

SCA 工具选型评估清单

面向 POC 验证的实用打分表 · 安势信息 Sectrend · sectrend.com.cn

一 · 检出能力

检查项	合格标准	
片段级检测	能识别复制粘贴、二次封装的开源代码片段,而非仅读清单文件	
传递依赖深度	完整依赖树解析,版本精确定位	
二进制与容器分析	对无源码交付物(固件、镜像、SDK)也能还原成分	
AI 生成代码覆盖	能检出 AI 助手复现的开源片段	

二 · 数据质量

检查项	合格标准	
漏洞源覆盖	多源(CVE、CNVD、EUVD、厂商公告)加自有情报	
情报时效	要求给出从披露到可检出的实测时长	
许可证知识库	片段级许可证识别,含例外条款与双重许可	

三 · 误报治理

检查项	合格标准	
版本精确匹配	漏洞对应你的确切版本,而非仅包名	
可达性分析	标注漏洞函数是否被实际调用	
策略定制	严重度阈值、许可证策略、按项目覆盖	
误报处理成本	POC 期间测量每 100 条告警的处理分钟数,而非仅看告警总数	

四 · 工程融入

检查项	合格标准	
CI/CD 集成	原生 Jenkins/GitLab CI 门禁;API 对接自建流水线	
增量扫描	日常扫描仅分析变更;在 10 个真实 PR 上测量新增流水线耗时	
超大仓库	要求给出你代码规模下的参考扫描时长	
离线/隔离部署	完全离线安装+漏洞情报离线更新(监管行业刚需)	

五 · 合规输出

检查项	合格标准	
SBOM 导出	同一次扫描导出 SPDX 与 CycloneDX,覆盖 NTIA 最低要素	
NOTICE 生成	按版本自动生成署名文件	
审计证据	报告可用于客户尽调、并购与监管场景	

VEX 支持	可利用性声明,降低下游三层过滤成本	
--------	-------------------	--

用自己的代码跑这份清单:先用 CleanSource SCA 社区版(免费)扫描,再带着结果进入结构化 POC。sectrend.com.cn

© 安势信息 Sectrend · CleanSource SCA · CleanBinary · CleanCode · SkillSec —— AI 与软件供应链安全