Automated Security Operations

Manual incident response processes, inefficient workflows and difficulty hiring and retaining qualified personal leaves security teams struggling to keep up with an ever-increasing volume of alarms. This despite having vested heavily in a wide array of security solutions and the staff required to triage, investigate and resolve emerging threats in a fast growing threat landscape.

Swimlane automates and orchestrates the incident response, collecting alert and event data from virtually any security platform with minimal effort. It automatically centralizes and responds to alerts using automated workflows to reduce mean time to detect and respond (MTTD/MTTR). Customizable, KPI-driven dashboards and reports deliver the intelligence necessary to adapt to new threats and drive continuous operational improvements.

The Problem

Organizations are losing the battle against attackers. Overburdened security administrators are manually performing repetitive and time-consuming tasks to track, mitigate and resolve security events across multiple security platforms. But despite the time and effort, they can’t analyze or adequately prioritize the security alerts and events necessary to protect their networks. And a lack visibility into their team’s current activities, metrics, and performance leaves security managers struggling to justify additional resources.

The Solution

Swimlane's automated orchestration and workflow expedites the entire incident response management process, from initial event notification to remediation and closure. It automatically gathers key information, builds decision cases, and executes critical actions to prevent and/or remediate threats based on logical incident response processes. Extensive out-of-the-box integrations and an API-first architecture enables software-defined security (SDS) to operate with any organization’s existing security infrastructure.
Swimlane delivers security automation and orchestration that maximizes the capabilities of an organization’s security infrastructure and staff. Intuitive, highly-customizable dashboards provide real-time enterprise visibility into threats and security processes.

**Unified Cross-Ecosystem SecOps Visibility**

Swimlane tracks all enterprise security tasks and delivers centralized access to cases, reports, dashboards and metrics. It automatically standardizes incident response and notification processes to streamline communications, accelerate resolution, and mitigate risk.

**Consistent, Scalable Incident Response Processes**

Swimlane captures best practices to improve an organization’s security capabilities, efficiency and performance. Standardization promotes rapid incident response and resolution; automation allows the system to scale and execute preapproved processes without human intervention.

**Faster Mean Time to Resolution (MTTR)**

Swimlane automates the incident response management process for threats identified by existing monitoring and detection systems. Visualizing threat intelligence and case history allows Swimlane to provide situational awareness of an incident and related event that may actually be part of a larger attack.

**Automated Threat Defense**

Swimlane delivers security orchestration through extensive integration with 3rd party platforms, replacing slow and manual threat response with machine-speed decision making and remediation. Automation and software-defined security (SDS) methods leverage vendor APIs to rapidly respond to and eliminate threats earlier in the kill chain.

**Comprehensive Key Performance Indicators**

Swimlane dashboards and metrics deliver real time visibility into the performance, capacity and ROI of an organization’s security operations investment. It delivers comprehensive insight into the specific variables that are impacting productivity, efficiency and effectiveness.