

Security pilot scorecard

Use one copy per tool on the same agreed scope. Fill the PDF with a compatible reader, or print it. Establish criteria before reviewing results; leave unknown outcomes explicitly unknown.

Tool / version / configuration

Repositories / application / analyzed commit

Security reviewer / application owner / pilot dates

Authorized scope and exclusions

Acceptance criteria: evidence, impact, duplication, and review policy

Success thresholds: coverage, reviewer time, evidence quality, and cost

Access / data handling / permissions / agreed deployment model

Keep tests within authorized scope. Select success thresholds with engineering; this scorecard does not supply benchmark targets or guarantee performance.

Results with a boundary.

Preserve raw artifacts and review notes. Report attempted and successful checks separately. A result count measures reports; accepted unique findings require review and deduplication.

Coverage: successful checks / in-scope checks; failures and exclusions

Unique accepted findings / duplicates / dismissed / still undecided

Reviewer time + sample size (for example, 4 hours across 12 reviewed findings)

Evidence quality: revision, affected code, impact rationale, verification limits

Remediation: reviewed suggestions / accepted changes / verified fixes

Cost assumptions: license, integration, review time, and operating effort

Decision + rationale / remaining unknowns / next action and owner

Reviewer / review date / links to scan and test artifacts

Useful measures: accepted-findings ratio = accepted unique findings / reviewed unique findings; verified-fix ratio = independently verified fixes / attempted fixes. Always record denominators. These are pilot workflow measures, not total detection recall or proof of security.

[Read the sample report](#)