BREAKWATER ASOC / AGENTIC AI SECURITY OPERATIONS CENTER

Bring agentic AI to your SOC. Keep control of the response.

Breakwater ASOC connects evidence across IT, IoT and OT. Use AI to investigate threats and rehearse response options. Your team authorizes change and verifies the outcome.

YOUR EVALUATION STARTS WITH AN OPERATIONAL QUESTION

What would justify the next step?

Choose a critical service, a software decision or a recurring investigation. Agree what your team needs to learn before committing to broader adoption.

01

Evidence

Can we inspect the basis?

02

AI contribution

Does it improve the work?

03

Human control

Can we verify authority?

01 **Discover / Understand exposure**

Trace candidate attack paths around one critical service. Review asset relationships, supporting records and the assumptions to test in digital rehearsal.

02 **Provenance / Resolve a software finding**

Review one source revision and a known finding set. Test validation, AI explanations and software or cryptographic context for the engineering decision.

03 **Response / Reach an authorized proposal**

Use one reproducible investigation. Examine Council reasoning, rehearse an intervention and test its approval, verification and recovery boundaries.

Start focused. Connect the workflow deliberately.

Expand across products when asset, service and source relationships are established. Agree how evidence moves between teams and which handoffs are manual or integrated.

01 / SCOPE, OWNERSHIP & READINESS

Agree the plan. Give every boundary an owner.

Create one evaluation brief with your sponsor, technical lead and Breakwater. Fix the comparison scope and success criteria before reviewing results.

Agree together	Record before the first run
Decision & baseline	The service or case, existing workflow, input sample, review effort and the adoption question.
Inputs & mappings	Authorized observations, repository revision and time window; asset, service and source identifiers at each handoff.
Data & AI	Data location, access, retention and deletion; model configuration, network dependencies and permitted external processing.
Operating scope	Supported collectors, integrations and adapters; collection methods, test environment, exclusions and stop conditions.
People & schedule	Sponsor, security lead, engineering or operations owner, approvers and recovery contact; readiness tasks and review dates.

Separate the activities you authorize.

01

Demonstration

Inspect the workflow using agreed example inputs. Establish what to evaluate.

02

Controlled trial

Compare reproducible cases in the agreed model or lab. Test failure paths.

03

Site activity

Authorize collection or change explicitly, with operating windows and recovery ownership.

Your team owns the business decision.

Provide the baseline, permitted inputs and service requirements. Review findings and approve operational activity through your change process.

Breakwater confirms the evaluation path.

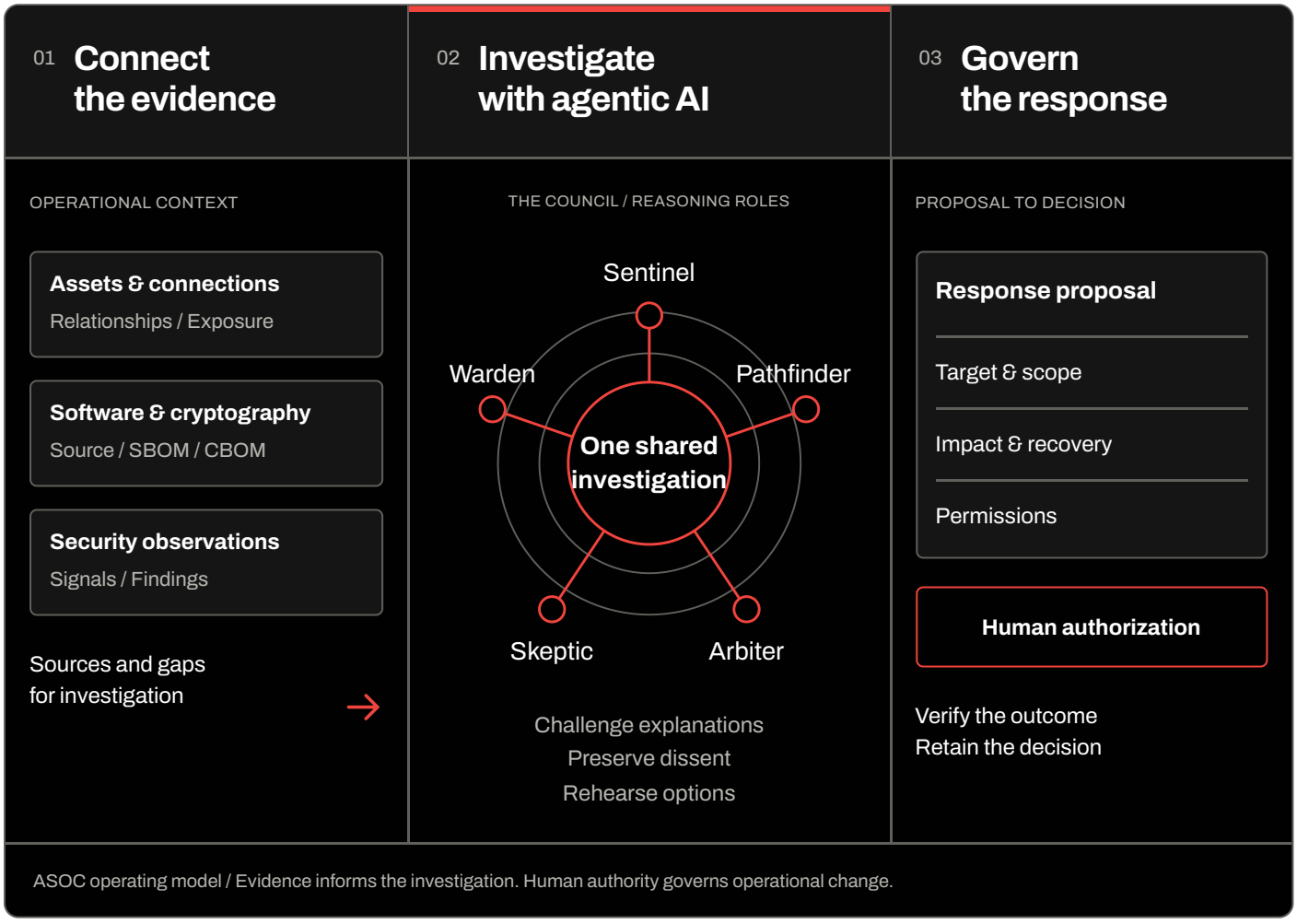
Establish supported configuration, prerequisites and integration work. Agree staffing, timing and commercial terms for the selected scope.

For restricted or disconnected environments, test the required workflow with its actual model, identity, update and network dependencies.

02 / DEMONSTRATE VALUE & CONTROL

Agentic AI investigation. Human-controlled response.

Investigate unusual activity after a workstation rollout. Use asset and source evidence to examine intrusion and authorized maintenance before proposing containment.



Challenge the reasoning.

Trace the conclusion to its sources. Test the Skeptic's alternative, review Warden's proposal and retain missing evidence, dissent and reviewer corrections.

Test the control boundary.

Rehearse the proposed operation and target. Test changed scope or expired approval, then retain the human decision, service checks and recovery outcome.

03 / EVALUATE THE COUNCIL'S REASONING

Agentic AI investigation. Human-controlled response.

Use the workstation case to assess each role's contribution. Compare its explanation with the evidence, record reviewer corrections and test the proposed response.

Sentinel Triage the signal	01	Classifies the activity and identifies a relevant attack technique.	**Does the workstation activity warrant an intrusion investigation?**
Pathfinder Reason about the attack path	02	Examines a plausible attack sequence and the attacker's possible next step.	**Where could this access lead, and which relationship needs checking?**
Arbiter Interpret the wider pattern	03	Assesses whether the activity suggests human-operated intrusion or automated noise.	**Does the sequence support a coordinated intrusion?**
Skeptic Test a benign explanation	04	Proposes an alternative explanation and examines whether it survives the evidence.	**Could the authorized rollout explain the same observations?**
Warden Prepare the response option	05	Proposes a specific containment action for review, rehearsal and authorization.	**Which host, session or key should the team consider restricting?**

Make disagreement useful.

If maintenance could explain the signal, inspect the rollout record before accepting the attack hypothesis. Retain unresolved questions in the case.

Carry reasoning into action.

Review the proposed containment against service dependencies. The next step is rehearsal and human authorization, followed by outcome verification.

The Council routes reasoning tasks to the configured model backend. Roles may use distinct models or share a model, depending on deployment. Evaluate the actual outputs and evidence behind each conclusion.

04 / CLOSE-OUT & ADOPTION DECISION

Leave with a decision. And the evidence behind it.

Review the scorecard, operating effort and remaining gaps with your sponsor and operational owners. Decide whether the evidence supports expansion.

THE EVALUATION DELIVERABLE / ONE SHARED DECISION BRIEF

Outcome	What the evaluation established against the agreed criteria, including failed or incomplete checks.
Evidence	Sources, validation and AI outputs, rehearsal findings, approvals and verification results.
Operating fit	Required integrations, model/data dependencies, staffing, cost assumptions and ownership.
Recommendation	The decision, accountable owner, unresolved work and conditions for the next review.

01

Expand

Criteria met. Authorize the next service or business unit with its own scope.

02

Refine

Resolve gaps or narrow the question. Agree what to repeat and who owns it.

03

Stop

Record why the fit is insufficient and what would change the decision.

Take the product checks into your plan.

Use the two-page briefs for the workflow you select.

Discover →
Assets, attack paths & rehearsal

Provenance →
Source validation & AI grounding

Response →
Council reasoning & control gates

Bring your priority. Build the plan together.

Outline the environment and decision, then agree the scope with Breakwater.

Build your PoC brief → **Request a demo →**