SCA Tool Evaluation Checklist

A practical scorecard for proof-of-concept evaluations · Sectrend · sectrend.com.cn

1 · Detection capability

Check item	What good looks like	■
Snippet-level scanning	Identifies copied/vendored open source fragments, not just manifest entries	■
Transitive dependency depth	Full tree resolution with version-accurate identification	■
Binary & container analysis	Composition visibility for artifacts without source (firmware, images, SDKs)	■
AI-generated code coverage	Detects open source fragments reproduced by AI assistants	■

2 · Data quality

Check item	What good looks like	■
Vulnerability source coverage	Multiple sources (CVE, CNVD, EUVD, vendor advisories) plus proprietary intelligence	■
Advisory latency	Ask for measured time from disclosure to detectability	■
License knowledge base	Snippet-level license identification incl. exceptions and dual licensing	■

3 · False-positive governance

Check item	What good looks like	■
Version-accurate matching	CVE applies to your exact version, not the package name	■
Reachability analysis	Flags whether vulnerable functions are actually called	■
Policy customization	Severity thresholds, license policies, per-project overrides	■
Triage cost	Measure minutes per 100 findings during POC — not finding totals	■

4 · Engineering fit

Check item	What good looks like	■
CI/CD integration	Native Jenkins/GitLab CI gates; API for custom pipelines	■
Incremental scanning	Routine runs analyze only the diff; measure added pipeline time on 10 real PRs	■
Very large repositories	Ask for reference scan times at your codebase scale	■
Offline / air-gapped deployment	Fully offline install with offline vulnerability-intel updates (regulated industries)	■

5 · Compliance output

Check item	What good looks like	■

SBOM export	SPDX and CycloneDX from the same scan, NTIA minimum elements covered	■
NOTICE generation	Auto-generated attribution files per release	■
Audit evidence	Reports usable in customer due diligence, M&A and regulatory contexts	■
VEX support	Exploitability statements to cut downstream triage cost	■

Run the checklist on your own code: start with CleanSource Community Edition (free) or request a guided POC at sectrend.com.cn.