SWIMLANE

Protecting Complex Energy Infrastructure Worldwide

Energy Customer Success

- Triage over 250,000 SIEM events and 450 SIEM alerts per day
- 100 percent of alerts at least partially automated
- 15 percent of alerts automated end-to-end

"Swimlane has helped us automate low-level alerts, which has helped our team focus on more proactive hunts. This single pane of automation (not 'glass') makes it easier to automate processes, review activity and prioritize responses."

- Fortune 500 Energy Conglomerate Customer

Cybersecurity Threats and Critical Infrastructure

The energy and utilities industry faces many of the same security challenges as other industries, but the stakes are often much greater. While financial gain and data theft are issues that span industries, energy and utilities companies are increasingly seeing attacks aimed at disruption or destruction. According to a recent study by Deloitte, the energy sector is one of the three most targeted industries, behind only critical manufacturing and communications.

As digital transformation results in a confluence of information technology (IT) systems and operational technology (OT) systems and their data, organizations incur more risk as the attack surface increases. With an ever-expanding threat landscape, more sophisticated nation-state threat actors, and the risk to human safety and economic activities, the need for better energy infrastructure risk management is greater than ever.

Reduce Risk Through Orchestration and Automation

Readiness to respond to cyber threats is a major challenge facing the utilities sector. Whether this is due to internal organizational failures, technical deficiencies or other reasons, the result is blind spots that leave your organization vulnerable.

Swimlane helps you respond to cyberattacks at machine speeds using intelligent automation and orchestration. The vendor-neutral security orchestration, automation and response (SOAR) platform integrates with your existing IT and OT security tools and manages the influx of alerts generated by these disparate solutions. With Swimlane, you can automate the incident response process easily and effectively.

Energy and utilities companies around the globe rely on Swimlane to understand their unique security orchestration and automation needs. Backed by the leading energy investment and innovation firm Energy Impact Partners (EIP), Swimlane is designed to help energy and utility companies:

- Minimize energy infrastructure and industrial control (SCADA/IT/OT) security risks.
- Optimize SOC/NOC operations security effectiveness, analyst resources, and costs.
- Integrate all IT and security operations tools for cross-ecosystem visibility.
- Automate complex workflows and incident response processes.

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.

Address Top Security Challenges with Swimlane

Alert Triage

Security teams are overwhelmed by the number of alerts from their SIEM tools. Organizations are left vulnerable as analysts can only investigate a fraction of the true alerts that come in each day. Swimlane automates your alert triage processes, quickly identifying and eliminating false positives while escalating valid threats and performing a range of activities from initial analysis and validation to full remediation.

Phishing

Phishing is one of the most common types of cyberattacks and thus can produce a large number of alerts. Additionally, manually investigating and remediating all phishing attempts takes more time and manpower than exists in many organizations. Swimlane integrates with your existing security solutions and provides a centralized platform to automate the investigation and quarantine of suspecting phishing emails.

Insider Threat

Whether malicious or negligent, insider threats represents the majority of breaches. Researching and validating these threats requires extensive effort. Swimlane uses orchestration to integrate multiple tools for rapid insider threat detection and response. Security automation then triggers workflows, pushing threat incidents through the investigation and response process and only alerting teams when human intervention is required.

Compliance Tracking

Maintaining compliance is a large challenge for many organizations in the energy and utilities sector. Swimlane is ideal for helping track compliance. The platform integrates with tools across your security stack, enabling you to automate the collection of audit evidence and the building of audit packages.

Proving Security ROI for Energy Customers Worldwide

The unique architecture of Swimlane's SOAR platform—as a solution that aggregates data from multiple sources—makes it easy to track metrics across your entire technology stack:

- **Reduce mean time to resolution (MTTR)**. Swimlane connects to your existing security tools, aggregating incident data and actions inside the platform. Faster access to relevant alert data and the ability to execute remediation actions at machine speeds reduces your MTTR. Every step in the process is tracked, so you can see how each part of your SecOps program contributes to resolving incidents effectively while also surfacing optimization opportunities.
- **Maximize staff efficiency**. Swimlane decreases errors and increases staff efficiency by allowing your analysts to engage in investigation and enforcement actions directly within the platform. This removes the need to toggle between different tools to complete incident resolution steps. In-depth activity tracking and flexible dashboards provide detailed performance metrics that measure how both individual employees and teams respond to different types of incidents.
- **See the value of automation**. Swimlane allows you to cut costs through automating time intensive incident resolution tasks. The platform calculates ROI for you by tracking the difference between manual incident response execution versus an automated response. This presents a quantifiable ROI, making it easy to justify the value of SOAR to your executive staff.

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