BREAKWATER ASOC / PROVENANCE EVALUATION

Test the evidence. Improve the engineering decision.

Provenance grounds the Agentic AI SOC in software evidence. Evaluate source replay, in-product AI assistance and cryptographic context on one fixed repository revision.

ILLUSTRATIVE STARTING QUESTION / CRYPTOGRAPHY BEFORE RELEASE

Does this finding justify a change, and can another reviewer reproduce it?

A cryptographic finding needs a release decision. Engineering must establish what the source shows, what remains unknown and who owns the next check.

Source finding → Validation & AI review → Engineering decision

01

Freeze the comparison

Agree the revision, inputs and known findings, including a refuted example. Record your current review process.

Retain: A fixed sample, baseline and acceptance criteria.

02

Replay and challenge

Replay cited evidence. Have an independent reviewer corroborate or challenge the finding and record the rationale.

Retain: Source locations, validation states and reviewer decisions.

03

Examine the AI assistance

Ask the configured model helper to explain the finding. Check its citations and assertions against the same revision.

Retain: Prompts, answers, references and reviewer corrections.

04

Make the engineering handoff

Review SBOM and CBOM context. Assign deployment, protocol and compatibility checks before deciding on remediation.

Retain: An owned action, unresolved questions and verification plan.

Source replay validates source evidence. Deployed behavior and exploitability require their own checks; make those dependencies explicit in the decision.

ACCEPTANCE CRITERIA / REPRODUCIBILITY & ENGINEERING VALUE

Make the finding useful. Make the decision traceable.

Compare the same revision and finding sample with your current review process. Agree thresholds before the trial, including how incorrect or unresolved findings will be handled.

EVALUATION SCORECARD / AGREE TARGETS WITH YOUR TEAM

What to assess	Evidence to retain	Measures to agree
Source integrity	Revision, cited locations and source replay results.	Reproducible findings; missing or mismatched source references.
Validation quality	Independent checks, counter-evidence and human rationale.	Correctly retained or refuted findings; unresolved cases and review effort.
AI grounding	Helper configuration, prompts, answers and cited code.	Supported citations, unsupported assertions and reviewer corrections.
Software & crypto context	SBOM/CBOM entries linked to source and migration questions.	Traceable entries; missing owner, protocol or deployment context.
Engineering usefulness	Disposition, remediation owner and planned verification.	Review time versus baseline; handoffs accepted or returned for context.

Agree source and model access first.

Confirm repository readiness, supported languages and authorized inputs. Approve model configuration and external source handling. Name the independent reviewer and engineering owner; authorize any source change separately.

YOUR EVALUATION DELIVERABLE / DECISION BRIEF

Scope & baseline

Revision, sample and comparison method.

Validated findings

Replay results, corrections and rationale.

AI & coverage gaps

Unsupported assertions and missing context.

Engineering decision

Action, owner and verification criteria.

Bring a finding engineering needs to resolve.

Request a Provenance demo