻场工程师协同处置，确保本地化快速恢复。

1. 项目既往情况

无

1. 技术服务要求

（一）项目服务要求

1. 对我院至少50个核心信息资产提供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，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：采用线上团队+线下服务进行整体化服务；

3. 需对我院进行安全评估，全面梳理漏洞、弱口令、潜伏威胁、安全事件、攻击行为、互联网暴露面等问题；

4. 需进行核心资产系统脆弱性和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，并提供详细的举证信息及可落地建议，服务商需对服务范围内发现的每一个高危可利用漏洞自动化匹配防护规则，防护率可达到99%；

5. 服务商支持实时抓取互联网最新漏洞威胁情报和事件情报与我院服务资产信息进行匹配后向我院进行精准推送，及时协助进行安全加固；

6. 针对我院安全运维服务，需要定期向我院进行安全服务汇总和报告，其中服务期间交付物要求包括：

（1）《漏洞清单》&《漏洞举证报告》报告频率：至少每月一次

（2）《威胁情报通告》，报告频率：按需触发，不限次数

（3）《安全运营周报》，报告频率：至少每周一次

（4）《安全运营月报》，报告频率：至少每月一次

（5）《安全运营季度报告》，报告频率：至少每季度一次

（6）《安全运营年度报告》，报告频率：至少每年一次

7. 本次服务建设平台需支持与我院现有的主要安全组件进行联动对接（下一代防火墙、上网行为管理系统、态势感知系统），支持实时接收安全组件检测到的安全事件信息、安全日志数据，在发生安全事件时可提供7\*24小时的及时响应和闭环处置服务。

8. 提供运营资产内的挖矿专项检测，需能够综合运用威胁情报、行为关联分析等方式，具体检测发现文件传输(上传下载) 阶段的异常，及时告警挖矿早期的准备动作，实现及时预警。

9. 7\*24小时服务团队

专属服务经理：为用户配置一名经验丰富的安全专家作为专属服务经理。

实时专家咨询：安全专家对用户咨询或上报的安全问题进行及时响应并给出建议，如主机加固建议咨询、安全事件处置建议咨询等。

节假日值守：安全值守专家进行7\*24小时安全监测，对发生的安全事件进行及时响应并在节假日期间每日进行值守总结，在服务群发送值守总结快报。

（二）项目线下驻场要求

1. 服务方式：驻场服务

2. 人数要求：不少于 2 人。

3. 提供安全运维服务。

4. 提供安全运营服务。

5.提供 IT设施运维服务。

6. 驻场人员需按照科室要求进行值班工作。

7.我院现有网络安全设备为：深信服防火墙、深信服EDR、深信服态势感知、深信服探针。

1. 潜在供应商所需特殊资质要求

营业范围：必须包含技术服务，技术开发，安全技术防范系统设计施工服务等技术类经营范围。

1. 商务要求条款

1、服务期限：合同签订所规定的服务时间。

2、服务地点：采购人指定地点。

3、付款方式：合同签订后，通过应急演练、漏洞扫描取得完整的应急演练报告、漏洞扫描报告后支付合同全款。采购人付款前，供应商向采购人开具合法有效的增值税发票，否则采购人有权拒绝付款。

1. 验收标准

参照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）的要求进行验收。

提供服务期间所生成的《漏洞清单》&《漏洞举证报告》《威胁情报通告》

《安全运营周报》《安全运营月报》《安全运营季度报告》《安全运营年度报告》等相关安全报告，全年内未发生重大安全事故则视为验收合格。