BREAKWATER ASOC / DISCOVER EVALUATION

Put Discover to the test. Start with one critical service.

Evaluate Discover's role in the Agentic AI SOC: asset visibility, integrated attack paths, digital rehearsal and AI assistance. Agree the question, evidence and acceptance criteria.

ILLUSTRATIVE STARTING QUESTION / SUPPLIER ACCESS

What could this connection reach, and what must we verify before approval?

A supplier needs remote access for maintenance. Security and operations must review the route, supporting evidence and implications for critical systems.

Supplier access → Maintenance host → Critical service

01

Scope the decision

Name the service, owners and collection boundaries. Capture the existing inventory and what the team already knows.

Retain: A scoped question, baseline and agreed success criteria.

02

Review the assets

Review collected identities, observations and unresolved assets with the responsible owners.

Retain: An asset review with coverage gaps and assigned follow-ups.

03

Trace and rehearse

Inspect the candidate path. Compare agreed simulated scenarios and identify assumptions requiring site validation.

Retain: A reviewed path and a scenario comparison with assumptions.

04

Investigate and decide

Check an AI-assisted answer against its sources. Review the proposed access scope with security and operations.

Retain: A sourced decision brief, open questions and owners.

Schedule around site readiness and operational windows. Simulation and observation are distinct inputs; live changes require separate authorization.

ACCEPTANCE CRITERIA / EVIDENCE, USEFULNESS & CONTROL

Agree what good looks like before you start.

Agree the sample, baseline and acceptance thresholds before collection. Measure the results on the same scope; retain sources and reviewer decisions.

EVALUATION SCORECARD / AGREE TARGETS WITH YOUR TEAM

What to assess	Evidence to retain	Measures to agree
Asset visibility	Reconciled inventory, identity decisions and collection gaps.	Confirmed, unresolved and missed assets; unexplained baseline differences.
Attack-path relevance	Reviewed relationships, source records and the critical destination.	Relationships with source evidence, stated assumptions and unresolved gaps.
Digital rehearsal	Selected environment, scenario inputs and results.	Input and result changes between scenarios; assumptions requiring site validation.
AI-assisted investigation	Question, answer, cited records and reviewer corrections.	Traceable citations, unsupported statements and reviewer corrections in sampled answers.
Decision usefulness	Access recommendation, open questions and comparison with the baseline.	Review time, unresolved questions and owner acceptance versus the baseline.

Agree the operating conditions.

Name security, asset, operations and decision owners. Agree collection scope, AI configuration and permitted evidence. Approve external data handling for MCP assistance; authorize live changes separately.

YOUR EVALUATION DELIVERABLE / DECISION BRIEF

Scope & baseline

Service, inputs and comparison point.

Evidence & findings

Reviewed assets, routes and scenario results.

Open questions

Unresolved assumptions and assigned checks.

Decision & owner

Proceed, narrow, resolve gaps or stop.

Bring your highest-priority service.

Request a Discover demo