合同编号：郑大-竞磋-2023-0025

郑州大学河南省教育信息安全监测中心省教育系统安全威胁情报库建设项目采购合同

甲方：郑州大学

乙方：河南尔享科技有限公司

本合同适用于郑州大学所有运行在校园网络上以满足学校教学、科研、管理和服务而建设，用于信息收集、存储、传输、处理、维护、使用和发布等用途的计算机软件类项目采购。其他类软件采购可参照本合同。

一、 合同内容及要求

1、合同内容

乙方根据甲方项目需求，完成河南省教育信息安全监测中心省教育系统安全威胁情报库建设项目，具体内容应充分满足合同附件1-技术参数部分所有要求。项目建设内容主要包括：1）完成威胁情报管理平台开发部署，支持对多源情报的采集、本地存储、情报管理、统计查询和情报订阅等功能；支持针对本地采集的日志告警进行本地情报生产功能；支持以API接口形式提供本地情报的应用等功能；2）提供和NTI情报源的数据同步，其中，恶意IPv6情报，数量10万；其它原始威胁情报数量600万条，新增同步IOC威胁情报数量10000

条/周；3）项目服务期三年。

2、合同要求

甲乙双方在签订合同的同时，签订《郑州大学信息系统建设网络安全责任协议》和《郑州大学信息系统建设信息安全保密协议》。

二、合同总价款

本合同总价款为人民币（大写）肆拾肆万柒仟圆整（￥447000.00元）。

序号	产品名称	单价（元）	数量	合计（元）	交货期
1	绿盟威胁情报平台V4.0(绿盟NTIPNX1-SNC)	447000.00	1	447000.00	自合同签订后30个日历日内
总计		人民币肆拾肆万柒仟圆整（￥447000.00元）			

三、质量要求或服务标准，乙方对质量负责的条件和期限

3.1 项目基本要求

1）乙方须按合同要求提供符合磋商文件要求的产品，且应达到乙方投标文件及澄清文件中明确的技术标准。甲方如果发现乙方所供产品不符合合同约定，甲方有权单方解除合同，由此产生的一切后果由乙方承担。

2）项目启动后，甲方人员应参与项目开发及系统整合实施过程的测试等相关工作。

3）乙方负责在项目完成后将项目实施所涉及的全部相关技术文件资料，以及系统测试、验收报告和系统测试使用的测试数据等文档汇集成册提交给甲方，并提供所有资料的电子文档；同时，提供本项目所有软件产品和数据资源的电子文件。

4）乙方负责在项目完成后对甲方人员进行免费的系统运维、二次开发等涉及项目后续发展的有关技术培训。

5）乙方应提供完整的项目实施计划、详细的工作内容安排及过程控制和验收方案等。

6）乙方应在合同签订后10个工作日内将威胁情报管理平台部署到甲方指定位置。

7）乙方应保证甲方在使用其所提供的产品时免受第三方提出侵犯其专利权、商标权或保护期的起诉。

3.2 项目实施计划

乙方根据本次项目的项目需求和时间周期的要求，项目工期计划为：

1）合同签订后1个日历天内完成需求确认工作。

2）合同签订后10个日历天内完成系统的功能、性能及安全相关测试。

3）合同签订后15个日历天内完成系统部署上线及相关试运行工作。

3.3 项目实施管理

乙方应对项目实施进行科学严格的管理，能够对项目进行系统计划、有序组织、科学指导和有效控制，促进项目全面顺利实施。

3.4 文档管理

乙方应根据开发进度及时提供有关文档，包括但不限于系统开发设计文档、数据库设计文档、系统安装部署手册、用户操作手册、常见故障及解决方案白皮书等。

3.5 用户培训

用户培训按照项目实施阶段进行，具体正式上线部署阶段，乙方将根据合同要求对用户方人员进行培训，在培训前，乙方负责编写《培训计划》，并负责准备和发放培训材料；乙方将派遣有经验的培训人员对用户进行培训。

四、服务约定

1、交货时间：自合同签订后30个日历日内。

2、交货地点：郑州大学南校区省教科网网络中心。

3、交货方式：甲方指定方式。

五、验收标准、方法

1、软件产品已经完整的部署在甲方提供的指定服务器资源上，配置学校内网IP地址，使用安全合规的测试数据，并在此运行环境上进行信息系统的功能测试、性能测试、安全测试等工作。

2、功能测试。乙方提交软件产品的功能测试报告，并对功能测试报告的真实性承担责任。乙方依据软件产品采购时的技术参数要求并结合功能测试用例等完成软件产品的功能测试，形成功能测试报告。

3、性能测试。乙方提交软件产品的性能测试报告，并对性能测试报告的真实性承担责任。甲方按照乙方提供的软件产品采购技术参数要求，提供硬件环境，乙方使用此硬件环境，在用户量、数据量的超负荷下，对软件运行时的相关数据进行分析测试，形成性能测试报告。

4、安全风险评估。乙方提交由甲方网络管理中心出具的安全基线配置核查报告和系统漏洞扫描报告；

5、其他验收文档。

乙方提交软件产品包括系统开发设计文档、数据库设计文档、API接口技术文档、系统安装部署手册、用户操作手册、常见故障及解决方案白皮书等相关验收材料。

六、结算方式及期限

根据本项目的具体情况，经甲乙双方协商后，结算费用按照阶段进行相应的比例支付，具体如下：采用人民币转账计算方式。乙方开具以郑州大学为客户名称的发票。

项目验收合格并经审计后，甲方向乙方支付合同总价款的95%，即人民币（大写）肆拾贰万肆仟陆佰伍拾元整（￥424650.00元）；质保期满30天内，甲方向乙方支付剩余的全部款项。

七、质保约定

乙方免费在交付终验后三年内提供系统服务，具体约定如下：

1、乙方在质保期内免费提供产品的运维、升级以及非模块级的功能需求变更、部署结构变化等服务。

2、乙方对于本项目中存在的Bug、缺陷、安全风险隐患等，在质保期内外均提供持续的修补和消除服务。

3、乙方根据甲方所有业务系统的需求和运作规律，有针对性地制定项目系统平台的运维和售后服务保障方案，建立完善的售后服务体系。

4、乙方在售后服务过程中提供完善的文档记录，包括故障处理报告、健康巡检报告、系统性能检测调优报告、系统安全检测报告、服务年度报告等。

5、乙方提供故障分级响应机制，按照售后服务计划和质量保证承诺向甲方提供优质的技术支持服务。

6、质量保证期内，自接到甲方的故障报修后，乙方2小时内派遣专业技术人员到达故障现场，技术人员在24小时内解决问题，直至软件系统正常运行及相关资源正常使用。

八、售后服务承诺

1、服务内容

1） 乙方承诺提供原厂商3年的质保。质保期自项目验收合格之日起开始计算。

2） 乙方承诺在质保期内免费提供产品的运维、升级以及非模块级的功能需求变更、部署结构变化等服务。

3) 乙方承诺对于本项目中存在的Bug、缺陷、安全风险隐患等，在质保期内外均提供持续的修补和消除服务。

4) 乙方承诺根据甲方所有业务系统的需求和运作规律，有针对性地制定项目系统平台的运维和售后服务保障方案，建立完善的售后服务体系。

5) 乙方承诺在售后服务过程中提供完善的文档记录，包括故障处理报告、健康巡检报告、系统性能检测调优报告、系统安全检测报告、服务年度报告等。

6) 乙方承诺提供故障分级响应机制，按照售后服务计划和质量保证承诺向甲方提供优质的技术支持服务。

2、响应方式和响应时间

故障级别	响应时间	技术人员到场时间	解决时间
I级：属于紧急问题；其具体现象为：系统崩溃导致业务停止、数据丢失、网络安全事件和安全隐患。	7*24小时实时响应	2小时内到达现场	3小时
II级：属于严重问题；其具体现象为：出现部分部件失效、系统性能下降但能正常运行，不影响正	7*24小时实时响应	2小时内到达现场	8小时

常业务运作。			
III 级：属于较严重问题；其具体现象为：出现系统报错或警告，但系统能继续运行且性能不受影响。	7*24 小时实时响应	2 小时内到达现场	12 小时
IV 级：属于普通问题；其具体现象为：系统技术功能、安装或配置咨询，或其他显然不影响业务的预约服务。	7*24 小时实时响应	2 小时内到达现场	即时

3、响应电话：0371-63288507

九、履约担保

无。

十、违约责任

1、乙方违约：乙方提供的服务内容不符合约定的质量要求或服务标准，甲方有权解除或终止合同，并要求乙方按合同总价款的 5%支付违约金，给甲方造成经济损失的，乙方还应按给甲方造成的经济损失如数赔偿；乙方未按约定期限交付标的物，每迟延一天须按合同总价款的 1%向甲方支付违约金。如果乙方对合同迟延履行超过合理期限，甲方有权解除或终止合同，并且要求乙方赔偿由此给甲方造成的经济损失。

2、甲方违约：甲方未能按双方约定的方式和期限支付合同价款，按有关法律规定对乙方承担违约责任。

十一、其他

1、组成本合同的文件及解释顺序为：投标书及其附件、本合同及补充条款；磋商文件及补充通知；中标通知书；国家、行业或企业（以最高的为准）标准、规范及有关技术文件。

2、双方在执行合同时产生纠纷，协商解决，协商不成，由郑州市仲裁委员会仲裁，不服仲裁向甲方所在地人民法院提起诉讼。

3、本合同未尽事宜，由甲乙双方协商后签订补充协议，与本合同具有同等法律效力。

4、乙方在合同中提供的乙方名称以及开户银行、户名、账号在合同终止前不得更改。

5、本合同共17页，一式十份，甲乙双方各四份，采购代理机构二份。

6、本合同双方签字盖章后生效，合同签署之日起至合同内容执行完毕为本合同有效期。

（本页为合同盖章页，无正文）

甲方（盖章）：郑州大学

法定代表人或代理人：

单位地址：郑州市高新区科学大道100号

电话：0371- 67781503

开户银行：工商银行郑州中苑名都支行

户名：郑州大学

账号：1702021109014403854

签订日期：2023.7.20

乙方（盖章）：河南尔享科技有限公司

法定代表人或代理人：

单位地址：河南省郑州市高新技术产业开发区银屏路15号

电话：0371-63288507

开户银行：中国建设银行郑州文博支行

户名：河南尔享科技有限公司

账号：41050167283500000130

签订日期：2023.7.20

签约地点：

附件 1　技术参数

技术参数内容及要求
一、平台功能 1. 要求集群分布式本地软件部署，支持硬件资源动态增加及软件平台免费节点扩容； 2. *支持通过插件化的方式快速添加情报源，可自定义情报源名称，情报源接入支持“拉取”和“推送”两种模式，支持 JSON/CSV/TXT/XML 情报源格式，可按情报源及情报类型配置准确度评分； 3. 提供和云端情报库情报信息的同步，要求具有 2 小时的同步频率； 4. 支持威胁预警功能，包含威胁通告和相关的处置建议； 5. 支持界面通过各种筛选条件，灵活获取批量 IOC 情报，筛选条件包含但不限于：时间（任意的时间范围）、情报类型（IP、域名、URL、样本 HASH）、威胁等级（高、中、低）、情报状态（有效/失效）、行业标签、录入方式等；情报导出格式支持 json、CSV 格式； 6. 支持界面通过各种筛选条件，灵活获取批量漏洞情报，筛选组合条件包括：更新时间（任意的时间范围）、威胁等级（高、中、低）、热度（高、中、低）、是否有 POC，漏洞名称支持关键字模糊搜索； 7. 支持界面通过关键字、时间范围、报告分类（专题报告、威胁热点、安全研究、行业动态）、报告标签（DDOS、botnet、物联网、金融、政府、运营商、工控、漏洞、APT、周报、月报）模糊查询战略情报； 8. 支持本地情报查询，在联网情况下支持一键跳转云端情报平台（无需再次登录），自动更新云端 IO 情报到本地；

9. *要求在本地平台进行可视化追踪溯源，用知识图谱展示 IP、域名、事件的各种关联关系；

10. *支持灵活的 API 数据输出，提供批量和特定应用场景的 API，包括：IP/URL/域名/样本 hash 的单一和批量检索 API、支持漏洞（漏洞名称或漏洞编号）/事件（事件名称）/攻击组织（id）的检索 API、通过 API 批量获取指定“应用情景”情报数据，如通过 API 输出高危类型的矿池/C2/僵尸网络/DDOS 等情报数据，可通过 API 输出用户内部的威胁情报数据（如手工录入的高危情报等），输出格式支持：STIX2.0；

11. 支持定期自动生成统计报告，可自定义配置“统计报告”任务，配置项包括：报告类型/内容、生成周期（单次生成/定时生成）、报告名称、收件邮箱等；生成的报告可在任务页面进行下载（word、csv），也可定期发送到指定邮箱；

12. *提供攻击组织档案馆，其中 APT 组织档案数量 300 个；

13. *支持基于本地的网络和安全设备日志，进行本地高级情报生产，提供生成本地攻击团伙情报的能力；

14. *支持对本地攻击团伙的持续监控，提供攻击团伙活动监控大屏和分布大屏；

二、情报数据

15. 支持基于本地的网络和安全设备日志，生产关基团伙情报数据，并提供对关基团伙情报的活动监控大屏和分布大屏。

16. 提供基于本地网络和安全设备日志的情报生产-团伙运营报告，每周生成运营报告，并支持通过配置进行邮件发送。

17. 情报数据种类包括 IOC（恶意 IP、恶意域名、恶意 URL、恶意 HASH）、IOC 相关联的上下文情报（如 IP 开放的端口、服务等），漏洞情报、威胁事件情报、攻击组织情报、攻击事件情报、威胁通告和处置报告、战略情报。其中原创漏洞 130 个；战略报告需覆盖网络安全整体趋势、DDOS 攻击、物联网、Botnet 专项研究报告、IP 惯犯与 IP 团伙专项研究报告、金融行业报告等；

18. *恶意 IPv6 情报，数量 10 万；其它原始威胁情报数量 600 万条，新增同步 IOC 威胁情报数量 10000 条/周；

19. *所有威胁情报数据在数据库中应为明文存储，便于客户对威胁情报的直接使用和二次加工；数据存储结构符合国标规范、国际 STIX 规范，数据明文列表展示、可进行情报数据的全生命周期管理；

20. 威胁情报数据的描述应符合国际标准 STIX V2.0，并支持对应的 API 输出；

21. 可通过 Restful API 进行威胁情报数据获取，为了保证传输过程的安全性，API 需使用 HTTP 加密协议；

三、互联网威胁情报网站

要求提供互联网上的威胁情报网站集中查询接口，便于实时查询最新的威胁情报，必须同时满足如下条件：

22. 能提供全球攻击源 IP 实时分布；

23. 能提供强大而灵活的搜索功能，支持 IP、域名、文件 HASH 查询；

24. 支持任意关键字查询，如输入事件名称、组织名称等；

25. 支持带有逻辑表达式的高级查询，包括如下场景：一键查询最近 30 天的 IP、域名、漏洞、威胁事件情报数据；

四、处置手册

针对热点漏洞和热点安全事件，能提供及时的威胁预警通告，并能提供相应的处置手册，必须同时满足如下条件：

26. *威胁预警通告需提供 PDF 离线下载版本，1 周 1 篇；

27. *针对威胁预警通告，需提供详细的处置手册，且能提供 PDF 离线下载版本；

五、安全研究能力

能够提供高价值战略情报，必须同时满足如下条件：

28. *连续 6 年以上（含 6 年）发布过年度 DDoS 攻击态势报告；

29. *连续 2 年以上（含 2 年）发布过年度网络安全观察报告；

30. *连续 2 年以上（含 2 年）发布过年度僵尸网络（Botnet）趋势分析报告；

31. 不仅能覆盖传统的互联网领域，还应能覆盖物联网领域，并连续 2 年以上（含 2 年）发布过年度物联网专项安全研究报告；

32. 提供热点威胁周报和月报，且周报和月报里必须包含热点漏洞和热点威胁事件信息；

六、产品要求

33. 产品取得威胁情报产品软件著作权；

34. 产品具有威胁情报产品的 CNNVD 兼容性认证；

35. *产品入选 Gartner 全球威胁情报市场指南（Market Guide）推荐产品（Market Guide for Security Threat Intelligence Products and Services 报告）；

七、厂商要求

36. *厂商参与威胁情报领域的国家标准《信息安全技术网络安全威胁信息格式规范》制定。

37. *厂商被 IDC 列入威胁情报市场“领导者”象限。

38. 厂商获得由中国信息安全测评中心颁发的信息安全服务(安全开发类二级)资质证书。

39. 厂商获得由中国信息安全测评中心颁发的信息安全服务(安全工程类三级)资质证书。

40. 厂商获得 ISO 22301 业务连续性管理体系认证证书。

41. 提供厂商针对本项目的授权及售后服务承诺函并加盖原厂公章。

附件 2：售后服务承诺

1、服务内容

1）乙方承诺提供原厂商 3 年的质保。质保期自项目验收合格之日起开始计算。

2）乙方承诺在质保期内免费提供产品的运维、升级以及非模块级的功能需求变更、部署结构变化等服务。

3）乙方承诺对于本项目中存在的 Bug、缺陷、安全风险隐患等，在质保期内外均提供持续的修补和消除服务。

4）乙方承诺根据甲方所有业务系统的需求和运作规律，有针对性地制定项目系统平台的运维和售后服务保障方案，建立完善的售后服务体系。

5）乙方承诺在售后服务过程中提供完善的文档记录，包括故障处理报告、健康巡检报告、系统性能检测调优报告、系统安全检测报告、服务年度报告等。

6）乙方承诺提供故障分级响应机制，按照售后服务计划和质量保证承诺向甲方提供优质的技术支持服务。

2、响应方式和响应时间

故障级别	响应时间	技术人员到场时间	解决时间
I 级：属于紧急问题；其具体现象为：系统崩溃导致业务停止、数据丢失、	7*24 小时实时响应	2 小时内到达现场	3 小时

网络安全事件和安全隐患。			
II 级：属于严重问题；其具体现象为：出现部分部件失效、系统性能下降但能正常运行，不影响正常业务运作。	7*24 小时实时响应	2 小时内到达现场	8 小时
III 级：属于较严重问题；其具体现象为：出现系统报错或警告，但系统能继续运行且性能不受影响。	7*24 小时实时响应	2 小时内到达现场	12 小时
IV 级：属于普通问题；其具体现象为：系统技术功能、安装或配置咨询，或其他显然不影响业务的预约服务。	7*24 小时实时响应	2 小时内到达现场	即时

3、响应电话：0371-63288507

乙方（盖章）：河南尔享科技有限公司