

Swimlane for MSSPs

Why Swimlane for MSSPs?

- Largest US independent SOAR vendor committed to vendor neutrality.
- Multi-Tenant SOC Platform
- 1000s of ready integrations
- Custom integrations - fast and free
- Intelligent Case Management
- Drag-and-Drop Workflow Builder
- Context-Driven Investigation
- Secure Remote Response
- Customer-Facing Reports and Dashboards
- Crisis and Communications Management

Swimlane clients have seen a decrease of 20-40X in MTTD and MTTR.

Expanding Service Levels and Offerings with Swimlane

As companies quickly expand their remote workforce and add cloud-based technologies, they also open additional endpoints thus increasing their exposure to threats and attacks. With this increased risk, many companies look to managed services as a way to quickly address their growing needs. The opportunity for managed security service providers (MSSPs) is great, and it's even greater when optimizing your SOC operations and revenue opportunities with Swimlane.

Deliver Complex Managed Services

MSSPs must deliver high-performance services across diverse clients, processes and technologies while maximizing your own resources and business operations. Swimlane provides powerful detection, response and management capabilities that enable MSSPs to provide improved levels of service while also scaling and growing your business.

Optimize Services

The security skills shortage affects all organizations but the impact and loss of skilled staff to managed services providers can be devastating to your operations and bottom-line. Swimlane enables MSSPs to manage clients and technology tools from a central workbench to deliver powerful incident response while optimizing internal SOC resources.

Swimlane helps MSSPs:

- Manage multiple clients from a single, unified platform
- Establish, standardize, customize and automate response workflows for clients
- Prioritize and optimize analyst tasks across the SOC in a single workbench
- Demonstrate additional value for clients with improved SLA performance by automating manual tasks and providing analysts with all the needed queries and research.
- Improve and verify the mean time to detect, respond and remediate the alert.

Common MSSP Use Cases

- Phishing Triage
- SIEM Triage
- EDR
- Vulnerability Management
- Perimeter Alarm Remediation
- Certificate Expiration
- More

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.

Expanding Services and Growing Revenues

Beyond improving security operations, Swimlane can help generate additional streams of revenue with such use cases as:



VPN Access Monitoring

With so many users now working outside the office, it is more important than ever to monitor an organization's remote-access and other VPNs.



Domain Squatting

Configuring a domain squatting use case to automatically monitor a client's domains is an easy win. This automation provides visibility to newly registered domains containing a specified URL and prevents attackers from registering similar domains.



Credential Dump Monitoring & Validation

Every day there's a new headline of a breach— making it impossible for administrators to reset user's passwords for every incident. By automating the monitoring of credential dumping, verification, lock and reset, the analyst can focus on remediation.



Managed Detection and Response

Swimlane works with many MSSPs to help them evolve from reactive monitoring services to proactive detection and response services- easing the lift to train analysts in how to interact with a client's environment and automate manual tasks.



Swimlane as a Service

When costs or SLAs drive clients to pull services in-house, Swimlane offers MSSPs an opportunity to continue with the account with services such as threat intelligence as a service and advanced investigation capabilities.



Threat Intel and Advanced Investigation

Quality threat intelligence can be costly. With Swimlane, MSSPs can provide threat intelligence research and comprehensive malware or forensic investigation resources.

With Swimlane, MSSPs can streamline and enhance incident response to go beyond management and monitoring to offer additional services at scale.

“
...in just one week you've given us 341 hours of analyst actions for just phishing triage. This will allow us to increase our customer base 3-4 X without having to hire more engineers and analysts.

-VP of SOC Operations, Service Provider