



Know what happened and what matters

SOAR — Security Orchestration, Automation and Response — helps leaders turn an uncertain security signal into an owned decision. Its agentic reasoning layer connects evidence from existing tools, compares safer response options and keeps operational authority with people.

A decision under pressure

A privileged identity behaves abnormally. An unfamiliar workload appears on the path to a payment service. East-west traffic rises. Isolate too early and settlement may stop; wait too long and exposure may spread. The leadership team needs a common picture before it changes a critical service.

What SOAR is

A workspace that connects evidence from existing security tools with business context, response rehearsal and human approval.

Who it serves

Security leaders, incident responders, service owners and engineers who share responsibility for the outcome.

01 / Understand

See the signal in the context of identities, assets, services and time.

02 / Compare

Examine plausible paths and rehearse response choices before change.

03 / Decide

Name the owner, authority, recovery plan and proof of success.

Why leaders care

The discussion moves from alert volume to business consequence, ownership and evidence.

What remains human

The product can assemble, explain and propose. Approval and operational accountability remain with people.

The objective is a faster decision that remains explainable after the incident.



Turn evidence into a shared picture

SOAR helps the team separate observed facts, informed interpretation and unanswered questions.

The same story, seen four ways

The identity signal alone is ambiguous. Service and flow context show why the affected workload matters. Candidate paths reveal what might be connected. Replay lets a second reviewer examine the same window.

Observed

Signals, timestamps, identities, assets and relationships that came from approved sources.

Inferred

Explanations and candidate paths produced from the available evidence, with uncertainty left visible.

Missing

Stale, absent or conflicting inputs that could change the conclusion.

Owned

The next question, responsible person and decision deadline carried into the case record.

Existing tools raise the signal. SOAR carries its evidence, uncertainty and ownership into the cross-team decision.



Rehearse the decision before the change

Compare credible options without confusing a modeled consequence with a guaranteed outcome.

Rehearsal is a decision test

The team replays the same evidence and compares response choices in a suitable digital twin, recorded environment or controlled range. The goal is to expose dependencies and recovery needs before a real service is changed.

Option A / Contain

What exposure may fall, which users or services may be interrupted and how access is restored.

Option B / Monitor

What additional evidence is needed, how long the team will wait and which condition triggers action.

Option C / Compensate

Which reversible control reduces risk while a durable fix is prepared.

What rehearsal can show

Likely consequences, assumptions, dependencies, recovery steps and the checks needed after action.

What it cannot prove

A model is not the live estate. Simulated results stay labelled and do not authorize execution.

Rehearsal changes the meeting from “What should we do?” to “Which tested option will we own?”



Make the response accountable

A governed response has a named owner, explicit authority, recovery conditions and fresh verification.

01 Assign the owner

Name the service owner and the person responsible for the investigation.

02 Set the boundary

Define the target, permitted action, expiry, recovery plan and evidence required for approval.

03 Act through a controlled path

Use a supported, separately configured execution path only after authorization.

04 Verify and retain

Check both the original risk condition and service health with fresh evidence; preserve the execution record and remaining gaps.

A useful management record

Question, evidence, alternatives, decision, owner, authority, result and next review date.

A responsible adoption decision

Expand, narrow, pause or stop based on reproducibility, operating effort, integration readiness and unresolved risk.

SOAR closes the loop when the action, outcome and accountable owner are all visible.