

长垣市公安局采购手机取证分析系统及 APP溯源分析系统项目 采购合同

项目编号：长财磋商采购-2023-78

采购方：长垣市公安局

供应商：河南灵创电子科技有限公司

签订日期：2023 年 9 月



项目名称：长垣市公安局采购手机取证分析及 APP 溯源分析系统项目

项目编号：长财磋商采购-2023-78

甲方：（采购人）长垣市公安局

乙方：（中标供应商）河南灵创电子科技有限公司

甲、乙双方根据《中华人民共和国采购法》、《中华人民共和国民法典》等法律法规的规定，按照 长财磋商采购-2023-78（招标编号）的招标结果签订本合同。

1. 货物内容

1.1 货物名称：详见附件 1

1.2 技术参数：详见附件 1

1.3 数量（单位）：详见附件 1

2. 合同金额

本合同金额为人民币（大写）：576400 元（¥伍拾柒万陆仟肆佰元整）。

乙方账户信息：

户名：河南灵创电子科技有限公司

开户行：中国工商银行股份有限公司郑州桐柏路支行

账号：1702021309200243430

3. 技术资料

3.1 乙方按招标文件规定的时间向甲方提供使用货物的有关技术资料。

3.2 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。

4. 知识产权

乙方保证所提供的货物或其任何一部分均不会侵犯任何第三方的知识产权。

5. 产权担保

乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、查封等产权瑕疵，由此给甲方造成的损失（包括但不限于甲方赔付第三方的费用及由此给甲方造成的诉讼费、律师费等）由乙方赔偿给甲方。

7. 转包或分包

7.1 本合同范围的货物，由乙方直接供应，不得转让他人供应。

7.2 除非得到甲方的书面同意，乙方不得部分分包给他人供应。

7.3 如有转让和未经甲方同意的分包行为，甲方有权给予终止合同。

8. 工期、项目地点

8.1 工期：10 日历天

8.2 项目地点：甲方指定地点

9. 货款支付

付款方式：货到安装、调试，验收合格后付合同价款的 100%

10. 税费

本合同执行中相关的一切税费均由乙方负担。

11. 货物包装、发运及运输

11.1 乙方在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

11.2 使用说明书、质量检验证明书、随配附件以及清单一并附于货物内。

11.3 乙方在货物发运手续办理完毕后 24 小时内或货到甲方 48 小时前通知甲方，以准备接货。

11.4 货物在交付甲方前发生的风险均由乙方负责。

11.5 货物在规定的交付期限内由乙方送达甲方指定的地点经甲方验收符合约定标准后视为交付，乙方同时需通知甲方货物已送达。

12. 质量保证及售后服务

12.1 乙方提供的货物是全新、未使用过的，并完全符合强制性的国家技术规范和质量规范和招标文件规定的质量、规格、性能和技术规范等的要求。

12.2 乙方提供的货物经正确安装、正常运转和保养，在其使用寿命期内须具有符合质量要求和产品说明书的性能。在货物质量保证期之内，乙方须对由于设计、工艺或材料的缺陷而发生的任何不足或故障负责。

12.3 根据甲方按检验标准自己检验结果或委托有资质的相关质检机构的检验结果，发现货物的数量、质量、规格与合同或样品及样品小样不符；或者在质量保证期内，证实货物存在缺陷，包括潜在的缺陷或使用不符合要求的材料等，甲方应尽快以书面形式通知乙方。乙方在收到通知后 7 日内应免费维修或更换有缺陷的货物或部件。如果乙方在收到通知后 7 日内没有弥补缺陷，甲方可以采取必要的补救措施，但由此引发的风险和费用将由乙方承担。

12.4 合同项下货物的质量保证期为自货物通过最终验收起 36 个月之内，因人为因素出现故障外，乙方对货物出现的质量及安全问题负责处理解决并承担一切费用。

12.5 合同项下货物质量保证期满后，因人为因素出现的故障不在免费保修范围内。对超过保修期的货物终生维修，维修时只收部件成本费。

12.6 在使用过程中发生故障，乙方在接到甲方通知后在 24 小时内到达甲方现场，24 小时内解除故障。

13. 调试和验收

13.1 乙方交货前对产品作出全面检查。

13.2 货物运抵现场后，甲方依据招标文件上的技术规格要求和国家有关质量标准在3个工作日内组织初步验收，并制作验收备忘录，签署验收意见。初步验收不合格的不予签收。

13.3 甲方对乙方提供的货物在使用前进行调试时，乙方负责安装并培训甲方的使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验收并签署验收意见。

13.4 对大型或技术复杂的货物，甲方应邀请国家认可的专业检测机构参与初步验收及最终验收，并由其出具质量检测报告。

13.5 验收时乙方必须到现场，验收完毕后作出验收结果报告。

14. 索赔

14.1 如果货物的质量、规格、数量、重量等与合同或样品及样品小样不符，或在质量保证期内证实货物存有缺陷，包括潜在的缺陷或使用不符合要求的材料等，甲方有权根据有资质的权威质检机构的检验结果向乙方提出索赔(但责任应由保险公司或运输部门承担的除外)。

14.2 在根据合同第12条和第13条规定的检验期和质量保证期内，如果乙方对甲方提出的索赔负有责任，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

14.2.1 在法定的退货期内，甲方将货物款退还给乙方，乙方按合同规定将货款退还给甲方，并承担由此发生的一切损失和费用，包括利息、银行手续费、运费、保险费、检验费、仓储费、装卸费以及为保护退回货物所需的其它必要费用。如已超过退货期，但乙方同意退货，可比照上述办法办理，或由双方协商处理。

14.2.2 根据货物低劣程度、损坏程度以及甲方所遭受损失的数额，经双方商定降低货物的价格，或由有权的部门评估，以降低后的价格或评估价格为准。

14.2.3 用符合规格、质量和性能要求的新零件、部件或货物来更换有缺陷的部分或/和修补缺陷部分，乙方承担一切费用和 risk 并负担甲方所发生的一切

直接费用。同时，乙方方应按合同第 12 条规定，相应延长修补或更换件的质量保证期。

14.2.4 如果在甲方发出索赔通知后 7 日内，乙方未作答复，上述索赔应视为已被乙方接受。如乙方未能在甲方提出索赔通知后 10 日内或买方同意的更长时间内，按照本合同第 14.2 条规定的任何一种方法解决索赔事宜，甲方将从合同款中扣回索赔金额。如果这些金额不足以补偿索赔金额，甲方有权向乙方提出不足部分的补偿。

15. 违约责任

乙方逾期交付货物的，乙方按逾期交货总额每日万分之五向甲方支付违约金。逾期超过约定日期 10 个工作日不能交货的，甲方有权选择同意延长交货期或解除本合同。甲方同意延长交货期的，延期交货的时间由双方另行确定。乙方仍按上述规定向甲方支付延期交货违约金。违约金由甲方从待付货款中扣除。乙方因逾期交货或因其他违约行为导致甲方解除合同的，乙方向甲方支付合同总值 30% 的违约金，如造成甲方损失超过违约金的，超出部分（包括但不限于甲方购买同等产品及服务多支付的费用以及由此给甲方造成的诉讼费、律师费等）由乙方继续承担赔偿责任。

16. 不可抗力事件处理

16.1 因不可抗力造成违约的，遭受不可抗力一方应及时向对方通报不能履行或不能完全履行的理由，并在随后取得有关权威机构出具的证明后的 15 日内向另一方提供不可抗力发生以及持续期间的充分证据。基本于以上行为，允许遭受不可抗力一方延期履行、部分履行或者不履行合同，并根据情况可部分或全部免于承担违约责任。

16.2 本合同中的不可抗力指不能预见、不能避免并不能克服的客观情况。包括但不限于：自然灾害如地震、台风、洪水、火灾；政府行为、法律规定或其适用的变化或者其他任何无法预见、避免或者控制的事件。

17. 合同纠纷处理

因本合同或与本合同有关的一切事项发生争议，由双方友好协商解决。协商不成的，任何一方均可向长垣市人民法院提起诉讼。

18. 违约解除合同

18.1 在乙方违约的情况下，甲方可向乙方发出书面通知，部分或全部终止合同，同时保留向对方追诉的权利。

18.1.1 乙方未能在合同规定的限期或甲方同意延长的限期内提供全部或部分货物，按合同第 15.3 的规定可以解除合同的。

18.1.2 乙方有转让和未经甲方同意的分包行为，按合同第 7.3 的规定可以解除合同的。

18.1.3 乙方未能履行合同规定的其它主要义务的。

18.1.4 在本合同履行过程中有腐败和欺诈行为的。

18.2 在甲方根据上述第 18.1 条规定，全部或部分解除合同之后，应当遵循诚实信用原则，全部或部分购买与未交付的货物类似的货物或服务，乙方应承担甲方购买类似货物或服务而产生的额外支出。部分解除合同的，乙方应继续履行合同中未解除的部分。

19. 其他约定

19.1 本采购项目的招标文件、中标供应商的投标文件以及相关的澄清确认函（如果有的话）均为本合同不可分割的一部分，与本合同具有同等法律效力。

19.2 本合同未尽事宜，双方另行补充。

19.3 本合同正本一式肆份，具有同等法律效力，甲、乙双方各执贰份。自采购合同签订之日起 7 个工作日内，甲方按照有关规定将合同副本报同级财政部门备案。

19.4 签定地点：



甲方：长垣市公安局

单位地址：

法定代表人：

委托代理人：张文书

电 话：

乙方：河南灵创电子科技有限公司

单位地址：河南省郑州市金水区东风路
与新科路28号院28号楼17层1706号

法定代表人

委托代理人：李磊

电 话：18503852338

签订日期：2013年9月22日



附件 1

序号	设备名称/ 规格型号	技术参数和要求	单位	数量	金额
1	盘古石手机取证分析系统 V5.0 9900T50	<p>1.1 硬件参数</p> <p>处理器不低于 Intel i7 9700K 3.6GHz</p> <p>内存不低于 64G</p> <p>存储不低于 512G SSD+8TB HDD *2</p> <p>显卡: RTX 2070 8GB</p> <p>2.1 手机解锁及镜像提取</p> <p>1. 支持 iOS 系统版本, iOS 7.0-iOS 16.2</p> <p>2. 支持 iOS 设备, iPhone 4, iPhone 4s, iPhone 5, iPhone 5c, iPhone 5s, iPhone SE, iPhone 6, iPhone 6 plus, iPhone 6s, iPhone 6s plus, iPhone 7, iPhone 7 Plus, iPhone 8, iPhone 8 Plus, iPhone X, iPhone XS, iPhone XR, iPhone XS Max, iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, iPhone SE2, iPad, iPhone12, iPhone12 Pro, iPhone 13 mini, iPhone 13, iPhone 13 Pro, iPhone 13 Pro Max, iPhone 14, iPhone 14 Plus, iPhone 14 Pro, iPhone 14 Pro Max;</p> <p>3. 支持 Android 系统版本, Android 2.0-Android 12.0;</p> <p>4. 支持华为手机 Harmony OS 2.0、3.0 手机系统;</p> <p>5. 支持 Android 设备品牌, 包括华为、OPPO、Realme、vivo、IQOO、小米、红米、荣耀、三星、魅族、中兴、努比亚、一加、锤子、坚果、联想、索尼、诺基亚、Moto、黑鲨、ROG、谷歌、酷派、海信、8848、小辣椒、华硕、夏普、美图、360、HTC、LG、金立等国内外品牌;</p> <p>6. iOS 设备提权提取, 通过临时提权的方式提取镜像(完整的文件系统)以及深度的 Keychain 数据, 范围(iPhone 5s-14 Pro, iOS 9.0-iOS 16.1.2)</p> <p>7. iOS 设备快速提取, 通过临时提权的方</p>	套	1	398400

	<p>式精准快速地提取指定的应用数据或系统数据(含 Keychain), 范围(iPhone 5s-14 Pro, iOS 9.0-iOS 16.1.2)</p> <p>8. iOS 密码工具, iTunes 备份密码提取, 范围(iPhone 5s-14 Pro, iOS 9.0-iOS 15.4.1);</p> <p>9. 支持提取 iTunes 无法备份的应用数据提取, 绕过系统限制, 提取无法备份的应用数据, 包括微信收藏附件、QQ 多媒体附件、Telegram、Potato、Signal、Twitter、Gmail 等;</p> <p>10. iOS 设备常规备份或加密备份提取, 范围(iPhone 4-14Pro, iOS 7.0-iOS 16.2);</p> <p>11. Android 设备解锁, 支持的手机品牌包括华为、OPPO、vivo、小米、锤子、坚果、美图等, 支持的系统版本从 Android 4-Android 9, 支持的方式包括利用高通 9008、MTK vcom、adb 等删除或禁用屏幕密码;</p> <p>12. 华为隐私空间密码破解, 支持 EMUI 9.0 系统的华为手机;</p> <p>13. 支持小米手机分身锁屏密码绕过;</p> <p>14. Android 设备应用锁/隐私密码绕过或禁用, 支持的手机品牌包括华为、OPPO、vivo、小米、荣耀、Realme、IQOO、红米、三星等;</p> <p>15. 支持绕过 vivo 文件保密柜密码;</p> <p>16. 华为镜像提取, 通过提权方式一键获取逻辑镜像(完整文件系统), 支持 EMUI 8.0 至 EMUI 9.1, 麒麟 659、960、970、980 芯片 30 多款设备;</p> <p>17. Android 设备 Pan ADB 镜像提取, 通过临时提权(免拆机刷机)的方式提取镜像(完整的文件系统)或物理镜像, 支持的芯片包括高通、MTK、麒麟等, 范围(Android 6-Android 12)</p> <p>18. 支持三星设备的临时提权, 支持 8.0-11 系统版本;</p> <p>19. Android 设备 Pan ADB 快速提取, 通过</p>		
--	---	--	--

	<p>临时提权(免拆机刷机)的方式精准快速地提取指定的应用数据或系统数据,支持的芯片包括高通、MTK、麒麟等,范围(Android 6-Android 12)</p> <p>20. Android 设备基于电脑手机助手备份协议等的高级备份,可自动点击提取,支持的手机品牌包括华为、OPPO、vivo、小米、荣耀、IQOO、Realme、红米、三星等,其中OPPO、Realme 为基于 WiFi 的高级备份;</p> <p>21. 支持在高级备份无法获取微信、QQ 等官方分身聊天记录中的语音、图片、视频及文件时,通过代理程序获取到这些数据并将其关联到聊天记录;</p> <p>22. OPPO 高级备份支持绕过隐私密码(搬家锁)进行数据提取,支持到 Android 12;</p> <p>23. 华为克隆,利用华为手机自带克隆功能完成数据提取;</p> <p>24. 华为隐私空间克隆,利用华为手机自带隐私空间克隆功能完成数据提取;</p> <p>25. Android 设备基于手机备份应用备份到本地后进行提取,可自动点击提取,支持的手机品牌包括华为、OPPO、小米、荣耀、红米、魅族等;</p> <p>26. 支持 Google ADB 备份及 APK 降级备份,其中降级完成后将自动安装回原始版本的 APP;</p> <p>27. 支持在提取过程中安装代理程序,利用代理程序获取手机基本信息、系统日志及应用程序列表等,在应用数据提取开始之前支持显示手机里的所有第三方应用程序;</p> <p>28. 8+N 路并行取证,所有提取方案均支持多路,支持并行提取同一型号设备,包括 iOS 提权、Pan ADB、华为高级备份、vivo 高级备份、三星高级备份、小米高级备份等方案,提取、解析任务分离,同时支持 N 路的解析任务;</p> <p>29. 智能引导式取证,提取过程中,需要人为干预的地方会结合图文提示进行引导,并</p>		
--	---	--	--

	<p>提供相关的 FAQ;</p> <p>30. 连接设备将弹框提示接入的型号, 可同时显示多台设备, 不论在任何页面均可在右下角显示当前连接的设备数量;</p> <p>31. 支持缓存手机基本信息和应用列表, 二次连接或中途断开的情况下无需安装代理程序重新获取;</p> <p>32. 支持显示历史提取任务, 显示的内容包括名称、存储路径、时间、类型、结果等, 可查看相应的详细日志, 并可根据时间或关键字快速筛选或查询;</p> <p>33. MTK 镜像提取, 支持 MTK 芯片的 Android 手机物理镜像提取;</p> <p>34. 高通 EDL/9008 镜像提取, 支持高通芯片的 Android 手机物理镜像提取;</p> <p>35. 华为 Fastboot 镜像提取, 支持华为 Fastboot 模式物理镜像提取;</p> <p>36. 三星 system 提取, 可提取 Android9、10 三星设备的部分文件系统;</p> <p>37. APK 提取, 支持提取 Android 设备中的 APP 安装文件;</p> <p>38. IPA 提取, 支持提取 iOS 设备中的 APP 安装文件;</p> <p>39. Android、iOS 截屏取证, 支持与其他取证方式的数据关联;</p> <p>40. 支持提取 SIM 卡中的数据;</p> <p>41. 支持在工具箱中单独提取 Android 设备的内部存储空间;</p> <p>42. 支持在工具箱 AirDrop 哈希转换手机号码</p> <p>43. 支持在工具箱提取苹果日志文件;</p> <p>2.2 数据解析/数据浏览/高级分析</p> <p>1. 支持 18 种常见检材格式的解析, 包括苹果文件夹、iTunes 备份、苹果 Tar 文件、苹果 Zip 文件、安卓物理镜像 (dd)、YunOS 备份 (目录)、OPPO 自备份、vivo 自备份、小米自备份、魅族自备份 (目录)、魅族自备份 (*.zip)、ADB 备份文件、安卓文件</p>			
--	--	--	--	--

	<p>夹、华为备份文件夹、SignalBackup 文件、安卓 Tar 文件、安卓 Zip 文件、SimCard Zip 文件等多种检材解析；</p> <p>2. 设备主要硬件信息与唯一标识等，包括手机厂商、型号、芯片、系统版本、IMEI、MEID、IDFA (iOS)、UDID (iOS)、是否 root、硬件平台等的相关信息；</p> <p>3. 系统基本信息，通讯录、短彩信、iMessage 消息 (iOS)、通话记录、多媒体 (拍摄的文件，包含缩略图)、日历、录音、通话录音 (Android)、备忘录、书签、语音备忘录 (iOS)、SIM 卡记录、系统输入法等；</p> <p>4. 系统日志及其他日志信息，开关机日志、Wifi 日志 (iOS)、应用日志、通讯行为 (iOS)、AirDrop 使用记录 (iOS)、电量使用日志 (iOS)、屏幕锁定状态 (iOS)、通知历史 (iOS)、推送消息历史 (iOS)、应用安装 (iOS)、应用 Internet (iOS)、应用使用 (iOS)、音频使用 (iOS)、相机使用 (iOS)、流量使用、备份历史 (iOS)、蓝牙日志 (iOS)、定位使用 (iOS)、配件连接历史 (iOS)、飞行模式历史 (iOS)、运营商注册历史 (iOS)、屏幕快照 (Android)、蓝牙设备、用户帐户、设备用户 (Android)、基站、用户词典、粘贴板 (iOS)、情景模式 (华为) 等；</p> <p>5. 应用列表，对每个应用提供版本号、应用标识 (包名)、安装路径、文档路径等信息；</p> <p>6. 即时消息，微信、企业微信、QQ、Soul、陌陌、探探、钉钉、默往、城信 (iOS)、蝙蝠、聊呗极速版、闲聊、Blued、旺信、人人网 (iOS)、遇见、蜜语、米聊、千牛 (iOS)、ICQ、阿里旺旺 (iOS)、子弹短信、有信、易信、多闪 (iOS)、Letstalk、野火 (iOS)、叮咚 (iOS)；</p> <p>7. 即时消息 (境外)，WhatsApp、Telegram、Telegram X (iOS)、twitter、Potato、Skype、Skype 中国版 (Android)、Sugram、Facebook、Messenger (iOS)、Signal (iOS)、Bria</p>			
--	--	--	--	--

	<p>Mobile(iOS)、KakaoTalk、Line、Viber、Tango、Yippi(iOS)、secret(iOS)；</p> <p>8. 浏览器，UC 浏览器、QQ 浏览器、Safari、Chrome、火狐浏览器(iOS)、百度浏览器、Opera 浏览器(iOS)、手机百度、百度极速版(Android)、安卓浏览器、系统浏览器、；</p> <p>9. 微博社区，新浪微博、百度贴吧、小红书(iOS)；</p> <p>10. 电子邮件，系统邮件、QQ 邮箱、网易邮箱大师、Gmail；</p> <p>11. 电子商务，淘宝、支付宝、京东、闲鱼；</p> <p>12. 地图导航，高德地图、百度地图、苹果地图、谷歌地图、腾讯地图；支持在线地图；</p> <p>13. 商旅出行，携程、去哪儿、航旅纵横、铁路 12306；</p> <p>14. 网络共享，百度网盘、DropBox(iOS)、Google Drive(iOS)、360 安全云盘；</p> <p>15. 健康，苹果健康、三星健康；</p> <p>16. 工具，Google 文档(iOS)、Google 表格(iOS)、快牙(iOS)、茄子快传、SSR、向日葵、米家；</p> <p>17. 输入法，系统输入法、搜狗输入法；</p> <p>18. 影音娱乐，抖音、快手(Android)、全民 K 歌、火山小视频；</p> <p>19. 金融理财，挖财记帐理财；</p> <p>20. 手机安全，360 手机卫士、腾讯手机管家(Android)；</p> <p>21. iOS Keychain，iOS 系统 Keychain 信息完整提取，包括：证书、账户密码、iTunes 备份密码、身份、网络密码、密钥等信息，经分析后，还包括应用 Token、AppleID、WiFi、邮箱帐号等；</p> <p>22. iOS 推送消息，显示推送消息的主题、内容、来源、时间、阅读日期等；</p> <p>23. 手机卡包，iOS 钱包分析，如手机卡、登机牌等；</p> <p>24. wifi 和 基站信息，可查看苹果基站信息，包括经度、纬度、时间等；</p>			
--	--	--	--	--

	<p>25. 删除恢复，恢复已删除的记录，直观区分正常和已删除记录；支持但不限于：通讯录、通话记录、短彩信、多媒体(基于缩略图的恢复)、备忘录、录音、微信、企业微信、QQ、支付宝、钉钉、陌陌、默往、探探、闲聊、Blued、Letstalk、soul、城信、微博、易信、Twitter、Line、sugram、viber、Chrome 浏览器、火狐浏览器、QQ 浏览器、夸克浏览器、手机百度、抖音、QQ 邮箱、高德地图、携程、淘宝、京东、百度贴吧、多卡宝等近百个应用；</p> <p>26. 过滤栏，根据数据特性进行相关过滤，快速定位数据；</p> <p>27. 信息溯源，全局搜索到的记录或任意一条记录可右键“转到”回溯到原始位置，方便查看上下文；</p> <p>28. 位置信息聚合，所有涉及位置信息（设备连接的 WIFI(含 BSSID)、基站、常去位置、图片位置等）的提取汇聚，可以在地图集中展示；可以根据需要，选择一定范围的地理信息，按时间进行轨迹展示；</p> <p>29. 多页面同时浏览分析，系统支持跨案件、跨检材地同时浏览多个应用数据，以 Tab 页面的形式展示；</p> <p>30. 语音通话分析，电信语音通话和 VoIP 通话记录合并分析；</p> <p>31. 文件聚合，支持按照文件类型进行聚合。文件类型包括但不限于：视频、音频、图片、数据库、办公文档、压缩文件等。同时支持各应用的多媒体文件分类聚合；</p> <p>32. Airdrop 隔空投送，电话哈希自定义号冠转换手机号；</p> <p>33. 文件系统展示，证据镜像支持文件系统结构展示。可以直接查看文件内容，导出文件等；</p> <p>34. Cookies，对聚合浏览器和内嵌 Web 组件应用的 Cookies 进行分析；内容包括来源应用、地址、键、值、最后访问时间和过期时</p>			
--	--	--	--	--

		<p>间;</p> <p>35. 全文检索, 提供全文检索功能, 对证据手机所有数据进行搜索;</p> <p>36. 自定义报告, 自定义报告功能, 可设置报告的基础设置、生成项目、是否包含重复数据和删除恢复数据, 报告格式等; 报告支持 HTML 格式导出;</p> <p>37. 数据导出, 可对单个标签页数据导出, 支持导出 HTML、Excel、CSV 等类型文件; BCP 数据包导出, 支持批量导出 BCP 数据包;</p>			
2	<p>盘古石星源 APP 溯源分析系统 V2.0</p> <p>PGS-9280</p>	<p>数据处理</p> <p>1、支持通过用户手动上传、采集工具自动上传、平台对接、互联网爬取的方式的 APP 汇聚。</p> <p>2、支持对主流加固厂商加固后的 APP 能做到自动脱壳, 支持最新一代的商用 dvm 壳的自动脱壳技术。</p> <p>3、支持样本的特征信息提取, 包括字符串、样本 hash、签名 hash、应用名、开发者、内嵌文件名、内嵌文件 hash、url、domain、ip、手机号码、邮箱、class、method、权限、组件等超 25 个维度</p> <p>4、支持对样本文件进行代码深度分析, 准确识别可能存在的恶意行为, 并给出具体的代码位置, 对于每种恶意行为问题, 给出详细的描述及代码位置, 对于同一恶意行为, 根据触发条件给出高中低三种危险级别。</p> <p>5、支持动态分析, 将样本在模拟环境中运行, 采集样本运行时的网络信息、文件操作信息、系统 api 调用、高权限操作等, 使用自动化测试并建立其中的关联关系。能够分钟级别给出判定结果。</p> <p>6、支持 SDK 快速识别, 并且平台至少具备 1500 个以上的第三方 sdk 的特征, 方便快</p>	套	1	178000

		<p>速识别。</p> <p>功能需求</p> <p>1、支持 1080P 大屏展示监控数据,数据包括可实时显示命中监控规则的 APP;APP 的分布数据,近一段时间 APP 增长趋势;APP 入库的排名;监控命中 APP 的排名;证书关联 APP 的排名。</p> <p>2、支持对全库样本(千万级规模)进行多维度搜索,包括字符串、样本 hash、签名 hash、应用名、开发者、内嵌文件名、内嵌文件 hash、url、domain、ip、手机号码、邮箱、class、method、权限、组件等超 25 个维度进行搜索支持。</p> <p>3、支持应用样本详情查看,可查看应用的包名、大小、版本、开发者、来源、文件 hash、历史版本等基本信息,同时可查看提取到样本的 IP、域名、邮箱、手机号、签名证书、运行截图等信息。</p> <p>4、支持提取到应用样本的代码信息,包括内部文件、URL、类名、方法名、字符串、Receiver、Provider、Service、Activity 等内容。</p> <p>5、支持发现 APP 漏洞,将漏洞分为高危、中危、低危,并生成 APP 漏洞报告,报告包括漏洞分布、漏洞排行,每个漏洞的描述、解决方法、以及涉及漏洞的代码。</p> <p>6、支持恶意行为发现,将恶意行为分为高危、中危、低危,可生成应用样本的恶意行为报告,报告包括恶意行为分布、行为的描述、涉及恶意行为的代码。</p> <p>7、支持全库的应用监控,可通过多种特征自定义规则对全库样本(千万级规模)进行规则扫描,对新增样本进行规则监控,对规则命中结果自动聚合统计;支持的特征组合</p>			
--	--	---	--	--	--



		<p>应不少于应用名、包名、文件 hash、开发者、证书 hash、证书发布者、证书使用者、字符串、权限、方法名、类名、成员/变量、域名、ip、邮箱、内嵌文件 hash、内嵌文件路径、Receiver、filter、Provider、Service、sender、Activity、maxSDK、minSDK、targetSDK 等 27 项内容。</p> <p>8、支持手动添加多个应用进行关联分析，关联内容包括共同的可疑 IP、域名、邮箱、证书、电话，并可根据关联生成关联图谱，快速发现应用之前的关系。</p> <p>9、支持对样本源码交互能力，提供对样本在线分析的交互式分析环境，包括配置关联、代码跳转到定义、交叉引用、调用序列、类层次关系等功能，可直接在线完成上下文分析。</p>			
<p>合计（含税）大写：伍拾柒万陆仟肆佰元整 小写：576400 元</p>					