BREAKWATER ASOC / AGENTIC AI SECURITY OPERATIONS CENTER

Give software decisions a traceable basis.

Breakwater Provenance brings source evidence and in-product AI assistance into the Agentic AI SOC. Follow a cryptographic finding from the release queue to an accountable engineering decision.

ILLUSTRATIVE SCENARIO / A RELEASE UNDER REVIEW

A crypto finding needs an engineering answer.

A release contains a flagged public-key operation. Security needs to understand the exposure; engineering needs to know what the key does, which services depend on it and what a change could break.

01	02	03	04
Source	**Finding**	**Context**	**Decision**
Exact revision	Cited operation	Role & consumers	Owner & next step

The decision

Should this finding change the release plan, trigger more validation or start a migration workstream?

Security needs a defensible conclusion.

Show where the finding came from, which checks ran and what remains unresolved.

Engineering needs a precise task.

Identify the code, protocol role and affected consumers before selecting a change.

PROVENANCE'S ROLE IN ASOC

Give agentic investigation a source it can inspect.

Provenance connects findings, validation and software context. AI helps explain cited code and identify missing evidence. Human review determines the disposition and the engineering follow-up.

01 / SOURCE VALIDATION & AI ASSISTANCE

Explain the finding. Make the checks reproducible.

Keep the source snapshot, validation record and AI explanation together. Another reviewer should be able to inspect the basis for the conclusion.

PROVENANCE / CHECKS YOU CAN INSPECT

1V	2V	3V	4V
Detector	**Source replay**	**Corroboration**	**Human review**
Inspect the finding	Match the saved source	Inspect independent checks	Record the decision

In-product AI assistance Explain cited code / Identify missing context / Prepare a follow-up

AI supports the review. The record shows which checks ran and what the reviewer decided.

01 **Locate the exact source**

Open the referenced file and line in the saved revision. Establish where the finding originated and which analysis covered the code.

02 **Inspect the validation record**

Source replay checks the citation against the saved source. Review independent corroboration and the checks that were unavailable.

03 **Record the human judgment**

Confirm, refute or leave the finding unresolved, with a reason and an owner. A validation stage records work performed, not a probability of compromise.

IN-PRODUCT AI / A USEFUL FOLLOW-UP

“What does this key do, and which assumption is still unproven?”

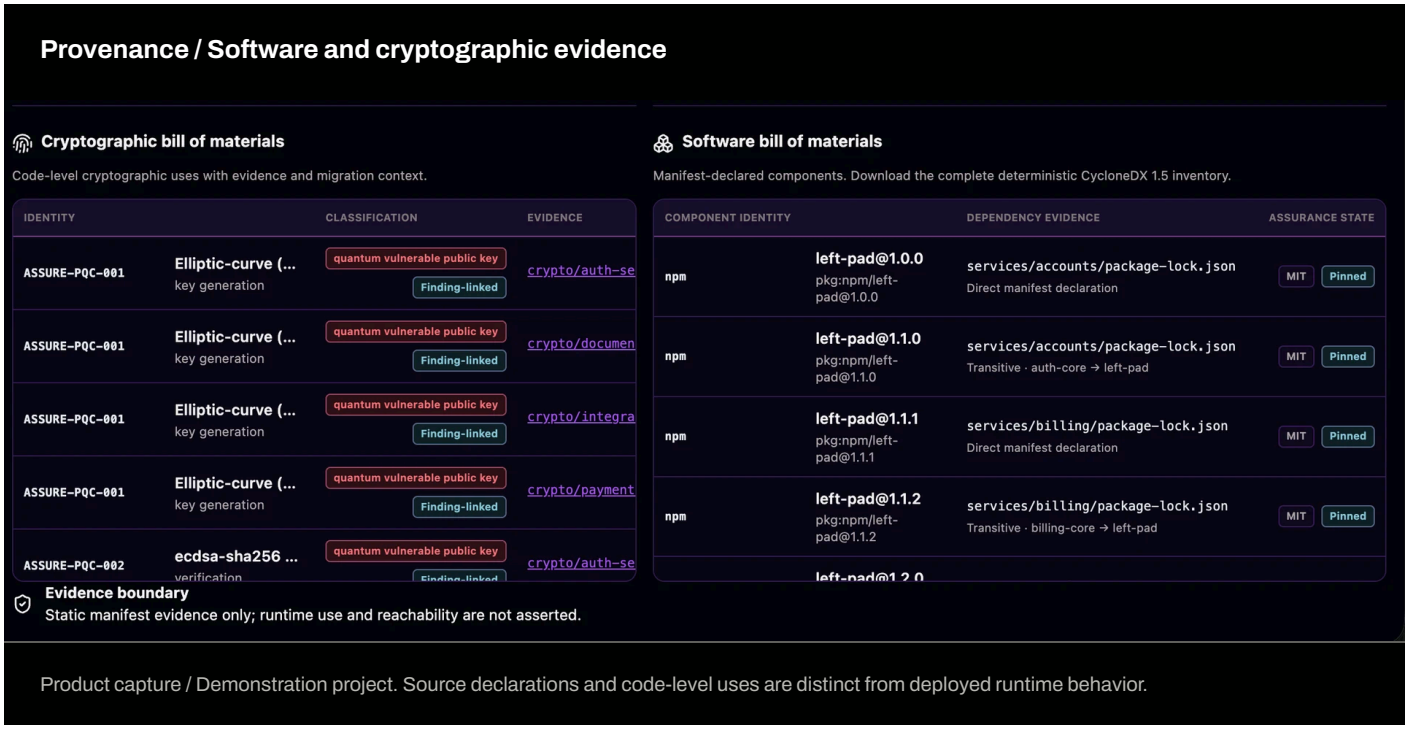
A configured model helper can explain the cited code and suggest the next source to inspect. Check named files and behaviors against the evidence. Authorize source handling for the chosen provider.

Source replay establishes citation integrity. Runtime behavior and exploitability require their own appropriate checks.

02 / SOFTWARE & CRYPTOGRAPHIC CONTEXT

Turn the inventory into a migration question.

SBOM and CBOM records give the investigation a starting point. Use them to identify dependencies, cryptographic uses and the owners who can explain their operational role.



SBOM / Follow the dependency.

Inspect component identity, dependency type and declaring source. Identify the deployed consumers with engineering.

CBOM / Establish the crypto role.

Open the use and source location. Establish its role in signing, key exchange or another protocol function.

Build a transition brief the owner can use.

Role

What does the operation protect?

Consumers

Which systems and formats depend on it?

Lifetime

How long must protection hold?

Compatibility

What must an upgrade preserve?

PQC planning: use the owner's protocol and compatibility evidence to choose the migration approach and the tests it requires.

03 / ENGINEERING DECISION & HANDOFF

Make the next step clear enough to own.

A useful review ends with a disposition, the supporting evidence and a bounded engineering task. Keep release authority separate from the assistance that informed it.

ILLUSTRATIVE DECISION RECORD / CRYPTOGRAPHIC FINDING

Resolve the protocol role.

Disposition	The source use is identified; protocol role and deployed consumers still need confirmation.
Retain	Source revision, cited location, replay and corroboration results, AI follow-ups and reviewer rationale.
Engineering task	Identify callers, protocol role and compatibility requirements. Propose a change with tests and recovery.
Decision owners	Security reviews the evidence; the service owner establishes impact; the release owner decides what can ship.
Verify	Review the revised source, repeat applicable checks and test the required application behavior.

ONE AGENTIC AI SOC / THREE CONNECTED PRODUCTS

Software evidence for the Agentic AI SOC.

Discover adds asset context. Provenance supplies software evidence. Response contributes agentic investigation and governed response. Together, they support a traceable decision with human authority at each handoff.

Agree supported inputs, interfaces and evidence mappings for the selected deployment.

Bring a finding your team needs to resolve.

Review one finding, its AI explanation and the evidence behind the engineering handoff.

Request a Provenance demo → **Explore Provenance**