BREAKWATER ASOC / AGENTIC AI SECURITY OPERATIONS CENTER

Before you approve access, understand where it leads.

Discover grounds agentic AI investigation in asset and attack-path evidence. Follow a supplier-access decision through Breakwater ASOC, from investigation to human authorization.

ILLUSTRATIVE SCENARIO / A SCHEDULED MAINTENANCE WINDOW

The work is necessary. The access still needs scrutiny.

A supplier needs remote access to maintain an engineering system. The inventory names the maintenance host; a scanner lists weaknesses. Security and operations need to establish what that host can reach and what a restriction could interrupt.

01 **Supplier access**

02 **Maintenance host**

03 **Engineering system**

04 **Critical service**

The decision

What access is justified, and what must be checked before it is authorized?

Security needs a defensible route.

Identify the relationships and exposures that could connect the access point to a critical service. Retain the records behind the finding.

Operations needs a workable choice.

Review the maintenance dependency, service impact and recovery assumptions before selecting an intervention.

DISCOVER / THE FOUNDATION FOR AGENTIC INVESTIGATION

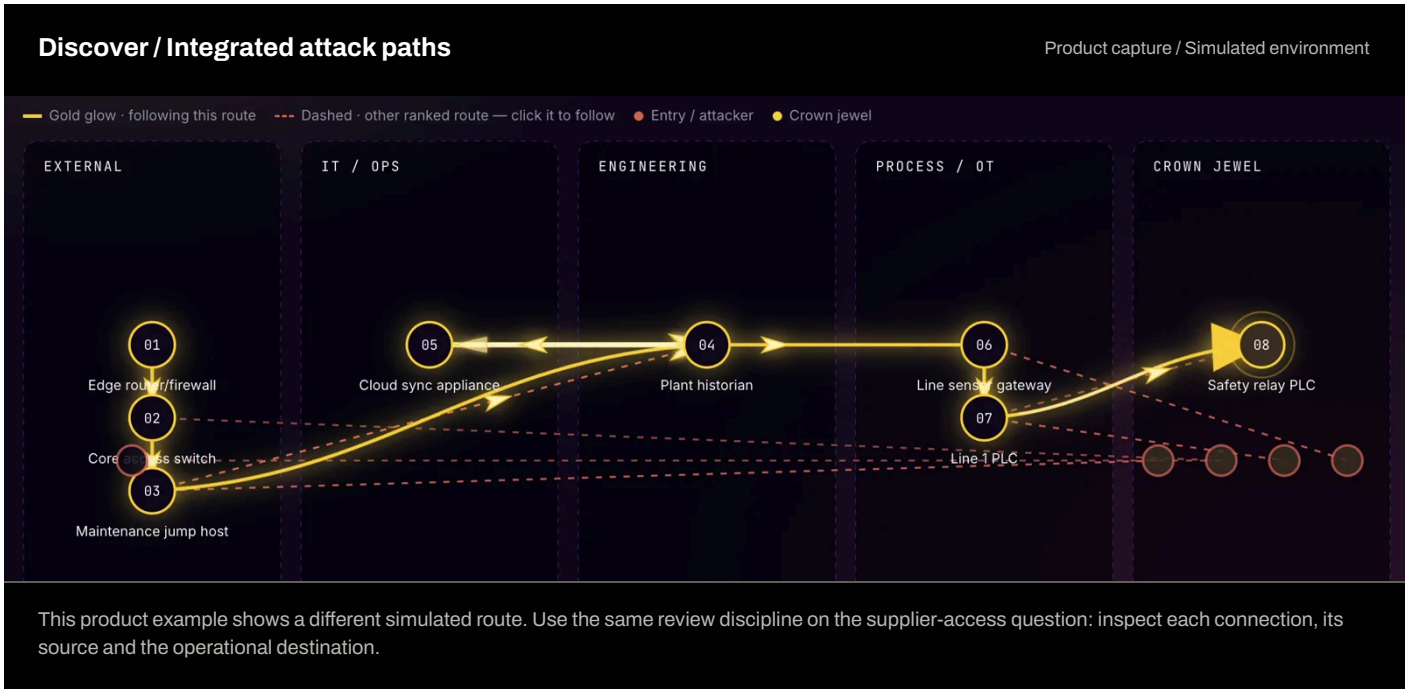
Ground agentic AI in operational reality.

ASOC connects discovery, investigation, rehearsal and governed response. Discover supplies asset and attack-path evidence. AI helps examine the case; your team authorizes operational change.

01 / ESTABLISH THE EVIDENCE

Make the path explainable.

Trace each relationship to its source. Review asset identities, inferred connections and evidence gaps before accepting the route.



This product example shows a different simulated route. Use the same review discipline on the supplier-access question: inspect each connection, its source and the operational destination.

01 **Resolve the asset identity**

Confirm the maintenance host and destination with their owners. Assign unresolved identities for review.

02 **Inspect the relationships**

Inspect the record behind each connection. Check its age and relevance to the proposed access.

03 **Separate exposure from confirmation**

Check candidate vulnerability matches and route conditions. Assign checks for actual access and exploitability.

DISCOVER / EVIDENCE FOR AGENTIC INVESTIGATION

“Which records support this route, and what still needs verification?”

Use a cited Discover prompt or an authorized read-only MCP connection to your approved assistant. Specify the relevant run, inspect the cited records and correct unsupported conclusions before using the answer in the decision.

02 / DIGITAL TWIN & DIGITAL REHEARSAL

Explore the options. Protect the maintenance objective.

Digital rehearsal adds scenario evidence to the ASOC investigation. Compare access options against the maintenance requirement before proposing an operational change.

A SHARED MODEL FOR SECURITY AND OPERATIONS

Environment
Systems & relationships

→

Scenario
Access & intervention

→

Review
Results & assumptions

Discover's simulator supports manufacturing, datacenter, power-substation / SCADA and IoT / OT fleet environments. Choose the environment relevant to the decision and record where it differs from the site.

Compare choices against the same objective.

Illustrative review questions for the supplier-access scenario; agree the supported scenario controls during evaluation.

Option to examine	Security question	Operational question
Retain the proposed route	Which critical systems remain reachable in the model?	What monitoring and access conditions would the owner require?
Narrow the access scope	Which relationships would the proposed restriction remove?	Can the supplier still perform the required maintenance?
Use a different access path	Does the alternative introduce another route or dependency?	What must be prepared, tested and recoverable first?

Retain the comparison.

Record the model, scenario inputs, result changes and assumptions. Link each option to the operational requirement it must preserve.

Plan the site checks.

Ask the service owner which modeled dependencies match reality. Define the checks needed before relying on a simulation result.

Rehearsal informs the proposal. Production changes follow the team's authorization, verification and recovery process.

03 / REACH A REVIEWABLE DECISION

Give the next reviewer a clear basis to act.

Bring the access question, evidence and rehearsal findings into one decision brief. Make the remaining checks and their owners as visible as the recommendation.

ILLUSTRATIVE DECISION BRIEF / SUPPLIER ACCESS

Verify access before authorization.

Purpose	Enable the agreed maintenance task for the engineering system.
Evidence needed	Confirmed asset identities, the reviewed route and records supporting the required access.
Open checks	Verify the destination and permissions. Confirm maintenance dependencies and the recovery procedure.
Owners	Security reviews the route; operations validates service needs; the change owner authorizes the final scope.
Verification	Agree how to check the authorized access and required service behavior, and when to end the access.

BREAKWATER ASOC / AGENTIC AI WITH HUMAN CONTROL

One Agentic AI SOC. A connected decision.

Discover connects assets and attack paths across IT, IoT and OT. Provenance adds software and cryptographic evidence. Response's AI Council challenges explanations and prepares proposals. ASOC brings them together for agentic investigation and human-controlled response.

Agree supported interfaces, evidence mappings and review responsibilities for the deployment.

See Discover in the ASOC workflow.

Bring a critical service. Explore how evidence, AI and human judgment shape the next step.

Request a Discover demo →

Explore Breakwater Discover