紫金山实验室
Purple Mountain Laboratories

协议编号：【 F2025D030040 】

服务采购合同

项目名称：紫金山实验室网络韧性多赛道测评与可视化展示定制开发服务项目

甲　方：紫金山实验室（采购人）

乙　方：南京赛宁信息技术有限公司（供应商）

第一条　　合同标的

乙方根据甲方需求向甲方提供下列网络韧性多赛道测评与可视化展示定制软件开发服务，具体的开发内容如下：

（1）云网互联安全韧性测试子系统

交付要求：交付一套云网互联安全韧性测试子系统，该子系统须包含但不限于以下可工作的测试环境：传统WEB服务、传统WEB服务+WAF防护、单路异构WEB服务+WAF防护、同构冗余WEB服务+WAF防护、异构冗余WEB服务+WAF防护、动态冗余WEB服务+WAF防护等至少6种配置环境。

功能要求：平台需提供分阶段开放功能，允许甲方管理员通过后台界面，自定义测试场景的触发解锁条件和开放顺序（如：完成特定任务、达到特定分数后解锁）。

验收标准：提供平台后台管理功能演示，验证6种测试环境可正常部署、启动，且分阶段开放功能可按预设条件准确触发。

（2）车联网安全韧性测试子系统

交付要求：交付一套车联网安全韧性测试子系统，该子系统须提供至少两个韧性测试阶段，包括但不限于黑盒积分争夺、黑盒安全测试。黑盒积分争夺阶段需提供传统栈溢出漏洞测试环境；黑盒安全测试阶段需提供拟态加固栈溢出漏洞测试环境和整车渗透验证测试环境。

功能要求：支持测试队伍在不获取目标系统内部信息的情况下，通过逆向分析、模糊测试等手段挖掘并利用栈溢出漏洞。支持测试队伍绕过基础防护，实现远程代码执行或权限提升，最终获取系统控制权并夺取Flag。支持测试阶段开放管理功能，允许管理员通过后台管

理界面，设置测试阶段对测试队伍的开放和隐藏。

验收标准：提供平台后台管理功能演示，验证韧性测试阶段环境可正常部署，且测试阶段设置开放和隐藏正常生效显示。

（3）物联网安全韧性测试子系统

交付要求：交付一套物联网安全韧性测试子系统，该子系统须提供物联网典型设备黑盒安全测试环境，包括但不限于智能门锁、家用WiFi路由器、摄像头等真实设备测试。

功能要求：支持测试队伍完成从漏洞发现到稳定利用的全测试过程，包括但不限于绕过设备防护机制、实现持久化控制或数据窃取等。支持对各测试队伍的测试轮次进行运维管理，包括轮次新增、编辑、删除和查询等功能。

验收标准：提供平台后台管理功能演示，验证韧性测试环境可正常部署，设备信息可正常运维显示，测试轮次流程管理正常运转。

（4）人工智能安全韧性测试子系统

交付要求：交付一套人工智能安全韧性测试子系统，该子系统须提供拟态加固前后的多模态大模型对抗性攻击对比测试环境。

功能要求：支持测试队伍在黑盒条件下构造“恶意图片-文本对”诱导模型输出违规指令或泄露训练数据，支持测试队伍提交漏洞复现测试结果，并以攻击成功率、隐蔽性等指标对测试结果进行量化评分。

验收标准：提供平台前后台管理功能演示，验证拟态加固前后的多模态大模型测试环境正常部署，大模型界面可正常实现问答功能，测试队伍提交测试结果可正常下载阅览，量化评分结果可正常录入、自动计算和显示。

（5）新型关键安全韧性测试子系统

交付要求：交付一套新型关键安全韧性测试子系统，该子系统须

提供信创软硬件、可信计算、工控PLC等测试环境，可模拟高危漏洞攻击和极端场景测试。

功能要求：支持测试队伍对信创软硬件、可信计算、工控PLC等测试环境进行接入，通过纯黑盒测试模式，测试队伍在完全未知目标系统内部实现细节的情况下，对信创软硬件、可信计算环境、工控PLC等进行漏洞挖掘与利用。支持对各测试队伍的测试轮次进行运维管理，包括轮次新增、编辑、删除和查询等功能。

验收标准：提供平台后台管理功能演示，验证信创软硬件、可信计算、工控PLC等测试环境正常部署，测试设备信息可正常运维显示，测试轮次流程管理正常运转。

（6）测评报告生成及沉淀子系统

交付要求：交付一套测评报告生成及沉淀子系统，该子系统需包含测评报告生成模块及全局流量监控与存储模块。

功能要求：测评报告生成模块支持提供结构化的测试报告（如PDF格式），报告模板需包含测试概述、攻击路径分析、漏洞详情、防护效果评估、整改建议等章节。支持记录并归档所有攻击日志，并支持按测试任务、时间、团队进行关联查询和下载。

全局流量监控与存储模块支持对所有测试环境的网络流量进行全量捕获，捕获率≥99.5%。支持存储原始PCAP数据及元数据（元数据至少包含五元组、时间戳、协议类型），默认保留周期≥30天。提供流量检索界面，支持按五元组、时间范围进行组合查询，查询结果列表返回时间≤3秒。提供脚本记录功能，支持对测试期间通过HTTP、FTP、TFTP、SMTP等明文传输协议上传的附件脚本文件进行记录查询。

验收标准：完成一次完整测试任务后，提供一份完整的测试报告；

管理员可在后台对攻击日志等信息进行查询和导出。使用测试流量发生器注入模拟流量，验证捕获率；使用平台检索界面执行典型查询操作，使用秒表验证响应时间。

（7）云网互联安全态势展示子系统

交付要求：交付一套云网互联安全态势展示子系统，至少提供3D可视化和2D看板两种视图模式。

功能要求：支持可视化3D态势大屏展示传统WEB服务、单路异构WEB服务、同构冗余WEB服务、异构冗余WEB服务、动态冗余WEB服务等环境相关的测试过程与数据。大屏须实时（数据延迟≤3秒）展示以下信息：

排行榜：支持对相关测试队伍得分排名情况的展示。

攻击态势：支持以3D动效展示攻击源、攻击目标、攻击类型和频次。

攻击统计：支持以选手发起的角度，按次数、攻击结果等维度将所有测试团队的攻击数据进行分类展示。

攻破详情：支持展示被成功攻破的设备、攻破时间、利用的漏洞类型。

攻击日志：支持攻击日志采集和展示功能，可将拟态设备的所有日志进行收集，并提供按时间、按设备、按日志类型等的条件查询。

验收标准：在现场部署大屏，模拟多支队伍同时进行攻击操作，验证数据显示的实时性和准确性。测试所有筛选功能是否正常工作。

（8）车联网安全态势展示子系统

交付要求：交付一套车联网安全态势展示子系统，至少提供3D可视化和2D看板两种视图模式。

功能要求：支持可视化3D态势大屏展示商用ADAS、商用车载网

关和拟态ADAS设备相关的测试过程与数据。大屏须实时（数据延迟≤3秒）展示以下信息：

排行榜：支持对相关测试队伍得分排名情况的展示。

攻击态势：支持以3D动效展示攻击源、攻击目标、攻击类型和频次。

攻击统计：支持以选手发起的角度，按次数、攻击结果等维度将所有测试团队的攻击数据进行分类展示。

攻破详情：支持展示被成功攻破的设备、攻破时间、利用的漏洞类型。

攻击日志：支持攻击日志采集和展示功能，可将拟态设备的所有日志进行收集，并提供按时间、按设备、按日志类型等的条件查询。

验收标准：在现场部署大屏，模拟多支队伍同时进行攻击操作，验证数据显示的实时性和准确性。测试所有筛选功能是否正常工作。

（9）物联网安全态势展示子系统

交付要求：交付一套物联网安全态势展示子系统，至少提供3D可视化和2D看板两种视图模式。

功能要求：支持可视化3D态势大屏展示智能门锁、家用WiFi路由器、摄像头等设备相关的测试过程与数据。大屏须实时（数据延迟≤3秒）展示以下信息：

排行榜：支持对相关测试队伍得分排名情况的展示。

攻击态势：支持以3D动效展示攻击源、攻击目标、攻击类型和频次。

攻击统计：支持以选手发起的角度，按次数、攻击结果等维度将所有测试团队的攻击数据进行分类展示。

攻破详情：支持展示被成功攻破的设备、攻破时间、利用的漏洞

类型。

攻击日志：支持攻击日志采集和展示功能，可将拟态设备的所有日志进行收集，并提供按时间、按设备、按日志类型等的条件查询。

验收标准：在现场部署大屏，模拟多支队伍同时进行攻击操作，验证数据显示的实时性和准确性。测试所有筛选功能是否正常工作。

（10）人工智能安全态势展示子系统

交付要求：交付一套物联网安全态势展示子系统，至少提供3D可视化和2D看板两种视图模式。

功能要求：支持可视化3D态势大屏展示多模态大模型相关的测试过程与数据。大屏须实时（数据延迟≤3秒）展示以下信息：

排行榜：支持对相关测试队伍得分排名情况的展示。

攻击态势：支持以3D动效展示攻击源、攻击目标、攻击类型和频次。

攻击统计：支持以选手发起的角度，按次数、攻击结果等维度将所有测试团队的攻击数据进行分类展示。

得分统计：支持统计展示单次得分最高、单次攻击最有效、单次攻击最隐蔽等队伍。

验收标准：在现场部署大屏，模拟多支队伍同时进行攻击操作，验证数据显示的实时性和准确性。

（11）新型关键安全态势展示子系统

交付要求：交付一套新型关键安全态势展示子系统，至少提供3D可视化和2D看板两种视图模式。

功能要求：支持可视化3D态势大屏展示信创软硬件、可信计算、工控PLC等设备相关的测试过程与数据。大屏须实时（数据延迟≤3秒）展示以下信息：

排行榜：支持对相关测试队伍得分排名情况的展示。

攻击态势：支持以3D动效展示攻击源、攻击目标、攻击类型和频次。

攻击统计：支持以选手发起的角度，按次数、攻击结果等维度将所有测试团队的攻击数据进行分类展示。

攻破详情：支持展示被成功攻破的设备、攻破时间、利用的漏洞类型。

攻击日志：支持攻击日志采集和展示功能，可将拟态设备的所有日志进行收集，并提供按时间、按设备、按日志类型等的条件查询。

验收标准：在现场部署大屏，模拟多支队伍同时进行攻击操作，验证数据显示的实时性和准确性。测试所有筛选功能是否正常工作。

2、系统性能指标要求

（1）系统支持峰值并发在线选手数≥200人；

（2）系统支持并发设备接入能力≥20台；

（3）单份韧性测试结果报告最大支持文件大小≥100MB；

（4）支持韧性测试展示大屏3D场景帧率≥30FPS；

（5）不同韧性测试结果横向对比排行榜实时刷新延迟≤3秒；

（6）支持韧性测试展示大屏数据推送延迟≤3秒。

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

1、本合同项下服务总价款为人民币 叁拾捌万玖仟元整（大写）（¥389,000.00 元）。除此之外，甲方不再向乙方支付任何其他费用。

2、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，以及乙方认为需

Nov 20, 2025, 16:36

要的其他费用等。

3、本合同总价款还包含乙方应当提供的伴随服务费用。

第三条　　服务保证

乙方所提供的服务应符合合同规定的要求；若无特殊说明，按国家有关部门颁布的标准及规范为准。

①验收合格后免费提供 3 年维保服务。

②维保期内，供应商需提供 7*24 小时热线电话、远程网络等技术支持服务。

③维保期内，系统故障须提供快速响应机制，故障报修的响应时间为即时，到达现场的时间为 2 小时，现场服务响应时间须在 2 小时内；小型故障恢复时间为 4 小时，严重故障恢复时间为 24 小时内，并及时有效的提供解决方案。

第四条　　保密及知识产权

1、双方均应保护对方的知识产权，未经对方同意，任何一方均不得对对方的资料及文件擅自修改、复制或向第三方转让或用于本合同以外的项目。如发生以上情况，泄密方需向披露方承担【 8 】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

开户名： 南京赛宁信息技术有限公司

开户行：南京银行江宁科学园支行

账 号：0179280000001143

第八条 违约责任

1、甲方无正当理由拒收服务、拒付价款的，由甲方向乙方赔偿 合同总价的 5% 的违约金。

2、若乙方不能在约定时间内交付服务成果的，由乙方向甲方支付 合同总价的 10% 的违约金。

3、乙方逾期提供服务、交付服务成果的，每逾期 1 天，乙方向甲方偿付总价款的 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。

4、乙方所交付的服务不符合合同规定的，甲方有权拒收并解除合同；无论甲方拒收与否，乙方均应向甲方另行支付 合同总额 5% 的违约金。

5、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）。

第九条 争议的解决

1、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，则向甲方所在地人民法院提起诉讼。

2、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__伍__份，甲方执肆份，乙方执_壹_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：2025 年 11 月 8 日	乙　　方：南京赛宁信息技术有限公司 （盖章） 法人代表:高庆官 地址: 南京市江宁区秣周东路 12 号 邮编: 211111 电话: 025-84981178 授权代表（签字）： 签订日期：2025 年 11 月 6 日