## **采购需求**

**（一）、服务总体要求**

★1.供应商为采购人提供信息安全防护服务须原厂服务，服务分为线上与线下服务，并且线上服务与线下服务的安全厂家不能为同一厂家。

2.供应商为本次项目配备漏洞检测工具、安全基线检查工具、自动化渗透测试工具、应急响应工具等服务工具，并确保提供的工具符合国家法律法规的要求，因服务工具产生的纠纷均由供应商自行承担。

3.供应商为本项目服务质量的直接责任方。统筹线上线下安全厂商为采购人提供7\*24小时整体网络安全、系统安全及数据安全的防护保障及应急响应服务。

★4.在服务期限内提供不少于一名工程师在国家法定工作日内的驻场服务。在非工作时间提供不限次数的现场支持服务，技术服务人员到达现场时间不大于1小时，紧急故障要求到位时间不大于30分钟，并提供二线服务团队技术支持。

5.供应商在服务期内须按照服务要求，定期主动组织线上线下安全厂商开展全网段业务系统包含但不限于基线核查、渗透测试、漏洞扫描、攻防演练等安全检测服务。对查找出的安全隐患问题建立台账，跟踪处置结果，形成报告提交采购人。

6.供应商在服务期内须配合采购人完善并输出相关安全管理制度、流程，建立适合采购人的安全防护体系，并严格按照既定的制度、流程，贯穿于安全服务工作中。

7.供应商在服务期内针对采购人现有安全组网架构，及日常安全服务过程中发现的威胁及潜在风险，为采购人输出安全整体且完善的规划方案，为采购人后续安全建设的依据。

8.供应商应依据“医院信息互联互通标准化成熟度测评标准”及“电子病历系统应用水平测评标准”中对网络安全的要求，梳理对标采购人安全建设的不足，配合采购人进行针对性的整改，为相关评级工作提供技术支持。

9.供应商在服务期内须主动配合采购人分析、排查、处置各业务系统运行期间出现的运行卡顿、访问失败、报错等各类系统性问题。确因安全设备或防护策略所导致的影响业务问题，应第一时间组织相关厂商建立专项人员团队，制定科学可行方案（含应急方案）限时处置。形成报告提交采购人。

10.供应商在服务期内须对采购人安全设备及业务资产常态化主动开展包含但不限于整体安全监测、日常运维、全网段业务关系策略梳理、病毒处置、弱口令检测、互联网端业务、资产、域名、端口等安全检测防护保障服务。

11.供应商在服务期内对采购人业务系统检测出的安全隐患确因实际原因无法整改或短期无法整改的，要制定专门安全加固方案及实施方案的工具与技术。保障采购人系统安全运行。

12.供应商在服务期内对每次安全服务与处置进行详细记录，按照每周、每月、每季度、每半年及全年进行工作汇总，主动向采购人按时间节点提供安全防护工作报告，报告内容应以数据支撑为主，详实反映服务期间发生的安全事件、隐患处置等内容。

13.供应商在服务期内须按照采购人信息安全防护实际情况，对专项检查、护网演习、重保防护及应急突发事件等提供专业安全服务团队现场技术支持。针对各类安全事件及通报问题，应准确定位，溯源问题，提出安全可行的处置与整改方案。并根据问题开展全网排查,形成报告提交采购人。

14.供应商对本次安全服务项目组建1支不少于6人安全服务经验丰富的服务团队，分工协作完成本项目中的各项服务，项目团队中不少于1名项目经理负责服务期内全过程安全服务保障工作、不少于1名高级渗透测试工程师、不少于1名信息安全运维工程师、不少于1名数据安全工程师，不少于1名安全设备运维工程师、，不少于1名网络设备运维工程师确保项目的顺利实施。

15.供应商在服务期内因服务缺陷导致采购人服务范围内的资产发生网络安全事件时，采购人有权要求供应商赔偿该事件给采购人直接造成的生产中断损失、数据恢复费用、第三者责任、应急响应损失、网络勒索损失，赔付金额不得低于20万人民币，**须提供承诺函。**

16.供应商在服务期间内，提供包括但不限于以下汇报材料并根据技术服务要求提供相应的技术文档：《全网拓扑结构图》《分析与处置报告》、《漏洞管理举证报告》、《漏洞清单》、《服务资产表》、《安全服务运营报告》、《应急响应报告》、《事件分析与处置报告》、《安全策略表》、《安全通告》、《季度汇报PPT》、《年度汇报PPT》。所提供数据必须真实准确。

17.供应商在服务期内须根据采购人工作需要，配合提供各类临时性安全保障服务。

**（二）、技术服务要求**

2.1 线上服务

2.1.1连续性安全保障（7\*24小时）

为采购人不少于50个核心资产（数据中心资产IP数量）提供7\*24小时连续性的安全保障。不论是白天、黑夜、节假日供应商须应做到7\*24小时在线服务，配置一名经验丰富的安全专家作为专属服务经理，并组建专属服务群，实时响应采购人咨询的网络安全相关问题。

2.1.2服务保障要求

1）分析研判通知时效：从安全日志上传分析研判到通告给采购人的时间方面，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15分钟，一般事件的通告时间少于30分钟；

2）遏制影响时效：在配备的边界防护服务设备和安全防护软件的情况下，重大威胁与事件的遏制影响完成时间少于15分钟，一般威胁与事件的遏制影响完成时间少于30分钟；

3）安全事件经过原厂服务人员的确认后，通告给采购人的各类安全事件的准确率不低于99%（即误报不能超过1%）；

4）供应商应当承诺，服务范围内的所有安全事件的闭环处置比例达到100%。

5）须满足重大事故应启动应急响应机制，工作时间15分钟之内云端专家进行响应，非工作时间30分钟之内云端专家进行响应，2小时上门处置。

6）在具备供应商的边界防护设备的情况下，要求线上供应商可以对服务范围内发现的每一个高危可利用漏洞提供防护规则，并且承诺防护率达到99%。

7)事件闭环时间：经采购人授权后，供应商及原厂服务人员协助进行安全事件的闭环，一般安全事件的闭环完成时间少于8小时，重大事件的闭环完成时间少于24小时。

2.1.3安全现状评估

1）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。

2）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。

3）应使用扫描组件对资产开展暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险。

4）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。

2.1.4脆弱性管理

1）漏洞扫描与验证：针对服务资产的系统漏洞和Web漏洞进行全量扫描，并针对发现的Web漏洞进行验证，验证漏洞的真实性及分析发生后可造成的危害。

2）漏洞修复优先级排序与通告：基于漏洞扫描结果、资产重要性及漏洞的威胁情报，对漏洞进行重要性排序，确定修复的优先级；并将最终结果通告给采购人。

3）漏洞可落地修复方案：对漏洞进行分析并输出可落地的修复方案，通过工单系统跟踪修复情况。

4）高可利用漏洞防护：支持一键防护扫描组件发现的高可利用漏洞。

5）漏洞复测与状态追踪：对修复的漏洞进行复测，及时更新漏洞工单的漏洞修复状态。

6）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。

7）针对安全组件收集的弱密码流量及日志进行分析验证，有针对性的进行内外网的弱口令检测，并将检测发现的问题通过工单系统跟踪修复状态。

2.1.5威胁管理

1）7\*24小时威胁鉴定：线上供应商依托于安全能力平台的大数据分析和威胁检测能力实时监测用户网络安全状态，对平台监测到的安全威胁进行分析鉴定，识别到真正的安全事件。

2）精准威胁情报推送：实时抓取互联网最新威胁情报与详细资产信息进行匹配，对最新威胁情报进行通告与排查。

3）可针对内/外网或特定业务系统及特定漏洞，基于采购人业务定制检测逻辑，尽可能快地发现漏洞或攻击痕迹，发现潜在的安全隐患和已失陷的主机/被钓鱼成功的员工/账密信息泄露等，最大限度地降低攻击者造成的危害，评估造成的损失等内容，最终帮助采购人验证风险并推动发现的问题和隐患进行闭环处理

4）策略检查：对安全组件上的安全策略进行统一检查，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。

5）策略调优：根据安全威胁/事件分析的结果以及处置方式，按需对安全组件上的安全策略进行调整工作。

2.1.6安全问题处置

1）提供7\*24小时威胁分析和鉴定服务，安全告警上传至服务平台依托于平台的大数据分析和威胁检测能力实时监测用户网络安全状态，对平台监测到的安全威胁进行分析鉴定，自动生成服务工单，识别到真正的安全威胁。

2）提供7\*24小时的响应机制，应对采购人咨询或上报的安全问题进行及时响应并给出建议，如主机加固建议咨询、安全事件处置建议咨询等，响应时间不得超过30分钟。

3）7\*24小时威胁鉴定：分析研判包括但不限于对脆弱性、异常流量、攻击日志、病毒日志等数据进行采集和实时分析研判，支持将同一资产的多个告警进行聚合分析发现各类安全事件并生成工单，并在告警详情中展示告警的基本信息，涉及的业务信息、攻击趋势、威胁详情、攻击原理、处置建议等内容，并支持根据采购人情况提供备注。

2.1.7服务要求

为采购人提供的服务成果展示门户；具备服务质量可视化展示，能通过可视化的数据，清晰的了解供应商的服务水平，至少包括脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、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，以验证供应商所承诺的服务指标（或称为服务SLA）。**提供服务成果展示门户中服务质量监控相关的截图证明。**

2.1.8综合人工服务

1）梳理采购人现有的信息安全管理体系现状，包含组织架构、制度文档、业务流程等；梳理采购人当前的网络架构与安全现状，包含网络拓扑、安全设备、安全措施等；梳理采购人业务清单、重要程度及等级保护要求等.

2）结合采购人安全基线标准，对被评估对象进行配置规范检查，通过与标准基线比对，发现配置层面的安全隐患。

3）对漏洞扫描结果，在与采购人进行沟通确认之后，对其中部分漏洞进行验证确认，并协助用户进行加固。（数据库、核心应用服务器等联系相关厂商人员进行处理）。

4）根据操作系统安全评估及漏洞扫描、安全检测、日志分析和配置检测中发现的问题，对服务器、网络设备、数据库系统等安全漏洞进行修补，加强安全配置、安全加固处理。

5）勒索预防服务：每半年开展勒索病毒风险排查，协助采购人进行勒索隐患加固，快速识别勒索病毒风险并做好加固工作，确保勒索风险全面可视，提高勒索病毒免疫力。

6）处置勒索病毒、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。

7）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，指导并进行安全加固、提供整改建议、防止再次入侵。

8）安全防护巡检：从整体安全防护体系分析业务系统防护策略，包括但不限于网络设备、主机设备、安全设备等。

9）安全设备巡检：对网络中的安全设备进行状态检查、策略调优、系统备份。

10）持续升级巡检：持续优化防护模块，不断协助采购人更新设备安全等特征库和软件版本。

2.1.9安全设备对接与数据采集

1）供应商提供的线上安全托管服务云端平台应当支持对接采购人的主要安全设备，包括互联网出口防火墙、安全态势感知等，支持实时接收安全设备检测到的安全事件信息、安全日志数据提供7\*24小时的服务；

2）提供安全托管服务云端平台支持对接的上述安全设备的能力证明，展示详细的对接步骤。

3）安全托管服务云端平台须做好严格的安全防护，并严格按照《信息安全技术—网络安全等级保护基本要求》完成等级保护测评工作，服务云端平台至少通过等级保护三级测评。

**2.2 线下服务**

2.2.1资产安全运营与安全体系建设服务

针对采购人的互联网、前置区、内网及公共区域电子信息设备等区域，具实提供基础信息调研、暴露面资产梳理、全网现状分析、安全策略梳理等服务；对采购人的网络安全管理体系和网络安全技术体系分别提供安全管理制度建设咨询和数据安全体系建设咨询等服务。

2.2.2基础信息调研

1）服务内容：采用资产探测工具与技术，针对采购人信息系统涉及的资产进行周期性识别，同时对各类资产服务端口现状进行嗅探与分析，结合服务工程师调研补充信息，最终完成资产底图绘制，形成清晰可见的资产分布、服务端口状态、及维护管理信息于一体的IT资产安全状态库。资产状态库中包括但不限于：设备型号、设备功能、互联情况、资产使用年限、资产所有人等相关信息。

2）服务范围：互联网、前置区、内网

3）服务周期：服务周期12个月，服务期内不少于2次。

4）交付成果：《资产状态库》

2.2.3暴露面资产梳理

1）服务内容：结合业务系统暴露面系统开放情况，开展互联网暴露面摸底分析，从暴露面资产IP地址、域名、端口、承载业务、承载网络、互联关系等方面，全面识别暴露面资产面临的威胁实况，明确主管部门与责任人，持续做好互联网暴露面收敛工作，进一步降低互联网暴露面风险。

2）服务范围：互联网

3）服务周期：服务周期12个月，服务期内不少于12次。

4）交付成果：《暴露面资产跟踪表》

2.2.4全网现状分析

1）服务内容：对采购人机房及网络环境进行资产调研与评估，对采购人目前全局网络进行分析，包括网络现状、设备位置、互联情况、安全域划分、边界防护情况等。

2）服务范围：互联网、前置区、内网

3）服务周期：服务周期12个月，服务期内不少于4次

4）交付成果：《机柜位置图》、《网络拓补图》

2.2.5安全策略梳理

1）服务内容：对安全设备策略进行梳理和分析，梳理访问控制策略，确保服务器IP及端口访问控制列表、防火墙NAT和过滤策略符合最小化白名单原则，关闭一切不必要的对外开放服务。

2）服务范围：互联网、前置区、内网

3）服务周期：服务周期12个月，服务期内按需提供

4）交付成果：《策略清单表》

2.2.6安全管理制度建设

1）服务内容：依据网络安全相关法律法规、安全管理体系标准规范及医疗行业最佳实践，梳理当前安全管理制度体系，识别安全管理风险点，提供体系优化建议，协助采购人建立完善的网络安全管理体系，建立体系动态改进机制。

2）服务范围：采购人网络安全管理体系

3）服务周期：服务周期12个月，服务期内按需提供

4）交付成果：《安全管理制度报告》

2.2.7数据安全体系建设

1）服务内容：从网络安全架构建设、数据安全技术体系建设、密码安全技术建设等方面开展系统分析，结合采购人实际情况，识别安全需求、分析威胁与风险、设计全局体系框架，协助采购人建立全面的网络安全防御体系。

2）服务范围：采购人网络安全技术体系

3）服务周期：服务周期12个月，服务期内按需提供

4）交付成果：《数据安全报告》

2.2.8安全检测服务

针对采购人涉及的重要业务系统开展安全基线合规检查、安全漏洞治理工作；针对经过采购人授权的系统及相关资产开展安全渗透测试工作。

1）安全基线合规

服务内容：通过全局信息系统风险点安全核查为采购人提供丰富完整的信息系统风险点风险与分析报告；提高信息系统整体脆弱识别能力；依据核查结果与采购人的业务模式特点，提供针对有效的安全处理方案，避免信息系统危害持续增加，到达可知、可控管理风险的安全目的，满足采购人信息业务系统脆弱核查需求，最大限度降低采购人信息系统安全运营成本。

服务范围：采购人涉及的重要业务系统

服务周期：服务周期12个月，服务期内按需提供

交付成果：《安全基线合规核查报告》

2）安全漏洞治理

服务内容：对业务系统相关资产开展漏洞检查工作，检查是否存在系统漏洞，将发现问题及时发送系统负责人，并跟进漏洞整改完成情况，验证漏洞修复效果。

服务范围：采购人涉及的重要业务系统

服务周期：服务周期12个月，服务期内按需提供

交付成果：《漏洞检测报告》、《漏洞跟踪表》、《漏洞修复确认表》

3）安全渗透测试

服务内容：对于采购人涉及的相关资产开展渗透测试工作，采用人工+工具方式完成，通过黑盒和白盒两种方法进行全方位检查。对新发现资产开展渗透测试检查，规避可能存在的风险。

服务范围：限于经过采购人授权的系统及相关资产

服务周期：服务周期12个月，服务期内按需提供

交付成果：《渗透测试报告》、《渗透测试复测报告》

2.2.9安全运维

1）风险预警通告

服务内容：通过各种形式收集网络安全风险情报，向采购人提交最新的操作系统漏洞、最新病毒信息、最新安全威胁等情报信息，提供及时准确的网络安全动态和黑客可能使用的攻击方法。同时提供更精确、准确、及时的安全预警及应对解决方案。

服务范围：包括产品安全通告、全球重要厂商安全通告、操作系统安全通告、知名应用系统安全通告、知名安全组织的安全通告，提供最新的安全形势报告、安全攻击报告、安全漏洞报告、安全事件报告，提供最新关于安全病毒、安全漏洞的预防建议和补丁下载地址，信息安全监管要求（及时通告国家及监管部门对行业的最新要求）

服务周期：服务周期12个月，每周向客户发送安全通告

交付成果：《安全风险预警通告》

2）日常安全评估

服务内容：对采购人信息系统进行漏洞扫描、基线核查，挖掘系统web层面、服务器层面的安全隐患及公共区域电子信息设备安全隐患进行全面排查。并提出对应的修复建议或解决方案。同时包括APP、小程序、新上线业务系统等安全评估。

服务范围：采购人涉及的重要业务系统

服务周期：服务周期12个月，服务期内按需提供

交付成果：《安全风险评估报告》

3）威胁分析与风险审计

服务内容：每月对信息系统内安全设备进行一次风险审计与威胁分析，主要对硬件信息、设备状态、威胁日志、运行数据、安全日志等数据进行统一采集、整理和分析，识别潜在威胁和隐蔽风险，最终输出审计月报。

服务范围：安全设备

服务周期：服务周期12个月，服务期内不少于12次

交付成果：《威胁分析与风险审计月报》

2.2.10安全保障服务

1）重大节假日保障服务

服务内容：在重大安全事件、重大节日、事件或活动前期（或期间）进行保障服务；分析各类安全设备产生的安全事件或日志信息，获取攻击中存在的各类病毒、蠕虫、非法访问、攻击事件，并进行及时的处理。根据安全风险和安全问题情况有针对性地采取措施，帮助整改解决问题，及时进行策略调整和优化降低风险。

服务范围：全院信息化系统，按需保障

服务周期：按需提供

交付成果：《安全保障总结报告》

2）实战化攻防演习

服务内容：根据实际情况完成攻防演练方案编写，通过演练方案指导攻防演练工作的开展（包括前期隐患排查、风险处置加固、安全意识提升与评估、监测值守保障、应急处置、总结分析等），确保演练工作的效果。

服务范围：全院信息化系统，攻防演习

服务周期：服务周期12个月，服务期内不少于2次

交付成果：《攻防演练方案》

3）安全事件应急响应

服务内容：当发生安全事件时，及时了解攻击相关技术环节内容、攻击者的来源，取得相关现场的数据证据，同时需与采购人确认核实是否对业务产生影响。在发生安全事件时，第一时间处理并联系相关支撑团队，抵达现场，保障采购人网络安全。涉及的工作环节包括：1、接到事件报告；2、根据事件级别进行不同级别的响应方式，包括电话、现场等；3、协调其他外部资源进行处理；4、编制应急响应情况报告，说明事件原因、处置措施等。

服务范围：全院信息化系统，按需提供

服务周期：按需提供

交付成果：《应急响应报告》

**★2.3技术服务要求需提供线上及现场原厂安全服务承诺函。**