SWIMLANE

Banking and Financial Services Security Orchestration, Automation and Response (SOAR)

Automate Operations for Better Security and ROI

Research shows banking and financial services organizations are hit by security incidents 300 times more often than other industries. As bad actors, nation-states, and organized crime syndicates continue to change the threat landscape, financial institutions' complex IT ecosystems are constantly at risk.

Compounding the issue, the cybersecurity skills gap continues to grow and CISOs are unable to hire enough talent to adequately mitigate the threats. The weight of the problem falls squarely on the Security Operations teams working tirelessly to protect their organizations in a multi-cloud, hybrid IT world where security events, network outages, and application downtime are costing companies billions of dollars from reputational damage, theft, data exfiltration, fraud, and non-compliance fines industry wide.

Financial Customer Success

- Improve mean-time-to respond MTTR by 75 percent
- 100 percent of alerts at least partially automated
- 25 percent of alerts automated end-to-end

"The Swimlane team did a great job in getting us up and running quickly. We saw immediate value from the Swimlane solution with a 50 percent decrease in our mean-time-to-detect (MTTD) and decreased alert volume by one-third."

- Fortune 250 Holding Company

Financial Services and Swimlane

Swimlane's security orchestration, automation and response (SOAR) solution expedites the entire incident response management process, from initial event notification to remediation and closure. It automatically gathers key information, builds and manages decisions and 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 enable software-defined security (SDS) to operate with any organization's existing security infrastructure including the specialized systems that are used to support banking and financial services.

Financial Services companies around the globe rely on Swimlane to understand their unique security orchestration and automation needs. Swimlane delivers a SOAR solution for Financial Services that maximize the capabilities of an organization's security infrastructure and staff and provides intuitive, highly-customizable dashboards to provide real-time enterprise visibility into threats and security processes.

Financial Services customers use Swimlane for a number of use cases across security operations, network and cloud operations, compliance and risk, threat management and incident response. Some examples include:

- SIEM Alert Triage
- Insider Threat
- Data Loss Prevention
- Threat Hunting
- Incident Response and Management
- Compliance and Risk Management
- Phishing Triage

About Swimlane

Swimlane is at the forefront of the security orchestration, automation and response (SOAR) solution market. By automating time-intensive, manual processes and operational workflows and delivering powerful, consolidated analytics, real-time dashboards and reporting from across the security infrastructure, Swimlane maximizes the incident response capabilities of over-burdened and understaffed security operations.

The unified defense platform offers a broad array of features 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 organization.

Swimlane Financial Success: Automating Phishing Response

According to the *Verizon Data Breach Incident Report*, up to 70% of breaches associated with a nation-state or state-affiliated actors involved phishing. Organizations are overwhelmed with phishing attacks and internal phishing reports and need a way to reduce the risk without overwhelming their security teams.

A global financial institution was compromised via phishing emails and watering hole attacks. These techniques overwhelmed and rendered their systems and processes completely ineffective, allowing connection to URLs that had been previously reported malicious.

Using Swimlane to automate the submission of suspicious URLs directly into their perimeter protection, the customer was able to increase input from 200 manual submissions to over 8000 per year.

While users are not perfect, they are one of the many sources of intelligence gathering that can help improve mean-time-to-detect (MTTD) of threat actor infrastructure being used to target your organization. Automation with Swimlane allows organizations to effectively ingest and evaluate user submitted information in real-time while effectively implementing improvements to perimeter protection to decrease risk and improve overall security posture.

To learn more about how Swimlane can help reduce security risk and improve your security operations, please visit www.swimlane.com.