**SOAR** | INVESTIGATION, REHEARSAL AND GOVERNED RESPONSE

PRODUCT GUIDE · 01 / 04

SECURITY INVESTIGATION AND GOVERNED RESPONSE

# Move from a noisy signal to a governed response without losing the evidence.

SOAR is a security investigation and governed-response workspace for SOC analysts, threat hunters and IT engineers. It brings supplied evidence, assisted investigation and controlled rehearsal into the decision about what should happen next.

### The moment

Leah sees repeated failed sign-ins in the incident channel while the customer portal still works. The service owner asks whether isolating the host would interrupt orders. More alerts will not settle that question. Leah needs evidence, operational context and an accountable decision.

### Who uses it and where

SOC analysts, incident responders, IT engineers and service owners use Chat, Console, Live and Replay workspaces to investigate available inputs. Deployment and inference choices depend on the installation. Agree the local environment, permitted external connections, inputs and supported response adapters before the pilot.

**BRING**
Authorized logs, events, estate records or supported live feeds

**LEAVE WITH**
An investigation tied to its inputs, subjects and time basis

**BRING**
A bounded question and operational context

**LEAVE WITH**
Candidate paths, unresolved assumptions and a rehearsal where supported

**BRING**
A service owner and an approved action boundary

**LEAVE WITH**
A response proposal, required approvals, verification and recovery checks

### The workflow

Start with a question and inspect the input. Analyze and explain the result. Examine relevant relationships and consequences. Rehearse where a suitable model or controlled environment exists. Prepare an action for the responsible owner. Use a supported authorized path for execution, then verify the effect with fresh evidence.

### Why consider SOAR

Evaluate whether the analyst, engineer and service owner can inspect the same reasoning and continue one another's work. Evidence and explicit assumptions make the response easier to challenge before a change reaches a real service.

**WHAT THIS ENABLES**

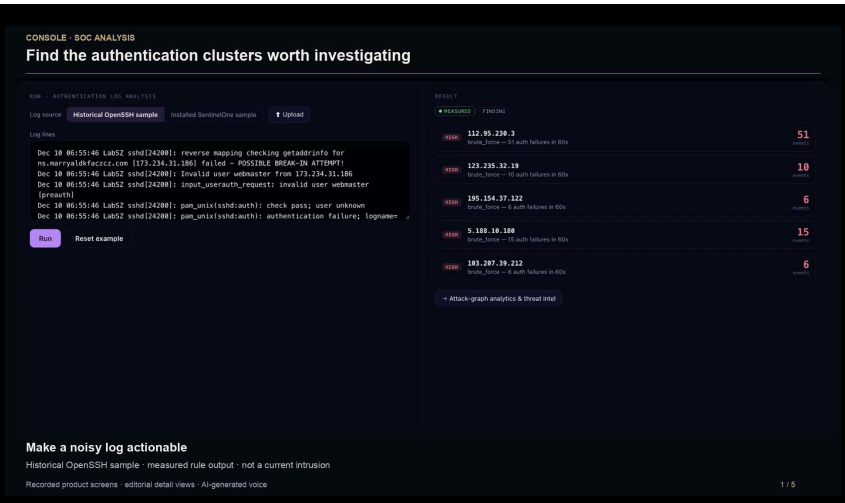
**An urgent signal becomes a bounded investigation and a decision someone is responsible for making.**

**SOAR** | INVESTIGATION, REHEARSAL AND GOVERNED RESPONSE **PRODUCT GUIDE · 02 / 04**

SECURITY INVESTIGATION AND GOVERNED RESPONSE

# The evidence changes the response

Leah reconciles the same event window, follows its provenance and gives the next analyst enough context to reproduce the result.




SOAR interface overview from the recorded demonstration. The full frame shows the supplied authentication log, reconciled result list and investigation context; it does not establish a real intrusion or customer incident.

### A practical walkthrough

Supply authorized log input and confirm its time basis. Run the analysis and reconcile the count with the original records. Establish which host and account are involved before drawing a conclusion. Carry the result and unresolved question into investigation or an owner handoff.

### Ask a question that can change the decision

Did a successful sign-in follow? Does the address belong to the intended subject? What does the application host support? Which additional source would distinguish an attack from an operational error? Use assisted explanation to locate the next check, and inspect the evidence behind the answer.

### Use Live and Replay with their provenance

Live views can expose collected or imported estate and flow observations, depending on configuration. Replay lets reviewers inspect the same recorded interval. Check source, vantage, timestamp and real, injected or modeled labels before using a record in a decision.

### Tip for missing activity

Check whether inputs arrived, whether the time window includes them and whether the source was enabled. No events in a selected view is not proof of a quiet or safe environment.

**WHAT THIS ENABLES**

**A second analyst can reproduce the result, inspect the same time window and explain the remaining uncertainty.**

**SOAR** | INVESTIGATION, REHEARSAL AND GOVERNED RESPONSE PRODUCT GUIDE · 03 / 04

SECURITY INVESTIGATION AND GOVERNED RESPONSE

# The team rehearses the consequence

Leah connects the signal to estate context and candidate paths, then tests a response in a model or approved range before anyone treats it as an operational action.

**CAPABILITY**
Console and assisted investigation

**WHAT IT CONTRIBUTES**
Analysis and explanation of available records.

**WHAT TO VERIFY**
Source references, operation performed and limits of model narrative.

**CAPABILITY**
Estate and live evidence

**WHAT IT CONTRIBUTES**
Asset, relationship and flow context from supported sources.

**WHAT TO VERIFY**
Placement, ingestion status, identity mapping and freshness.

**CAPABILITY**
Attack-path reasoning

**WHAT IT CONTRIBUTES**
Candidate routes and their construction context.

**WHAT TO VERIFY**
Evidence for each relationship; a route rank is not breach probability.

**CAPABILITY**
Digital twins and replay

**WHAT IT CONTRIBUTES**
Scenarios, recorded windows and possible consequences.

**WHAT TO VERIFY**
Whether the substrate is modeled, injected, replayed or an authorized range.

**CAPABILITY**
SOC and threat hunting

**WHAT IT CONTRIBUTES**
Bounded questions and a handoff for the next analyst.

**WHAT TO VERIFY**
Time budget, alternative explanations and stopping condition.

**CAPABILITY**
IT response proposals

**WHAT IT CONTRIBUTES**
Drafts for patch, access, configuration or containment questions.

**WHAT TO VERIFY**
Commands, targets, side effects and recovery; generated code is review-only.

**CAPABILITY**
Governance and verification

**WHAT IT CONTRIBUTES**
Safety-case and approval primitives on supported execution paths.

**WHAT TO VERIFY**
Which adapter enforces authority, its expiry and the fresh result after execution.

### Collection and evidence handling

Where configured, SOAR can bring estate, flow, enrollment and diagnostic records into the investigation. During evaluation, verify authentication, storage, tenant separation, freshness and screen wiring. Secure-envelope records remain labeled as coming from a named but unverified collector until the installation verifies the carried signature.

**WHAT THIS ENABLES**

**The owner can distinguish an observed condition, a modeled consequence, a generated proposal and an authorized action.**

**SOAR** | INVESTIGATION, REHEARSAL AND GOVERNED RESPONSE PRODUCT GUIDE · 04 / 04

SECURITY INVESTIGATION AND GOVERNED RESPONSE

# The authorized path ends in verification

Leah and the response owner narrow the scope, review the proposal, use a separately authorized adapter where configured and check fresh evidence after the action.

1 **Prepare the evidence and operating boundary**

Choose where reasoning runs and which connections are permitted. Local inference does not itself make an installation disconnected. Offline operation needs a controlled process for model weights, software and intelligence updates. Confirm adapters, roles, retention, recovery and the evidence available to each reviewer.

2 **Give the service owner explicit control**

A generated patch or firewall program is a draft. Static checks can flag defects but cannot authorize it. Supported range or local execution paths have their own gates; establish that approval, scope, expiry and evidence checks apply to the exact path used. Team responsibilities in a book are not proof of permission enforcement everywhere.

3 **Compress scope while preserving control**

Choose the critical service and highest-consequence exposure. Collect the evidence needed for the immediate decision. Prepare a reversible compensating control with the owner, rehearse where feasible, approve within the existing change process and verify service health plus the original condition. Retain deferred work and an expiry for temporary measures.

4 **Use investigation and rehearsal for urgent migration**

Containment or an interim control may reduce a particular exposure. It does not replace post-quantum cryptography (PQC) migration or make previously exposed data quantum-safe. Use Secure and Assure to establish inventory and source context, then track the remaining migration with service owners. Do not promise an automatic portfolio-wide fix.

5 **Make the adoption decision**

Choose an investigation with reproducible inputs, a measurable handoff and a service owner. Include stale evidence and a failed dependency in the pilot. Require a decision to expand, narrow, pause or stop. Use the full SOAR book for investigation, deployment and response detail.

**WHAT THIS ENABLES**

**The response can be time-bounded and proportionate without confusing a proposal, containment or rehearsal with a verified fix.**