

合 同

合同编号：

甲方(采购人全称)：河南省新乡市中级人民法院

乙方(中标人全称)：新乡市科汇电子有限公司

乙方持河南省国贸招标有限公司签发的成交通知书，根据招标文件、乙方的投标/报价等文件[项目编号：豫财磋商采购-2025-108]，按照《中华人民共和国政府采购法》、《中华人民共和国民法典》等有关法律、法规，甲乙双方经协商一致，达成以下合同条款：

一、本合同名称：河南省新乡市中级人民法院全市两级法院天眼威胁实时监测预警感知系统三年期授权服务项目

二、本合同总价为人民币 1578000.00 元(大写：人民币壹佰伍拾柒万捌仟元整)。

本合同内容附件如下：

附件 1：服务内容及服务要求

附件 2：服务承诺

1. 乙方在此保证全部按照合同规定向甲方提供服务，并负责可能的弥补缺陷。
2. 甲方在此保证全部按照合同规定的时间和方式向乙方支付合同价或其他按合同规定应支付的金额。

三、服务方式与期限

1. 服务方式：7×24 小时电话咨询服务；5×8 小时远程技术支持服务。
2. 服务期限：三年。

四、付款程序、方式及期限

经甲方验收合格后，甲方向乙方一次性付清合同总价款(其中卫滨、牧野、凤泉、辉县、卫辉、新乡县、原阳县、延津县、封丘县、获嘉县、长垣县 11 家基层法院各支付 9 万元，剩余合同价款由新乡市中级人民法院支付)对于各院负担的合同金额，乙方分别为 11 家基层法院开具符合国家规定的发票。

五、甲乙双方应严格遵守招标文件要求，如有违反，按招标文件的规定处理。

六、项目招标文件及其修改和澄清、乙方投标文件、乙方在投标中的有关承诺及声明均为本合同的组成部分。

七、本合同签订和履行适用中华人民共和国法律，因履行合同发生的争议，由甲乙双方友好协商解决，如协商不成的，任何一方均可向签订合同地人民法院提起诉讼。

八、本合同未尽事宜，甲乙双方可签订补充协议，与本合同具有同等法律效力，但不能违反招标文件及乙方的投标或报价文件所规定的实质性条款。

九、知识产权：

乙方须保障甲方在使用该项目或其任何一部分时不受到第三方关于侵犯专利权、商标权或工业设计权的指控。如果任何第三方提出侵权指控，乙方须与第三方交涉并承担可能发生的一切费用，如甲方因此而遭致损失的，乙方应赔偿该损失。

十、合同生效、备案及其它

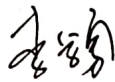
1. 本合同经双方代表签字并加盖公章后生效
2. 本合同一式六份，乙方持两份，甲方持四份。

甲方(公章)：河南省新乡市中级人民法院

地址：新乡市牧野区宏力大道与鸿源街交叉口
西 150 米

法定代表人或

授权委托人(签字)：



电话： 0373-2731305

乙方(公章)：新乡市科汇电子有限公司

地址：新乡市人民路豫程小区 8-1 号楼
4 层东北户

法定代表人或

授权委托人(签字)：



电话： 0373-3056556

开户银行：工行健康路支行三八分理处

账号： 1704320209201016043

签约时间：2015 年 4 月 28 日

签约地址：甲方所在地

附件 1：服务内容及服务要求

一、更新及维保服务内容

本项目我公司维保服务内容如下：

TSS10000-A58 威胁情报升级及软件维保服务 1 项

天眼 TSS10000-S53 流量传感器威胁情报升级及软件维保服务 2 项

天眼 TSS10000-S53 流量传感器威胁情报升级及软件维保服务 11 项

二、服务具体要求

1. 我公司提供原产品规则库更新服务、系统版本升级服务，升级后需达到如下要求：
 - 1.1 支持手动和 FTP 方式批量导入 PCAP 包对离线流量采集，文件大小不低于 1 个 G；并记录 PCAP 包导入记录及检测状态。
 - 1.2 支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：tcp、udp、icmp、http、dns、dhcp、smtp、pop3、imap、webmail、db2、oracle、mysql、mssql-db、PostgreSQL、sctp、sybase、smb、sip、ftp、snmp、telnet、nfs、ssl、ssh、ldap、radius、kerberos、netbios、ntp、vnc、ipv6 等。
 - 1.3 支持配置网络日志外发的标准模式、精简模式、自定义模式，支持外发的网络日志的类型包括：TCP 流量、UDP 流量、异常流量、SSL 加密协商、登录行为、域名解析、文件传输、FTP 控制通道、LDAP 行为、web 访问、邮件行为、数据库操作、telnet 命令、旁路阻断、MQ 流量、Radius 行为、Kerberos 行为、ICMP 流量、syn 流量等 19 种网络日志。每种网络日志，都支持自定义配置外发的字段。
 - 1.4 支持常见攻击行为检测，支持 HTTP 双向流量动态检测，检出类型包括：SQL 注入，命令执行，代码执行，跨站脚本攻击，权限绕过，暴力破解，扫描工具，数据库攻击，敏感信息泄露，挖矿检测，蠕虫传播，目录遍历，文件包含等。
 - 1.5 支持灵活开启机器学习模型，增强检测精度，模型至少包括：ICMP 隧道检测、DNSTunnel 检测、HTTP 隧道检测、CS 流量检测、MSF 检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH 爆破登录成功检测
 - 1.6 支持通过主机资产详情查看全部关联告警，同时针对单个资产也支持检索场景配置，关联告警支持按照 IP 归并，支持多维统计，包括但不限于：告警资产数量，不同攻击结果/攻击维度的资产数量，失陷资产组分布，未处置告警/全部告警、不同攻击结果/攻击维度告警数量、告警类型分布情况、攻击阶段分布情况、告警趋势图。
 - 1.7 支持场景化管理告警，可以根据不同的检索条件及顺序、列表字段及顺序生成自定义检索场景，并支持拖拽调节自定义场景顺序
 - 1.8 支持三级及以上级联部署，下级分析平台向上级分析平台发送告警和相关信息，在上级分析平台上进行汇总展示
 - 1.9 支持实时显示攻击源 IP 的画像信息，包括 IP 访问行为、IP 告警信息、网络测绘信息、处置建议、威胁级别、情报标签、关注热度、首次发现时间、最近发现时间等。
2. 我司提供的维保内容包括软件故障判断、软件报修登记以及版本优化升级的服务。7×24 小时电话咨询服务；5×8 小时远程技术支持服务
3. 拟派人员：我司派驻三名服务人员进行系统升级维保服务，拟派人员需具备相关技术能力。

附件 2：服务承诺

我司承诺质保期：采购人合同验收合格之日起 3 年；

我司维保内容：包括软件故障判断、软件报修登记以及版本优化升级的服务。7×24 小时电话咨询；5×8 小时远程技术支持服务。

我司拟派人员：我方派驻不少于三名服务人员进行系统升级维保服务，拟派人员具备相关技术能力。