濮阳医学高等专科学校基础网络铺设及安全运维项目

合 同 书

甲方：濮阳医学高等专科学校

乙方：郑州云智信安安全技术有限公司

合 同

采购编号：濮财市直招标采购-2023-58—2

采购人（以下称甲方）：濮阳医学高等专科学校

供应商（以下称乙方）： 郑州云智信安安全技术有限公司

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》等相关法律法规的规定，甲乙双方按照濮阳医学高等专科学校基础网络铺设及安全运维采购项目（**安全运维**）结果（采购项目编号：濮财市直招标采购-2023-58），遵循平等、自愿的原则，经友好协商，签订本合同。

一、合同标的

乙方应当根据采购公告、投标（响应）文件及中标（成交）通知书等并按照甲方需求提供下列货物。

序号	产品名称	品牌	型号	参数	单位	数量	单价	总价
1	明御综合日志审计分析平台	杭州安恒	DAS-LOG-120	详见以下表格	台	1	81000.00	81000.00
2	AiNTA 流量审计分析平台	杭州安恒	DAS-ABL-SP800		台	1	77000.00	77000.00
3	AiLPHA 高级威胁检测与分析系统	杭州安恒	DAS-ABL-AXDR1800		台	1	193000.00	193000.00
4	安全托管运营服务 MSS	杭州安恒	MSS-P20		年	1	134000.00	134000.00
合计总报价		大写：肆拾捌万伍仟元整 小写：485000.00 元						

产品技术参数

序号	产品名称	技术参数
1	明御综合	1.硬件规格：标准 1U 硬件，1 个 console 口，至少含 6 个千兆工作管理口(1 管理

	日志审计分析平台	口+1HA 口+4 审计口），硬盘≥2T，内存≥8G，单电源 2.功能扩展： （1）采用解决方案包上传对产品进行功能扩展，无需要代码开发； （2）支持 kafka 日志接收转发、大数据安全域同步、APT 沙箱报告转发等大数据联调功能，Kafka 收发支持 SSL 加密。 （3）支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配； （4）支持系统配置备份自动备份至远程服务器。 3.日志收集： （1）支持 Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP 协议日志收集； （2）支持使用代理(Agent)方式提取日志并收集，对 Agent 进行统一管控，包括卸载、升级、启动及停止操作； （3）支持将日志收集策略统一分发； （4）支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等 4.日志分析： （1）日志支持文本方式输出给第三方平台，进行数据共享； （2）内置 5000+解析规则，支持对收集的 5000+设备类型日志进行解析（标准化、归一化），解析维度多达 200+，解析规则可以根据客户要求定制扩展； 5.支持分词算法的日志解析 （1）可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息； （2）内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为 6 大类 50+子类的安全分析场景。 6.日志查询：支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。 7.脆弱性管理：支持内置 73000+条 CVE 漏洞数据知识库；支持内置数十项符合 OWASP 的 Web 漏洞数据知识库。 8.告警功能：支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警； 9.用户管理：用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户；提供一键式故障排除功能； 10.资产管理：注册用户资产时，提供自动发现识别能力； 11.支持在 IPV6 混合网络中进行审计日志资产识别。
2	AiNTA 流量审计分析平台	1. 硬件要求：内存：≥16GB；硬盘：可用硬盘容量≥2TB，千兆 RJ45 网口≥6 个 2.情报管理：支持显示情报基本信息、情报更新记录，支持查询同步到本地的情报信息。 3.告警归并：支持展示高度聚合告警列表，对告警进行自动归并；支持多维度告警查询，支持威胁告警快速过滤，包括筛选、排除操作。 4.组网划分：支持自定义添加组网配置，并可根据配置对资产信息进行组网划分。 5.流量采集 ：支持自定义流量采集策略，包括过滤策略和采集策略，支持根据 IP 和协议进行过滤，包括 DNS、FTP、HTTP、HTTPS、IMAP、KRB5、LDAP、POP3、RDP、SMB、SMTP、SSH、TELNET、TLS 等。

		6.产品具备对维度深层次检测 APT 攻击方法的能力 7.弱口令检测： （1）页面支持多种类型弱口令策略可选，支持的口令字典库 50000 种以上； （2）支持自定义弱口令字典，可选不同格式弱口令，支持导入自定义弱口令列表； （3）WEB 登录参数灵活可配，支持字符串和正则表达式配置； （4）支持 Base64 编码弱口令和 md5 散列弱口令检测。 8.暴力破解： （1）支持 HTTP、FTP、Telnet、SMB、邮件（SMTP、POP3、IMAP）、RDP、MySQL、Oracle、SQL Server、PostgreSQL、Redis、Mongodb、SSH 等暴力破解检测，SSH 暴力破解支持爆破登录结果判定； （2）支持暴力破解检测策略自定义，支持添加暴力破解白名单功能。 9.扫描策略：支持端口扫描、主机 IP 扫描、Ping 扫射，支持自定义告警阈值。 10.域名检测：支持对 DNS 隐蔽隧道通信和 DGA 域名进行检测，用户可自定义域名检测域名长度和告警阈值，也可以选择是否检测 DGA 域名家族。 11.跨三层 MAC 地址获取： （1）支持跨三层 MAC 地址获取，用户可新增指定 SNMP 服务器，配置包括服务器 IP、ARP OID、获取时间间隔、每次获取最大个数、SNMP 版本（V1、V2C、V3）； （2）支持自动识别或手动添加交换机的 MAC 地址并进行识别排除，可自定义配置自动识别的个数阈值。 12.数据同步： （1）支持通过 Kafka、syslog 接口向态势感知平台报送流量审计数据与风险告警信息，Kafka 推送支持传输加密，支持 SSL、SASL 认证+SSL、Kerberos 认证+SSL 加密。 （2）支持通过 API 接口向态势感知平台推送资产信息。 （3）支持通过 API 接口向态势感知平台推送三层 MAC 地址信息
3	AiLPHA 高级威胁检测与分析系统	1.硬件要求：CPU≥2*16 核 32 线程、硬盘≥8T*4 、内存≥32G*8、网卡≥4 千兆电口，2 万兆光口； 2.行为审计与可疑通信检测：支持违规操作、违规访问、违规应用、违规外发等 300 种以上行为审计检测规则，可针对任意单条规则进行启用和禁用。支持隧道通信、可疑内容、恶意 IP、恶意域名、恶意证书、远程控制等 2000 种以上可疑通信检测规则，可针对任意单条规则进行启用和禁用； 3.扫描探查检测：支持端口扫描、服务扫描、Web 扫描、扫描器指纹检测 等 300 种以上的扫描探查检测规则，可针对任意单条规则进行启用和禁用。 4.漏洞利用检测：支持 SMB 漏洞、RDP 漏洞、软件漏洞、设备漏洞、系统漏洞、拒绝服务漏洞、shellcode 等 6000 种以上漏洞利用检测规则，可针对任意单条规则进行启用和禁用。 5.恶意文件检测：支持挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell 等 18000 种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用。 6.配置风险检测：支持弱口令风险、明文传输风险、HTTP 配置风险、中间件配置风险、数据库配置风险、服务配置风险等 300 种以上配置风险检测规则。 7.主机和账号异常检测：支持端口异常、主机对外扫描、主机对外攻击等主机异常检测能力，对任意单条检测规则支持启用和禁用。 支持登录异常、暴力破解、行为异常等账号异常检测能力，对任意单条检测规则支持启用和禁用。 8.Web 攻击检测：支持 Webshell 请求、XSS 攻击、SQL 注入、远程代码执行、命令注入、远程文件包含、本地文件包含、文件上传、路径遍历、信息泄露、越权访问、XXE

		注入、网页篡改、SSRF 攻击等 14 类、8000 种以上 web 攻击检测规则，对任意单条检测规则支 持启用和禁用。 9.产品具备 CC 攻击的检测方法的能力 10.加密攻击检测 ：支持解密流量检测特定攻击 11.支持 AI 规则引擎、AI 智能新型引擎，检测加密流量攻击 12.资产指纹识别：支持 Web 应用类指纹信息识别，识别类型：Web 服务器（OA、企业建 站系统、博客、门户、在线阅读等）、Web 组件、Web 中间件、邮件服务器等，识别 Web 应用类型指纹数量 18000+
4	安全托管运营服务 MSS	1. 资产发现与服务范围内资产管理：服务提供方应通过主动扫描和被动流量识别的方式 进行全网资产发现。服务提供方应在服务过程中持续对资产进行标签标记，要求平台具备标签类型、标签名称、标签权重、标签置信度等内容。 2.互联网暴露面检测：服务提供方应在用户提供的根域名、IP 等信息的基础上，对用户 在互联网上暴露的 IP 资产、指纹资产等信息进行搜集，并在人工检查整理后将报告发送至用户。服务提供方应具备专业的红队平台，在服务过程中能够自主选择暴露面搜集内容和深度，如选择全量或常见 CMS、邮箱、Github 信息等 3.互联网漏洞管理服务：服务提供方应支持 web 漏洞扫描结果+V 确认，表示该漏洞可靠性达到 90%以上，帮助用户快速的确认和处理漏洞。 服务提供方应 具备 CVE、CNVD、CNNVD、EXP、POC 等不同标签的漏洞情报、需要关注的重视程度，并能 够及时从包括安全客、freebuf、看雪论坛等平台获取安全资讯。 4.服务范围内资产威胁检测分析与处置：服务提供方应通过云端安全托管运营平台对服务内资产提供 7*24 小时威胁监测，并分析检测各项安全隐患，包括且不限于漏洞利用、弱密码、Webshell 写入、异常登录、木马回连等安全风险和异常行为。服务提供方应具备策略编排模块，能够及时针对用户提出的需求进行策略编排，包含策略模式、策略条件、策略类型、策略等级等内容。 5.安全运营知识库：服务提供方应具备专业内部服务知识库，提供包括攻击、威胁狩猎、风险管理、应急响应在内不少于 7 个维度的运营知识，要求储备内容不少于 3000 万字，方便时刻为用户提供所需的安全运营知识。 6.服务范围：为 20 个核心业务资产提供全年的 7*24 小时安全托管运营服务； （1）含 1 年资产管理服务，基于设备发现的资产与资产台账，为资产重要性进行分级打标； （2）含 1 年 2 次的互联网暴露面检测服务，搜集暴露的 IP、域名、端口等信息。 （3）含 1 年 4 次的互联网开放系统漏洞扫描管理服务，对互联网资产验证与修复跟踪。 （4）含 1 年 7*24 小时的服务范围内资产威胁检测与分析服务。 （5）含 1 年的服务范围内资产事件处置与应急响应服务。 （6）含 1 年 4 次的服务组件调优服务。 （7）含 1 年的情报订阅服务。 （8）含 1 年 2 次的复盘汇报服务。 （9）含按规定频率提供的各服务项报告。

二、合同价款

1. 本合同项下总价款为人民币（大写）肆拾捌万伍仟元整（￥485000.00 元）。

2. 本合同金额系固定不变价格，本合同总价款包括货物设计、材料、制造、包装、运输、安装、调试、检测、售后服务及将货物运至指定地点所发生的运费、装卸费等货物伴随服务的费用和所需缴纳的一切相关税费。

3. 本合同项下的采购资金付款进度按招标文件规定，按以下方式支付：

乙方合同履行达到 100%(条件)时，一次性全额付款，即人民币（大写）肆拾捌万伍仟元整（￥485000.00 元）；

4. 甲方付款前乙方应出具合法的发票。

三、交货和验收

1. 交货时间：自签订合同后 45 日历天内安装、调试、培训、验收完毕 。

对于甲乙双方协商进行分批交货的，可以补充详细的《分批交货进度要求》，作为本合同的补充。

2. 交货地点：濮阳医学高等专科学校

在送货前，乙方与甲方沟通确定具体交货时间、地点等交接货相关事宜，以便甲方做好接货准备。

3. 乙方交付的货物应当符合采购结果（含采购公告及响应文件等）所规定的货物名称、规格型号、数量等要求。乙方提供的货物不符合采购结果和本合同约定的，甲方有权拒收货物，由此引起的风险及损失由乙方承担。

4. 乙方应当将所提供货物的使用说明书、原厂保修卡等附随资料和附随配件、工具等交付给甲方；乙方不能完整交付采购结果规定的货物及附随资料、配件或者工具的，视为未按照合同约定交货，乙方应当在甲方指定的期限内负责补齐，因此导致逾期交付的，由乙方承担相关违约责任。

5. 乙方在甲方完成现场验收之日起自签订合同后 45 日历天内安装、调试、培训、验收完毕 ，验收合格的，甲方应当签收验收单或向乙方出具验收合格书。

6. 乙方提供的货物经甲方质量验收不合格的，乙方应当无条件进行重新返修、返工制作、更换，直至甲方验收合格为止，所需费用由乙方自行承担，同时，乙方应当承担相应的违约责任。

7. 本合同项下的货物及追加、更换、补充的货物（含零件、 部件、配件）的风险自货物经甲方签字确认收到货物时转移。

8. 由于不可抗拒因素，导致交付延期的产品，应该在同等价位不变的情况下使用最新版本的产品。

四、乙方保证

1. 乙方保证对其出售的货物享有所有权或处分权，并且没有法律、法规禁止或限制出售的情形。同时，乙方出售的货物也没有侵犯第三人的知识产权和商业秘密等权利。如甲方使用该货物构成上述侵权，乙方承诺承担全部相关责任。

2. 乙方保证所提供的货物的技术规格符合采购结果规定的技术规格，货物符合中华人民共和国的设计和制造生产标准或者行业标准。

3. 乙方保证货物是全新、未拆封且未使用过的原装合格正品（包括零部件）。如货物需安装或配置软件，乙方保证相关软件均为正版软件。

4. 乙方应当保证提供给甲方的合同货物符合采购文件的要求；所用材质的质量应当符合相关国家、行业标准要求；所用材质的环保要求应当符合国家强制性环保要求。乙方承诺对其所供货物及原材料的质量负责。

5. 根据甲方及项目需要，乙方应免费提供相关技术服务培训，包括但不限于以下内容：

(1) 技术知识介绍与讲解；

(2) 实际操作与演练；

(3) 案例分析与讨论；

(4) 答疑解惑；

(5) 其他甲方及项目要求的培训内容。

6. 系统集成不收取任何费用（包含接口费和工时费），如果涉及到二次开发，可另外协商。

五、保密条款

1、自本合同签订之日起，甲乙双方承担相互保密的义务和责任。乙方因履行本合同而获知的甲方的信息资料，包括但不限于文字、表格、图片、音视频以及各种介质提供的资料文件，只能用作履行本合同之用，双方同意严格保密，并不得用于任何其它任何用途。未得到甲方许可不得将上述信息资料透露给任何第三方。因其违约行为给甲方造成的损失，乙方应承担全部赔偿责任。

2、乙方在本条约所触及项目中了解到的甲方信息及相关资料均属机密资料，非经甲方书面同意不得以任何方式对外透露，并应采取积极措施予以保密。

3、乙方如依当属法令规定需提供甲方资料时，可按规定提供，但须书面通知甲方。

4、本合同的无效、解除或终止不影响上述保密条款的效力及履行。

六、保修条款

1. 本合同所购硬件设备质保期为叁年，安全托管运营服务 MSS 服务期限壹年。质保期内免费保养维修，乙方在接到甲方服务通知后 1 小时内响应，6 小时内到达现场服务，24 小时内解决问题，如 24 小时内不能及时解决问题则提供备用软件服务，直到原软件修复，一切费用由乙方承担。

2. 免费保养维修期内，乙方负责上门对其提供的货物进行保养、维修和系统维护并不得收取任何费用。

七、合同解除

1. 乙方逾期交付货物超过___15___日的。

2. _____/_____

甲方根据上述情形主张解除合同的，应当书面通知乙方。

八、违约责任

1. 乙方逾期交货的，每延误一日则必须向甲方偿付合同总价款的违约金，但该违约金原则上不超过合同总价款的 10%。如因有关政府部门超期审批等原因造成甲方付款迟延的，不视为甲方违约，甲方不承担违约责任。

2. 乙方所交付的货物品种、型号等不符合采购结果及本合同规定的，甲方有权拒收，乙方应当向甲方支付合同价款总额 10%的违约金。如甲方拒收的，乙方应当在甲方指定的时间内补发符合竞价采购结果及本合同规定的货物。

3. 乙方未履行本合同项的其他义务或者违反其在投标（响应）文件中的相关承诺/声明/保证的，应当按照合同价款总额的 10%向甲方承担违约责任。

九、争议解决方式

1. 因货物质量问题发生争议的，应当邀请甲方认可的质量检测机构对货物质量进行鉴定，鉴定费由乙方承担。

2. 因履行本合同引起的或者与本合同有关的争议，甲乙双方应当通过友好协商方式解决；如协商不能解决争议的，任何一方可以向甲方住所地有管辖权的人民法院提起诉讼。

十、合同组成部分

采购公告、采购文件的需求明细、答疑内容、补充通知、投标（响应）文件、中标通知书、乙方在招投标过程中所作的其他承诺/声明/书面澄清以及在合同执行中甲乙双方共同签署的补充或者修正文件等文件均属本合同不可分割的组成部分，与本合同正文具有同等法律效力。以上合同组成文件与本合同正文存在不一致的，以本合同为准。

十一、合同生效

本合同自甲乙双方签字盖章之日起生效。合同一式六份，甲方四份，乙方两份。

甲方：濮阳医学高等专科学校

地址：濮阳市城乡一体化示范区文岩街商鞅路交叉口向东160米路北

法人定代表人/代理人：

联系电话：0393-6815016

开户银行：中原银行开州路支行

账号：601002161036409

签订地点：濮阳医学高等专科学校

签订时间：2024 年 2 月 5 日

乙方：郑州云智信安安全技术有限公司

地址：河南省郑州市高新技术产业开发区河阳路186号9号楼

法人定代表人/代理人：张晓

联系电话：0371-55906595

开户银行：中国光大银行股份有限公司郑州淮河路支行

账号：52100188000045631

签订地点：濮阳医学高等专科学校

签订时间：2024年 2 月 5 日