
Published on 22 Jan 2015

Phoenix Data Security recently announced the launch of Swimlane, a new security operations management platform and company focused on empowering enterprises and government agencies with data-driven automation and orchestration for incident response and improved security operations.

Swimlane centralizes an organization’s security alerts, alarms and incidents to automate resolution and deliver a better ROI on current and future security investments. Using software-defined security (SDSec) methods and security orchestration, Swimlane reduces manual effort by automatically responding to alerts, gathering related threat intelligence and automating the implementation of security controls, all which aides in protecting the organization from future attacks.

Swimlane co-founders Cody Cornell, CEO and Brian Kafenbaum, COO, who have been information security consultants to some of the world’s largest companies and government organizations, spun Swimlane off from their cyber security consulting and services firm Phoenix Data Security. The software platform was developed to fill a market gap for a solution that would significantly reduce the expense and time associated with the manual effort of managing the rapidly growing number of security activities that is required of a modern Security Operations Center (SOC).

“As an industry we have become very good at detecting malicious activity and generating alerts, so threat detection is no longer the issue. Swimlane’s purpose is to automate incident response—reducing hours, if not days, of work down to minutes—better enabling an organization to respond and take action,” said Cornell.

A Market Ready for Innovation

Swimlane enters a growing market ready for innovation and growth. Hackers stole more than
500 million American financial records in the past year, making the U.S. financial sector one of the most targeted in the world, FBI and Secret Service officials warned. The attacks included Target, Home Depot, JPMorgan Chase, and many others. Industry research firm Gartner reported that 2014 worldwide information security market growth will exceed $73 billion.

**Swimlane Platform: Improving Security While Reducing Costs**

Swimlane integrates with an organization’s existing technologies and is a purpose-built security automation platform. Its many distinct features include:

- **Automated Security Response** - Automatically unify, analyze and resolve alerts from existing security tools leveraging a single stream management process.

- **Increased Situational Awareness** - Arm security analysts with related discoveries and threat intelligence to rapidly and logically triage and resolve their assigned incidents.

- **Achieve Earlier Attack Chain Response** - Proactively gather evidence and quickly remediate attacks from threat actors using automated software-defined security methods.

- **Optimize Staff and Reduce Costs** - Improve efficiency, standardize processes and automate tasks so organizations can maintain a stronger, more cost-effective security team.

- **Provide Real-Time Visibility and Oversight** - Gather security metrics, dynamically generate reports, and simplify the creation of dashboards for real-time operations management.

- **Enable Expert Threat Response** - Prioritize alerts, standardize workflows and guide remediation to allow all security analysts to resolve cases with expert proficiency.

Swimlane was designed from the ground up with flexibility in mind and the ability to adapt and easily integrate into an enterprise.
“Swimlane does not tell you how to structure your security operations, it adapts to you,” said Kafenbaum. “Automation makes us more efficient, ensuring corrective or preventative action is taken on every alert. The consequence of missing an alert or not responding in time has proven to cost millions of dollars.”