SWIMLANE

SANS | Research Program

Product Briefing

Security Operations with Swimlane:

Insights from the 2024 SANS Institute Survey

July 2024

The job of the SOC gets bigger every day. The budget often does not. Staffing is the eternal struggle for SOC managers, while analysts strive to build their knowledge and protect organizational assets. Fortunately, powerful tools are available to help bridge the gap between what you have and what you need.

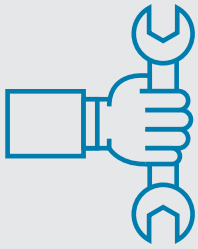
Swimlane

Swimlane's guiding principle is to empower SOC teams through AI-enhanced automation that serves as the system of record for any environment, use case, or stakeholder. They believe that if you invest in quality security automation, you'll improve the barriers to successful security operations that protect the organization without burning out its people.

Its security automation platform goes beyond the SOC to help all parts of the security operation accomplish more with less. By bringing information into a central repository, Swimlane helps tear down silos between the SOC and operations teams.

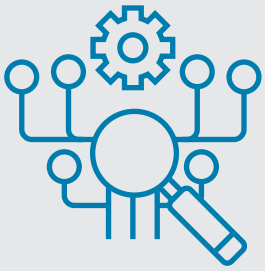
Swimlane provides a cloud-native and low-code solution to manage incidents and cases collaboratively with inputs from all sources, not just the standard stack of cybersecurity tools. This level of orchestration enables infinite integrations that facilitate the monitoring of identities, access, permissions, and data, all at the same time. From a single pane in Swimlane Turbine, an analyst can run queries, automate remediation steps, and conduct investigations – even collaborate with others in Teams and Slack conversations.

Key Findings



Lack of automation and orchestration is the single most reported problem by respondents to the SANS SOC Survey.

Staffing issues – high staffing requirements and lack of skilled staff combined – are the top barrier SOC teams face.



Another barrier is lack of enterprise-wide visibility into the SOC operation.

SANS SOC Survey respondents were clear: SOC teams need more automation and orchestration capabilities and better-trained staff to accomplish their goals. Yet many times, budgets won't stretch and the right candidates aren't available. With Swimlane Turbine, an organization can train a new SOC analyst in a couple of weeks, instead of spending months on the underlying tools.

Turbine saves time in the onboarding phase, so the new person becomes an asset more quickly. With the time saved, that person can now train to become a subject-matter expert wherever the team needs one. And that's before you add in the time saved and expertise gained from using Turbine's, robust case management application, which streamlines and standardizes incident response processes based on lessons learned and best practices.

Turbine goes well beyond the capabilities of traditional SOAR applications with its cloud-native architecture, low-code approach, robust case management, and AI-enhanced features. The priority when building Swimlane Turbine has been flexibility, scalability, and simplicity, because not only are organizations different from one another, but they're all different from what they were six months ago. Depending on your organization's needs, it can deploy in the cloud, on-premises, or in an air-gapped environment. See Figure 1.

Thanks to Canvas, Turbine's low-code playbook building studio, most of the work to deploy and build automation can be done in a no-code fashion. The beauty of low-code is that Turbine also offers SOC teams the ability to write a little quick Python code to make something work exactly how they want it to. AI-enhanced features simplify the Python scripting experience so that teams can build in Turbine without requiring master coders at every stage of the game.

Infinite integrations are available for Swimlane Turbine. This capability is the secret behind Swimlane's ability to take automation beyond the standard use cases – customers use it to automate threat hunting, vulnerability management, identity provisioning, patch management, auditing, and even compliance. If an integration is needed but not yet available, Swimlane will build it on-demand at no cost.

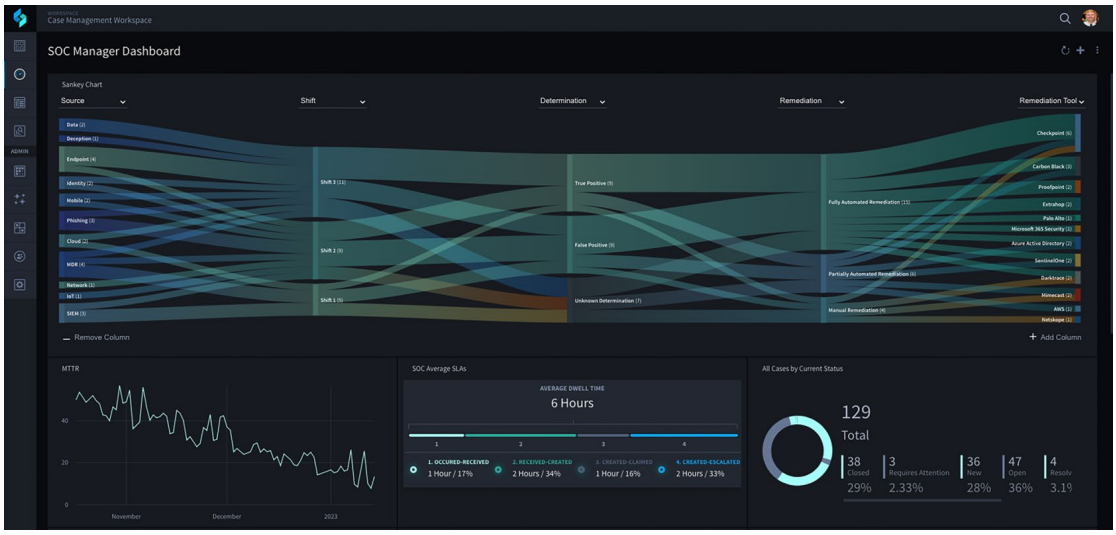


Figure 1. Swimlane Turbine SOC Manager Dashboard

Swimlane Hero AI is a collection of AI-enhanced innovations built on Swimlane's own secure large language model, available in Turbine. Features like case summarization, recommended actions, secure crafted prompts, text-to-code scripting assistants all work to make SOC teams more efficient without losing granular control by humans.

Many SANS SOC Survey respondents also noted issues with visibility into their organization's activities. Turbine provides SOC teams with seamless enterprise-wide visibility by aggregating and prioritizing all SecOps activities through robust case management, highly composable dashboards, and reporting. These visual applications help managers make good decisions and analysts work more effectively.

If you're ready to bring the power of AI-enhanced security automation to the job of making your SOC – and your whole security organization – more effective, visit **https://swimlane.com**