SWIMLANE

Swimlane SOC Solution Bundle

Automate your essential SecOps processes in 2 weeks or less

Maximize ROI with Complete End-to-End Solutions

The Swimlane SOC Solution Bundle combines pre-built automation solutions that every SecOps team needs. This Turbine bundle includes pre-built solutions for phishing, SIEM alert triage and EDR or XDR alert triage. Each SOC Solution is ecosystem-agnostic and includes dozens of playbooks, pre-built dashboards, and reports.

The SOC Solution Bundle pairs these carefully curated use case solutions with case management and threat intelligence applications. All solutions and applications included in the SOC Solution Bundle are professionally implemented by Swimlane in two weeks or less, with no additional cost. This holistic solutions offering delivers practical, quick wins while also fueling technical expertise through unlimited complimentary online training resources in the first year. Customers leveraging Turbine and the SOC Solution Bundle have achieved:

240%

Return on Investment

Fast & seamless implementation maximizes first-year ROI

95%

Alert Volume Reduction

Dramatically reduce alert volume by automating phishing and alert triage.

4.9★

Star Service Satisfaction

Experience Swimlane's 4.9-star services and support experience for yourself, or hear more from Gartner Peer Insights.

End-to-end SOC Solutions

Building a security operations center (SOC) is an art and a science, and for many, getting started with automating SOC processes seems daunting. Swimlane has been helping customers get started with automation for the past decade, so we've learned a thing or two about what a solid SOC automation foundation looks like. These insights are now directly incorporated into pre-built solutions that are available for all Swimlane Turbine customers.

Swimlane Phishing Triage Solution

The Swimlane Phishing Triage Solution supports 100% of email detection sources. It enriches observables and leverages multiple, carefully curated playbooks to execute dozens of actions on your behalf, per phishing investigation. The Phishing Triage Solution comes complete with an executive summary report of actionable insights related to reported phishing incidents.

Swimlane Alert Triage Solutions

Swimlane Turbine integrates with any API and offers pre-built SOC solutions for common ingestion sources. 100% of SIEM, EDR, and XDR providers are supported by the Swimlane Alert Triage Solutions. In the Alert Triage solution, Turbine ingests alerts through webhooks and APIs, enriches observables, and feeds data into applications like case management and summary dashboards.

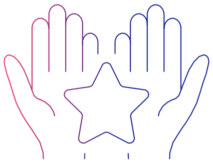
Turbine Applications

Threat Intelligence

- Multi-vendor IOC enrichment
- Enrich result normalization
- Threat intelligence metrics dashboard
- Enrich observables with case management

Case Management

- Outbound notification templates
- Case status & escalation
- Reassign case owner
- Case and incident management dashboard



Experience Swimlane’s 4.9 Star Service & Support

As the world’s largest independent security automation company, we are 100% dedicated to delivering best-in-class automation solutions, and it shows. We are proud to have earned an industry-leading 4.9/5 star rating on Gartner Peer Insights for services and support.

Swimlane is the leader in AI-enabled, low-code security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record to reduce process and data fatigue while quantifying business value and security effectiveness. The cloud-scale Turbine platform combines human and machine data into actionable intelligence for security leaders. For more information, visit swimlane.com.