SWIMLANE

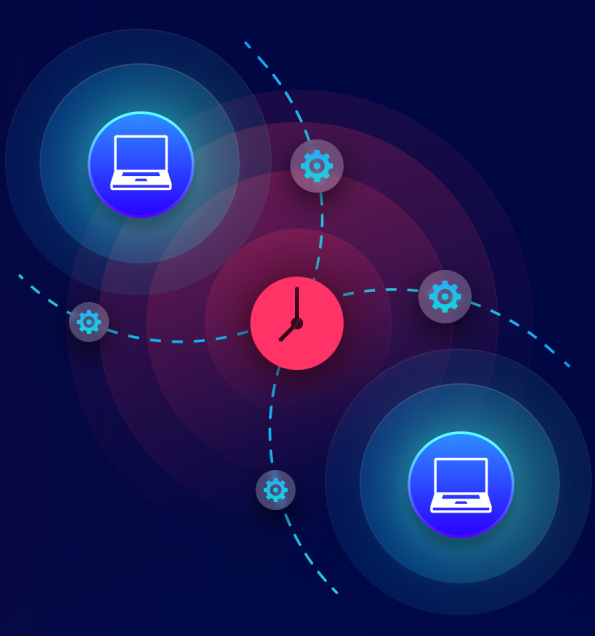
5 Signs Your SOAR is Causing Chaos

Your security operations center (SOC) wasn't designed to drown in alerts, false positives, siloed tools, and inflexible workflows. Yet that's exactly where many SOAR platforms leave you—stuck in a cycle of complexity and confusion. If your team is overwhelmed, burned out, or just simply stuck, it's not you. It's your SOAR.

Let's explore the five red flags that your SOAR platform is causing chaos rather than clarity.

1

You're burning time jumping between consoles, chasing context across too many tools.



CHAOS EFFECT

Critical alerts get delayed or missed because you waste time switching tools instead of responding to threats.

PRO TIP

Consolidate investigation workflows with a tool that pulls context into a single, unified view, reducing noise and speeding up response.

2

You're piecing together incident data because your SOAR lacks the visibility and flexibility to manage investigations effectively.

CHAOS EFFECT

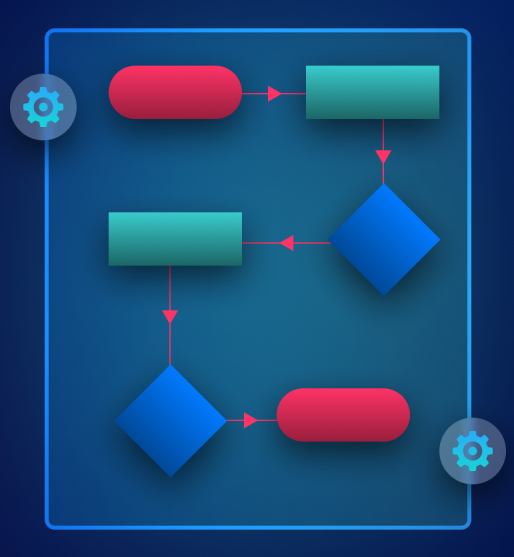
Investigations stall and critical context gets missed, putting your response at risk.

PRO TIP

Select a platform that integrates seamlessly across your entire toolset and offers a unified, case-centric view of incidents.

3

You're turning into an accidental developer when simple workflow tweaks break your automation.



CHAOS EFFECT

You waste hours debugging fragile workflows instead of focusing on threat response.

PRO TIP

Opt for a tool specifically designed for security teams rather than software engineers.

4

You're drowning in false positives with no way to filter the noise.

CHAOS EFFECT

You're burnt out and missing real threats while chasing alerts that don't matter, leading to risk exposure.

PRO TIP

Utilize AI-powered automated alert triage to enhance alerts and automatically surface high-fidelity threats.

5

You're stuck with a platform that only works with its own tools (i.e. vendor lock-in).

CHAOS EFFECT

You're unable to connect to the 30+ tools your SOC actually relies on, instead of optimizing your stack—slowing innovation and response.

PRO TIP

Invest in a platform with native support for any API, not just one vendor's ecosystem.

CLARITY IN ACTION:

GDS's AI Automation Transformation

GDS needed to take control of the chaos that their SOAR tool couldn't manage. Slow updates and limited support were stalling progress and hindering agility. They turned to Swimlane for a responsive partnership and hands-on engineering collaboration. With the Swimlane Turbine AI automation platform, GDS brought control to their operations—rapidly improving efficiency, visibility, and performance.

GDS'S OUTCOMES

- Added the capacity of 20 virtual analysts
- Record number of cases analyzed
- 2 hours saved per threat detection and response

> "The only way to measure your SOC's operational effectiveness is with a platform like Swimlane. It allows you to predictively design playbooks and measure human costs through the lens of time savings. Swimlane is the only platform that I've used today that does that effectively."

Tracey Webb
Director of Information and Cybersecurity Operations, GDS.

Are you ready to extend beyond SOAR?

Download our eBook to explore a smarter, more scalable alternative to traditional SOAR at swimlane.com/resources/e-books/ai-automation-beyond-soar/

Explore Swimlane

THE LEADER IN AI AUTOMATION FOR EVERY SECURITY FUNCTION