JOINT SOLUTION BRIEF

Achieve the most cost-effective security cloud with Swimlane and AWS

Reduce the friction highly-distributed security operations teams experience during investigations and threat containment processes

→ Benefits

Increase Efficiency and ROI

Minimize analyst time spent on manual triage and incident response by automating cloud security workflows

Reduce SecOps Complexity

Reduce silos and increase visibility by integrating disparate security tools and processes.

Optimize KPIs

Regain time to focus on strategic work that reduces risk by improving MTTR and MTTD.

Challenges

SecOps teams are overwhelmed by complex environments and alert fatigue

Security teams struggle to effectively manage complex SOC's that have an average of 47 security tools that generate 10,000+ alerts per day. This results in silos, inefficiencies, alert fatigue and costly human errors.

The average financial impact of a data breach is $3.86 million. Between the lost business, regulatory fines, expensive remediation efforts, loss of customer trust and diminished reputation the cost of a data breach is too great for enterprises to be reactive. Security leaders know this, but between the cybersecurity skills shortage and expense of qualified talent, hiring more people is not always a viable solution.

The Swimlane Solution

Full-stack cloud-native security automation for AWS Security Cloud

In order to prevent breaches, enterprises need to improve their cloud security posture. The most cost-effective way to operationalize cloud security is to leverage full-stack cloud-native automation. Swimlane and AWS partner to bring low-code security automation building blocks to AWS cloud environments.

This partnership unites the world's most prominent hyperscaler, AWS, with the industries most performant and scalable security automation and orchestration engine, Turbine. As a result, the Turbine and AWS Security Lake integration reduces alert fatigue for analysts, helps engineers develop more secure cloud ecosystems, and provides CISOs with the ability to quickly identify security trends.

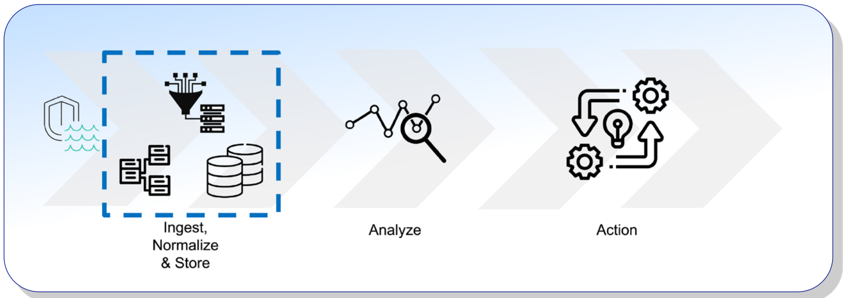
Featured Use Case: Alert Management

Challenge

A security analyst is manually triaging contextless alerts. Meanwhile, an unauthorized user attempts to access a sensitive database in the organization's AWS environment. An alert is triggered. The analyst needs to find this one-in-a-thousand, and respond effectively.

Solution

Turbine ingests the alert, queries additional intelligence sources, and enriches the data to provide the analyst with a summary of the attack within a robust case management interface. Low-code playbooks quickly execute predefined response actions while the analyst maintains control.

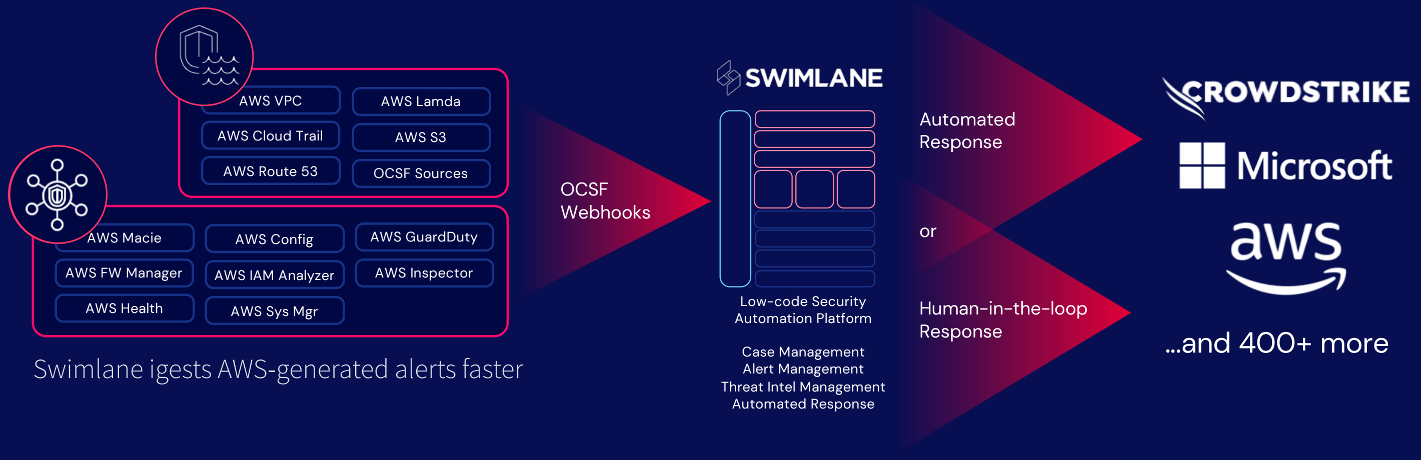


AWS Security Lake simplifies the workflow process enabling customers to get their first value faster

Results

The analyst blocks the unauthorized user from accessing the database or continuing to dwell within the AWS environment. Post-incident reports and dashboards automatically compile key data in plain language for the executive team to review the incident.

Swimlane on AWS



AWS VPC
AWS Lamda
AWS Cloud Trail
AWS S3
AWS Route 53
OCSF Sources
AWS Macie
AWS Config
AWS GuardDuty
AWS FW Manager
AWS IAM Analyzer
AWS Inspector
AWS Health
AWS Sys Mgr

Swimlane igests AWS-generated alerts faster

OCSF Webhooks

SWIMLANE

Low-code Security Automation Platform

Case Management
Alert Management
Threat Intel Management
Automated Response

Automated Response

or

Human-in-the-loop Response

CROWDSTRIKE
Microsoft
aws
...and 400+ more

→ Swimlane Turbine and AWS Security Lake help organizations aggregate, manage, and analyze log and event data to enable faster threat detection, investigation and incident response

→ Turbine ingests and enriches large volumes of data from AWS Security Lake and third-party sources.

→ Turbine is a cloud-native security automation platform, built on AWS infrastructure. Its unparalleled performance and scalability enables advanced automation use cases that were previously unavailable to AWS customers.

→ Both platforms are OCSF compliant so the integration is poised to deliver a seamless customer experience.

Features

OCSF-compliant

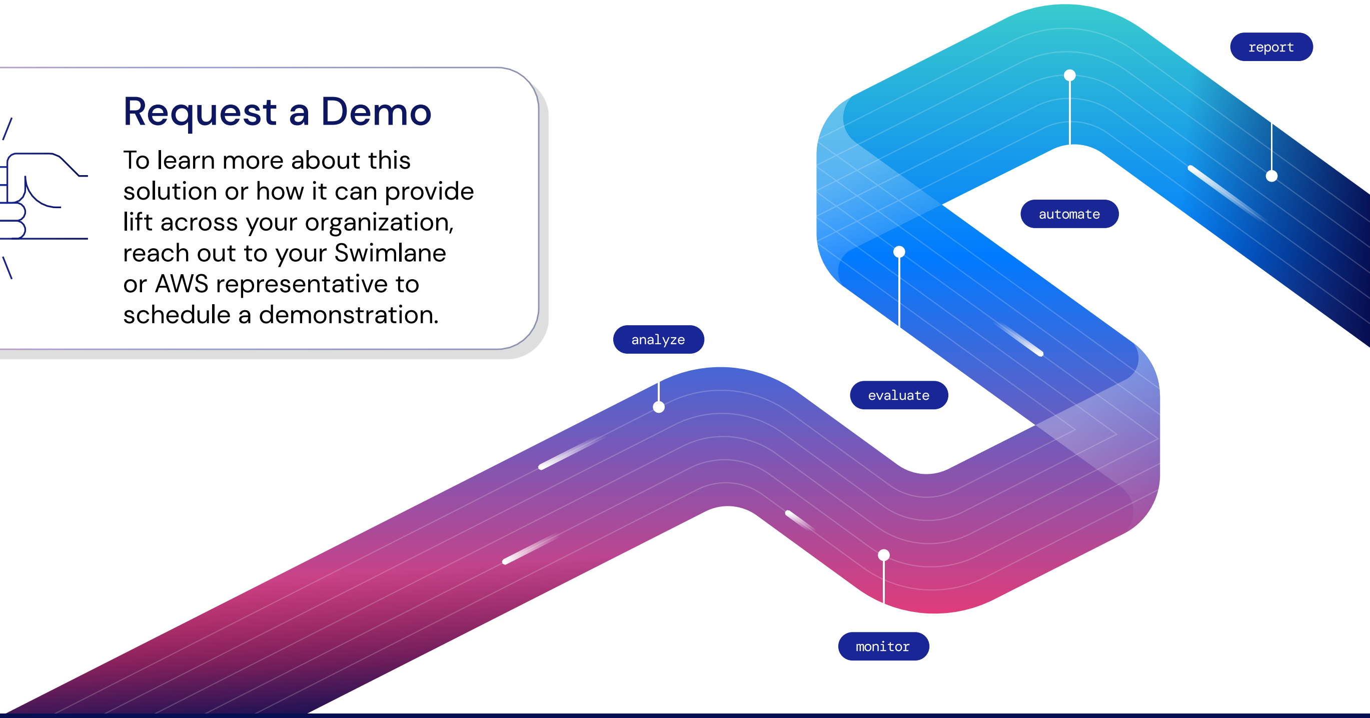
Turbine and Amazon Security Lake uniquely share Open Cybersecurity Schema Framework (OCSF) support, enabling seamless data between the platforms. This feature removes the need for developers to create custom mapping for security alerts from new data sources. As a result, SecOps can reduce the hours spent implementing and managing integrations in order to increase the cost-effectiveness of their security cloud.

Centralized data analysis and management

By integrating diverse security tools into a single platform, collaboration is improved while reducing silos and increasing visibility. Additionally, compliance management is simplified with enhanced reporting capabilities through centralized case management for security data and audit logs.

Request a Demo

To learn more about this solution or how it can provide lift across your organization, reach out to your Swimlane or AWS representative to schedule a demonstration.



SWIMLANE

Corporate Headquarters
363 Centennial Pkwy Suite 210
Louisville, CO 80027
1-844-SWIMLANE

Better Together

About Swimlane

Swimlane is the leader in cloud-scale, low-code security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record that helps overcome process and data fatigue, chronic staffing shortages, and quantifying business value. The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders. Learn more at: swimlane.com

About Amazon Web Services

Since 2006, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs. To learn more about AWS, visit aws.amazon.com