采购合同

采购计划号：_____ 合同编号：_____

采购人（甲方）：岑溪市人民医院 供应商（乙方）：广西元析科技有限公司

项目名称：岑溪市人民医院采购数据中心杀毒软件授权及安全运营服务

项目编号：WZZC2025-C3-810125-GXRL

签订地点：岑溪市 签订时间：_____

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律、法规规定，按照竞争性磋商文件规定条款和乙方响应文件及其承诺，甲乙双方签订本合同。

第一条 合同金额

1.1 本合同项下相关金额约定如下：

（1）含税总金额：人民币 494,900.00 元（大写：肆拾玖万肆仟玖佰元整）；

（2）不含税金额：人民币 490,000.00 元（大写：肆拾玖万元整）；

（3）对应税金：人民币 4,900.00 元（大写：肆仟玖佰元整）。

双方确认，上述金额为固定结算金额，除本合同另有约定外，任何一方不得单方变更。小写金额与大写金额不一致时，以大写金额为准。

第二条成交内容

序号	服务名称	数量	单位	单价	总价	备注
1	杀毒软件	1	项	63600.00	63600.00	深信服统一端点安全管理系统V6.0
2	安全运营服务	1	年	222300.00	222300.00	深信服：安全托管服务 MSS-10
3	数据库防护系统	1	套	115000.00	115000.00	深信服：DBF-SW-2110
4	防火墙	1	台	89000.00	89000.00	深信服：AF-1000-FH2150B-WY
5	数据安全防泄密模块	1	项	5000.00	5000.00	深信服：AC-1000-B1200
合计金额大写：人民币 肆拾玖万肆仟玖佰元整 （ ¥ 494900.00 ）						

备注：技术参数：详见合同附件1。

第三条　提交服务成果要求

3.1 服务期：　自合同约定服务期起始之日起,1年内完成全部服务内容　。

3.3 提交服务成果地点（或服务地点）：按采购单位指定。

3.4 乙方必须按报价文件承诺的服务响应条款向甲方提供服务。

第四条　产权

4.1 乙方应保证所提供的服务或其任何一部分均不会侵犯任何第三方的专利权、商标权或著作权。

4.2 乙方保证所交付服务的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。如乙方所交付服务有产权瑕疵的，视为乙方违约，按照本合同第10.3项的约定处理。但在已经全部支付完合同款后才发现有产权瑕疵的，乙方除了支付违约金，还应赔偿甲方由此产生的一切损失，并承担因产权瑕疵而侵犯任何第三方的专利权、商标权或著作权所产生的一切法律责任。

第五条　技术资料

5.1　甲方应向乙方提供甲方自身现有或掌握的、提交服务成果所必需的有关数据、资料等。但甲方没有义务负责向乙方提供自身不掌握的相关数据、资料等。

5.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

第六条　验收

6.1　乙方应对提交的服务成果作出全面检查和整理，并列出清单，作为甲方验收和使用的技术条件依据，清单应随提交的服务成果交给甲方。

6.2 乙方在指定地点提交服务成果后，甲方应组织专家进行评审。

6.3　甲方组织专家评审会对乙方提交的服务成果进行评审，评审通过后，上报甲方审定。在上述验收过程中，需对服务成果进行修改完善的，乙方要提供服务直至甲方审定通过方为验收合格。

6.4 对复杂的服务，甲方可请国家认可的专业机构参与验收，并由其出具验收报告，相关费用由甲方承担。

第七条 付款方式

7.1 合同签订且工程师入场，并完成杀毒软件授权及设备交付，且提交服务方案，经甲方审核通过后，25个工作日内，支付50%合同金额款项，计￥247450.00元（大写：贰拾肆万柒仟肆佰伍拾元整）；

7.2 乙方提供半年服务工作报告，经甲方审核通过后，25个工作日内，支付40%合同金额款项，计￥197960.00元（大写：壹拾玖万柒仟玖佰陆拾元整）；

7.3 乙方提交年度服务工作报告，经甲方审核通过后，25个工作日内，支付10%合同金额款项，计￥49490.00元（大写肆万玖仟肆佰玖拾元整）。

第八条 履约保证金

履约保证金：无

第九条 税费

本合同执行中相关的一切税费均由乙方负担，合同另有约定的除外。

第十条 违约责任

10.1 甲方无正当理由拒收服务的，甲方向乙方偿付拒收服务费总值的百分之五违约金。

10.2 甲方无故逾期接收和办理服务费支付手续的，甲方应按逾期付款总额每日万分之五向乙方支付违约金，但最高不超过逾期付款总金额的百分之五。

10.3 乙方逾期交付服务的，乙方应按逾期提供服务总额每日万分之五向甲方支付违约金，由甲方从待付服务费中扣除。逾期超过约定日期20个工作日不能提供服务的，甲方可解除本合同。乙方因逾期提供服务或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

第十一条 不可抗力事件处理

11.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

11.2 不可抗力事件发生后，不能履行合同的一方应以书面形式通知对方，并寄送有关权威机构出具的证明。

11.3 不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合同。

第十二条 合同争议解决

双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向合同签订地法院起诉，合同签订地在此约定为广西岑溪市。相关诉讼费、律师费、保全费等费用均由违约方承担。

第十三条 合同生效及其它

13.1合同经双方法定代表人或授权代表签字并加盖单位公章后生效（委托代理人签字的需后附法定代表人授权委托书，格式自拟）。

13.2合同执行中涉及采购资金和采购内容修改或补充的，须经财政部门审批，并签书面补充协议报财政部门备案，方可作为主合同不可分割的一部分。

13.3本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

13.4下述合同附件为本合同不可分割的部分并与本合同具有同等效力：

（1）成交通知书

（2）竞争性磋商采购文件服务需求一览表

（3）竞标函

（4）竞标报价表

（5）商务、技术条款偏离表

（6）服务承诺书

第十四条 合同的变更、终止与转让

14.1 除《中华人民共和国政府采购法》第五十条规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或终止。

14.2 乙方不得擅自转让其应履行的合同义务。

第十五条 其他事项

15.1 本合同一式五份，具有同等法律效力，甲方执二份，乙方执二份，采购代理机构执一份（可根据需要另增加）。

15.2 本合同甲乙双方签字盖章后生效，自签订之日起七个工作日内，采购人或采购代理机构应当将合同副本报同级财政部门备案。

甲方：（章） 岑溪市人民医院 2025年11月19日	乙方：（章） 广西元析科技有限公司 2025年11月19日
单位地址：岑溪市北山路2号	单位地址：广西壮族自治区梧州市岑溪市岑城镇城厢街十组（沙基路 5 号旁黄业钧屋三楼 302 室）
法人或委托代理人：	法人或委托代理人：
电话：0774-8201011	电话：17687433408
开户银行：农行岑溪市支行营业部	开户银行：中国工商银行股份有限公司岑溪市工农路支行
账号：20317101040006334	账号：2104370209300044015

附件 1：技术参数要求

序号	名称	数量	竞标响应
1	杀毒软件	1项	1.. 产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署；本次提供服务器客户端安全防护软件51套；
			2.单一管理控制中心统一管理分别部署在WindowsPC、Windows服务器、Linux服务器以及国产化服务器的客户端软件；
			3.▲提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数；
			4.支持跳转链接至云端威胁情报中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析；
			5.通过智能识别终端环境情况和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整客户端的资源占用(CPU、IO等），为业务让出资源，不卡业务，对业务零摩擦；
			6. 客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O风暴；
			7. 支持勒索可疑行为检测，通过行为AI能力对勒索信、命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截；
			8. 支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具；
			9. 支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell检测和威胁处置方式、暴力破解的威胁处置方式和Windows白名单信任目录；
			10. 支持配置不同的权限角色，支持超级管理员、普通管理员（管理）、审计管理员（查看）三种权限，并配置可管辖的终端范围，支持管理员账号限制IP登录；支持管理员账号采用双因素认证；
			11. ▲为方便病毒进行快速处置和持续监测，展示与当前院内正在使用的安全设备（防火墙、安全感知平台、上网行为管理）的联动状态，防止出现因设备断线导致缺少关键数据；
			12. 支持与院内安全感知平台进行联动，当检测到某主机有僵木蠕毒的C2通信时，支持手动或自动化将恶意域名信息下发到本产品做C2通信的封锁拦截，实现精准防远控，且安全态势感知的此事件不再重复告警；
			13. 支持与院内的防火墙进行联动，当检测到某主机有僵木蠕毒的C2通信时，支持手动或自动化将恶意域名信息下发到本产品做C2通信的封锁拦截，实现精准防远控，且防火墙的此事件不再重复告警；

			14.支持与院内的上网行为管理进行联动，支持管理员在上网行为管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息；包含三年规则库和软件升级服务；
			15. 支持基于威胁情报的病毒文件哈希值、行为、域名、网络连接等各项终端系统层、应用层行为数据在全网终端发起搜索,挖掘潜伏攻击，快速定位出全网终端感染该威胁的情况；
			16. 支持不同攻击阶段的主要攻击手法检测，对包括但不仅限于以下攻击手法精准检测，执行、持久化、权限提升、防御逃逸、凭证窃取、横向移动等攻击手法检测记录。显示事件详情，展示攻击手法对应的高危操作和威胁实体；
2	安全运营服务	1年	1. ▲服务资产数量：10个资产（业务系统）；服务频率：1年7*24小时。
			2.服务支持：全资产和精确资产两种模式暴露资产收集模式。收集到的暴露面信息包括域名、域名标题、IP地址、开放端口、资产指纹、移动端暴露面，并且能采集对应暴露资产的访问截图向甲方举证。
			3. ▲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，为甲方做好每一个高危可利用漏洞的防护工作，包括但不限于为甲方提供漏洞修复方案和安全设备防护策略,以及帮助甲方配置防护规则，保证甲方不因此出现重大事件和损失；
			4. 7*24小时威胁鉴定：具备云端检测和分析平台，通过采集甲方安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，为甲方提供7*24小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示；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，并支持根据客户情况提供备注；
			5. 服务支持：为甲方自定义配置安全规则，以满足日益复杂的安全趋势所带来的安全监测需求；
			6. ▲安全专家结合威胁情报主动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。
			7. 策略管理：安全专家每月对安全组件上的安全策略进行统一管理工作，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。
			8.云端服务平台具备丰富的策略检查工具（40种策略检查的工具），支持排查安全设备防护策略配置的合理性。
			9. 为甲方提供7*24小时的安全守护，不论是白天、黑夜、节假日都能做到7*24H在线服务，并且在节假日期间每日为甲方提供《节假日值守总结》
			10. 为了保障服务质量和加强与甲方的沟通，乙方承诺为甲方配置一名经验丰富的云端安全专家作为专属服务经理,并且实时响应甲方咨询的网络安全相关问题；

			11. 提供的服务成果展示门户（或用户 Portal），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。
			12. 提供的服务监控门户（或用户Portal）具备服务质量可视化展示，能通过可视化的数据，清晰地了解安全专家的服务水平，包括漏洞闭环率、漏洞平均响应时长、漏洞平均闭环时长、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，已验证乙方所承诺的服务SLA。
			13. 为确保本次服务有效性，项目启动前召开方案实施会议,甲方有权要求乙方提供演示平台对服务平台进行功能演示,确保满足本次服务安全需求。如无法满足，进行定制化修改，直至满足本次服务全部需求。
			14. 为甲方提供一次以下运营整改服务，整改后需达到三级等保测评要求： ①网络设备运营服务； ②安全设备运营服务； ③漏洞详情运营服务；
3	数据库防护系统	1套	1. 支持向代理、桥接代理、策略路由部署模式；
			2. 支持分布式部署，各节点状态可在界面统一管理，配置、策略自动同步至节点；
			3. 支持Oracle、MySQL、Oceanbase、TDSQL、TBase、ElasticSearch、Teradata、MongoDB、Hive等主流数据库；
			4. 支持GaussDB、达梦、人大金仓、南大通用、神舟通用等国产数据库；
			5. 支持MySQL数据库TLS链路加密协议；内置缺省刷库、拖库、撞库等防护策略；
			6. 支持系统登录时的多因子身份认证，多因子包括但不限于手机动态令牌的OTP登录、短信认证、密码认证；
			7. ▲支持客户端语句过滤白名单功能，包括PLSQL Developer、SQL Developer、DBArtisan、SQLPlus、Navicat、SQL Server Management Studio、Console等客户端，缺省白名单超过100条；
			8. 提供虚拟补丁防护，内置多种数据库漏洞补丁，包括SQL注入、缓冲区溢出等漏洞检测规则，可识别并阻断外来攻击。其中Oracle数据库漏洞数量500个；
			9. 支持告警配置及多种告警发送方式，包括FTP、邮件 、SYSLOG、SNMP等；
			10. 支持基于网络五元组配置包过滤策略规则；
			11. 支持日志内容能够详尽地记录访问行为发生的具体特征，包括数据库名称、操作类型、数据库用户、操作对象、数据库IP、会话ID、客户端IP、主机名、系统用户名、客户端端口、捕获时间、执行时长、动作、记录方式、风险等级、匹配策略、SQL内容、SQL结果、SQL模式、会话ID、返回行数等，并支持日志回放；

			12. ▲支持业务字典功能。用户可在业务字典中配置业务IP、业务账号、业务操作、业务操作对象四个维度对应的业务语句,为用户查询日志时提供经过翻译更易读的SQL语句，业务字典配置可通过模板导入，快速配置；
4	防火墙	1台	1. 性能指标：网络层吞吐量20Gbps，应用层吞吐量10Gbps，并发连接数300万，每秒新建连接数9万；
			2. 硬件指标：产品采用多核并行处理架构，配置8个千兆电口，4个千兆SFP口，2个万兆SFP+口，1U机箱；
			3. 产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式；
			4. 产品支持链路连通性检查功能，支持基于3种以上协议对链路连通性进行探测，探测协议包括DNS解析、ARP探测、PING和BFD等方式；
			5. 产品支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持3种的调度算法，包括带宽比例、加权流量、线路优先等；
			6. 产品支持多对一、一对多和一对一等多种地址转换方式;
			7.产品支持IPsec VPN和SSL VPN功能；
			8.产品支持IPSec VPN智能选路功能，根据线路质量和应用实现自动链路切换；
			9. 产品支持3种以上的用户认证方式，包含但不限于单点登录、本地账号密码、外部账号密码认证；
			10. 产品支持对9000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；
			11. 产品支持多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求；
			12. 产品支持对ICMP、UDP、DNS、SYN等协议进行DDOS防护；
			13. 产品支持https解密功能，支持TCP代理和SSL代理；
			14. 产品支持对压缩病毒文件进行检测和拦截，压缩层数支持16层；
			15. 产品内置13800种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则；
			16. 产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过120万种，可识别主机的异常外联行为；
			17. 产品内置超过4500种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL 、网站扫描、网页木马等攻击类型进行防护；
			18. ▲产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；

			19. 产品可识别IT、OT、IoT混合资产，获取IP、MAC、操作系统、类型、厂商等信息，终端类型包括但不限于： （1）PC、瘦客户机、手机、平板、交换机、路由器、防火墙、无线控制器、服务器等IT资产 （2）摄像头、门禁、打印机、投影仪、VOIP设备、条形码扫描仪、医学图像打印机、呼吸机、心电图仪、监护仪、放射系统等IoT资产。
			20. ▲产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危IP；
			21. ▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；
			22. 产品支持云威胁情报网关技术，通过云端未知威胁主动探测技术，达到5min内未知威胁情报全网设备下发，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全；
			23. 提供：产品质保和软件升级3年；
5	数据安全防泄密模块	1项	1. 支持按照内部文件来源的服务器IP、域名、端口、URL路径等方式区分敏感数据源和非敏感数据源，可识别的来源类型包括但不限于WEB业务系统、共享服务器、代码库、办公工具等；
			2. 支持按照数据接收对象的IP、域名、端口、URL等方式进行定义敏感行为，支持的接收对象分类包括但不限于：内部WEB业务系统、内部共享服务器、内网CS工具、内部代码仓库、邮箱等；
			3. 支持基于文件来源、文件类型、文件名、文件大小、文件敏感内容、文件MD5等因素配置敏感数据分析类型，支持自定义敏感等级；
			4. ▲支持基于敏感数据来源追踪数据流转的过程，包括但不限于敏感数据流转过程中的文件下载、文件复制、文件剪切、文件夹重命名、文件重命名、修改后缀、压缩、加密压缩、解压、另存为等异常动作，并支持以流转图或时序图的方式进行可视化展示数据流动轨迹；
			5. 审计策略基于时间、用户对象、文件类型等维度进行策略自定义，支持文件外发时自动截屏，并配置策略离线生效；
			6. 可对IM聊天软件、邮件客户端、云笔记、网盘、浏览器、远程协助工具、文件传输工具、会议软件、打印机、文件解密等途径的文件外发行为进行审计；
			7. 文件外发管控策略基于时间、用户对象、外发程序、浏览器类型、是否敏感数据等维度进行自定义，支持终端提醒功能，提醒内容可自定义，可配置文件外发时自动存档，支持离网持续管控；
			8. ▲支持通过剪贴板进行外发时可以基于剪贴板的内容进行外发管控；
			9. 防泄密平台会通过文件流转审计跟踪文件的操作行为，能对重命名、压缩、加密压缩后的文件进行源头文件的追溯封堵,避免文件变形逃逸封堵；
			10. 支持对文件另存为一个新的文件时，新文件仍能根据文件最初的来源进行管控；
			11. 可通过列表展示风险事件的事件信息、用户信息、聚类事件数量、时间和处理状态，可查看事件详情并对事件进行处理；

			12. 支持对特定的文件进行文件指纹匹配，可设置匹配程度；支持按照日期、外发通路、用户/用户组、文本相似度进行过滤；
			13. 支持对所有审计的日志进行汇总展示，包括文件外发日志、操作审计日志、邮件外发日志、即时通讯日志、外接设备日志、文件解密日志等；
			14. 查看详细的文件流转跟踪图，包含文件的全流程操作的记录，从文件下载、文件操作、文件外发的记录。 （数据安全防泄密模块属于全网行为管理设备模块升级；具有防泄密核心功能。属于授权内容部分。）

附件 3：服务承诺书

承诺如下：

1. 当系统出现故障时，立即响应，4小时内工程师解决问题，如未解决立即安排二线工程师在12小时内到达现场，到达现场后8小时内需排除故障，恢复业务正常状态。

2. 当发生突发性故障时，乙方能够按照相应处理流程在规定的响应时间内快速排查解决，最大程度的抢救数据，保证数据完整性。同时协助甲方对数据库所在整个软硬件环境出现的问题，进行故障排除。并按甲方要求，及时形成事故处理报告及改进意见。

3.售后服务时间及内容

序号	货物名称	售后服务时间及内容
1	杀毒软件（1项）	提供3年软件升级服务，在软件升级服务期内，对软件内核进行版本升级及更新
2	安全运营服务（1年）	提供1年 7*24小时的安全守护，不论是白天、黑夜、节假日都能做到7*24小时在线服务,并且在节假日期间每日都能为甲方提供《节假日值守总结》
3	数据库防护系统（1套）	提供3年软件升级服务，在软件升级服务期内，对软件内核进行版本升级及更新
4	防火墙（1台）	提供3年硬件质保和软件升级服务，在服务期内，整机给予保修并对软件内核进行版本升级及更新
5	数据安全防泄密模块（1项）	供1年软件升级服务，在软件升级服务期内，对软件内核进行版本升级及更新

供应商名称（盖章）：广西元析科技有限公司