From Manual to Automated: Enhance Incident Response Process

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.

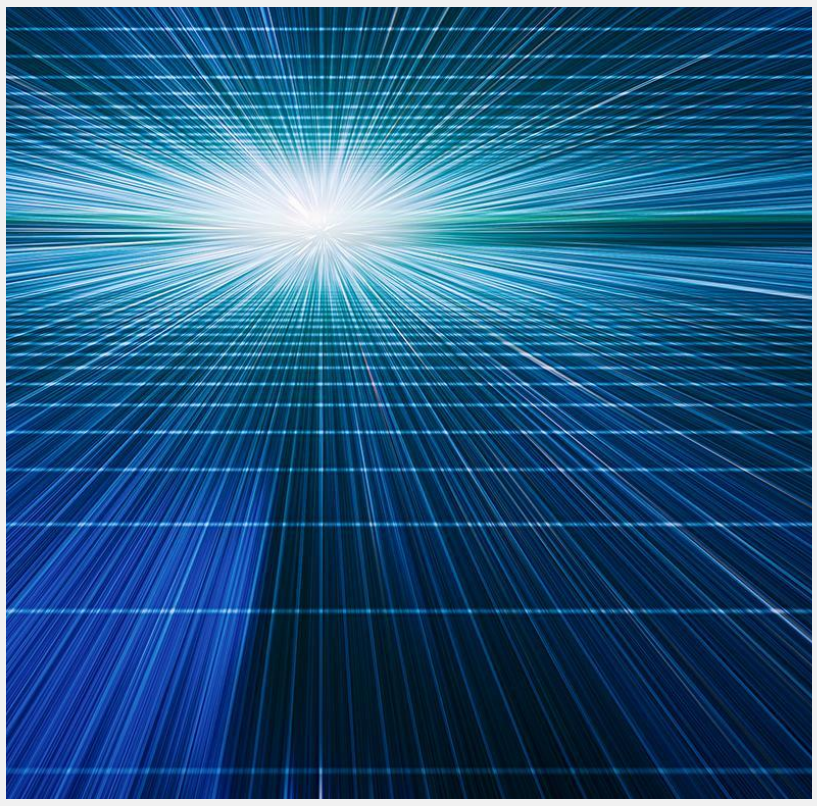
The average financial impact of a data breach is $3.86 million. Between the lost business, regulatory fines, expensive remediation efforts, loss of customer trust and diminished reputation the cost of a data breach is too great for enterprises to be reactive. Security leaders know this, but between the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

The Swimlane Solution

Low code security automation to achieve the most cost-effective and scalable security

Swimlane Turbine maximizes the incident response capabilities by automating time-intensive, manual processes and operational workflows. Its features address security activities, such as prioritizing alerts, remediating threats, and improving performance throughout the entire security organization. Additionally, Swimlane and AWS partner to bring low-code security automation building blocks to AWS cloud environments, offering the most cost-effective way to operationalize cloud security and leverage full-stack cloud-native automation.

Overall, Turbine and AWS integrations aim to reduces alert fatigue for analysts, help engineers develop more secure ecosystems, and provide CISOs with the ability to quickly identify security trends.



Benefits

Automate alert triage and streamline incident response workflows for your AWS infrastructure with Swimlane Turbine.

Improve Incident Response

When alert consolidation, correlation, and enrichment is automated analyst gain the context that they need to manage cases and trigger automated response actions at machine speed. This enables analysts speed MTTD, MTTR and reduce the dwell time of threats.

Optimize KPIs

Turbine ingests data and automatically summarized actionable incident details in case management. Each stakeholder is able to view relevant KPIs through customizable low-code dashboards and reports. This provides visibility into important metrics like SLA compliance, MTTR trends over time, dwell time by analyst, and ROI of the security program.

Reduce SecOps complexity

Turbine connects siloed tools, telemetry sources and teams. This unified approach to automation helps to streamline any security use case and results in reduced risk and faster remediation, ensuring a streamlined and efficient incident response process.

Swimlane Contact: Kevin Alexandra | kevin.alexandra@swimlane.com

Swimlane Turbine on AWS

Swimlane Turbine enables AWS customers to streamline incident response and automate the management of security alerts by leveraging Turbine to bolster the security operations center (SOC) team's ability to investigate and respond to threats against their AWS environment. AWS customers can implement Turbine to automate many of their formerly manual tasks to improve the speed and consistency of responding to and handling any security alerts that arise. Turbine makes it easy to connect a customer’s AWS environment with their set of security tools. Customers can then use Turbine to specify and customize tasks to be performed while also continuously monitoring any aspect of the operations through its case management, dashboards and reports.

SWIMLANE

Case Study: Cylitic Security

Challenges

Customers use Cylitic Security to mitigate their risk exposure to cyber-risk with top-tier protection, insurance and automated security certification. Central to this is the challenge to monitor all AWS infrastructure & services to ensure uptime, security and compliance are maintained..

Solution

The combination of Swimlane and AWS empowers Cylitic Security to seamlessly ingest AWS GuardDuty findings, gather logs from AWS CloudTrail and CloudWatch. The integration with AWS Security Hub also facilitates rapid ingestion of data stored within S3 Cloud Storage.

Results

Swimlane’s partnership with AWS has been a game-changer for Cylitic Security. It has enabled the team to respond faster and more effectively to security incidents, while also providing a comprehensive view of their security posture across their AWS environment.

Features

Security Lake Integration

Swimlane Turbine ingests information from AWS Security Lake and Security Hub. Turbine takes immediate action on AWS events through low-code playbooks and case management. This pre-built integration speeds the time to value for AWS and Swimlane customers and enhances the ROI they receive from both platforms.

OCSF-compliance

Turbine’s OCSF-compliant content removes the need for developers to create custom mapping for security alerts from new data sources.

GuardDuty, CloudTrail and CloudWatch Connectors

Swimlane Turbine ingests AWS GuardDuty findings automatically, enriches data by using open-source intelligence tools, and gathers logs from AWS CloudTrail and AWS CloudWatch. Once a determination has been made, Turbine can automatically perform appropriate remediation actions, such as blacklisting an IP, quarantining an Amazon Elastic Compute Cloud (EC2) instance, and/or taking a snapshot of an EC2 instance.

Visit AWS Marketplace or Swimlane.com to learn more.

Get started with Swimlane Turbine solutions on AWS

Swimlane Contact: Kevin Alexandra | kevin.alexandra@swimlane.com

aws PARTNER