附件

网络安全运维服务项目技术和商务要求

1. **项目背景**

为保障医院网络安全，需专业的安全团队进行日常安全运维保障服务，包括不限于漏洞检测、渗透测试、补丁安装等，最大程度上保障系统业务的安全稳定运行。

1. **技术参数**

**(一)维保服务基本要求**

1、信息资产管理要求：提供安全工具对院区信息资产进行全面发现和深度识别，包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑，并将信息录入到安全运营平台中进行管理。并在后续服务过程中触发资产变更等相关服务流程，确保资产信息的准确性和全面性。

2、安全设备服务要求：服务期间，应按照三级等保或院方要求的网络安全标准，提供所需的安全设备，若原有安全设备损坏且新设备尚未购买到位期间，提供备用安全设备临时使用。

3、资产安全运营服务：主动对所监控业务做扫描发现，重要网络安全事件和安全漏洞快速预警通告和检测，检测结果第一时间定向推送院方，能够支持电话及微信端实时推送告警信息，并建立安全事件的进度监控机制，提供处置服务。

4、基线配置核查要求：检查支撑信息化业务的主机操作系统、数据库、中间件的基线配置情况，确保达到相应的安全防护要求。检查项包含但不限于帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况。

5、▲提供服务平台要求：

（1）采用的服务平台应基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案，**提供在服务平台申请主动响应的实际界面截图证明。**

（2）采用的服务平台支持对安全事件推送处置和响应建议、处置动作包括缓解措施及建议、通过建议描述、业务影响标签和安全效果标签清晰明确指导下一步响应动作，可一键封禁IP、隔离主机等。支持在线实时沟通离线留言咨询，获取服务提供方技术支持。**（需提供截图证明并加盖原厂商公章）**

（3）采用的服务平台支持最新热点事件视图，对最新热点事件进行时间轴展示，可展现漏洞名称、风险等级、CVE编号、可检测情况，影响资产、威胁标签、爆发时间及风险评估。

（4）采用的服务平台支持查看ATT&CK攻击矩阵攻击命中全景图，可清晰了解安全事件中被黑客技战术利用的情况，可查阅命中技术ID、命中次数、技术描述和参考来源**（需提供截图证明并加盖原厂商公章）。**

6、▲客观的修复优先级指导：投标供应商需提供客观的修复优先级指导，不能以脆弱性危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度**（提供脆弱性优先级排序截图，展示优先级排序情况并加盖原厂商公章）**。

7、▲脆弱性验证服务要求：针对发现的脆弱性问题进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可能造成的危害。针对已经验证的脆弱性，自动生成工单，安全专家跟进修复状态，各个处理进度透明，方便招标方清晰了解当前脆弱性的处置状态，将脆弱性处理工作可视化**（提供服务工具脆弱性工单截图，需展示当前脆弱性的处置状态并加盖原厂商公章）**。

8、▲网络侧服务工具要求：投标供应商所采用网络侧服务工具需具备内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则**（提供截图证明，服务工具应为国产且具备国家信息安全漏洞库兼容性资质证书）**。

9、勒索病毒事件分析：投标供应商需分析判断主机是否感染了勒索病毒；是否已感染勒索病毒文件；根据已发生的漏洞攻击行为分析判断否存在勒索病毒攻击等。

10、挖矿病毒事件分析：投标供应商需分析是否感染了挖矿病毒/木马；是否处于挖矿状态；根据已发生的漏洞攻击行为分析判断是否存在以植入挖矿木马为目的的漏洞攻击等。

11、蠕虫病毒事件分析：投标供应商需确认文件是否被感染，定位失陷的代码并进行修复。

12、针对漏洞利用攻击行为、Webshell上传行为、Web系统目录遍历攻击行为、SQL注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点。

13、失陷主机分析：投标供应商需对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议。

14、潜伏威胁分析：投标供应商需分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出解决建议。含：对外攻击、APT C&C通道、隐藏外联通道等外联威胁行为。

**(二)**★**运维服务人员要求**

投标供应商投入本项目的团队人员应至少设立1名安全技术主管。安全技术主管应具备较强的技术水平及人员管理能力，**具有网络安全方面国家或行业认证证书（投标时提供证书复印件），**负责整个项目的实施组织及协调管理。

现场派驻的1名网络安全工程师，具备两年以上网络安全工作经验，**取得相关资质证书（投标时提供证书复印件），**熟悉网络安全产品使用与维护，对路由器、交换机等网络设备有基本的配置能力。采购单位有权根据派驻人员服务情况，决定是否更换人员。投标供应商在服务期内不得主动随意更换服务人员，如需对服务人员名单做出变更，需提前一个月书面通知采购单位，且更换人员必须满足标书要求，经采购单位书面认可后方可变更。

**（三）安全服务清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **产品/服务** | | **功能简述** | **频次** |
| 安全运维服务 | 互联网暴露面安全评估 | 通过WEB安全扫描设备，对互联网/专网/VPN等网络出口暴露面检测，对互联网暴露的业务系统进行安全漏洞进行安全进行检测。 | 1年 |
| 信息资产管理 | 1.资产发现与识别：借助安全工具对用户资产进行全面发现和深度识别，并在后续服务过程中触发资产变更等相关服务流程，确保资产信息的准确性和全面性。  2.资产信息梳理与管理：结合安全工具发现的资产信息，进行服务范围内资产的全面梳理，并将信息录入到安全运营平台中进行管理。 | 不少于2次/年 |
| 漏洞管理 | 1.通过漏洞扫描工具识别系统安全漏洞，结合多种信息对识别的漏洞进行优先级排序，最后提出切实可行的漏洞修复方案。  2.实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等。  3.提供密码字典，有针对性的进行内网弱口令检测，并将检测发现的问题跟踪修复。 | 1年 |
| 威胁管理 | 1.威胁分析与通告：实时监测网络安全状态，对攻击事件自动化生成工单,及时进行分析与预警。攻击事件包含境外黑客攻击事件、高级黑客攻击事件、持续攻击事件。实时监测网络安全状态，对病毒事件自动化生成工单,及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发DOS型、C&C访问型、文件感染型、木马型。  2.流行威胁通告与排查：结合威胁情报，排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固。办公内网端依据客户工作安排，提供人员现场驻点监测网络安全状态服务。  3.主动分析与响应：每月主动分析病毒类、攻击类、漏洞利用类、失陷类的安全事件，并提供相应解决方案。  4.策略管理：每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于安全水平，针对威胁能起到有效的防护效果。  5.持续攻击对抗：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗。 | 1年 |
| 渗透测试服务 | 1. 由具备高技能和高素质的安全服务人员发起、并模拟常见黑客所使用的攻击手段对目标系统进行模拟入侵。 2. 渗透测试服务的实施过程应符合《GB/T30279-2013 信息安全技术安全漏洞等级划分指南》、《GB/T 28458-2012 信息安全技术安全漏洞标识与描述规范》、《GB/T 30279-2013 信息安全技术安全漏洞等级划分指南》、《GB/T20984-2007 信息安全风险评估规范》、《GB/T 31509-2015 信息安全风险评估实施指南》及行业相关标准规范要求。 | 不少于2次/年 |
| 基线检查/安全加固检查 | 通过该服务避免人为疏忽或错误，或使用默认的安全配置，给业务系统安全造成风险，而制定安全检查标准，并且采取必要的安全检查措施，使业务系统达到相对的安全指标要求。 | 不少于2次/年 |
| 事件管理 | 1.事件分析与处置：实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。  2.针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，快速恢复业务，消除或减轻影响。  3.应急响应：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务，同时还原攻击路径，分析入侵事件原因，指导安全加固、提供整改建议、防止再次入侵。 | 1年 |
| 文档报告管理 | 投标供应商每月需提供巡检报告、分析报告、设备配置变更报告、故障告警及处理报告、事件分析与处置、渗透测试报告、渗透测试过程记录等报告文档，并每季度及年度进行工作汇总报告。 | 1年 |
| 安全督查服务 | 主管部门下发相关安全检查通知后，将协助院方进行相关政策的解读和消化，根据要求准备相关资料并根据文件要求进行自查，不足之处立即整改；在主管部门检查过程中，投标供应商应全力配合进行人员访谈、资料准备；根据主管部门的建议完成整改之后，提交整改报告。 | 按需 |
| 安全应急响应 | 当主机或网络正遭到攻击或发现入侵成功的痕迹，而又无法当时解决和追查来源时。投标供应商应安排专业技术团队提供现场服务解决问题，查找后门、漏洞，保存证据和追查来源，处理包括DDoS攻击事件、主机恶意代码（病毒）攻击事件、网页篡改事件等。 | 按需 |
| 重要时期保障服务 | 重要时期安全保障服务主要针对业务重要IT系统资产，包括主机、应用等系统运行维护场景。针对互联网IT服务业务、IT资产为服务对象，提供重要时期安全保障服务，在重要活动开始至结束期间，提供经验丰富的安全专家至用户现场进行安全值守支持。 | 按需 |
| 应急响应演练 | 通过设定发生的安全事件而进行的以检验应急响应工作、评估应急响应预案为目的的演习和检验行为。 | 不少于1次/年 |
| 安全培训服务 | 从信息安全的基础出发，围绕什么是信息安全、信息安全攻击的常用手段有哪些，以及信息安全中涉及到的标准、协议、技术手段、工具/产品、过程方法等，通过对安全领域和知识的清晰划分和描述，最终能够形成一张信息安全的知识结构图 | 不少于2次/年 |
| 7\*24H在线应急响应 | 当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，提供包括事件检测与分析、风险抑制、问题处置、协助业务恢复的服务，最大化降低安全事件带来的影响。 | 1年 |

1. **商务要求（**★商务要求不允许负偏离**）**

（一）服务时间、地点与方式

1.服务地点：福建省福州市西二环北路156号用户指定地点。

2.服务期：仅限于在本合同签订生效之日起一年内启用，自服务正式上线/启用之日起算服务期限。

3.服务方式：中标供应商免费提供热线咨询、现场指导、远程技术支持、现场故障排除、故障设备维修、系统软件升级、安全运维服务等。

（二）售后服务

1.维保期内：投标供应商须承诺在服务期内提供免费技术支持。

2.投标供应商须承诺履行军事保密义务，在军事行动中提供应急支援保障服务。

3.投标供应商须承诺，全年内电话7天\*24小时响应，驻点保证5天\*8小时/周全年的服务响应。班外时间（含节假日）出现紧急故障，本地维护工程师应在2小时内到达现场进行处理。紧急情况时1个小时内到达现场，非紧急时工作时间与医院同步。

4.日常维护及服务标准：投标供应商应承诺在合同期内提供免费网络安全运维和技术咨询服务。投标供应商必须在福建省有固定售后服务工作站（提供工程师电话和技术维修力量情况和维修的详细地址及联系方式）。

5.投标供应商必须按岗位要求提供参与本项目维保服务的人员名单、证书复印件、投标供应商为其缴纳社保证明。

6.其他服务要求：本项目相关设备及服务应符合军队保密和信息安全要求。

（三）专利权和保密要求

投标供应商应保证使用方在使用该货物（服务）或其任何一部分时，不受第三方侵权指控。同时，投标供应商不得向第三方泄露采购机构提供的技术文件等资料。

（四）付款及结算方式

1.合同签订并生效后，服务满半年后经院方考评质控后14个工作日内医院向中标供应商支付合同款50%，年度服务期满后，中标供应商向医院提交相关维护材料报告，并经过经院方质控考核合格后，无特殊情况下14个工作日内支付合同款的50%，最终支付款必须扣除质控考核扣款。

2.在合同签订生效后，服务满半年支付50%合同款前，中标供应商要求付款应提交下列单证和文件：

（1）金额为有关合同价格50%并扣除质控考评扣款部分后金额的正式发票。

（2）院方出具的半年度质控考评文件。

3.在验收合格后，支付50%合同款前，中标供应商要求付款应提交下列单证和文件：

（1）金额为有关合同价格50%并扣除质控考评扣款部分后金额的正式发票。

（2）院方出具的质控考评文件。

（3）医院需求部门签发的验收合格文件。

（五）验收要求

1.验收标准

按照招标文件技术参数要求、投标人响应情况及采购单位网络安全运维服务的相关要求进行验收。

2.验收程序和方法

服务期满一年后10个工作日内进行验收，验收时需按采购单位项目归档资料清单提供交付成果，包括但不限于以下资料：维保期实施组织过程资产、年度运维总结报告、常见问题及解决手册等。