广州市黄埔区中医医院2025-2026年度网络与数据安全运维和三级等保测评服务项目需求明细

（一）技术要求-★oracle数据库运维服务

序号	服务内容	详细参数
1	基础运维服务	定期（每月至少一次）对招标方 oracle 数据库全资产巡检并出具巡检报告。
2		数据库故障排查及优化： 提供 7*24 小时应急响应服务，接到故障起 5 分钟有效响应，对于一般故障提供远程服务，如远程无法解决时需要 1 小时内到场服务，2 小时解决问题。重大故障 5 分钟有效响应，30 分钟内到场服务，1 小时解决问题。其次根据故障现状，针对性为招标方提供数据库优化方案，从根本上解决问题。
3		根据招标方需求创建数据库存储结构、数据库对象，在必要时，在保证数据安全的前提下协助优化数据库的存储，制定数据库备份和恢复应急预案，在医院数据出现突发情况时，能及时进行数据恢复处理。
4		根据招标方实际需求提供数据库迁移服务。

（二）技术要求-远程安全托管运营服务

序号	指标项	详细参数
服务	政务云平台主机37台、院内数据中心服务器13台，合计需实时监测的服务资产50台。	

▲1	服务基本要求	提供 1 年的线上安全托管运营服务，为招标方提供 7*24H 的安全值守，扩展持续有效的安全运营能力,保障可承诺的风险管控效果。中标方提供的线上服务平台应当支持对接及联动招标方网络中已部署的主要安全设备，包含下一代防火墙、安全态势感知和终端 EDR,通过实时接收安全设备检测到的安全事件信息和安全日志数据，为招标方提供精准有效的安全运营服务。（需提供加盖中标方公章的承诺函）
2	服务内容要求	资产识别和梳理：中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。
▲3		暴露面梳理：中标方应提供安全工具对医院服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，实现对暴露面资产可管可控，降低暴露面资产产生的风险。服务工具应当支持以机构为单位的全资产收集和以具体目标为单位的精确资产收集两种模式，收集到的暴露面信息需覆盖域名、域名标题、IP 地址、开放端口、资产指纹、移动端暴露面等维度，确保暴露面梳理工作的有效性和全面性。（需提供服务工具具备以上暴露面梳理能力的证明截图）
4		高危可利用漏洞防护：针对服务范围内资产扫描到的高危可利用漏洞，中标方应当为招标方做好每一个高危可利用漏洞的防护工作，包括但不限于为招标方提供漏洞修复方案和安全设备防护策略，以及帮助招标方配置防护规则，保证招标方不因此出现重大事件和损失。
5		脆弱性验证：提供脆弱性验证服务，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造成的危害，将脆弱性处理工作可视化。

▲6		脆弱性复测：中标方需提供脆弱性复测措施，及时检验脆弱性真实修复情况。招标方可按需针对指定脆弱性问题，指定资产等小范围进行，降低脆弱性复测时的潜在影响范围。（需提供脆弱性复测功能的证明截图）
▲7		漏洞修复优先级排序：中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，还应考虑资产的重要性以及威胁情报（漏洞被利用的可能性）三个维度。（需提供漏洞优先级排序功能证明截图）
8		中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、微信等方式告知招标方。
9		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招标方可以在平台上直接发起服务咨询，线上服务人员进行紧急响应和处置。
10		中标方需为招标方提供服务成果展示界面，应具备服务质量可视化展示，招标方能通过可视化的数据，清晰地了解安全专家的服务水平。
11		中标方应面向招标方提供定期的勒索病毒入侵风险专项排查，中标方应按照勒索预防检查表开展勒索风险评估，勒索预防检查表应当包含勒索高危利用漏洞、端口、安全策略、勒索攻击行为几个维度。
▲12		中标方需为招标方提供移动端服务过程展示界面，支持实时直观地查阅服务的每日运营动态。运营动态需包括事件通告、威胁通告、威胁情报、服务报告、夜间值守快报等，并支持自定义进行筛选和管理。（需提供移动端服务过程展示界面中支持查阅每日运营动态的截图证明）

▲13		中标方需为招标方提供移动端服务过程展示界面，支持直观地查阅服务推送的各种安全事件/威胁的详细专家审核研判过程,需包含安全事件详细的基本信息、入侵路径、影响主机、主机调查、数据包分析等内容。（需提供移动端服务过程展示界面中支持查阅服务推送的各种安全事件/威胁的详细专家审核研判过程的截图证明）
▲14		中标方需为招标方提供移动端服务过程展示界面，通过可视化数据统计的方式，让招标方了解当前待办事项、运营成果，从安全日志、告警分析、事件/威胁分析、漏洞分析、风险资产分析 5 个维度，进行安全风险可视化呈现，搭配 GPT 解读，让招标方全方面了解当前安全运营成果。（需提供移动端服务过程展示界面中支持展示当前待办事项、运营成果以及对运营成果的 GPT 解读的截图证明）
▲15		中标方需为招标方提供移动端服务成果展示界面，支持将漏洞管理的结果通过邮箱分发给相应的业务责任人，支持分批发送和统一发送两种方式。（需提供移动端服务成果展示界面中支持发送漏洞管理结果到相应业务责任人的截图证明）
▲16		服务平台应具备钓鱼演练工具，需支持自定义钓鱼邮件模板、批量发送邮件、攻击过程沉浸式大屏展示、演练对象风险操作跟踪（风险操作清单、用户画像）、演练日报统计等。（需提供安全托管服务钓鱼演练能力项的证明截图）
17		要求中标方为招标方提供的服务成果展示界面可以直观地管理服务过程中生产的服务报告和交付物，包括但不限于《项目启动会 PPT》、《首次安全风险分析报告》、《威胁情报》、《安全运营周报》、《安全运营月报》、《安全运营季报》、《年度总结汇报》等。

▲18	服务指标要求	为了降低招标方因网络安全事件造成的损失和影响，中标方应当按照以下服务指标和要求为招标方提供服务（需提供加盖中标方公章的承诺函）： （1）分析研判通知时效(MTTA)：从安全日志上传分析研判到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 15 分钟，一般事件的通告时间少于 30 分钟； （2）遏制影响时效(MTTC)：在配备中标方的边界防护服务组件和端点防护服务组件的情况下，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）事件闭环时间(MTTR)：经招标方授权后，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。

（三）技术要求-风险评估服务

序号	技术类型	详细参数
服务资产		政务云平台主机、院内数据中心设备及单位（含各分门诊）网络设备、安全设备、终端计算机，含数据库、中间件等。
1	服务频次	定期（每年一次，共 1 次）。
▲2	预警通报服务	定期和在需要的时候提供漏洞预警信息，安全通告预警信息包括最新的安全漏洞，病毒，安全补丁以及最新的入侵手法等。
3	资产识别	依据相关国家标准或国际标准，对招标方的信息资产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、业务部门、责任人、用途、操作系统、数据库、中间件等。 资产识别方式包含但不限于：自研工具扫描探测、人工访谈调研和实地核查等。 资产类别应按照相关规范分类，包含但不限于以下几大类： 业务应用—业务信息系统，如 HIS 系统、OA 系统等 网络结构—网络拓扑结构图。 文档和数据—业务信息系统相关文档、数据

		库数据、设计方案、操作手册、业务数据等。 软硬件资产—服务器设备、安全设备、存储设备、应用软件、操作系统、中间件、数据库、网络设备等。 物理环境—机房。 组织管理—方针、规章制度等。 人力资源资产--组织架构、岗位职责等。 依据相关规范，中标方应根据资产识别结果，科学、合理地对资产进行重要性赋值，明确资产价值。 中标方应针对资产识别情况及问题及时汇报。
4	脆弱性识别	依据相关国家标准或国际标准，根据资产识别结果，采用不同手段对资产进行全面的脆弱性识别，及时发现、处置脆弱性，避免或降低脆弱性被威胁利用的几率造成的影响。 脆弱性分类应至少包括但不限于以下三类： （1）技术性弱点—系统、程序、设备存在的漏洞或缺陷，如网络结构设计问题和代码漏洞。 （2）操作性弱点—软件和系统配置、操作中存在的缺陷，包括人员在日常工作中的不良习惯，审计和备份的缺乏。 管理弱点--策略、程序、规章制度、人员意识、组织结构等方面的不足。 （3）脆弱性识别方式包含但不限于:自研工具自动探测、人工访谈调研、文档审阅和实地核查等。
5	威胁识别	依据相关国家标准或国际标准，对存在脆弱性的资产进行威胁的全面识别，及时发现潜在威胁的原因，避免或降低威胁发生的概率。 威胁来源应至少包括但不限于以下四类： 人员威胁——包括故意破坏和无意失误。 系统威胁——系统、网络或服务的故障。 环境威胁——电源故障、污染、液体泄漏、火灾等。 自然威胁——洪水、地震、台风、滑坡、雷电等。 通过技术手段识别服务器中可能存在被植入的后门程序、潜伏未触发的病毒木马等安全威胁。 中标方应对威胁利用率极高的风险提出整改建议，配合招标方及时处置。

6	防护能力评估	依据相关国家标准或国际标准，对招标方现有的防护能力进行评估，评估内容包含但不限于： 预防控制措施情况，如：已有安全策略和防护程序情况、软件版本和补丁管理、安全域和访问控制、管理体系建设及落实、安全意识培训等。 检测控制措施情况，如：网络入侵检测能力、主机入侵检测能力、安全事件报告流程。 响应控制措施，如：应急响应机制、系统备份与恢复机制、安全事件响应能力等。 根据识别结果的现状，提出建设性意见，避免重复采购相关设备或服务。
7	风险分析	中标方应组织专家团队，对存在和潜在的风险进行全面分析，保证风险分析的科学性、合理性及风险处置的可操作性。 中标方应在风险分析完成后，组织召开相关会议，将风险评估实施过程全生命周期发现的情况或问题统一反馈，并提出可落地的建议或方案。
8	可落地建设方案	根据资产识别、脆弱性评估、威胁评估、防护能力评估的输出结果进行风险分析之后，通过自研平台输出风险评估报告，风险评估报告中应符合业务需求的安全整改建议。
9	服务交付物	《安全风险评估报告》 《安全建设方案》

（四）技术要求-漏洞扫描服务

序号	服务类型	详细参数
服务资产		政务云平台主机、院内数据中心设备及单位（含各分门诊）网络设备、安全设备、终端计算机，含数据库、中间件等。
1	服务频次	定期（至少每季度一次）。
2	服务内容	（1）资产梳理：梳理需要保护的业务系统，IP，域名并形成资产信息梳理表，并录入系统。 （2）漏洞扫描：针对通用 web 漏洞扫描、系统漏洞扫描、数据库漏洞扫描；针对检测网站源码、数据库备份文件、SVN 文件、系统

		重要配置、日志文件向外网泄漏行为进行信息泄漏检测。针对受保护的业务资产提供弱口令的探测服务，内置包含通用性字典弱口令探测，行业性字典弱口令探测。 （3）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。 （4）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）。 （5）漏洞通告：中标方需要提供真实的漏洞信息以及紧急漏洞通告，方便招标方清晰了解当前漏洞状态。 （6）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。 （7）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。复测措施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（提供服务工具复测功能截图） （8）漏洞状态追踪：对发现的漏洞建立状态追踪机制，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） （9）漏洞报告：中标方需提供阶段性提供漏洞管理报告，报告中需直观展示服务效果、下一步工作计划以及漏洞处置建议。
3	服务交付物	每月提交《漏洞管理服务报告》、《漏洞扫描报告》、《漏洞分类处置方案》。

4	服务工具要求	漏扫工具要求: （1）WEB 漏洞检测： 支持行业通用标准 OWASP，支持通用 WEB 漏洞检测，如：SQL 注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、已知漏洞组件包含、敏感信息泄露等。 支持信息泄漏类漏洞检测，如：mail 地址、敏感目录暴露、内部 ip 地址、会话令牌、源码、数据库备份文件、SVN 文件、系统重要配置、日志文件向外网泄漏等。 支持对新爆发的 0day 漏洞检测，如：struts s2-045 漏洞等。 （2）系统漏洞检测 支持多种系统漏洞检测技术，如：支持基于漏洞库的漏洞扫描技术、基于 fuzz 测试的漏洞扫描技术和基于 banner 信息的漏洞扫描技术等。 支持对通用系统漏洞进行扫描，如：远程缓冲区溢出漏洞、远程拒绝服务攻击漏洞和远程代码执行漏洞等。 （3）弱口令排查能力 支持各类应用资产的弱口令扫描，支持自定义字典，支持设置弱口令扫描白名单，可以指定某个 ip 某个应用不执行弱口令扫描。

（五）技术要求-安全加固服务

序号	服务类型	详细参数
服务资产		政务云平台主机、院内数据中心设备及单位（含各分门诊）网络设备、安全设备、终端计算机，含数据库、中间件等。
1	服务频次	定期（至少每季度一次）。
2	网络设备安全加固	（1）对网络设备的管理员进行分级管理，权限更高的管理员的账号和口令的管理要求必须保证是最严格等级，同时对其他管理员的账号和口令的复杂度进行优化。 （2）对网络设备的登录账号进行加固，使其满足一定强度的认证要求，并对不同级别的授权策略进行优化。 （3）网络设备的服务配置方面，必须遵循最小化服务原则，关闭网络设备不必要的所有服务，修复网络服务或网络协议自身存在的安全漏洞以降低网络的安全风险。 （4）针对网络设备管理设置访问安全限制策

		略，只允许特定主机访问网络设备。 （5）根据安全级别要求，开启网络设备必需的监控日志记录，并支持一定周期的日志本地存储或外置存储。
3	主机操作系统加固	（1）对主机操作系统的管理员进行分级管理，确保不同管理员的账号和口令的管理要求差异化，同时对账号和口令的复杂度进行严格要求。 （2）确保主机操作系统的登录账号达到一定强度的认证要求，并对不同级别的授权策略进行优化。 （3）主机操作系统的网络服务、进程和启动项配置方面，必须遵循最小化服务原则，关闭主机操作系统不需要的所有服务，降低网络服务或网络协议自身存在的安全漏洞带来的安全风险。 （4）严格把控每个文件/文件夹的访问权限，只允许授权的账户访问此文件/文件夹。 （5）针对主机操作系统管理设置访问安全控制策略，只允许特定主机访问网络设备。 （6）按照安全级别要求，开启主机操作系统必需的监控日志记录，并支持一定周期的日志本地存储或外置存储。
4	数据库加固	（1）根据数据库管理员的分级管理策略制定差异化的管理员账号和口令的管理要求，对账号和口令的复杂度进行优化配置。 （2）针对数据库的登录账号进行一定强度的认证要求，以及对不同级别的授权策略进行优化调整。 （3）针对数据库管理设置访问安全访问限制策略，只允许特定主机访问网络设备。 （4）关闭不必要的服务，加固 TCP/IP 协议栈，使用加密通信协议。 （5）根据安全级别要求，开启数据库必需的监控日志记录，并支持一定周期的日志本地存储或外置存储。
5	中间件及常见网络服务安全加固	（1）完成针对应用的管理员分级管理，不同管理员的账号和口令的管理要求实现差异化，同时对账号和口令的复杂度进行优化。 （2）针对应用的登录账号进行一定强度的认证要求和不同级别的授权策略优化。 （3）根据安全级别要求，开启中间件及常见网络服务必需的监控日志记录，并支持一定

		周期的日志本地存储或外置存储。
6	服务 交付物	《安全加固报告》的具体内容应包含： （1）对加固过程的详细记录。 （2）对加固结果的详细记录。 （3）对未能实施加固（残余风险）的风险项进行详细说明，并提出安全补救措施和安全专家建议,为管理人员的后期维护提供参考。

（六）技术要求-网络安全渗透测试服务

序号	服务项	详细参数
服务 资产		政务云平台主机、院内数据中心设备及单位（含各分门诊）网络设备、安全设备、终端计算机，含数据库、中间件等。
1	服务 频次	定期（至少每半年一次）。
▲2	服务范围	渗透测试服务的范围主要包括甲方的操作系统、应用系统、WEB 程序和网络设备。 操作系统包括： （1）Windows、发行版 Linux、AIX、Solaris、FreeBSD 等主流系统。 （2）应用系统包括：Oracle、MySQL、MSSQL、Sybase、DB2.Informix 等主流数据库，Apache、IIS、Tomcat、Weblogic 等主流 WEB 服务器，FTP、DNS 等主流应用服务器。 （3）WEB 程序包括：ASP、PHP、JSP、.NET、Perl、Python、Shell 等语言编写的 WEB 程序。 （4）网络设备包括：常见厂商的路由器、交换机等设备。
3	测试位置	渗透测试服务根据测试的位置不同可以分为内部测试和外部测试： （1）内部测试是指经过用户授权后，测试人员到达用户工作现场，根据用户的期望测试的目标直接接入到用户的办公网络甚至业务网络中。这种测试的好处就在于免去了测试人员从外部绕过防火墙、入侵保护等安全设备的工作。一般用于检测内部威胁源和路径。 （2）外部测试与内部测试相反，测试人员无需到达招标方现场，直接从互联网访问用户的某个接入到互联网的系统并进行测试即可。这种测试往往是应用于那些关注站点的用户，主要用于检测

		外部威胁源和路径。
4	测试方法	根据测试的方法不同分为黑盒测试和白盒测试两类： （1）黑盒测试是指测试人员对除目标系统的 IP 或域名以外的信息一无所知的情况下对系统发起的测试工作，这种方式可以较好地模拟黑客行为，了解外部恶意用户可能对系统带来的威胁。 （2）白盒测试则是指测试人员通过用户授权获取了部分信息的情况下进行的测试，如：目标系统的账号、配置甚至源代码。这种情况用户模拟并检测内部的恶意用户可能为系统带来的威胁。

（七）技术要求-★等保测评服务

序号	服务项	详细参数
服务资产		等保三级测评系统范围：HIS、EMR、集成平台，共三个业务系统。
1	服务频次	一次，11 月 30 日前完成。
2	等保测评服务	（1）等保三级由中标方委托第三方测评资质机构完成测评(取得等保三级合格报告),并由中标方承担测评费用及整改费用。 （2）依据第三方测评机构出具《差距整改报告》进行合规整改、加固等,整改结果通过等保三级相关标准。 等保测评服务应提交以下成果： 《信息系统等级测评报告》，包括单元测评分析结果、整改测评分析结果、测评结论和安全整改建议等（每个系统一份）。

（八）技术要求-网络安全应急响应（按实际发生次数）

序号	服务类型	详细参数
1	响应事件范围	中标方应在招标方遇到重大或突发事件后按照要求的服务响应级别采取相关的措施和行动。帮助招标方正确应对安全事件，降低安全事件带来的损失和影响，并将业务以及网络恢复到正常状态。 本次招标的应急响应包含但不限于以下几类安全事件： （1）WEB 安全事件

		针对 B/S 类信息系统或网站遭受恶意入侵，利用网站进行反动信息、赌博、黄色等信息发布，传播危害国家安全、社会稳定和公共利益的内容的安全事件，包括但不限于：篡改、暗链、挂马、Webshell 等。 （2）恶意程序事件 针对遭受的各类恶意程序事件进行快速处置，包括不限于病毒事件/木马事件、蠕虫事件、僵尸网络事件、勒索病毒事件、挖矿病毒事件等。 （3）网络攻击事件 针对招标方由于信息系统的配置缺陷、协议缺陷、程序缺陷，造成的信息系统异常的安全事件进行应急响应。 （4）信息破坏事件 针对招标方信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的网络安全事件进行应急响应，包括但不限于系统配置遭篡改、数据库内容篡改、网站内容篡改事件、信息数据泄露事件等。 中标方应按以下要求及时提供应急响应服务: （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（如有需要）。 （4）安全事件溯源分析服务。 （5)编制应急响应情况报告，说明事件原因、处置措施等。
▲2	响应时间要求	中标方应提供 7*24 小时应急响应服务，提供应急响应服务方案; 安全事件要求应急团队须在 5 分钟内，对信息安全事件做出响应，并严格按照招标方信息安全等级要求迅速到达现场并解决问题： （1）特别重大事件（Ⅰ级），5 分钟作出响应，提供远程 7*24 小时响应服务、1 小时到达现场进行应急响应服务。 （2）重大事件（Ⅱ级），10 分钟作出响应，提供远程 7*24 小时、2 小时到达现场进行应急响应服务。 （3）较大突发事件（Ⅲ级），30 分钟作出响应，提供远程 7*24 小时响应服务、4 小时到达现场进行应急响应服务。

		（4）一般性突发事件（Ⅳ级），30 分钟作出响应，提供远程 7*24 小时响应服务、远程无法解决时，在 4 小时到达现场进行应急响应服务。 （5)每次故障处理完毕 3 个工作日内提供详细的故障处理报告。
3	服务频率	服务期限内提供安全应急响应服务，次数按实际发生次数。
4	服务交付物	《应急响应报告》 《安全加固报告》

（九）技术要求-重要时期安全保障服务（按实际发生次数）

序号	数量/频次	详细参数
▲1	预计 4 次/年，**最终按实际发生次数**	重大节日或时间段（如：两会、护网、攻防演练、国庆、春节等重要时期），现场值守保障招标方业务系统稳定运行，现场协助处置网络攻击、病毒感染、网络故障、安全设备故障等问题。 服务内容： （1）网站安全综合监控：对网站可用性、黑链、暗链、篡改、挂马等进行监测。 （2）扫描与评估服务：利用专业安全扫描工具对网站进行脆弱性扫描，人工评估漏洞。 （3）渗透测试服务：白帽子团队对网站进行人工渗透测试。 （4）整改与复检：针对漏扫和渗透结果，协助整改，并对整改后的站点进行复检。 （5）主机加固与检测：利用专业主机安全加固与检测响应工具，防止黑客“埋雷”。 （6)高危事件应急演练:协助设计重保期间，高危应急演练场景，并完成演练。 （7）模拟攻防演练：指导业主方完成攻守演练，发现应急处置的设计缺陷。 （8）重保期间服务“计划设计保障计划、通报流程、协作机制、处置规范及注意事项等。 （9）现场值守服务： 1）重保期间 7*24 小时安全监控与值守，针对网站可用性、黑链、暗链、篡改、挂马及其他安全事件进行分析和处置。 2）同步外部威胁情况，提前添加 IP 黑名单和设置安全策略。 3）每小时专属群汇报，每日提供日报，每周提供周报。

		4）远程人工日志分析，每日分析当天 web 全流量、各类告警、安全设备等日志。 （10）应急响应服务：值守期间，发生入侵等严重安全事故，及时关停站点，降低影响，提供事件初步分析。 （11）安全通告与预警：重保期间，发生的重大外部安保事件、高危漏洞威胁，第一时间通报预警，并协助修复。 （12）入侵审计服务：专家级入侵取证人员现场入驻，分析入侵路径和手段，攻击溯源。 （13）重保工作总结：对保障工作进行总结，提交报告。

（十）商务要求

序号	详细参数
1	中标方须承诺在项目服务期间：设置专职负责的项目经理 1 人，两年或以上安全领域从业经验，具有 PMP/CISP 资质，负责现场问题处理、沟通交流及管理；运维小组组员至少配备 2 名或以上具备 CISP 资质人员，7*24 小时值守服务；熟悉网络架构及配置、漏洞利用、攻击手法、资产薄弱点分析等技术手段，有能力独立处理和解决服务期间出现的网络安全故障。
2	工作所接触或掌握的信息系统所涉及的全部软、硬件管理用户名称及密码、数据库内的数据内容、购置或者拥有自主产权的计算机软件、数据、参考资料、合同文件、图纸及医院信息系统为资源产生的其它衍生内容，不得以任何方式、途径向第三方透漏。
★3	网络安全运维服务责任承担 由于包括但不限于网络安全运维服务不当等因素造成广州市黄埔区中医医院系统、数据感染病毒、加密等，中标方需承担全部责任并赔偿本单位的经济损失。
4	运维服务期间安全设备故障（硬软件系统）如当天无法修复的，24 小时内提供同等备机服务，以确保系统正常运行。
5	必须接受招标方的质量监督检查，提供真实有效的相关项目实施质量记录、证据，无条件接受招标方提出的合理质量问题整改要求，承担项目实施质量责任及因质量问题导致的项目进度延迟责任。