**2023年网络安全运维服务项目**

**用户需求书**

## 项目背景

近年来，医疗卫生系统信息安全事故频发，网络安全形势越来越严峻。为落实《中华人民共和国网络安全法》，响应“2023护网行动”要求，根据上级单位文件要求，我院需建立并完善网络安全运营监测预警和应急处置机制，提高网络安全防护和应急处置能力。通过开展漏洞扫描、病毒查杀、渗透测试等安全技术检测和风险评估工作，及时完成系统升级更新，全面消除系统存在的安全漏洞，有效避免网络安全事件。

## 项目建设清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **描述** | **数量** |
| 1 | 安全驻场服务 | 1、提供专职运维服务人员1名，大专及以上学历，半年以上安全服务经验。  2、按照医院的作息时间上下班考勤。  3、驻场人员需经过用户单位面试同意，人员确定后，1年服务期内不得随意变更(除用户方要求变更)。  4、需签订保密协议，在进行服务过程中，必须遵守国家法律法规，中标方及中标方系统服务人员应妥善保管自己的用户权限，如果发生涉密，则承担相应的违约责任甚至法律责任。  5、帮助医院建立从风险的发现，如漏洞、安全威胁等等，通知，整改跟进，整改落实，再次扫描，事件的确认归档等完整的安全事件闭环处理流程；安全设备巡检、故障解决、性能调优等等工作。 | 1项 |
| 2 | 资产梳理 | 针对医院所有生产系统及网络设备、安全设备、终端和移动终端、存储设备、应用系统，利用工具扫描资产，建立台账,通过对现有的网络环境进行资产分类，了解目前的安全现状以及薄弱性。梳理核心资产与边缘资产，核心资产重点防护，建立资产防护基线。对所有对外资产进行探测，梳理出各业务系统的资产信息，关闭对外暴露的多余端口。从而医院能更清晰明了知晓自身资产信息情况。 | 2次 |
| 3 | 制度梳理 | 1、针对医院现有管理制度进行梳理、完善。提供相关模板，让医院有更明确更高效性的管理制度。  2、上级部门检查需要的文档。 | 2次 |
| 4 | 漏洞扫描 | 通过漏洞扫描工具，定期对医院的业务系统、PC、网络设备、安全设备等开展漏洞扫描工作，发现漏洞问题，给出针对性的漏洞修复建议。 | 4次 |
| 5 | 基线核查 | 通过基线核查工具，发现服务器、网络设备、安全设备等 IT 设备自身存在的薄弱环节，并对脆弱性进行识别、分析、修补、检验，消除，降低 IT 设备的高风险隐患，防范安全事件发生，避免信息系统脆弱性被非法利用，增强信息系统安全防范能力，保障业务的可持续性。 | 4次 |
| 6 | 应急演练服务 | 提供应急演练服务，模拟黑客攻击，发起各类攻击事件，防守方检测和发现外部攻击，并对攻击采取相应的防护措施，导演方负责演练导演、监控进程、全程指导、应急处置、演习总结、技术措施与策略优化建议等技术咨询工作。 | 1次 |
| 7 | 安全培训服务 | 提供安全培训服务，通过安全专题培训的学习，进一步提高领导对信息安全工作的重视，加强提升信息安全主管部门专业化工作水平，保障业务连续稳定。 | 2次 |
| 8 | 重点保障服务 | 提供重要时刻安全保障服务，在重大节假日及检查行动中提供重要时期安全保障服务，进行安全保障工作，节假日前进行安全评估。针对如元旦、春节、两会、七一建党节、国庆等重大节假日时期提供重要的安全保障服务，突发紧急信息安全事件上门服务或协助完成市及区、行业等上级主管部门下发的联合检查其他检查指标及要求。 | 1项 |
| 9 | 安全运营托管服务 | 提供安全托管服务，主要是利用安全组件、云端安全运营平台、云端服务专家（即技术+人员+流程）的组合优势，建立7\*24小时的持续、闭环、主动的安全运营体系，帮助用户提前预警，快速研判，精准响应。同时提供安全体系建设规划的数据支撑，为安全建设提供正确的决策因素，提供50个资产授权。 | 1项 |
| 10 | 渗透测试 | 对应用系统模拟黑客攻击进行安全性测试，发现系统存在的安全问题，并对过程中发现的问题及风险提出安全加固建议，推动安全问题整改，并在整改后对应用系统进行复测。 | 25次 |
| 11 | 安全风险评估 | 1.资产识别：通过安全访谈和调研的方式，梳理信息系统资产和业务环境状况；  2.脆弱性评估：通过漏洞扫描、基线核查、漏洞验证等手段，识别业务系统安全脆弱性风险；  3.威胁评估：通过资产所处的环境条件和资产以前遭受威胁损害的情况，和重要资产的脆弱性情况，直接获得重要资产可能遭受哪些具体威胁的破坏，或对一些安全事件表面现象进行分析后，间接获得安全事件背后的威胁；  4.安全整改建议：基于安全评估结果分析信息系统安全风险和威胁，给出针对性的风险处理方案。 | 2次 |
| 12 | 上级安全检查迎检 | 根据卫健委加强网络与数据安全工作实施方案的通知或上级安全主管单位的政策、文件、安全专项检查的指标要求，开展安全自查、技术防护措施和安全整改及本年度的安全迎检工作。 | 1项 |
| 13 | 等保测评整改 | 协助医院重要系统开展网络安全等级保护相关工作，对信息系统的定期情况进行梳理，协助对未定级系统进行定级、备案，配合第三方测评机构对系统进行测评，根据测评结果协助医院进行整改。 | 1项 |
| 14 | 新系统上线安全评估 | 通过上线前的检测工作，对应用系统所覆盖的全部资产再次进行确认识别，完成对应用系统等级保护建设措施落实情况的合规性分析，对应用系统等级保护实施的各项安全措施和管理制度进行全面的风险评估，明确残余风险。 | 2次 |
| 15 | 移动资产攻击面监测订阅服务 | 移动资产SaaS一年订阅服务，包含微信公众号、小程序及暴露链接监测；资产发现；资产风险发现；数据泄漏排查服务。 | 1项 |