投　标　书

报价文件

招标编号：临[2024]3081 号-1

项目名称：2024 年网络信息安全防护项目（重招）

投标人名称：中国电信股份有限公司绍兴分公司（公章）

二〇二五年一月

目 录

第一章　开标一览表(报价表)

项目名称：2024 年网络信息安全防护项目（重招）

项目编号：临[2024]3081 号-1　　标项：一

服务类					
序号	**服务名称**	**功能、参数**	**数量**	**单价**	**总价**
1	重要资产安全服务（不少于15个）	**服务介绍：** 对卫生健康局重要的业务系统提供持续、高效的云服务平台安全监控和管理服务。通过该服务，能够快速响应主机、网络、应用、数据等安全产品的各类安全风险事件，利用安全编排自动化与响应技术进行智能分类和高效运营处置，并针对云资产进行持续风险监视和泄露监控等，同时提供远程值守团队进行入侵事件分析及应急保障，提升用户运营效率。 **服务技术要求：** 对卫生健康局重要的业务系统提供持续、高效的云服务平台安全监控和管理服务。通过该平台，能够快速响应主机、网络、应用、数据等安全产品的各类安全风险事件，利用安全编排自动化与响应技术进行智能分类和高效运营处置，并针对云资产进行持续风险监视和泄露监控等，同时提供远程值守团队进行入侵事件分析及应急保障，提升用户运营效率。 1. 暴露面梳理：投标方应使用安全工具对招标方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，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	1 年	105000	105000

		可控，降低暴露面资产的风险。 2. 具备互联网暴露面梳理的服务工具，该工具应当支持全资产和精准资产两种模式暴露资产收集模式，收集到的暴露面信息至少包括域名、域名标题、IP 地址、开放端口、资产指纹、网站截图、移动端暴露面，并且能采集对应暴露资产的访问截图向采购人举证，及对应暴露资产存在的漏洞，（需提供服务工具具备以上暴露面梳理能力的证明截图）； 3. 服务成果展示门户（或用户 Portal）应具备服务质量可视化展示，能通过可视化的数据，清晰的了解安全专家的服务水平，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，以验证投标方所承诺的服务指标（或称为服务 SLA），（需提供服务成果展示门户中服务质量监控相关的截图证明）； 4. 服务期内所提供的云端服务平台应通过国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部四部委联合组织的云计算服务安全评估，入选“通过云计算服务安全评估的云平台”名单（需提供明确写明为安全托管服务运营平台的名单截图）； 5. 服务期内所提供的云端服务平台应当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，服务平台至少通过等级保护三级测评；（需提供等级保护三级测评通过证明，包含报告首页、基本信息表、等级测评结论首页）；			

		6.针对服务范围内资产扫描到的高危可利用漏洞，应当做好高危可利用漏洞的防护工作，包括但不限于提供漏洞修复方案和安全设备防护策略，以及帮助业主配置防护规则，保证业主不会因此出现重大事件和损失；要求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（需工具制造商出具承诺防护率达到 99%并加盖投标人公章） **服务频率：** 全年不少于 15 个 **报告输出：** 《安全运营服务启动会 PPT》 《资产信息确认表》 《首次安全分析与处置报告》 《安全威胁、事件预警与处置报告》 《安全运营周、月、季、年报》			
2	重要平台安全巡检服务	**服务介绍：** 1、对局本级的网络及安全设备及平台专业人员定期现场运维，完成对平台的规则库升级、策略优化、事件分析和处置工作，输出安全报告，持续跟进安全风险发展态势。 2、根据用户需求时间，本项服务周期内提供至少 12 次。 **服务技术要求：** 投标人应保证采购人指定医疗机构信息系统正常运行并得到授权的前提下，对局本级的网络及安全设备及平台专业人员定期现场运维，完成对平台的规则库升级、策略优化、事件分析和处置工作，输出安全报告，持续跟进安全风险发展态势。 **服务频率：** 12 次/年	12 次 / 年	1500	18000

		报告输出： 《平台运维工作记录》 《安全事件分析与处置报告》			
3	应急响应服务	**服务介绍：** 1、在发生确切的网络安全事件时，应急响应实施人员应及时采取行动，限制事件扩散和影响的范围，检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件解决方案，追查事件来源，协助后续处置。 2、5 分钟内响应，1 小时内技术人员抵达现场处置。 **服务技术要求：** 1. 应在采购人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。帮助采购人正确应对安全事件，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。 应急响应时间要求 投标人应提供 7*24 应急响应服务，提供应急响应服务方案 遇到突发事件，5 分钟作出响应，1 小时内到达现场进行应急响应服务。 每次突发事件或事故处理完毕 1 个工作日内提供详细的故障处理报告 2. 应急响应工具要求： 2.1 支持非常用登录 IP、非常用登录时间的异常登录检测；支持终端扫描端口的异常扫描检测。 2.2 支持展示最新公布的热点漏洞信息，并且梳理出其中的高可利用漏洞统一展示在热点漏洞页面，方便运维人员一键对当前已接入的终端进行漏洞检测，同时支持设置热点漏洞定时检测（需提供产品截图	1 年	2000	2000

		证明并加盖投标人公章）。 2.3 应急响应工具具备应急恢复功能，防止在在发生安全事件时或误删除时对重要文件进行恢复，包括恢复引导扇区和主引导记录（需提供 CMA 或 CNAS 认证的第三方检测报告证明并加盖投标人公章）； 2.4 应急响应工具具备对发现的病毒能够有效清除，对于病毒的检测率和清除率达到 99%以上，误报率小于 0.1%（需提供 CMA 或 CNAS 认证的第三方检测报告证明并加盖投标人公章）； 2.5 应急响应工具支持通过内网主动探测，有效识别用户内网终端即未安装客户端（需提供关于“内网主动探测识别”功能的第三方测试报告证明并加盖投标人公章）。 **服务频率：** 根据用户实际需求响应，1 年 **报告输出：** 《应急响应处置报告》 《安全加固建议》			
4	渗透测试服务	**服务介绍：** 1、对局本级重要业务系统进行渗透，作为漏洞评估服务的重要补充，渗透测试服务更多关注漏洞被利用后对全网造成的影响和损失程度。站在黑客视角，实战化演练，采用无害攻击手段，模拟黑客真实的攻击行为，深度检验网络安全防线效果，为客户信息化安全建设方向提供有效依据。 尝试验证每一个漏洞的真实威胁，对各系统进行端口扫描，漏洞攻击，DNS、FTP、telnet 等进行漏洞测试，弱口令测试，数据库测试，口令猜解，拒绝服务攻击等，同时帮助用户真正理解漏洞的成因，做到	3 次/年	15000	45000

		自主可控可防，测试完成后，提出专业修复建议，协助解决安全问题。 2、根据用户需求时间，本项服务周期内提供至少 3 次。 **服务技术要求：** 投标人应保证采购人指定医疗机构信息系统正常运行并得到授权的前提下，模拟黑客攻击行为对信息系统进行非破坏性的入侵测试，查找针对信息系统的各种漏洞，帮助医疗机构理解应用系统当前的安全状况，发现在系统安全隐患并针对安全隐患提出解决办法，切实保证信息系统安全。 1.渗透测试方案要求：投标人应根据卫健系统的行业特殊性和采购人安全需求，设计针对性的渗透测试方案，并提交至采购人进行评审，渗透测试方案应包括但不限于渗透测试方法和流程、渗透测试风险评估和控制方案、渗透测试须采用商业检测工具或自有检测工具（所有渗透工具相应授权等问题需由投标人负责），提供渗透测试所面临的主要风险及相应的风险规避措施，渗透测试输出成果等。 2.渗透测试范围要求：包括但不限于以下范围的漏洞：WEB 应用系统渗透、主机操作系统渗透、数据库系统渗透等。 3.渗透测试内容要求：包括但不限于身份验证类、会话管理类、访问控制类、输入处理类、信息泄露类、第三方应用类等。 4.渗透测试报告要求：投标人应编写渗透测试报告并提交给采购人，报告应该阐明采购人业务系统中存在的安全隐患以及专业的漏洞风险处置建议。 **服务频率：** 3 次/年			

		报告输出： 《渗透测试报告》 《安全加固建议》			
5	三高一弱专项自查服务	**服务介绍：** 1、对卫健局医疗信息系统高危漏洞、高危端口、高危外联和弱口令等情况进行自查，并在指定时间内协助用户对相应问题进行整改或处置。 2、根据用户需求时间，本项服务周期内提供至少 2 次。 **服务技术要求：** 1、对卫健局医疗信息系统高危漏洞、高危端口、高危外联和弱口令等情况进行自查，并在指定时间内协助用户对相应问题进行整改或处置。 2、三高一弱辅助工具设备要求： 2.1 网络层吞吐量≥500Mbps，应用层吞吐量≥160Mbps。1U，内存≥4G，硬盘≥128G minisata SSD，电源：单电源，接口≥6 千兆电口。 2.2 支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Network Device、Media 漏洞攻击、Shellcode 漏洞攻击、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、IPS 云防护、Web 漏洞攻击等服务漏洞攻击检测（需提供以上各类攻击和防护的功能截图证明并加盖投标人公章） 2.3 内置 URL 库、IPS 漏洞特征识别库、应用识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库（需提供截图证明并加盖投标人公章）。 **服务频率：**	2 次/年	15000	30000

		2 次/年 **报告输出：** 《三高一弱专项自查报告》			
6	失陷主机定位检查服务	**服务介绍：** 1、利用先进的威胁检测工具，结合威胁情报能力，对内网中潜藏的高级威胁（勒索软件、挖矿及特种木马等）实现精准定位，弥补防病毒软件无法对新型蠕虫、免杀木马、特种木马有效识别的问题，结合人工验证，协助开展处置工作。 2、根据用户需求时间，本项服务周期内提供 1 次。 **服务技术要求：** 1、利用先进的威胁检测工具，结合威胁情报能力，对内网中潜藏的高级威胁（勒索软件、挖矿及特种木马等）实现精准定位，弥补防病毒软件无法对新型蠕虫、免杀木马、特种木马有效识别的问题，结合人工验证，协助开展处置工作。 2、失陷主机检查工具要求： 2.1 支持终端遥测源对 ATT&CK 框架中各种攻击类型的检测技术覆盖面 Windows 系统不低于 322 项，Linux 系统不低于 127 项（需提供 CMA 或 CNAS 认证的第三方检测报告证明并加盖投标人公章）； 2.2 支持告警智能定性分析，通过分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认、从而确认安全告警的优先级顺序，帮助安全人员高效的完成攻击告警的运营工作，可归类人工渗透攻击，包括定向攻击、攻防演练、内部测试。程序自动化攻击，包括监管通报、病毒、扫描器攻击。业务风	1 次/年	2000	2000

		险相关，包括脆弱性风险、业务不规范，和其他威胁。（需提供截图证明并加盖投标人公章）； 2.3 失陷主机工具制造商具有中国信息安全认证中心颁发的信息安全服务资质，风险评估（一级）（需提供证书复印件并加盖投标人公章）； 2.4 失陷主机工具支持自我保护能力，能够有在进行失陷主机检测时免受攻击（需提供 CMA 或 CNAS 认证的第三方检测报告证明并加盖投标人公章）。 **服务频率：** 1 次/年 **报告输出：** 《失陷主机定位检测报告》			
7	漏洞扫描与分析服务	**服务介绍：** 1、使用专业的漏洞扫描工具对在线设备(主机、数据库、中间件、网络设备等)及新上线设备进行漏洞扫描服务。包括主机扫描、网络扫描、数据库扫描等，用于分析系统、应用、网络设备存在的常见漏洞。扫描覆盖范围包括端口扫描、弱口令扫描、系统漏洞、网络设备漏洞、数据库漏洞、中间件漏洞、web 应用漏洞等，在扫描后进行分析，发现系统中的潜在漏洞并及时修复。 2、根据用户需求时间，本项服务周期内提供至少 4 次。 **服务技术要求：** 使用专业的漏洞扫描工具对在线设备(主机、数据库、中间件、网络设备等)及新上线设备进行漏洞扫描服务。包括主机扫描、网络扫描、数据库扫描等，用于分析系统、应用、网络设备存在的常见漏洞。扫描覆	4 次/年	8000	32000

		盖范围包括端口扫描、弱口令扫描、系统漏洞、网络设备漏洞、数据库漏洞、中间件漏洞、web 应用漏洞等，在扫描后进行分析，发现系统中的潜在漏洞并及时修复。 **漏洞扫描工具要求：** 1.支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情。（提供截图并加盖投标人公章） 2.支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行。（提供截图并加盖投标人公章） 3.支持域管理功能，系统默认内置终端接入域、运维管理域、其他业务域、核心业务域、核心交换域、对外服务域、外联域、互联网出口域等，可根据客户实际情况进行自定义管理。（提供截图并加盖投标人公章） 4.支持业务系统登记功能，保护等级支持第二级和第三级，可根据不同域类别添加资产到业务系统中。 5.产品支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表。（提供截图并加盖投标人公章） **服务频率：** 4 次/年 **报告输出：** 《漏洞评估报告》 《安全加固建议》			

8	重保服务	**服务介绍：** 在重大活动时期（攻防演练等）或当发生重大安全事件时，根据采购人要求通过派遣专业安全工程师开展安全检查，驻点保障以及应急值守等工作。 **服务技术要求：** 在重大活动时期（攻防演练等）或当发生重大安全事件时，根据采购人要求通过派遣专业安全工程师开展安全检查，驻点保障以及应急值守等工作，重保时间不少于 10 天。 **重保服务工具要求：** 1. 重保期间提供高级威胁阻断工具，能够识别网络中的应用并进行安全检测（需提供 CMA 或 CNAS 认证的第三方检测报告证明并加盖投标人公章）； 2. 重保期间提供高级威胁阻断工具，工具支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改（需提供 CMA 或 CNAS 认证的第三方检测报告证明并加盖投标人公章）； 3. 工具支持对服务器文件攻击进行检测防护，确保业务重要数据不会出现可用性问题（需提供 CMA 或 CNAS 认证的第三方检测报告证明并加盖投标人公章）。 **服务频率：** 根据用户实际需求响应（不超过 10 天），1 年 **服务价值：** 1、发现重要保障时期被保障单位信息系统可能存在的安全风险以及安全防御体系可能存在的薄弱环节，指导修复，提升安全防御能力。 2、确保重大活动、会议顺利圆满完成。	1 年	30000	30000

9	应急演练和攻防演练	**服务介绍：** 1.网络安全应急演练服务覆盖演练准备工作、演练环境搭建、演练剧本编写、演练彩排工作、正式演练大会、应急演练总结等各个阶段。通过应急演练工作，进一步明确各应急小组在应急响应工作中的职责，熟悉掌握应急响应的处置程序、方法和注意事项，有效提高单位整体应急响应的反应能力、指挥水平和实战能力，增强各部门应急人员之间的协调性，检验单位应急救援预案的可行性和可操作性，使其达到应急演练的预期效果。 2. 通过真实的攻击和防御场景，测试和评估组织的安全防护能力，识别潜在的漏洞和风险，并提供改进建议，协助卫健局对相应问题进行整改或处置，对特定的目标或系统组件如网络设备、服务器、应用程序等进行测试，发现系统中的漏洞和安全弱点。 **服务技术要求：** 全年组织不少于一次的网络信息安全应急演练和全系统的攻防演练。 **服务频率：** 1 次/年 **服务价值：** 1、提升单位在应对重大网络安全事件的应急响应能力，准确发现现有安全运维及应急流程中的不足和短板，对现有应急机制进行完善。 2、满足等保 2.0 标准《GB/T22239-2019 信息安全技术 网络安全等级保护基本要求》二级（含）以上要求：7.1.10.13 应急预案管理 a)应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；b）	1 次/年	30000	30000

		应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。 3、满足《中华人民共和国网络安全法》第三章第二十五条：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。 4.通过真实攻击，攻防演练可以帮助组织成员提高对安全威胁的认识和警惕性，增强安全意识。 5.验证组织的安全防御能力，包括入侵检测、入侵阻止、安全监控等方面，发现并改进安全策略和技术措施。			
10	杀毒软件	2700 个 Windows 终端通用授权许可【不分 windows 普通 PC 客户端与服务器端，用户可以自由调整而不产生额外费用，具备病毒查杀、补丁修复、勒索病毒诱捕、远程登录保护、漏洞攻击拦截、标准 API 接口、暴力破解防护、攻击溯源、软件捆绑安装拦截、U 盘注册、U 盘信任等功能】和 60 个 linux 系统授权许可，原厂三年程序版本与三年病毒库升级服务。 **服务技术要求：** 2700 个 Windows 终端通用授权许可【不分 windows 普通 PC 客户端与服务器端，用户可以自由调整而不产生额外费用，具备病毒查杀、补丁修复、勒索病毒诱捕、远程登录保护、漏洞攻击拦截、标准 API 接口、暴力破解防护、攻击溯源、软件捆绑安装拦截、U 盘注册、U 盘信任等功能】和 60 个 linux 系统授权许可，原厂三年程序版本与三年病毒库升级服务。	1 项	432500	432500

		1、要求系统支持中/英文界面，系统部署采用 C/S 架构，管理采用 B/S 架构，管理员只需通过浏览器登录控制中心，即可对系统进行管理 2、要求客户端支持 CentOS、Ubuntu、SUSE、Redhat 等主流 Linux 发行操作系统。需要 GNU libc 2.12 及以上版本 3、要求可按照安装密码、IP 地址范围来限制可以安装的终端，避免终端被随意安装。中标后提供截图证明。 4、要求中心可按全网统计软件安装情况，包括软件名称、发布者、版本号、安装率；可以提供软件安装、卸载日志；可对支持导出软件清单；按终端、按分组统计软件安装情况。 5、要求支持展示全网终端安全概览：终端在线数量、异常终端、今日防御事件、累计保护时长、最新安全动态、终端操作系统概览 6、要求支持定制防护策略以及策略细粒度配置：包括病毒防御（文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、Web 扫描）；系统防御（系统加固、应用加固、软件安装拦截、浏览器保护、摄像头防护）；网络防御（网络入侵拦截、对外攻击拦截、恶意网站拦截、Web 服务保护、爆破攻击防护、僵尸网络防护、远程登录防护）；访问控制（IP 协议控制、IP 黑名单、联网控制、网站内容控制、程序执行控制、设备控制）以及安全工具可根据不同分组需求定制不同的策略。 7、要求支持漏洞集中修复、统一修复高危漏洞、统一修复所有漏洞，并展示以修复补丁和未修复补丁的信息。			

投标总价合计金额大写：柒拾贰万陆仟伍佰元整　　小写：　￥726500

注：

1、投标人需按本表格式填写，不得自行更改，如无对应内容，则填写：“无或/”。

2、有关本项目实施所涉及的一切费用（详见前附表）均计入报价。**采购人将以合同形式有偿取得货物或服务，不接受投标人给予的赠品、回扣或者与采购无关的其他商品、服务，不得出现“0 元”“免费赠送”等形式的无偿报价，否则视为投标文件含有采购人不能接受的附加条件，投标无效；采购内容未包含在《开标一览表（报价表）》名称栏中，投标人不能作出合理解释的，视为投标文件含有采购人不能接受的附加条件的，投标无效。**

3、特别提示：采购代理机构将对项目名称和项目编号，中标供应商名称、地址和中标金额，主要中标标的的名称、规格型号、数量、单价、服务要求等予以公示。

4、符合招标文件中列明的可享受中小企业扶持政策的投标人，请填写中小企业声明函。投标人提供的中小企业声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。

5、报价低于项目预算 50%的，应当在报价文件中详细阐述不影响产品质量或者诚信履约的具体原因

投标人名称(电子签名)：中国电信股份有限公司绍兴分公司

日期：2025 年 1 月 17 日

第二章 投标人针对报价需要说明的其他文件和说明

无

投标人名称(电子签名)：中国电信股份有限公司绍兴分公司

日期：2025 年 1 月 17 日

第三章 中小企业声明函

我公司非中小企业参与投标。

投标人名称(电子签名)：中国电信股份有限公司绍兴分公司

日期：2025 年 1 月 17 日

第四章 残疾人福利性单位声明函

我公司非残疾人福利性单位参与投标。

单位名称(电子签名)：中国电信股份有限公司绍兴分公司

日期：2025 年 1 月 17 日