中国南方电网
CHINA SOUTHERN POWER GRID

韶关供电局基于私有化 DeepSeek 的网络安全分析应用-第三方测试技术规范书

韶关供电局数智运营中心

2026 年 11 月

一、概述

根据韶关供电局基于私有化 DeepSeek 的网络安全分析软件项目建设要求，结合韶关供电局网络安全应急分析工作实际情况，开展应用的功能测试、性能测试和安全测试工作，提高安全应急分析效率，形成智能化、规范化的网络安全分析作业流程，确保建设的应用功能、性能与安全性符合项目要求。

二、服务内容及范围

2.1 服务范围

广东电网有限责任公司韶关供电局数智运营中心。

2.2 项目背景

随着企业信息系统、云平台和终端设备持续扩展，网络安全运营面临告警数量庞大、数据来源分散、攻击链关联困难及专业人员不足等问题。白名单软件准入测试、安全设备日志与网络流量分析、数据提取等工作，传统上依赖运维人员逐个登录安全设备和服务器手动分析，对专业能力要求极高，且耗时耗力、出错率高、难以查找统计。为此建设基于私有化 DeepSeek 的网络安全分析软件：采用 PyQt5 构建本地化桌面应用，通过 Ollama 接入本地私有化 DeepSeek 深度推理模型（，构建本地规则引擎与 AI 大模型协同的混合研判架构，AI 服务不可用时自动降级为本地规则分析。平台涵盖流量分析、日志取证、Webshell 检测、钓鱼文本研判、源码审计、事件研判咨询六大功能模块，支持 PCAP 流量文件解析、EVTX/ZIP 日志取证、截图 OCR 文字提取、多智能体协同研判、敏感信息脱敏，以及 JSON/Markdown/TXT 多格式分析报告导出，分析全程数据不出域，有效提升威胁研判效率与安全应急分析水平。

2.3 项目范围

项目范围：根据韶关供电局基于私有化 DeepSeek 的网络安全分析软件项目建设要求，结合韶关供电局网络安全应急分析工作实际情况，开展应用的功能测试、性能测试和安全测试工作。

2.4 项目目标

根据基于私有化 DeepSeek 的网络安全分析软件项目建设要求，结合韶关供电局网络安全应急分析工作实际情况，开展应用的功能测试、性能测试和安全测试工作，提高安全应急分析效率，形成智能化、规范化的网络安全分析作业管理，确保建设的应用功能、性能与安全性符合项目要求。

2.5 测试内容和要求

2.5.1 功能测试

序号	服务内容	描述
1	安装部署与启动	测试应用运行环境配置、依赖安装及主界面能否正常启动
2	全局设置	测试 Ollama/DeepSeek 模型路由、接口超时、重试次数等运行参数的配置、保存与生效
3	环境诊断	测试 Ollama 服务、OCR 环境、PCAP 解析器的自动诊断功能
4	流量分析（文本）	测试 HTTP 请求/响应文本、流量日志文本的导入与智能分析功能
5	流量分析（文件）	测试 PCAP 流量文件解析、HTTP 请求提取与分析功能
6	日志取证	测试文本、ZIP、EVTX 等日志文件的取证分析，生成时间线、IOC 与证据
7	Webshell 单文件检测	测试单个脚本文件的网页后门检测功能
8	Webshell 批量扫描	测试网站目录批量扫描检测功能
9	钓鱼文本研判（单样本）	测试文本研判及截图 OCR 文字提取分析功能
10	钓鱼文本研判（批量）	测试批量样本目录扫描研判功能
11	源码安全审计	测试源码项目目录的安全审计功能
12	单模型快速研判	测试接入私有化 DeepSeek 大模型的事件快速研判功能
13	多智能体深度研判	测试取证分析师、漏洞专家、应急指挥顾问多智能体协同研判功能
14	模型服务对接	测试 Ollama/DeepSeek 接口调用与 AI 服务异常时本地规则引擎降级分析功能
15	结果导出	测试分析报告导出为 JSON、Markdown、TXT 及批量导出功能
16	任务控制	测试任务执行进度显示、运行日志输出与任务中断功能
17	其他配合工作	配合信息中心开展其他相关工作

2.5.2 性能测试

序号	服务内容	描述
1	启动性能	测试应用冷启动、热启动及主界面加载时间
2	大文件解析性能	测试大容量 PCAP 流量文件、EVTX/ZIP 日志文件解析的耗时与成功率
3	批量扫描性能	测试 Webshell 批量扫描、钓鱼样本批量研判在大批量文件场景下的吞吐量与耗时
4	报告导出性能	测试大批量分析结果导出 JSON、Markdown、TXT 及批量导出的耗时
5	资源占用与稳定性	测试任务执行期间的 CPU、内存、磁盘占用，以及长时间连续运行下的内存泄漏与稳定性

2.5.3 安全测试

序号	服务内容	描述
1	敏感信息脱敏	测试 APIKey、口令等敏感信息在界面展示、运行日志、导出报告中的脱敏处理及脱敏有效性
2	数据本地化	测试分析数据本地化存储与处理，验证分析全程数据不出域、无未授权对外传输
3	本地接口安全	测试 Ollama/DeepSeek 本地模型接口的访问控制与未授权访问防护能力
4	依赖组件安全	排查 PyQt5、Ollama、OCR 等第三方依赖组件的已知安全漏洞
5	操作审计	测试关键操作的审计日志记录与可追溯性

2.6 项目交付物要求

1. 基于私有化 DeepSeek 的网络安全分析软件功能测试报告。
2. 基于私有化 DeepSeek 的网络安全分析软件性能测试报告。
3. 基于私有化 DeepSeek 的网络安全分析软件安全测试报告。
4. 基于私有化 DeepSeek 的网络安全分析软件第三方测试总结报告。