**附件1**

**徐医附三院互联网资产渗透攻击测试服务调研详细要求**

# 项目需求

随着医疗信息化的不断发展，医院信息系统承载的敏感数据量持续增长，却也面临SQL注入、勒索病毒攻击、数据泄露等安全威胁。此类风险不仅可能导致诊疗中断、患者隐私泄露，更涵盖了《网络安全法》、《个人信息保护法》等法律法规的合规压力。为构建“事前防御-事中响应”的安全防护体系，保障核心业务稳定与数据安全，本次项目拟提供医院1次5个关键资产的渗透测试服务、4次全面漏洞扫描服务以及2次应急响应服务，服务期限为1年。

# 需求清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务项目** | **服务说明** | **服务次数** | **实施范围** |
| 1 | 渗透测试服务 | 依据相关规范，在保证用户信息系统正常运行前提下，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞。 | 5个资产，1次/年（含复测） | 互联网区域 |
| 2 | 漏洞扫描服务 | 使用专业检测工具和分析技术对核心区域安全设备及业务系统漏洞进行扫描，发现安全设备存在的漏洞，分析漏洞和配置缺失等，并评估漏洞风险程度 | 4次/年 | 互联网区域 |
| 3 | 应急响应服务 | 为客户提供应急响应全生命周期的支持。在安全事件发生之前，可以协助客户建立完备的应急预案并协助进行应急响应演练。一旦发生安全事件，提供及时有效的安全事件响应服务。 | 2次/年 | 数据中心 |

# 服务内容

## 渗透测试服务要求

1、渗透测试服务，是在医院授权的前提下，以模拟黑客攻击的方式，对医院业务系统的安全漏洞、安全隐患进行全面检测，最终目标是查找业务系统的安全漏洞、评估业务系统的安全状态、提供漏洞修复建议。

2、对医院业务系统的渗透测试，除使用产品和工具扫描外，需要进行人工渗透，渗透内容需要对发现的漏洞进行验证和利用。

3、服务频率：5个资产，1年1次（含复测）。

## 漏洞扫描服务要求

1、漏洞扫描实施要求

1）服务商对漏洞扫描的目标对象进行全面梳理和识别，识别内容包含但不限于资产类型、IP地址、责任人、用途、操作系统、数据库等。

2）服务商应提交漏洞扫描工具的情况（包括但不限于：设备厂商、设备型号、漏洞库、销售许可证等）、漏洞扫描工作方案（包括但不限于：目标对象、扫描时间、风险规避措施等）及漏洞扫描申请，被授权后，方可进行。

3）服务商应对漏洞扫描结果进行人工验证，保证漏洞扫描结果的真实性。

4）服务商应提交针对性的解决方案，保证漏洞修复可落地。

2、提供的漏洞扫描工具应具备对高可利用漏洞的管理并具备一键复测功能。

3、服务频率：1年4次。

## 应急响应服务要求

一旦安全事件发生，需要提供迅速和高效的响应服务，包括事件分析、应急处理、系统恢复和后续改进，以最大程度地减少损失和恢复业务正常运作。

3、服务频率：1年2次

## 其他要求

1. 提供日常巡检服务，至少每月1次对医院网络架构及安全设备等进行巡检，输出巡检报告并同步风险隐患；
2. 提供专项保障服务，在重大节假日及客户指定时间，需派驻1名工程师于现场提供技术支持服务和应急响应，保障业务系统安全稳定运行；
3. 提供渗透测试后的漏洞溯源服务：在开展渗透测试的同时，针对已发现的漏洞进行深度溯源分析；
4. 服务请求5分钟内响应，技术团队确保30分钟内抵达客户现场，启动应急处置流程。
5. 提供安全培训服务，提供2次安全意识培训或技术培训，提升全员的安全防护能力和安全意识。

# 公司要求

报名时需准备的材料：

1、营业执照副本；

2、业务人员授权（复印件）；

3、服务商须提供2个近三年以来江苏省内三级医院类似的安全服务案例（附合同复印件）；

4、服务商须具备ISO9001质量管理体系认证证书、ISO20000信息技术服务管理体系证书、ISO27001信息安全管理体系证书、CCRC信息安全服务资质认证证书（信息系统安全运维）、CCRC信息安全服务资质认证证书（信息系统安全集成）。