SWIMLANE

SANS | Research Program

PRODUCT BRIEFING

Agentic AI That Does the Work: How Swimlane Closes the Gap Between AI Adoption and Integration

Insights from the 2026 SANS SOC Survey

June 2026

The 2026 SANS SOC Survey outlines what most security operations teams already know: AI has arrived in the SOC faster than the organizational structures needed to govern and operationalize it. Seventy-nine percent of respondents report using AI or ML tools, yet only 36% have integrated those tools into a defined SOC workflow. Swimlane AI SOC was built for that gap, providing agentic AI automation that operates within the processes, tools, and oversight structures SOC teams already have, rather than adding another isolated capability that analysts must figure out how to apply.

The Foundation AI Needs to Work

The 2026 SOC Survey's findings on AI matter for procurement decisions because they identify the gap between adoption and integration within the organization, not in the technology. Teams that deploy AI without structure around how it is used, validated, or governed create a new category of risk, one where confident, well-formatted AI output is trusted by analysts who lack the context or tooling to challenge it.

Swimlane AI SOC was designed for teams that understand this risk and want to use AI in a controlled way. Its proprietary deep agents autonomously build investigation and response plans, generate executable playbooks for immediate deployment, and create reporting visualizations, ensuring that every AI decision remains explainable and every action is auditable. Teams decide which use cases allow more autonomy, where human review is required, and how every decision and action gets logged.

Key Findings

79%

use AI or ML tools, but adoption has outrun integration.

79% of SOC respondents use AI or ML tools, but only 36% have built those tools into a defined workflow. The majority are using AI individually, without governance or consistent validation, so outputs are trusted before anyone has established whether they should be. Swimlane AI SOC addresses this by embedding agentic AI into the SOC's existing workflows instead of adding another disconnected tool for analysts to manage.

24%

cite visibility as the top executive-level barrier.

24% of cyber leaders identify a lack of enterprise-wide visibility as the single biggest barrier to leveraging SOC capabilities, ranking it above staffing or automation gaps. The problem is not a lack of dashboards. Instead, the struggle is that evidence, workflow, ownership, and outcomes are spread across disconnected systems and do not stay connected as work moves through the SOC. Swimlane AI SOC addresses visibility at the workflow level, connecting data, cases, and outcomes across the team's existing environment.

70%

still measure activity over outcomes as their top SOC metric.

70% of respondents name number of incidents handled as their top-reported SOC metric, a distinction it has held for 10 consecutive year. It's also the metric used to set SOC budgets, yet it measures activity rather than whether the right threats were caught or contained. Swimlane AI SOC connects data, workflows, and outcomes on a single platform, giving leaders visibility beyond volume metrics.

Platform Capabilities

Should be this: Most SOC work still happens across too many systems, with too many manual handoffs between them. An analyst completing a single investigation may need to move between a SIEM, EDR, identity systems, threat intelligence, case management, ticketing, and reporting tools before they can close the case. Swimlane AI SOC orchestrates work across that entire environment without requiring teams to replace any of it (see Figure 1).

Agentic Defense with Deep Agents

Swimlane's AI agents build investigation and response plans across the team's existing tool stack, generating executable playbooks for immediate deployment. Rather than automating individual tasks in isolation, agents handle investigations from alert enrichment to documented closure, so the repetitive, multistep work that consumes analyst time gets handled without requiring a human to initiate each step across each system.

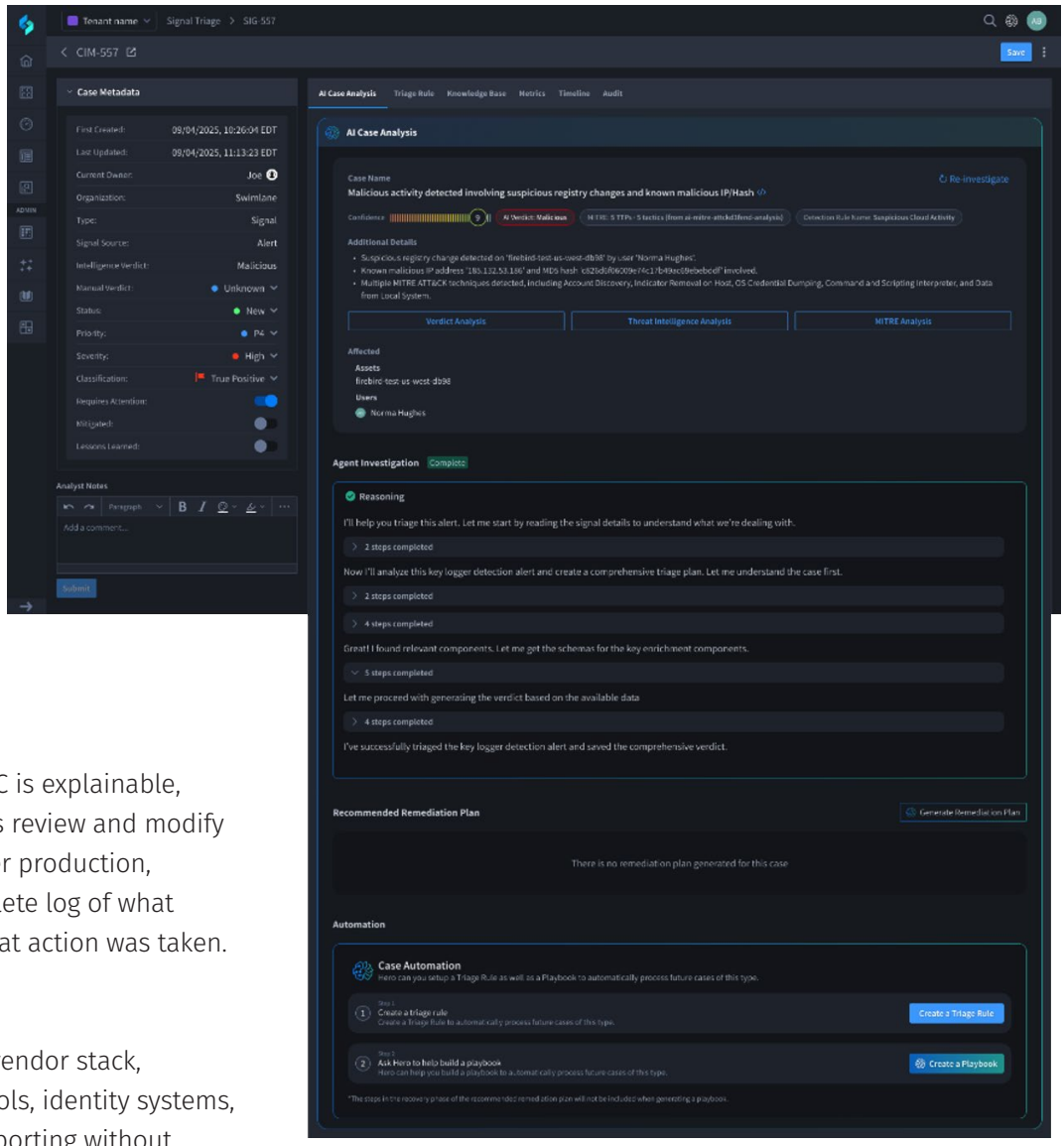

Figure 1. Swimlane AI SOC Interface

Transparency and Control

Every AI decision in Swimlane AI SOC is explainable, and every action is auditable. Teams review and modify AI-generated plans before they enter production, and the platform maintains a complete log of what happened, who approved it, and what action was taken.

Ecosystem Agnostic Integration

Swimlane AI SOC works across any vendor stack, connecting SIEM, EDR, XDR, cloud tools, identity systems, case management, ticketing, and reporting without requiring teams to replace existing investments, so visibility and response improve without a rip-and-replace.

Request a Demo