aws partner network

SWIMLANE

Security Orchestration, Automation and Response on AWS

The Challenge
Manual incident response and the growing number of security alerts

Manual incident response processes, inefficient workflows, and difficulty hiring and retaining qualified personnel leaves security teams struggling to keep up with an ever-increasing volume of alarms. Overburdened security teams are manually performing repetitive and time-consuming tasks to track, aggregate, and resolve security events across multiple security tools. Despite the time and effort spent, teams are not able to protect their networks because they can't analyze or adequately prioritize all incoming security alerts. Additionally, a lack of visibility into their team's current activities, metrics, and performance leaves security managers struggling to visualize team effectiveness and justify additional resources.

The Swimlane Solution
Faster, more efficient security response and remediation

Swimlane is a leader in security orchestration, automation, and response (SOAR) solutions. By automating time-intensive, manual processes and operational workflows, while delivering powerful, consolidated analytics and real-time dashboards and reporting from across the security infrastructure, Swimlane maximizes the incident response capabilities of over-burdened and understaffed security operations teams. Swimlane's focused array of features are aimed at helping security operations centers (SOCs) to address both simple and complex security activities, from prioritizing alerts to remediating threats and improving performance across the entire security organization.

Benefits

Improve Incident Response
When alarms and related context are consolidated, threats identified and acted upon at machine speeds with the Swimlane platform, your team has the bandwidth to react faster and more intelligently to stop attacks before damage is done.

Prove Efficacy Gains
Swimlane gathers relevant information and metrics automatically, allowing you to view KPIs through customizable dashboards and reports. Gain visibility into the state of security within your organization with various metrics, including mean-time-to-detect, mean-time-to-respond, ROI, and individual and team performance.

Standardize Processes
Eliminate the chance of key incident response steps being forgotten or not followed correctly. Swimlane's workflows can execute many steps automatically and provide analysts with the prescribed next steps where necessary, resulting in reduced risk and faster remediation.

Swimlane for AWS

Swimlane enables AWS customers to streamline incident response and automate the management of security alerts by leveraging the Swimlane platform to bolster the SOC team's ability to investigate and respond to threats against their AWS environment. AWS customers can implement Swimlane to automate many of their formerly manual tasks to improve the speed and consistency of responding to and handling any security alerts that arise.

Swimlane makes it easy to connect a customer's AWS environment with their set of security tools. Customers can then use Swimlane to specify and customize tasks to be performed while also continuously monitoring any aspect of the operations through Swimlane dashboards and reports.

Features

Integrated with AWS and Third-Party tools

Swimlane helps ingest AWS GuardDuty findings automatically, enriches data by using open-source intelligence tools, and gathers logs from AWS CloudTrail and AWS CloudWatch.

Additionally, Swimlane integrates into AWS SecurityHub which provides a comprehensive view of security alerts and security posture across your AWS accounts.

Automated Response

Once a determination has been made, Swimlane 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.

Swimlane Case Study – U.S. Government Agency

Challenges

A U.S. government agency with an outsized threat profile suffered from an ever-growing number of daily attacks. Much of their SOC's time was spent on rote manual tasks like cutting and pasting information to and from threat enrichment and ticketing systems or manually searching for information stored on various separate databases.

Solution

The agency's Security Operation Center Section Chief began exploring the possibilities of SOAR solutions. He realized much of the mundane and repetitive work that was clogging up processes could be automated. After researching and evaluating several solutions, the Section Chief selected Swimlane as the best solution to meet his agency's needs.

Results

Since implementing Swimlane, the agency has seen dramatic improvements in mean time to respond. For example, on routine threats and incidents, the agency is seeing reductions of 75-90 percent in response time. This impressive time savings is enabled by providing analysts with an instant global view of the threat, while simultaneously relieving them of tedious manual tasks like ticket generation, updates, and looking up information across various disparate systems.

Get started with Swimlane for AWS

Visit AWS Marketplace to get started.