项目编号:【 JSZC-320100-JZCG-T2026-0050 】

服务采购合同

项目名称：紫金山实验室软件漏洞测试与恶意软件行为分析项目

甲　　方：紫金山实验室　　（采购人）

乙　　方：四川战星科技有限责任公司　（供应商）

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律法规的规定，甲乙双方按照紫金山实验室的招标结果签订本合同。

第一条 合同标的

乙方根据甲方需求提供软件安全漏洞与利用技术测试平台和勒索软件行为分析与安全防护验证平台的开发服务，具体要求为：

A. 软件安全漏洞与利用技术测试平台

1.运行环境

(1) 提供完整的Windows编译工具链，配置必要的SDK环境变量和编译依赖库，禁用Windows自动更新机制，确保测试环境稳定性，提供编译环境配置文档；

(2) 要求开发一套C/S测试集验证框架，该框架服务器端可以获得测试集的执行状态，客户端要求能达到验证漏洞的测试条件；

(3) 要求提供调试环境，包括提供符号文件（PDB）及调试符号路径配置，支持WinDbg或Visual Studio调试器接入；

(4) 支持windows10以上操作系统。

2.基础漏洞测试集

(1) 基础漏洞测试集应覆盖主流漏洞类型，包括但不限于栈溢出、堆溢出、UAF、数组越界、整数溢出漏洞类型，漏洞类型不少于8种，每种漏洞类型测试集不少于4个，基础漏洞测试样例总共不得少于50个，x86和x64架构的测试集各不少于25个；

(2) 栈溢出要求包括地址覆盖、SEH覆盖等场景；堆溢出要求包括堆块元数据破坏、相邻堆块覆盖等场景；UAF要求包括对象释放后使用等场景；数组越界要求包括读越界、写越界等场景；整数溢出要求包括有符号溢出、无符号溢出、乘法溢出等场景；

(3) 测试样例按照统一的格式命名，格式为：[编号]_[漏洞类型]_[测试

样例名]_[架构]，所有源文件需遵循统一命名约定，每个漏洞类型独立目录存放；

(4) 每个测试样例需包含漏洞类型、触发条件、预期结果等信息；

(5) 每个测试样例需提供编译选项文档和对应的Makefile文件，明确指定如优化级别（如 /O0 或 /O2）、安全特性开关（如禁用 /GS）等编译选项，每个样例如有特殊编译需求需单独说明；

(6) 每个测试样例需尽量独立，减少外部依赖，如有依赖库，需在文档中列出；

(7) 每个测试样例需变量命名清晰，关键代码段需添加注释。

3.二进制利用手段测试集

(1) 二进制利用手段测试集应覆盖主流利用手段，包含但不限于unlink、shellcode、heap-overlapping、ROP、Stack Pivot、格式化字符串漏洞等利用手段，利用手段不少于8种，每种利用手段测试集不少于2个，利用手段测试样例总共不得少于40个，x86和x64架构的测试集各不少于20个；

(2) 二进制利用手段测试集应包含但不限于IAT、heap、stack三种地址泄露方式，每种泄露方式至少在2个不同手段中体现。

(3) 每个测试样例需包含利用手段、预期结果、利用步骤等信息；

(4) 每个测试样应至少达到弹出第三方进程（如计算器）、获取shell、生成新文件三个判断标准中的一种；

(5) 测试样例按照统一格式命名，格式为：[编号]_[利用手段]_[测试样例名]_[架构]，所有源文件需遵循统一命名约定，每个漏洞类型独立目录存放；

(6) 每种利用手段要求提供不少于1种的防护思路或加固方法，若加固方法有开源代码，需提供开源链接（如github等）。

4.网络应用漏洞测试集

(1) 网络应用漏洞测试集应包含至少4种漏洞类型，每种漏洞类型测试集不少于3个，网络应用漏洞测试样例总共不得少于30个，x86和x64架构的测试集各不少于15个；

(2) 漏洞类型至少包括但不限于栈溢出、格式化字符串、堆溢出、UAF等；

(3) 对网络应用进行漏洞收集，要求至少包含但不限于TCP，UDP等协议；

(4) 测试样例按照统一格式命名，格式为：[编号]_[漏洞类型]_[测试样例名]_[架构]，所有源文件需遵循统一命名约定，每个漏洞类型独立目录存放；

(5) 每个测试样例需包含漏洞类型、触发条件、预期结果等信息；

(6) 每个测试样例需提编译选项文档和对应的Makefile文件，明确指定如优化级别（如/O0或/O2）、安全特性开关（如禁用/GS）等编译选项，每个样例如有特殊编译需求需单独说明；

(7) 每个测试样例需尽量独立，减少外部依赖，如有依赖库，需在文档中列出；

(8) 每个测试样例需变量命名清晰，关键代码段需添加注释。

B. 勒索软件行为分析与安全防护验证平台

1.勒索软件行为分析

(1) 提供不少于120个样本的测试集，并且2020-2025年所出现的样本不少于20个；

(2) (1)测试样本应包含不少于15种家族；

(3) (2)测试样本应包含不少于6种加密算法，包括但不限于RSA、Curve25519、AES、ChaCha20、Salsa20等算法；

(4) (3)提供的测试样本中，需包含有双重或多重勒索行为的样本（比如加密文件、数据泄露、数据擦除、DDoS威胁等）；

(5) (4)对提供的样本进行特征解析，提取出勒索家族、加密算法、勒索行为、文件指纹、是否加壳、是否混淆、是否为自启动、是否提权、是否采用进程注入、是否规避检测机制、是否横向移动等，如有无法提供的需说明原因；

(6) (5)要求对测试样本进行分析，提供至少5份分析报告，报告中需要包括样本的网络行为（如攻击的服务和端口，勒索软件网络流量的分析等）、文件行为（如文件操作、注册表修改等）、API调用行为；

(7) (6)提供的勒索病毒测试环境要求逻辑隔离，可采用沙箱等方式；

(8) (7)勒索病毒运行的系统环境为windows10、windows11、windows server2012等平台。

(9) (8)提供测试集咨询和支持服务。

2.勒索软件安全防护验证

(1) 要求程序需要有非对称加密算法来上传加密密码，并且使用对称加密算法对所有文件进行加密；

(2) 程序需要有通信模块，并且包括服务器端和客户端，客户端执行后需要将加密密码和客户端设备的唯一识别码发给到服务器端，服务器端需要将信息进行记录；

(3) 程序要求加密的文件类型包。括.doc/.docx/.xls/.xlsx/.pdf/.jpg/.png且不少于30种类型；

(4) 程序在加密完文件后需要弹出窗口显示勒索信息，并且需要提供对应的输入窗口让用户输入解密密码，并且要求程序需要可以校验解密密码的正确性；

(5) 程序要求使用C/C++语言开发；

(6) 提供程序的编译环境；

(7) 以虚拟机方式（如vmware）提供运行测试环境；

(8) 提供程序咨询和支持服务。

乙方应按照投标文件中的承诺安排专人提供本合同项下的服务，未经委托人允许不得随意更换。

第二条 合同总价款

本合同项下服务总价款为人民币 壹拾壹万壹仟陆佰元整（大写）（¥111,600.00元），分项价款详见“附件：分项报价表”。（如有）除此之外，甲方不再向乙方支付任何其他费用。

本合同总价款包含乙方提供服务发生的所有含税费用、支付给员工的工资和国家强制缴纳的各种社会保障资金，以及投标人认为需要的其他费用等。

本合同总价款还包含乙方应当提供的伴随服务/售后服务费用。

本合同执行期间合同总价款不变。

第三条 组成本合同的有关文件

下列关于紫金山实验室 JSZC-320100-JZCG-T2026-0050 号标的采购文件及有关附件是本合同不可分割的组成部分，与本合同具有同等法律效力，这些文件包括但不限于：

（1）乙方提供的响应文件和报价表；（2）函件；

（3）分项报价表；（4）项目实施方案与服务说明；

（5）偏离表及说明；（6）服务承诺；

（7）中标通知书；（8）甲乙双方商定的其他文件等。

第四条 保密及知识产权

1、乙方应该保护甲方的知识产权，未经甲方同意，乙方不得对甲方的资料及文件擅自修改、复制或向第三方人转让或用于本合同以外的项目。如发生以上情况，乙方需向甲方承担【2】万元的违约金并承担一切由此引起的后果及赔偿责任。

2、如果乙方向甲方提供的服务或交付的工作成果涉及第三人知识产权等引发争议或诉讼，由乙方承担一切法律责任、费用和后果。若甲方因此而遭致诉讼和损失，则乙方还应赔偿甲方因此支出的律师费、鉴定费、交通费、诉讼费等一切合理开支和全部损失。

3、本项目所产生的一切成果及知识产权均归甲方所有。乙方不得以任何方式向第三方披露、转让、发表和许可使用有关的成果、信息、资料和文件。

第五条　　禁止贿赂条款

甲乙双方保证不向另一方及与本合作有关的任何第三方的工作人员直接或间接给予或收受任何可能影响公正执行公务的礼品、礼金、有价证券等财物，或接受、提供可能影响公正执行公务的宴请、旅游、健身、娱乐等活动安排。

如有一方违反本条规定，经核查清楚，守约方有权以书面形式通知违约方终止本合同，同时保留依法采取进一步法律措施的权利，违约方应承担由此造成的一切损失。

第六条 服务保证

1、乙方所提供的服务应与采购文件规定的要求及所附的偏离表相一致；若无特殊说明，按国家有关部门颁布的标准及规范为准。

2、乙方应保证服务完全符合合同规定的要求。

第七条 交付和验收

1、乙方应当在合同签订后__60__天内交付开发服务成果。

2、乙方交付的服务成果应当完全符合本合同、采购文件和响应文件所规定的要求。甲方自行组织或视情邀请相关专家或国家认可的检测鉴定机构参加验收，如乙方提供的服务成果不符合前述要求的，甲方有权拒收，由此引起的风险和责任包括不限于验收费用，由乙方承担。

3、质量要求

所有测试样例需遵循统一的格式命名和命名约定，变量命名清晰、关键代码段添加注释，确保测试环境逻辑隔离。分析报告须详尽，包括网络行为、文件行为和 API 调用行为。

4、验收要求

验收标准基于技术要求，包括测试集覆盖率、样本数量、家族多样性、加密算法类型等。交付内容通过甲方组织的验收测试，符合约定的技术指标和功能要求。交付内容包含以下项：

1）软件安全漏洞与利用技术测试平台 1 套，包含测试环境、基础漏洞测试集、二进制利用手段测试集、网络应用测试集。

2）勒索软件行为分析与安全防护验证平台 1 套，包含测试样本集、开发验证程序。

3）如上交付的 2 套平台，交付时需提供源代码，涉及的知识产权完全归紫金山实验室所有。

第八条 合同款支付

1、本合同项下所有款项均以人民币支付。

2、付款方式：

合同签订后，甲方支付合同总价款的 10%作为预付款。

供货结束并验收合格后，甲方支付合同总价款的 90%。

满足合同约定支付条件的，甲方收到乙方发票后 10 个工作日内，将资金支付到合同约定的乙方账户。

甲方开票信息：

单位名称：紫金山实验室

纳税人识别号：12320100MB19771475

开户银行：中国建设银行股份有限公司南京九龙湖支行

银行账号：32050159604400000585

联行号：105301001090

单位地址：南京市江宁区秣周东路 9 号

单位电话：025-52091570

乙方账户信息：

开户名：四川战星科技有限责任公司

开户行：四川银行股份有限公司会理会川路支行

账 号：11030306000001877

第九条 违约责任

1、甲方无正当理由拒收服务、拒付款的，甲方向乙方偿付合同总价的5%违约金。

2、甲方未按合同规定的期限向乙方支付款项的，每逾期 1 天甲方向乙方偿付欠款总额的 5‰滞纳金，但累计滞纳金总额不超过欠款总额的 5% 。

3、如乙方不能按合同约定提供服务、交付服务成果的，甲方有权要求乙方支付合同总价 5%的违约金。

4、乙方逾期提供服务、交付服务成果的，每逾期 1 天，乙方向甲方偿付合同总额的 5‰的滞纳金。如乙方逾期达 10 天，甲方有权解除合同，解除合同的通知自到达乙方时生效，乙方应向甲方另行支付合同总价款 25%违约金并赔偿给甲方造成全部损失。

5、乙方所提供的服务或交付的服务成果不符合合同规定的，甲方有权拒收。甲方拒收的，乙方应向甲方支付价款总额 5%的违约金。甲方未拒收的，采购中心发现后将向有关部门反映，并责成乙方按照采购结果提供服

务，同时视情况给予暂停一至三年参加南京市政府采购中心组织的政府采购活动的处理。

6、乙方在承担上述 4-5 款一项或多项违约责任后，仍应继续履行合同规定的义务（甲方解除合同的除外）。甲方未能及时追究乙方的任何一项违约责任并不表明甲方放弃追究乙方该项或其他违约责任。

7、乙方投标属虚假承诺，或经权威部门监测提供的服务不能满足采购文件要求，或是由于乙方的过错造成合同无法继续履行的，乙方应向甲方支付不少于合同总价 30%赔偿金。

8、违约方须承担守约方因追索权利产生的一切费用（包括诉讼费、保全费、保全担保保险费、律师费、差旅费、公证费、鉴定费等）。

第十条 合同的变更和终止

1、除《政府采购法》第 49 条以及第 50 条第二款规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或终止合同。

2、除发生法律规定的不能预见、不能避免并不能克服的客观情况外，甲乙双方不得放弃或拒绝履行合同。乙方放弃或拒绝履行合同，在三年内不得参加南京市政府采购中心组织的政府采购活动。

第十一条 合同的转让

乙方不得部分或全部转让其应履行的合同义务或其享有的合同权利。

第十二条 争议的解决

1、因服务的质量问题发生争议的，一方可邀请国家认可的检测鉴定机构对服务质量进行鉴定。服务符合标准的，鉴定费由甲方承担；服务不符合标准的，鉴定费由乙方承担。

2、因履行本合同引起的或与本合同有关的争议，甲、乙双方应首先通过友好协商解决，如果协商不能解决争议，则向甲方所在地有管辖权的人民法院提起诉讼解决争议。

3、在诉讼期间，本合同应继续履行。

4、双方确认本合同载明的地址可作为合同履行过程中相关文书、法院送达诉讼文书的地址，因载明的地址有误或未及时告知变更后的地址，导致相关文书及诉讼文书没能实际被接收的、邮寄送达的，相关文书及诉讼文书退回之日即视为送达之日；因一方拒收的，相关文书及诉讼文书退回之日即视为送达之日。

第十三条 诚实信用

乙方应诚实信用，严格按照采购文件要求和投标承诺履行合同，不向甲方进行商业贿赂或者提供不正当利益。

第十四条 合同生效及其他

1、本合同自双方盖章之日起生效。

2、本合同一式 陆 份，甲方执肆份，乙方执 贰 份，具有同等法律效力。

3、本合同应按照中华人民共和国大陆地区现行有效的法律进行解释。

（以下无正文）

（本页系编号　　《服务采购合同》签署页，无正文）

甲　　方：紫金山实验室 （盖章） 法人代表：尤肖虎 地　　址:南京市江宁区秣周东路9号 邮　　编: 电　　话: 授权代表（签字）: 签订日期:2026 年 3 月 11 日	乙　　方：四川战星科技有限责任公司 （盖章） 法人代表:刘紫宸 地　　址:四川省凉山彝族自治州会理县公园路63号一单元4楼1号 邮　　编: 电　　话: 授权代表（签字）: 签订日期：2026 年 3 月 11 日