# 长兴县中医院安全运维服务要求

## 一、配置清单响应要求

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **配置要求** | **数量单位** | **响应名称** | **响应规格参数** | **单价** | **价格（元）** |
| 1 | 安全运维服务 | 详见技术参数要求 | 20个 |  |  |  |  |

备注：以上价格为该项目总价格，包括：1年安全托管服务，软硬件授权、升级及原厂运维服务及质保服务。

## 二、技术参数要求

技术参数响应表

|  |  |  |
| --- | --- | --- |
| **服务类型** | **内容及要求** | **偏离情况** |
| 资产识别与梳理 | ▲运营中心检测服务以保障网络安全“持续有效”为目标，围绕资产、漏洞、威胁、事件四个要素，通过云端安全运营中心和安全专家团队有效协同的“人机共智”模式7\*24H持续性开展网络安全保障工作，与用户一同构建持续（7\*24小时）、主动、闭环的安全运营体系，提供不少于20个核心业务资产的安全托管服务，投标方需提供服务提供商盖章的承诺函证明。  投标方需借助安全工具对招标方资产进行识别和梳理，并在后续服务过程中根据识别的资产变化情况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。 |  |
| 投标方需结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息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；当资产发生变更时，安全专家对变更信息进行确认与更新。 |  |
| 安全现状评估 | 系统与Web漏洞扫描：对操作系统、数据库、常见应用/协议、Web通用漏洞与常规漏洞进行漏洞扫描。 |  |
| 弱口令扫描：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。 |  |
| 勒索病毒事件分析：投标方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。 |  |
| 挖矿病毒事件分析：投标方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。 |  |
| 问题处置 | 投标方需对发现的问题进行处置，包含内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等。 |  |
| 漏洞管理 | ★漏洞扫描与验证：投标方需提供不少于每月一次针对服务范围内的资产的系统漏洞和Web漏洞进行全量扫描，并针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。（需提供截图证明并加盖原厂商公章）。 |  |
| ★漏洞优先级排序：投标方需提供客观的漏洞修复优先级指导，不能以漏洞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（提供漏洞优先级排序截图，展示优先级排序情况，并加盖厂商公章）。 |  |
| 漏洞验证：提供漏洞验证服务，针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的漏洞，自动生成漏洞工单，安全专家跟进漏洞状态，各个处理进度透明，方便招标方清晰了解当前漏洞的处置状态，将漏洞处理工作可视化（提供服务工具漏洞工单截图，需展示当前漏洞的处置状态）。 |  |
| 漏洞修复建议：针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案（提供漏洞修复方案样本，需包含多种修复方案以及修复过程中可能引发的其他问题的解决方案）。 |  |
| 服务催单：针对服务平台生成的工单，招标方可按需催单，用户可在服务平台上采用邮件等方式提醒安全专家加快协助处置，督促投标方第一时间处理（投标方应提供服务平台漏洞工单处置提醒的功能截图）。 |  |
| 漏洞复测：需提供漏洞复测措施，及时检验漏洞真实修复情况。投标方要支持招标方可按需针对指定漏洞，指定资产等小范围进行，降低漏洞复测时的潜在影响范围（提供服务平台支持指定批量漏洞复测与单个漏洞复测的功能截图）。 |  |
| 漏洞状态总览：对发现的漏洞建立状态总览机制，自动化持续跟踪漏洞情况，清晰直观地展示漏洞的修复情况，遗留情况以及漏洞对比情况，使得招标方可做到漏洞的可视、可管、可控（提供漏洞管理功能平台截图，直观展示漏洞管理情况）。 |  |
| 最新漏洞预警与排查：投标方需实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。 |  |
| 最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议，处置建议包含两部分，补丁方案以及临时规避措施。 |  |
| 最新漏洞复测与状态跟踪：由投标方对该最新漏洞建立状态追踪机制；跟踪修复状态，遗留情况。 |  |
| 威胁管理 | 结合大数据分析、人工智能、云端专家提供安全事件发现服务：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态,发现各类安全事件，并自动生成工单。 |  |
| 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、暴力破解攻击事件、持续攻击事件（提供安全事件（如暴力破解）的工单举证截图，需展示当前安全事件的处置状态）。 |  |
| 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。 |  |
| 投标方需针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户。 |  |
| 投标方需每月主动分析病毒类的安全事件：提供病毒处置工具，并针对服务范围内的业务资产使用病毒处置工具进行病毒查杀，对于服务范围外的业务资产，安全专家协助用户查杀病毒。 |  |
| 投标方需每月主动分析攻击类的安全事件：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，当用户无防御措施时，提供攻击类安全事件的处置建议。 |  |
| 服务平台要求 | 支持面向招标方的安全态势展示，展示出当前招标方遭受的威胁事件信息以及脆弱性信息统计，并支持服务专家按照资产类别、威胁类型进行定制化筛选查看，能直观感受到招标方当前的风险态势情况。（提供服务平台漏洞表、事件表统计信息截图，并证明支持按照资产类别、威胁类型进行定制化筛选查看）。  ★为保证安全运营服务效果及质量，要本次投标的边界安全服务工具和安全感知服务工具能够接入长兴县卫生健康局MSS服务平台（需提供截图证明并加盖原厂商公章）。 |  |
| 服务平台支持面向招标方的安全报告与交付物管理，可生成、导出、下载各类安全报告，包括但不限于《安全服务值守日报》、《特殊时期值守报告》、《安全运营周报》、《安全运营月报》。（投标方提供服务平台支持上述交付物管理界面的截图）。  ★所有可导出报告支持按照自定义模块进行导出，可自定义模块必须包括但不限于事件管理、攻击威胁（外部攻击趋势、TOP5攻击IP等）、脆弱性管理（漏洞、弱密码）。（投标方应提供服务平台支持上述服务报告自定义导出的平台功能证明截图，并加盖厂商公章）。 |  |
| 支持展示出当前工单数量和工单处置状态，使得招标方能详细查看服务处置过程，查看安全事件闭环效果，掌握当前专家服务进度，监督服务质量。 |  |
| 支持展示出当前需要招标方审批的工单及其具体情况，使得招标方能完成与服务人员的协同处置，共同确保安全威胁和事件得到准确处置。 |  |
| Use case（安全规则）管理 | 支持自定义配置安全规则，包括配置源算子、解析规则算子、关联规则算子、Flinksql算子、union算子、标签算子、kafka算子、搜索引擎目的算子、自定义算子。通过组合不同算子，形成安全规则。 |  |
| 支持所有安全日志均经过安全规则筛选，生成威胁告警信息。 |  |
| ★投标方服务平台已支持的安全检测规则应超过1000个，且覆盖内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等；（需提供截图证明并加盖原厂商公章）。 |  |
| ★为了保证安全监测的效果，投标方的服务平台应具备检测规则的自定义功能，以满足日益复杂的安全趋势所带来的安全需求（提供服务平台支持检测规则自定义的功能截图，并加盖厂商公章）。 |  |
| 报告中心 | 支持配置报告模板和下载报告文件，报告的类型有pdf格式报告和word格式报告。 |  |
| 支持根据不同场景，灵活选择不同的组件组合形成新的报告模板，以便于招标方查看不同场景和维度的服务报告。可从时间范围，开始时间，结束时间、漏洞攻击，网络流量，恶意攻击，脆弱性等维度组合新的报告模板。下载报告时，选择相应场景的模板进行下载即可。 |  |
| 服务质量监督 | 业务安全状态监控：  投标方需为招标方提供服务监控门户（或用户Portal，区别于安全感知大屏），在门户中招标方可查看业务和资产安全状态信息，使得招标方能直观感受到当前的业务和资产安全状态，展示纬度至少包括服务资产安全评级、服务运营状态及成果、安全风险概览、最新情报。（提供监控门户中业务安全状态监控相关的截图证明）。 |  |
| ★针对医院的安全攻防往往是及时性极高的，因此医院需要拥有能够对安全威胁高效响应的安全服务。投标方需做出书面保证，从安全日志产生到事件通告给招标方的时间方面，按照国家标准对安全事件的分类分级指南，重大安全事件通告时间小于30分钟，一般事件的通告时间少于1小时。  在配备投标方的边界防护设备和终端防护设备的情况下，运营服务对于重大安全事件的遏制影响和处置完成时间小于1小时，对于一般事件的遏制影响和处置完成时间小于4小时，高级威胁和一般威胁的闭环处置比例达到100%。（需提供加盖服务提供厂商公章的SLA承诺函）。 |  |
| ★服务质量监控：  投标方提供的服务监控门户（或用户portal）应具备服务质量可视化展示，投标方能通过可视化的数据，清晰的了解安全专家的服务水平，至少包括漏洞闭环率、漏洞平均响应时长、漏洞平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长，已验证投标方所承诺的服务SLA。  （提供监控门户中服务质量监控相关的截图证明并加盖厂商公章） |  |
| 服务交付物 | 交付物名称：《安全服务运营报告》，报告频率：每周一次  交付物名称：《首次威胁分析与处置报告》，报告频率：一次  交付物名称：《事件分析与处置报告》，报告频率：按需触发，不限次数  交付物名称：《安全通告》，报告频率：按需触发，不限次数  交付物名称：《综合分析报告/运营月报》，报告频率：每月一次  交付物名称：《勒索风险排查报告》，报告频率：每季度一次  交付物名称：《季度汇报PPT》，报告频率：每季度一次  交付物名称：《年度汇报PPT》，报告频率：每年一次  中标后招标方有权要求中标方严格按照上述频率要求提供服务交付物，确保满足招标方安全需求。如中标方未能按时提供，招标方有权终止服务合同，中间产生任何费用由中标方自行承担 |  |
| 服务频率 | 7\*24小时持续专家服务，威胁发现及时响应。 |  |
| 服务资质 | ★为保证云端安全服务能力，投标方所投服务供应商具备CSA CS-CMMI5认证。 |  |

注：响应文件应对照在线询价文件的内容，逐条说明所提技术供参数已对在线询价文件的实质性技术条款（标“▲”的条款）做出了实质性的响应，在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”，并申明与规定一般项目条文的偏离和例外。特别对有具体要求的内容，投标人必须提供所投内容的具体说明，并附相关证明文件。

## 三、技术参数重要指标项响应证明材料

根据技术参数提供对应功能截图或证明材料如下：

## 四、商务要求响应

逐条响应，提供对应商务要求响应材料。

**商务要求响应：**

1. 免费提供网络安全托管服务，配合协调相关安全设备的安装调试及优化，服务必须按采购单位要求完成。
2. ▲响应文件中须提供供应商在长兴县范围内设有实体售后服务网点（公司或分公司），本地化服务须提供网点供应商营业执照副本、纳税证明、社保证明以上相关证明材料。
3. ▲质保期：原厂服务一年，响应文件中须提供原厂针对本项目服务的授权承诺函。
4. 标有“▲”号项的为废标项，不满足会造成在线询价响应文件无效；★项为重要指标项，须提供相应在线询价响应材料。所提供的产品必须符合技术参数中相应的配置、技术参数要求，技术参数要求逐条响应，未满足询价文件中要求的，采购人可取消成交，并报采监部门取消中标资格及追究相应的责任。