|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 技术规格及主要参数 | 单位 | 数量 |
| 1 | 准入控制 | 1.标准机架式设备，配置≥6个千兆电接口，≥2个千兆SFP光口插槽，≥2个万兆SFP+光口插槽，支持≥2个接口扩展槽，冗余电源； 2.整机最大吞吐≥8Gbps，提供≥300点准入授权，最大支持管理≥1000个终端设备，提供三年原厂硬件保修和技术支持服务； | 台 | 1 |
| 2 | 日志审计 | 1.标准2U机架式设备；配置≥6个千兆电接口，≥2个千兆SFP光口插槽，≥2个万兆SFP+光口插槽，支持≥2个接口扩展槽；硬盘容量≥6T SATA\*2 ，配置液晶屏; 2.日志处理性能（平均）≥4000EPS，含≥30个审计对象授权；提供三年原厂硬件保修和技术支持服务； | 台 | 1 |
| 3 | 安全服务 | 围绕医院网络安全综合防御体系，以已有安全组件为支撑，开展安全运维服务管理体系建设，增强医院安全总体防御能力。从业务上线前检测、风险评估、渗透测试、安全加固、安全运维监测、重保值守等维度来完善现有的安全防御体系： 1.业务上线前检测服务：提供信息系统上线运行前的安全检测服务，确保信息系统安全隐患清零上线，并提供检测报告，协助信息系统的漏洞整改和复测工作； 2.风险评估服务：从漏洞、配置弱点两个维度来发现资产的脆弱性，包括漏洞的脆弱性和配置暴露的脆弱性。通过工具自动化扫描与人工检查相结合的方式，发现信息系统服务器操作系统、数据库、中间件、网络及安全设备等存在的漏洞，分析漏洞和配置缺失、评估漏洞风险程度并定期输出整改建议 3.渗透测试服务：在用户允许授权的技术与工具，对某个特定信息系统进行渗透测试，以期发现和挖掘系统中存在的安全问题，然后输出渗透测试报告及修复建议。 4.安全加固服务：提供针对不同厂商的安全设备、网络设备、主机、操作系统、数据库、中间件、以及各种应用系统的配置进行检查，制定安全的配置基线；定期对网络安全设备进行策略的检查、梳理和修正，如防火墙的安全策略有效性及冗余性策略检查，根据业务需求实时进行策略调优，发挥网络安全设备的作用。针对新上线应用系统，进行安全漏洞检查与功能有效性测试，提供新系统安全上线检测报告； 5.安全运维监测服务：对网络设备、服务器、主机系统、应用服务等进行相应的事件监测，并对网络日志、流量进行具体分析，协助完成各项网络安全检查工作； 6.重保值守服务：在重要时期，对网络和重要信息系统提供应急安全保障服务，完成风险摸排、策略梳理、安全监测、分析研判、应急处置等工作； | 项 | 1 |