一、分项报价表

项目名称	聊城市卫生健康委员会全民健康信息平台运维服务项目			
报价（元，人民币）	（大写）壹拾肆万捌仟元整			
	（小写）148000			
工作内容	单位	数量	小计（元）	合计（元）
资产发现与体系化管理服务： 互联网暴露面检测服务： 周期性互联网暴露面检测服务以攻击者视角为原则，采用主动检测，被动监测相结合对方式，周期性对企业互联网暴露面排查，最大限度的发现暴露在外的安全风险并在不影响正常业务的前提下减少外连通道，收敛互联网暴露面.	项	1	4000	4000
资产发现与体系化管理服务： 资产测绘服务： 对现有资产进行测绘梳理，形成资产清单，建立资产管理制度等	项	1	4000	4000
资产发现与体系化管理服务： 敏感信息检测： 监测入侵类敏感信息泄露、接口类敏感信息泄露等事件，并实时跟踪敏感信息的流向和处理流程	项	1	2000	2000
脆弱性检测与防护服务：	项	1	4000	4000

渗透测试服务： 定期对应用系统进行安全检查，实施方式为专业工具和人工检查相结合的方式，可深入的挖掘应用系统中存在的可被黑客利用的安全漏洞，并对安全漏洞的可利用程度进行评估，提供渗透测试结果报告，针对发现的安全漏洞提供安全整改建议。				
脆弱性检测与防护服务： 漏洞扫描服务： 在不影响正常业务的条件下，周期性进行安全漏洞扫描，发现网络存在的高危安全漏洞及可能对造成的影响，出具修复建议，并提供整改后的漏洞复测服务。	项	1	1000	1000
脆弱性检测与防护服务： 基线核查： 对指定系统和设备等进行上线前的全面的安全配置核查和分析，协助查找设备在安全配置中存在的差距，并与安全整改与安全建设相结合，提升各类业务系统的安全防护能力和达到整体合规要求。	项	1	3000	3000
脆弱性检测与防护服务：	项	1	2000	2000

安全防护服务： 对客户的主机系统、应用系统、网络设备、安全设备等信息资产进行安全检查，发现信息资产中存在的安全漏洞和配置隐患，并提供周期性安全评估报告。检查范围包括但不限于补丁安装情况、访问控制策略、审核策略、权限设置、系统进程、本地安全策略、系统安全配置、安全审计策略、身份认证机制等。 针对网络节点设备的安全访问控制策略进行优化、检查、分析，梳理出空策略、过期策略、隐藏策略、冗余策略、宽松策略、可合并策略等可优化策略，协助对其进行精简和优化，收缩网络访问权限。通特征检测、查杀技术提升被动防护能力，降低网络安全风险。				
脆弱性检测与防护服务： 特征库升级服务： 现有安全设备特征库 1 年升级服务	套	1	40000	40000
威胁分析及响应服务： 安全感知分析服务：	项	1	5000	5000

对识别到的威胁进行主动响应，采取措施降低威胁可能造成的影响，协助闭环处置安全事件，并且通过对安全威胁的趋势分析，提供长期的安全规划及改进建议；运用配套工具实现整个网络内威胁发现、预警通报、跟踪溯源、处置等工作。协助对安全事件的预防与处置工作；对网络安全事件发生和发展趋势、处置措施、恢复方案等进行研究、评估，并提出相关改进建议。				
威胁分析及响应服务： 应急响应： 协助完成应急预案修订及应急处置工作，包括但不限于以下内容： （1）对网络安全应急制度体系进行修订，完善应急响应流程，对安全事件进行准确定位，及时响应处理，快速恢复系统运行，降低安全事件造成的损失和影响。 （2）对安全事件进行应急处置。发生安全事件后，安全专家必须在 0.5 小时内到场，24 小时内解决安全事件。及时消除安全事件不良后果，并总结安全事件形成、发生的原因；处理事件并提	项	1	3000	3000

交书面的安全事件调查分析报告。				
日常运营服务： 数据安全服务： 围绕数据的全生命周期，提供可行的数据安全治理体系咨询及方案落地服务。根据当前数据安全能力现状与能力目标的差距，给出切实可行的数据安全治理方案。	项	1	4000	4000
日常运营服务： 重保服务： 重大活动日提供 7×24 小时网络安全值守，对网络安全设备提供安全运维监控、安全加固和配置优化等服务，对发现的问题提出解决方案并及时处理。协助完成安全设备、系统的事件审计和日志分析工作。	项	1	2000	2000
日常运营服务： 培训服务： 每年组织不少于 1 次的信息安全意识提升培训，针对当前的安全形势，以及国内外重大安全事件，开展信息安全意识和技能培	项	1	1000	1000

训，加深对信息安全和技能的理解，提升安全意识水平和基本安全技能。同时面向技术人员组织安全技术培训，提升安全技术人员的安全管理和技术保障水平。				
日常运营服务： 网络安全检查服务： 对主要应用系统开展规范全面的网络安全自查和风险排查，形成完整的自查评估报告，指明存在的问题和整改加固建议，并协助开展问题整改，结束后进行复测并出具复测报告。 配合完成相关部门的网络安全检查工作，提供技术支持。根据工作需要，协助开展对区县及各级医疗机构的信息安全抽查，形成整体安全检测报告，提出下一步的工作意见和建议。针对发现的安全问题和隐患，协助整改加固需要开展的工作。	项	1	2000	2000
日常运营服务： 网络安全宣传服务： 网络安全宣传周期间，组织培训、网络宣传、安全资料发放等活动。	次	1	1000	1000

日常运营服务： 供应链安全检查服务： 针对供应链风险管控薄弱环节，尤其对掌握核心数据的相关系统供应链进行排查，深入分析薄弱环节、 深层次挖掘潜在风险、补齐工作短板弱项。	项	1	5000	5000
日常运营服务： 驻场运维服务： 提供驻场服务，提供日常监控巡检、故障排查与处理，以及安全事件响应与处置。	项	1	60000	60000
配套设备： 态势分析与安全运营系统： 提供态势分析、安全监测、安全处置、安全分析、资产管理、治理中心、知识情报等功能模块； 支持全网资产概述、高危资产、漏洞、告警趋势、安全日志趋势、告警统计、最新告警名称和影响范围、热点威胁等内容的相关展示； 支持主动发现漏洞功能并关联资产； 支持地图实时展示网络攻击态势，支持以不同颜色攻击线展示	套	1	5000	5000

攻击过程； 支持对攻击线索追踪溯源分析，追溯结果多维度展示， 支持日志详情查看、溯源、附件、一键封堵、加入白名单、加入关注名单、封堵申请等操作； 支持多维度威胁源画像分析，包括攻击链分布、威胁影响端口、威胁类型分布、遭受威胁资产、疑似失陷主机等； 支持管控拓扑图展示，支持拓扑动态提示管理设备产生的告警，支持查看选中设备的设备概览、设备详情、告警列表等信息； 支持设备概览和安全防御图切换，安全防御拓扑具备网络通信、网络防护、系统防护、用户管控、数据防护、应用防护多个类型的设备的拓扑架构展示，安全防御拓扑图支持在线离线设备标识； 支持内置多种分析模型，包括但不限于失陷状态、FTP 登录失败、敏感文件信息泄露、成功暴力破解、文件上传漏洞等，支持模型查看、启用、停用等操作，支持模型批量删除、批量启用、批				

量停用； 支持内生情报管理，包括恶意 IP 地址、恶意 URL、恶意样本、恶意域名、垃圾邮件等；				
总计	148000			
备注	无			

投标人名称（公章）：北京天融信网络安全技术有限公司

2026 年 03 月 10 日

注：1、表中内容可以根据项目实际情况进行增减。

2、表中位置不够可以另行附页。