网络安全卫士功能服务需求

一、7*24 小时安全托管运营服务（共三年）

需求：由服务提供商自行提供或依托我院现有安全监测系统为我院进行 7*24 小时自动化的安全托管运营服务，发现紧急的安全隐患能在十五分钟内及时分析并通知我院信息中心值班人员，同时配合信息中心及时处置安全隐患。

功能：

1、2 次/年的互联网暴露面检测服务，搜集暴露在互联网的 IP、域名、端口等信息。输出《互联网系统台账》

2、2 次/年的重要信息系统漏洞扫描管理服务，对重要系统漏洞进行验证与修复跟踪。输出《系统漏洞扫描报告》

3、7*24 小时/年（含节假日）的服务范围内资产威胁检测与分析服务。对服务内资产提供 7*24 小时威胁监测，分析各项安全隐患，包括勒索病毒攻击、漏洞利用、弱密码、挖矿、Webshell 写入、异常登录、木马回连等安全风险，并通过电话、短信、企业微信、服务号等方式及时告知医院信息中心并协助进行处理。

4、全年的信息系统处置与应急响应服务，并按应急处置结果输出《应急处置报告》。

5、全年的威胁情报订阅服务，同时须提供威胁情报处置办法。

6、含 2 次/年的复盘总结分析服务。

7、全年的网络安全咨询服务。对医院在网络安全相关的问题，能够及时解答，并协助医院进行处置。

8、本次提供的托管运营服务包括医院两个院区内/外网。

二、网络安全保障服务（每年一次，共三年）

需求：依靠安全公司技术力量作为后盾，若医院不能处理的疑难问题，需要专业技术人员协助分析和处理。重点应用在现场应急响应、应急处置、渗透测试、攻防演练值守等方面的安全服务。

功能：每年派驻至少一名专业的网络安全工程师到医院现场进行为期一周的安全值守，协助医院进行网络安全保障工作，包括以下内容：

1、安全分析研判：针对网络攻击告警事件进行深入分析，研判攻击造成危害和影响。

2、应急响应处置：针对入侵成功的行为采取应急处置措施，包括阻断攻击源、阻断远控服务器、隔离下线受害主机等。针对入侵成功行为进行全面回溯分析，查找攻击路径、漏洞利用，并进行业务系统恢复操作，详细记录安全事件处置全过程，记录内容至少应包括：安全事件详细信息、应急处置全流程信息。

3、提供 1 次/季度的现场安全巡检服务，对全院安全设备防护数据进行分析检测，发现隐患风险及时配合医院处置，并提供处置记录。

三、年度安全工作报告

每完成一年的服务需向医院提交年度工作报告，报告内容应包括网络安全评估、数据安全评估、服务开展情况等内容。