四、政府采购报价一览表

政府采购报价一览表

供应商名称(盖章)：贵州中科紫龙科技有限公司

项目编号：MCHC-DZ-ZC20256061

项目名称：网络安全外包服务

单位：（元）

序号	服务名称	服务内容	数量	单位	投标报价	备注	考核要求
1	日常安全运营服务要求	一、服务概述 1.综合运用丰富的技术经验及威胁情报知识库，借助安全感知平台等强大的设备对接能力及安全检测能力对安全日志、流量进行分析研判并对发现的威胁进行定位，并对分析发现的安全问题制定安全运营相关台账，做好安全问题通告和处置管理工作；根据医院现有的的网络安全制度，结合法律法规及监管单位的要求，以及网络安全发展态势进行制度修订；结合威胁情报、专家指导意见、风险评估、内部安全检查、基线检查、安全运营平台监测等安全 加固线索和加固处置服务等。 2.服务期内提供在医院本地部署一体化安全运营托管服务 平台（软硬件一体化），平台须具备 IT 资产管理、脆弱性管理、威胁监测、	/	全年	299000	持续安全运营服务	完成服务要求，提供相对应的运维材料，不发生重大人因安全事故

		响应与处置等能力，提供 7*24H 持续性开展网络安全保障工作，与医院一同构建持续、主动、闭 环的安全运营体系。服务 IT 资产包含医院终端电脑和服务器、云主机等，资产数量≥5000 个。 3.在服务过程中，需对分析发现的安全问题制定安全运营管理台账，做好安全问题通告和处置管理工作；根据医院现有的的网络安全制度，结合法律法规及监管单位的要求，以及网络安全发展态势进行制度修订；结合威胁情报、专家指导意见、风险评估、内部安全检查、基线检查、安全运营平台监测等安全加固线索提供加固处置服务。					
		二、服务内容 （一）威胁分析和通告 通过用户现场的安全设备或其他安全工具对医院资产进行脆弱性分析、威胁分析和安全事件处置。 （二）深度威胁分析和研判 对漏洞利用攻击事件、Webshell 上传事件、Web 系统 目录遍历攻击、SQL 注入攻击、系统命令注入攻击、信息 泄露攻击深度、口令暴力破解、Web 明文传输、弱密码、勒索病毒事件、挖矿病毒事件、蠕虫病毒事件、僵尸网络 攻击事件、SMB 扫描事件、RDP 暴破&SMB 暴破事件等安全事 件进行深度分析研判和处置。					

		（三）威胁主动响应 对内网脆弱性、入侵行为、潜伏威胁等安全问题进行主动响应，在授权情况对相关设备策略调整、系统升级、 系统备份等工作；对终端病毒进行处置。 （四）资产服务 1.结合专业安全人员，利用资产发现工具，全面梳理 xx 信息化基础设施已知资产、发现未知资产，资产信息包括服务器、应用，网络设备、安全设备等，同时，结合业务特点，对资产的重要性等情况进行梳理，形成资产清单，全面、精准解决资产边界盲区问题，为持续的信息化建设提供参考依据。提供《xx 资产梳理清单》，完成资产端口点对点策略配置工作； 2.API 资产梳理：根据业务系统梳理出所对应的 API 接口， 形成对应的 API 资产清单，通过 API 安全设备（如有）定期进行安全监测。 （五）结合威胁情报、专家指导意见、风险评估、内部安全检查、基线检查、安全运营平台监测等安全加固线索， 综合评判； （六）推进安全加固服务 估威胁影响级别、威胁影响范围等维度，制定安全加固方案，实施安全加固，检查安全加固结果，持续提供合 理的安全加固方案，安全					

		加固方案对象包括但不限于主机 系统、数据库、WEB 应用系统、微信小程序、移动 APP 等。输出《xx 安全加固报告》。 （七）制度修订服务 每年根据国家法律法规政策、上级监管单位及网络安全发展要求，每年修订一次 xx 的网络安全制度。输出《xx 网络安全制度》修订版。 （八）互联网暴露面排查 按月对医院互联网侧的资产进行暴露面排查，排查要求：落实贵州省人民医院 gz5055.com 域名及子域名包括的所有资产、小程序。排查以贵州省人民医院备案号或有 “贵州省人民医院”关键字的所有系统。根据排查结果进行核查，落实是否存在安全风险，并出具排查报告。 （九）排查医院的网络准入情况、U 盘开通以及杀毒软件安装情况，实时对安全设备进行监测，动态发现系统运行的安全情况。 （十）排查医院公共区域的大屏入网及外接设备安全策略配置情况，定期进行安全排查，避免屏幕被投放与医院无关的信息或其他更重要的安全事故。 （十一）院方安排的其他信息安全相关工作。 三、服务要求					

		（一）运营开始阶段 1.安服工具部署：服务期内需在医院本地部署一体化安全运营服务工具（含 2 台主平台设备和 2 台探针），安服工具需具备 IT 资产管理、脆弱性管理、威胁监测、响应与处置等能力。 2.资产管理服务 （1 ）资产梳理服务：探测单位主机、网站资产，包括探测主机操作系统、开放端口、应用服务、协议版本等，探测网站子域名、url、web 框架、备案号、微信小程序、微信公众号、APP 应用程序等，形成资产清单，并定时探测更新。 （2 ）攻击面检测服务：联动外网云端扫描系统，探测互联网上潜在的未知资产、不必要开放的资产，并自动验证互联网资产是否存在可利用漏洞、弱口令，提供暴露面收敛等相关整改建议。 （3 ）提供互联网暴露面收敛建议：建议用户关闭不必要开放到互联网的资产、端口、后台 url 页面，减少攻击面。 （二）持续有效运营阶段 1.脆弱性管理服务 （1）漏洞扫描服务：对主机、网络设备、操作系统、数据库、中间件等进行常态化的漏洞与弱口令扫描，提供漏洞、弱口令扫描结果台					

		账与整改建议。提供漏洞 优先修复建议：基于攻防视角评估资产漏洞风险，识别可实际产生风险的漏洞，提供漏洞修复的优先级建议，可大幅减少漏洞整改工作量。 （2）漏洞屏蔽：对于无法整改修复的漏洞，提供漏洞屏蔽技术手段，使扫描器扫得到资产，但扫描不到漏洞，规避漏洞暴露风险。 （3）网站风险监测：贵州省人民医院 gz5055.com 域名及子域名网站进行 7*24 小时网站监测，包含：web 漏洞、篡改、黑链/挂马、敏感文件、敏感词、可用性、域名劫持等 7 个维度开展实时监测，并可通过邮件、飞书、钉钉、企业微信等告警形式提供网站风险预警服务。 2.威胁管理服务 （1）流量威胁监测：旁路部署流量检测探针（含 8W+IDS 规则），监测互联网出口与服务器区域边界流量，基于威胁计分算法精准识别恶意 IP。 （2）蜜罐威胁诱捕：旁路部署高交互或无漏洞的仿真蜜罐，精准诱捕攻击蜜罐的失陷主机，实时零误报定位攻击威胁：勒索病毒传播、内网主机被远控后横向攻击（如钓鱼远控、供应链威胁）。 （3）主机威胁监测：在服务器上安装轻量级主机 Agent， 包括可在公有云主机安装，保护云主机；事前监测： 能识别与阻断主机攻击、					

		Web 攻击、暴力破解（SSH、RDP、SMB）和异常登录等入侵行为、针对服务器横向攻击行为，可识别 HTTPS 加密流量中的攻击行为；事后监测：实时监测 webshell、反弹 shell、网页篡改等行为。 （4）智能 AI+威胁情报服务：智能 AI 研判分析：自动威胁 告警进行降噪研判分析，自动研判出各种威胁类型： 非法外联、外网攻击、内网横向、暴力破解、利用成功等；威胁情报：关联全球威胁情报，精准检测网络中的病毒域名请求、恶意 IP 流量威胁。 3.处置与预警 自动化旁路阻断服务： （1）外网威胁实时封堵：专家精准研判外网威胁告警，使用旁路阻断技术，实时封堵外网攻击 IP 地址，大幅 降低被入侵风险； （2）内网非法外联阻断：自动阻断内到外的病毒木马外联行为。 （3）告警事件及时响应：发生相关风险告警，通过邮件、飞书、钉钉、企业微信等形式及时通知用户，及时响应。 （三）运营成果可视通过本地部署一体化安服工具，数据统一汇总在安服工具上，用户可随时使用安服工具的功能，以及各场景大屏展示功能。 （四）其他服务要求					

		1.推进安全加固服务：估威胁影响级别、威胁影响范围等 维度，制定安全加固方案，实施安全加固，检查安全加 固结果，持续提供合理的安全加固方案，安全加固方案 对象包括但不限于主机系统、数据库、WEB 应用系统、 微信小程序、移动 APP 等。 2.制度修订服务：每年根据国家法律法规政策、上级监管 单位及网络安全发展要求，每年修订一次 xx 的网络安全 制度。 3.排查医院的网络准入情况、U 盘开通以及杀毒软件安装 情况，实时对安全设备进行监测，动态发现系统运行的 安全情况，牵头处置排查、检测发现的问题。 4.排查医院公共区域的大屏入网及外接设备安全策略配置 情况，按月进行安全排查，避免屏幕被投放与医院无关 的信息或其他更重要的安全事故，输出排查报告，并针 对发现问题进行处置。 四、服务交付物 （一）《安全问题管理台账》：对所有安全设备上出现的 安全时间进行处置和闭环，形成安全事件处置台账； （二）《安全运营服务周报》、《安全运营服务分析月报》、《安全运营服务分析季报》、《安全运营服务年度 总结报告》； （三）《安全事件处置报告-日报》；					

		（四）《xx 网络安全制度》修订版《xx 资产梳理清单》 《xx 安全加固报告》《API 资产清单》《互联网暴露面排 查报告》。					
2	渗透测试服务	一、服务概述 在获得授权的情况下对指定的业务系统进行深层次的 漏洞挖掘和利用，模拟黑客展开渗透测试攻击，获取到该 业务系统的服务器权限以及最具价值的信息和资产。 二、服务内容 （一）前期交互阶段 与用户进行沟通、确定渗透测试的时间、范围、深度、测试方式（黑盒 OR 白盒、现场 OR 远程）等问题，并拿到用户签署的渗透测试授权函； （二）情报搜集阶段 服务团队在拿到用户授权后开始情报搜集工作，搜集阶段是对目标用户的系统进行一系列踩点工作，包括：基 础资产收集、互联网信息泄露搜集、指纹识别、业务系统 功能收集、接口信息收集等； （三）威胁建模阶段 在搜集到充分的情报信息之后，服务工程师对获取的 信息进行威胁建模与攻击规划。从大量的信息情报中理清 思路，确定出最可行的	按需	全年	270000		5 个工作日内出具渗透测试初测报告，不发生重大人为因素安全事故。

		攻击通道； （四）漏洞分析阶段 针对威胁建模阶段总结的测试方法进行逐一验证，通 过测试总结出可行的测试方法，排除不可行的测试方法； （五）渗透攻击阶段 对用户的业务系统进行攻击性测试； （六）报告输出阶段 渗透测试工作全部完成后输出报告，报告中阐明客户 系统中存在的安全隐患以及专业的漏洞风险处置建议； （七）汇报阶段 向用户汇报本次渗透测试的成果，并现场对用户提出 的疑问进行现场答疑； （八）漏洞复测阶段 当用户业务系统的漏洞修补完成后提供漏洞复测服务，用于验证业务系统的漏洞修补情况，并向用户提交复 测报告。 （九）推进漏洞整改工作 提出漏洞整改建议，并配合开展整改工作。 二、服务交付物					

		《渗透测试报告》、《渗透测试复测报告》 四、其他要求 为保障医院项目实施进展，在院方提出渗透测试需求后，5 个工作日内出具渗透测试初测报告（盖章），并完成资料归档。					
3	风险评估	一、服务概述 通过运用丰富的技术经验和专用工具对组织信息资产 面临的威胁、存在的脆弱性、现有防护措施及综合作用而 带来风险的发生可能性进行评估，最终提供完整的风险评 估报告及修复建议。 二、服务内容 （一）资产识别 使用专用工具对包括：业务系统、服务器、安全设备、网络设备等进行自动化扫描发现、识别、评估，可覆盖所有的资产，根据业务对资产的实际依赖程度区分重要资产，脆弱性识别、威胁识别、风险分析等后期工作将针对重要资产进行别； （二）脆弱性评估 1.漏洞扫描：使用专用工具的漏洞扫描功能，快速从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全漏洞，并给出关于安全隐患的详细信	1	次	45000		对医院信息安全建设及运维工作进行全面分析，完成服务要求，提供相对应的材料，不发生大人为因素安全事故。

		息； 2.基线配置核查：使用专用工具的基线配置核查功能识别信息系统的安全配置情况； 3.威胁评估：分析用户信息系统存在的威胁种类，确定威胁分类的标准；综合威胁来源、种类和其他因素后得出威胁列表；针对每项需要保护的信息资产，尽可能全面 的发现资产所面临的威胁； 4.防护能力评估：识别已有的安全控制措施，分析安全措 施的有效性，确定威胁利用弱点的实际可能性，指出当前安全措施的不足； 5.风险分析：综合考虑资产本身的价值、威胁发生几率、 脆弱性的破坏力、现有防护能力等因素分析资产可能存 在的安全风险，结合风险对业务战略的影响程度区别明 确风险处置计划； 6.风险评估报告：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，输出 风险评估报告，风险评估报告中为用户提供符合业务需求的安全整改建议 7.风险整改验证：在用户根据风险评估报告完成对应风险 项整改后，提供整改项结果验证。 三、服务交付物 （一）风险评估方案；					

		（二）资产识别清单； （三）脆弱性列表； （四）已有安全措施确认表； （五）风险评估报告。					
4	脆弱性扫描	一、服务概述 使用扫描工具对业务系统进行扫描，准确识别出注入缺陷、跨站脚本攻击、非法链接跳转、信息泄露、异常处 理等安全漏洞，全面检测并发现业务应用安全隐患。 二、服务内容 （一）准备阶段 对目标用户的服务范围内资产进行搜集，获取域名、 IP、网络拓扑等相关信息，作为后续的扫描资产范围；签署漏洞扫描委托授权函，获得用户的授权，约定漏洞扫描的时间和漏洞扫描工具；确认漏洞扫描设备接入点；与用户协商进行相关目标资产文件与数据的备份。 （二）扫描实施阶段 实施扫描阶段开始现场检查网络连通性情况，根据情况分配合理 IP，确保扫描工具能探测到扫描范围内的所有主机，且无防火墙等安全设备进行阻拦，之后开展漏洞 扫描；扫描过程中，如果目标系统出现	按需	全年	18000		按季度完成漏洞扫描和整改工作，拟定漏洞整改通知书，配合厂家完成漏洞修复工作

		无响应、中断等情 况，扫描人员会立即中止漏洞扫描，并配合客户进行问题排查，在确认问题以及完成系统修复之后，根据分析结果调整扫描方式，经客户再次授权同意的前提下才会继续进行其余的扫描；并对发现的安全漏洞，提供切合实际安全 解决方案，协助漏洞修复。 三、服务交付物 《资产漏评估报告》、《资产漏洞整改通知》以及《资产漏洞复测报告》,涉及系统弱口令方面时另须提供《系统弱口令核查报告》。					
5	安全设备巡检服务	一、服务概述 提供安全巡检服务，每月一次例行安全设备巡检，巡检内容为分为硬件状态检查、安全性检查和稳定性检查，定期对策略优化，制定策略优化报告。 二、服务内容 （一）硬件状态检查：设备电源指示灯，网口指示灯，设 备 ALARM 灯，CPU，内存等使用情况； （二）安全性检查：配置备份，规则库更新，软件升级， 预警补丁更新情况； （三）稳定性检查：设备流量负载情况分析，系统运行日 志分析，	/	全年	30000		每日完成设备巡检工作，输出相应的巡检报告，不发生重大人为因素安全事故。

		及时发现潜在风险。 三、服务交付物 《安全设备巡检报告》、《策略优化报告》 四、其他要求 驻场工程师每日对安全设备、网络设备运行情况进行巡检。					
6	应急演练服务	一、服务概述 据相关国家标准或国际标准，提供对应的应急演练场景专项应急预案模板，以指导应急响应团队应对与处置安全事件；制定应急演练方案及脚本并协助开展应急演练， 模拟安全事件发生及处置的全过程，提高应对安全事件的 处置能力，预防和减少安全事件造成的危害和损失。 二、服务内容（一） 1.安全事件应急演练：通过模拟各种突发事件场景进行，应急演练场景可分为：有害程序事件演练、网络攻击事 件演练、信息破坏事件演练、设备设施故障演练； 2.有害程序事件：内网传播型病毒应急演练、勒索病毒应急演练、挖矿病毒应急演练等； 3.网络攻击事件：漏洞攻击应急演练、后门攻击应急演练等；	3	次	45000	1 次全院应急演练工作开展，2 次科室内部应急演练工作开展	

		4.信息破坏事件：网站篡改应急演练、网页挂马应急演练等； 5.设备设施故障事件：网络设备、安全设备故障应急演练、服务器故障应急演练等； （三）拟定应急演练方案，配合开展全院信息系统故障应急演练。 三、服务交付物 《应急演练方案》、《应急演练总结报告》、《专项 应急预案模板》					
7	应急响应服务	一、服务概述 提供安全事件应急响应服务，一旦客户发生网络安全事件，驻场人员需立即响应，若发生重大安全事件则需安服技术团队人员立即远程响应，并提供技术支撑；项目经理 1 小时内现场响应处置，防止网络瘫痪、系统中断等。 二、服务内容 （一）应针对突发的安全事件，及时进行风险评估和处置。 （二）安全事件响应处理过程中，应按流程进行汇报，分析和处置。 三、服务交付物 《应急响应总结报告》、《应急响应事件记录单》、 《安全事件分析》	/	全年	10000		对安全事件积极响应，不发生重大人因安全事故

8	重大节日网络安全保障服务	一、服务概述 提供重要时期安全值守保障服务，安排指定的安全专 家在重要保障时期提供 7*24 小时现场驻场保障服务，确保重要时期客户业务的安全稳定运行。 二、服务内容 （一）在重大会议、节假日等特殊时期内，指派安全攻防 经验丰富的安全专家，对客户目标系统进行远程安全值守 和保障，对业务系统的安全状况进行安全监控和日志分 析。 （二）在重大节日期间，当目标遭受黑客入侵攻击时，值守人员应立即对入侵事件进行分析、检测、抑制、处理， 查找入侵来源并恢复系统正常运行，完成后给出应急响应 报告，报告中将还原入侵过程，同时给出对应的解决建议。 三、服务交付物 《重大节日保障方案》、《重大节日值守日报》、 《重大节日值守总结报告》	按需	全年	10600		按照服务要求，输出巡检报告， 不发生重大人为 因素安全事故。
9	网络安全培训	一、服务内容 （一）针对医院员工进行 2 次网络安全培训服务，提升员工网络安全	/	全年	12000		

		意识、规范安全用网； （二）针对信息科员工进行 6 次网络安全运维培训，提升 信息科技术人员网络安全运维能力。 二、服务交付物 提供定制化的安全培训服务，主要包括安全意识培训、安全管理宣贯培训、网络及安全设备安全运维培训、 操作系统及数据库安全运维培训、应用系统安全开发与运维培训等。					
10	日志审计综合分析服务	提供堡垒机、数据库、日志审计设备、API 接口管理等平台的日志审计分析，每日对运维日志进行审计，出具审计分析日报，及时发现可能存在的违规行为和安全隐患，为调整安全管理策略提供依据。	/	全年	38950		每日完成日志审计工作不发生重大人为因素安全事故。
11	医院互联网应用安全托管服务	一、服务概述 1.安全运营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，构建持续（7*24 小时）、主动、闭环的安全运营体系。 2.监测资产数量：65 个面向互联网应用的业务系统。	1	年	150000		完成资产动态监测，不发生重大人为因素安全事故。

		二、服务内容 （一）运营准备阶段 1.上线前策略检查 上线前安全专家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。 2.资产管理 ① 资产收集与录入：安全专家对服务资产进行收集，并将资产信息录入到安全运营平台中进行管理。 ② 资产指纹探测：持续服务过程中安全专家定期对资产进行指纹（操作系统、中间件、软件厂商等信息）探测， 并对指纹信息进行确认与更新，确保医院安全运营中心中资产指纹信息的准确性和全面性。 ③ 资产变更管理：持续服务过程中安全专家定期对资产进行存活性探测，当发现未存活资产或资产发生变更时， 安全专家对变更信息进行确认与更新，确保医院安全运营中心中资产信息的准确性和全面性。 3.安全现状评估与处置					

		对服务资产内漏洞问题、策略配置隐患问题进行归纳汇总，针对发现的问题提供修复方案与协助处理。 （二）持续有效运营 1.脆弱性管理 ① 漏洞扫描与验证：每季度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。 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用户。 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 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。 ⑤ 弱口令分析与管理：实现信息化资产不同应用弱口令 猜解检测，如：SMB、Mssql、Oracle、smtp、VNC、ftp、 telnet、ssh、mysql、tomcat 等。针对不同行业提供行业 密码字典，有针对性的进行内网弱口令检测。并将检测发 现的问题通过工单系统跟踪修复状态。					

		⑥ 最新漏洞通告与排查：实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行通告与排查。通告信息中包含最新漏洞信息、服务资产受影响情况。 ⑦ 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，修复方 案以及临时规避措施。 ⑧ 最新漏洞复测与状态跟踪：由安全专家对该最新漏洞建立工单进行持续跟踪。 2.威胁管理 ① 7*24H 威胁分析研判：基于云端安全能力平台，云端专家提供 7*24 小时的威胁监测：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，对安全告警和威胁进行分析研判，并生成生成工单。 ② 7*24H 威胁通告：安全专家将云端分析确认后的真实威胁、事件实时通过微信、邮件等方式向用户通告，并提 供处置建议。 ③ 威胁影响面分析：安全专家针对每一个真实的威胁和告警，进行					

		深度分析验证，分析判断受影响范围及是否攻击成功，将深度关联分析的结果通过服务群/邮件等方式　告知用户。 ④　威胁协助处置：安全专家针对分析结果提供对应的处 置或加固建议（如封锁攻击源、设置安全策略防护等措施），并协助用户闭环。 ⑤　流行威胁通告与排查：结合威胁情报，安全专家排查 是否对服务资产造成影响并通知用户，及时协助进行安全加固。 ⑥　策略检查：每季度安全专家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。 ⑦　策略调优：每季度安全专家根据安全威胁/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。 3.事件管理 ①　安全事件调查与分析：安全专家提供 7*24H 在线服务，针对主机发生的安全事件开展调查分析和影响面分析，对发生的安全事件进行人工鉴定和举证分析。 ②　安全事件处置：对客户网络内服务资产爆发勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，利用一些工具和脚本对恶意文件、代码进行根除，帮助客户快速恢复业务，消除或减轻影响。					

		③ 安全事件跟踪闭环：对发生的安全事件进行分级分类，并通过事件工单跟踪处置的情况，保障安全事件闭环。 ④ 重大事件应急响应：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。排查攻击路径、 恶意文件、清除。还原攻击路径，分析入侵事件原因，提供安全事件溯源结果。结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵。 （四）运营成果可视安全运营周报 安全专家每周对服务资产进行安全运营情况的分析总结并输出安全运营周报、月报、季度分析报告及半年、年度分析报告。					
投标总价合计金额 大写：**玖拾贰万捌仟伍佰伍拾元整** 小写：**928550.00 元**							
服务时间：合同签订后，服务期一年。							
服务地点：采购人指定地点。							
优惠条件及备注：/							

供应商法定代表人或授权代表签字：吴晓刚

职务：商务经理　　日期：2025年7月18日

注：

1. **请供应商按磋商文件中采购清单逐项填写；**
2. **本表所填单价均应包括其他所有费用；**
3. **此表可自行扩展。**