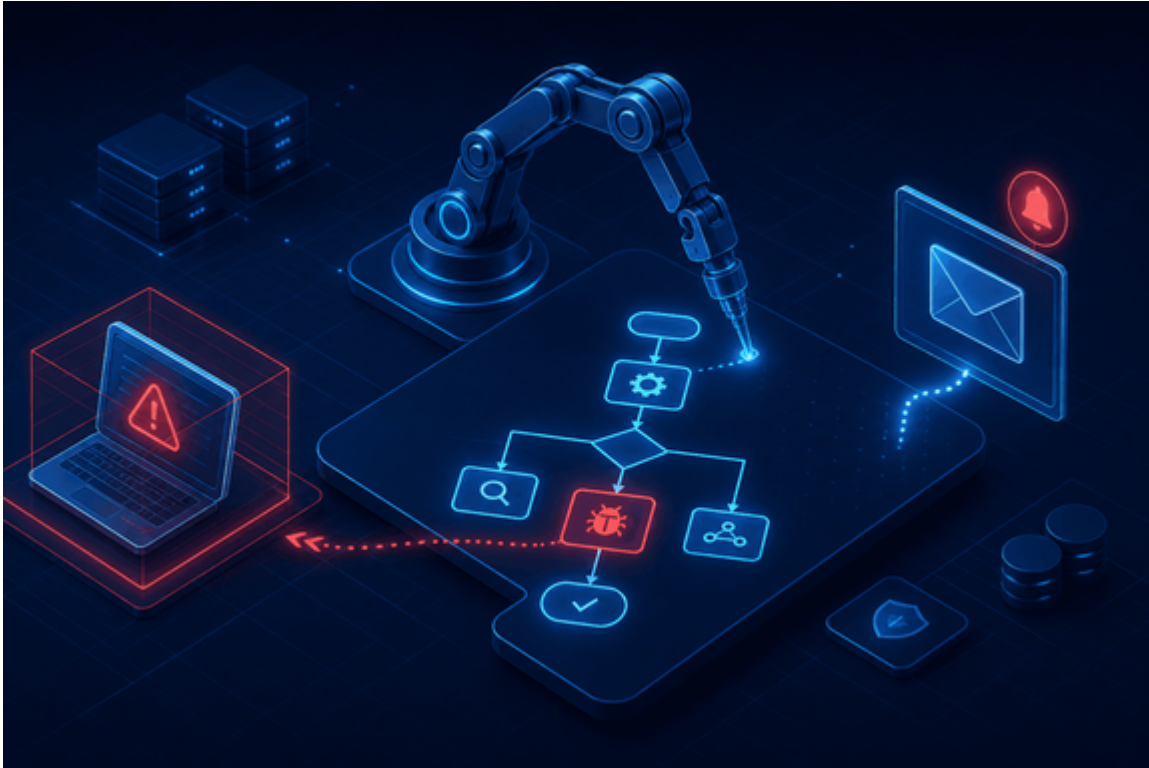


SOAR: When the SIEM Stops Watching and Starts Acting

Sun, Aug 16, 6:00 PM EDT · <https://scottslab.io/posts/soar-security-orchestration-automation-response>



TL;DR

SOAR extends a SIEM from detection into action, and the honest framing is a spectrum of how much human sits in the loop. One warning first: "playbook" reliably means the automated workflow, but "runbook" means whatever the vendor in front of you decided it means. There is no industry definition, so stop arguing about the word and say what you actually mean. The real design question isn't what to automate. It's what happens when automation fires on a false positive.

A SIEM tells you what's happening. SOAR does something about it. That's the whole relationship: Security Orchestration, Automation and Response sits on top of detection and closes the gap between "the SIEM noticed" and "something was done", which in a manual shop is measured in however long it takes an analyst to look.

First, the terminology trap

Exam-style material tends to split it this way: a **playbook** mixes human and automated steps and is tied to your incident-response policy, while a **runbook** is fully automated end to end.

That is not what the word means once you're inside a product, and it's worth knowing before a meeting goes sideways.

"Playbook" is the reliable one. In SOAR platforms it consistently means *the automated workflow*: the thing that executes, with conditional logic and API calls into your other tools. Splunk SOAR uses it exactly that way, and so does essentially every competitor.

"Runbook" is the unreliable one, and this is where I'd stop trusting any single definition:

- In Splunk's own ecosystem, the artefact an analyst *follows by hand* isn't called a runbook at all. It's a **workbook**, the case-management checklist, with playbooks attached to individual tasks where automation applies.
- Meanwhile "Azure Automation Runbooks" are *scripts*. Fully automated. The opposite of a manual document.
- Some vendors define a runbook as one narrow technical task and a playbook as the broader response framework: a completely different axis from how much automation is involved.
- And at least one major vendor's own documentation says plainly that in practice there is no difference and people use the two interchangeably.

So this isn't a clean inversion you can memorise. It's genuine industry-wide inconsistency, and the study definition is one convention among several rather than the wrong half of a neat swap.

The practical move is to stop arguing about the noun. Say **fully automated**, **automated with an approval gate**, or **documented manual procedure**. Those phrases mean the same thing in every room you'll ever stand in, and nobody has to guess which vendor's dialect you learned.

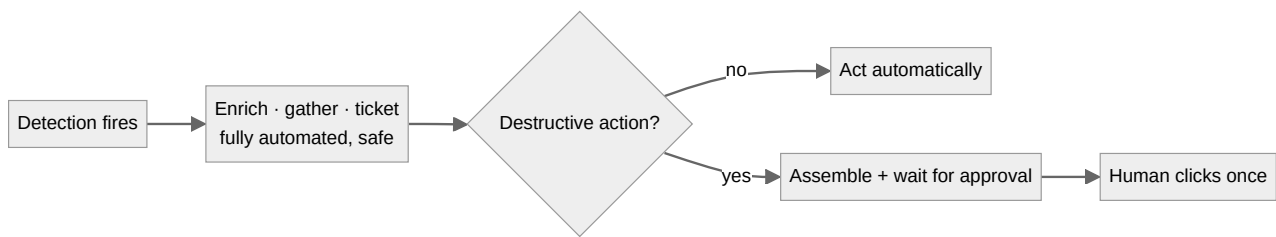
The spectrum that actually matters

Forget the labels and think about where the human sits:

Fully automated. The system acts the instant a detection fires. Right for fast, unambiguous, low-blast-radius responses: enrich an alert with threat intelligence, pull the file hash, open the ticket, gather context so the analyst opens a complete picture rather than a bare alert. Enrichment is where almost every SOAR programme should start, because it is enormously useful and **cannot hurt anything**.

Automated with an approval gate. The system assembles everything and waits for one click. This is the sweet spot for anything destructive: the analyst spends five seconds approving rather than five minutes gathering.

Documented manual. Judgment, legal exposure, or anything you can't yet trust to a rule.



The spectrum that actually matters

The question nobody asks until it's too late

Everyone designing automation asks "what can we automate?" The better question is: **what does this do when it fires on a false positive?**

Automatically isolating a host is the textbook example, and it's the right response to confirmed ransomware. Now run it against a noisy detection at 09:00 on a Monday. If the matched host is a domain controller, a payments gateway or the database everything depends on, your automation has just caused an outage that your detection rule merely *suspected* was an attack.

So the practical rules:

Scope by blast radius, not by confidence alone. Maintain a list of assets automation may never touch unattended. Confidence in the rule is not the only variable. Cost of being wrong is the other one, and it isn't uniform across your estate.

Make every automated action reversible, and know how. If you auto-isolate, the un-isolate has to be one step and someone has to have done it in a drill. An automation you cannot undo at 3am is a liability wearing a badge.

Run new automation in dry-run first. Log what it *would* have done for a couple of weeks. The list is always surprising, and it's much cheaper to be surprised in a log file.

Automate the response, not the decision, until the decision has earned it. Start with enrichment, graduate to gated action, and promote to unattended only for detections whose false-positive rate you have actually measured.

What it's really buying you

The pitch is speed, and speed is real. An attacker moving laterally is racing your response time, and automation doesn't get tired or paged at 3am.

But the bigger win is **consistency and attention**. A tired analyst at hour seven handles the fortieth phishing report differently from the first. Automation handles it identically every time, which both improves the floor and frees the humans for the work that actually needs a brain. Most SOC time is spent gathering context, not deciding, and gathering context is exactly what a machine is good at.

The trap is treating SOAR as a headcount substitute rather than an attention multiplier. Playbooks are code. They break when an API changes, they rot when a detection is retuned, and an unmaintained automation library fails silently in a way a human never would: it just stops doing the thing, and nobody notices, because nothing errored.

Automate the certain, gate the ambiguous, document the rest. Then test the automation the way you'd test anything else you depend on.

Written by Scott S. — Contact: scott@scottschlangen.com — scottslab.io — <https://scottslab.io/posts/soar-security-orchestration-automation-response>