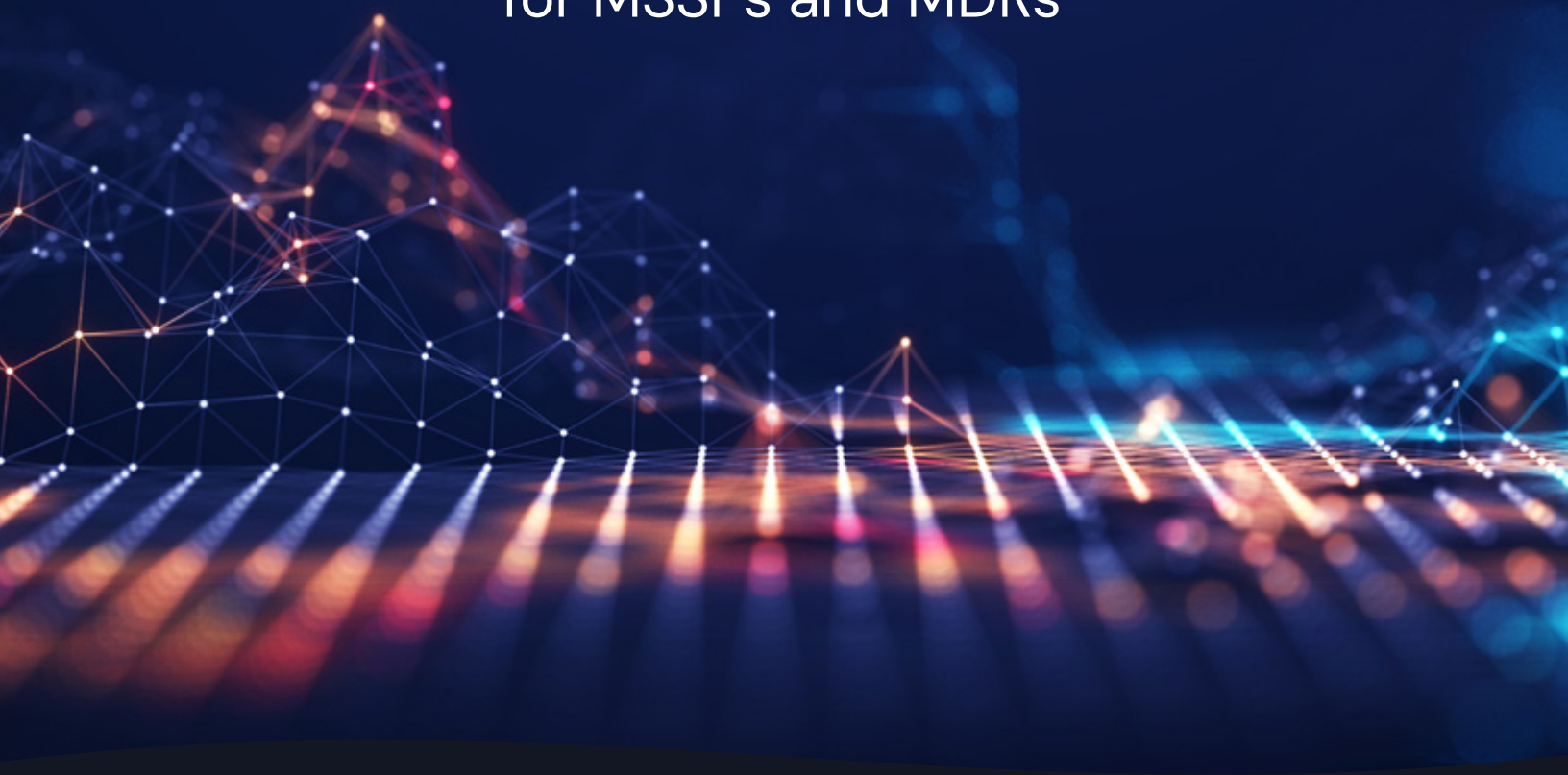
The Automation Imperative

Supercharging Efficacy and Scale for MSSPs and MDRs



SWIMLANE

Overview

Managed Security Service Providers (MSSPs) were initially established to manage and monitor on-premises hardware and security products for organizations. As digital transformation and cloud adoption accelerated, MSSPs shifted their business model to focus more on cloud delivery for service (SaaS) products like firewalls, secure web gateways, unified threat monitoring, security orchestration automation and response (SOAR) and security information and event management (SIEM) – which are all traditionally on-premises technologies.

Today, MSSPs are undergoing their next business model transformation, defined by the need to unify these disparate solutions. Architectural frameworks and solutions like Secure Access Service Edge (SASE), Extended Detection and Response (XDR) and Zero Trust are technology trends that have served as a catalyst to usher in the era of Managed Detection and Response (MDR) service offerings.

As MSSPs look to grow their business with MDR services, the need for unified security automation - and with it, scalability and flexibility - is more pervasive than ever. This eBook illustrates the critical role that automation plays in fueling MSSP and MDR business growth. You will learn:

- The **top 10 business challenges** that MSSPs experience
- **Business considerations** of how to leverage automation to increase profitability
- **Operational recommendations** and use cases for MSSPs who want to increase profitability through the ability to take on more customers.
- **Technical requirements** and capabilities needed for MSSPs to achieve automation-led growth
- The **benefits and outcomes** of MSSPs who already leverage Swimlane automation experience.

SWIMLANE

Top 10 MSSP Challenges That Automation Helps

The most common challenges that MSSPs face are not unique to service providers, rather they are shared among the entire security industry. However, MSSPs feel the industry's pain points more acutely than their enterprise counterparts due to the added complexity that comes from securing multiple unique environments simultaneously.

1

Alert fatigue

Analysts need to triage upwards of 10,000 alerts per day, with zero room for error. This requires the ability to accurately distinguish between true and false alerts at machine speed.

2

Evolving threat landscape

The attack surface is always expanding, and new attack techniques, malware variants and vulnerabilities emerge daily. Staying ahead of threats requires continuous monitoring and enrichment of various intelligence sources.

3

Security skills shortages

There are currently 2.7 million unfilled cybersecurity jobs globally. Enterprises and MSSPs alike struggle to hire and retain qualified analysts. For MSSPs, the high cost of talent has a direct impact on business growth and profitability.

4

Constant context switching

Adequate context about an alert is difficult to obtain for any security team. This challenge is compounded for MSSPs who have to navigate between the contextual nuances of multiple clients.

5

Complex and siloed technologies

MSSP analysts need to be proficient in multiple security platforms. They struggle with the complexity and time required to navigate the siloed tools, unique user experiences and data formats.

6

Compliance and regulatory requirements

GDPR, HIPAA, and PCI are just a few of the regulations that MSSPs help their customers audit and comply with. Ensuring continuous compliance with multiple regulations for various environments is no small task.

7

Communication and collaboration

MSSP security analysts need to be effective communicators while being skilled from a technology and security standpoint. Many find it challenging to translate technical details to non-technical stakeholders.

8

Threat hunting and incident response

MSSP's need to take a proactive stance to threat hunting and incident response for their customers. However, it's often challenging, if not impossible, to manually detect advanced persistent threats across multiple environments.

9

Scalability and performance

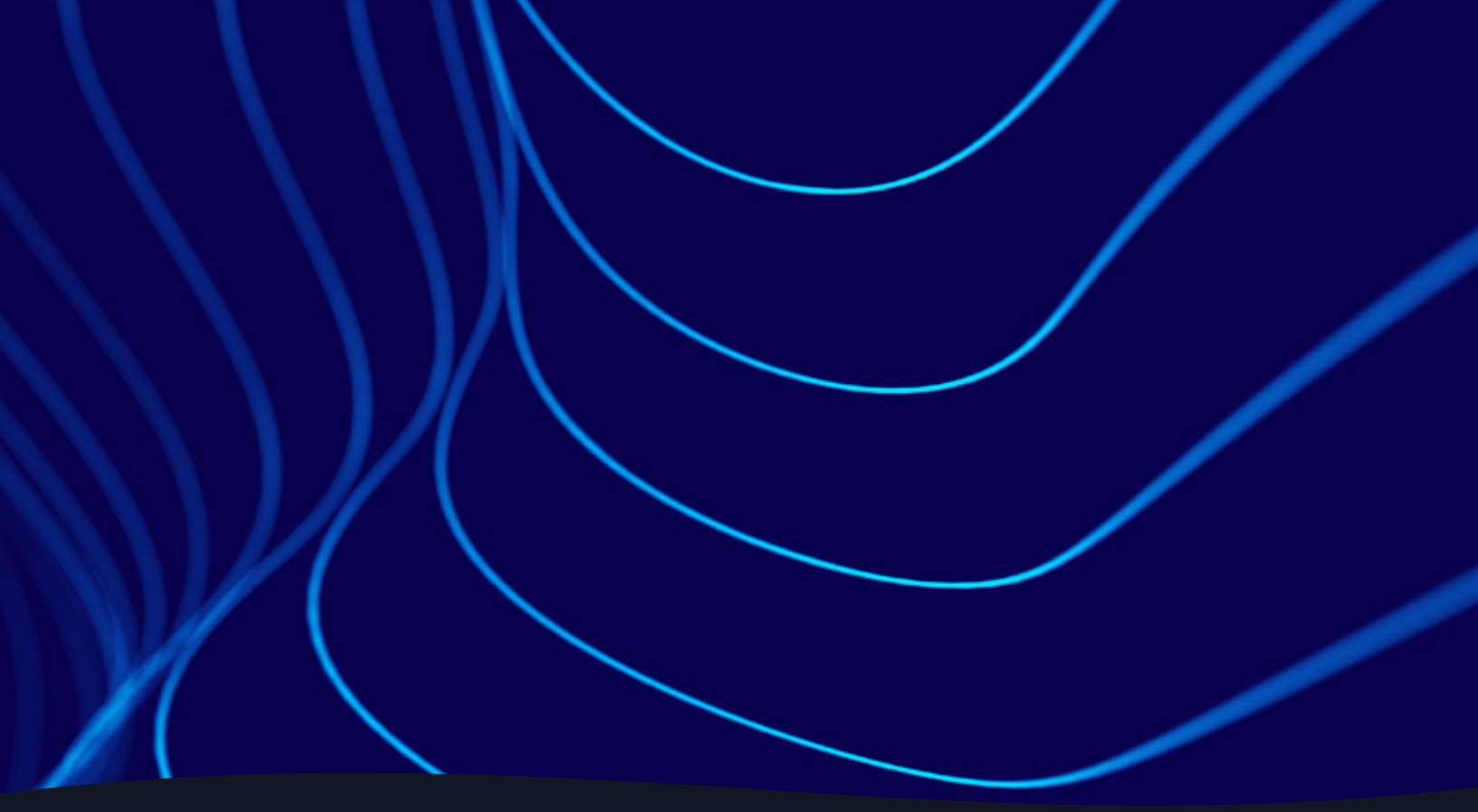
In order to increase profitability, MSSPs need the infrastructure and ability to ingest, enrich and respond to data at mass scale as their client base grows.

10

Emerging technologies and trends

Technology is always changing. From ChatGPT, to cloud computing and Internet of Things (IoT) devices, MSSPs need to build effective strategies to address the risks and opportunities presented by these innovations.

SWIMLANE



Why security automation is the key to MSSP business growth

Just like smaller and mid-sized organizations look to MSSPs as a way to avoid the capital and operational expenditures (CapEx/OpEx) associated with standing up a 24/7 security operations center (SOC), the most profitable MSSPs look to automation to reduce the cost of goods sold (COGS). Many detection-centric products offer micro-automation or SOAR-lite capabilities, but the reality is this is not enough to achieve the desired outcomes of unified automation and to alleviate the common pain points that MSSP security analysts face. MSSPs need a best-of-breed security automation platform in order to maximize profitability and exceed their customers' expectations in terms of **cyber-readiness**, **responsiveness**, and **results**.

SWIMLANE

Delivers Cyber-Readiness Outcomes

The notion that the attack surface is expanding is not news to anyone in the security industry. At the same time, the industry has all but accepted the reality that there will never be enough humans to fill the cybersecurity talent shortage. If left unchecked, this dichotomy results in more vulnerabilities, business-impacting breaches, ransomware, malware, fraud, insider threats – and the list goes on and on. These threats can halt business and have customer-facing impacts, like the loss of business trust and revenue.

Organizations worldwide turn to MSSP's to help deliver cyber-readiness business outcomes. With cyber security now being recognized as a business risk, MSSPs need the ability to translate their capabilities into meaningful metrics that C-level executives and board members can understand. Modern, unified security automation platforms offer capabilities that deliver cyber-readiness outcomes like community-sourced and enriched threat intelligence, cross-environmental alert context, and effective and human-readable KPI tracking.

SWIMLANE

Facilitates Next-Level Responsiveness

For MSSPs embracing any level of micro-automation capabilities today, the ability to absorb basic response actions for customers is practically table stakes. It's standard practice to manage detection services, acknowledge and assign alerts to analysts, or enrich threat intelligence. What differentiates good MSSPs from the great ones is the ability to take responsiveness to the next level by using best-of-breed automation to disrupt or contain an active threat for customers.

In order for an MSSP to be truly responsive on behalf of their customers, they need extreme flexibility in terms of use case creation and approvals. This requires a security automation platform that has the ability to integrate with anything, and that has features that support communication and case management.

Delivers Clear Results

MSSPs need the ability to tangibly show results to their customers. Results must be communicated in plain English (not tech speak) in order to be universally understood and influential. After all, two-thirds of decision-makers during the purchase or renewal of managed services do not have technical backgrounds. In order to resonate with these decision-makers, MSSPs need automated and visual dashboards and reporting capabilities. Low-code security automation platforms offer easy to highly customizable persona-driven reports that easily highlight key metrics like mean-time-to-resolution (MTTR), mean-time-to-detection (MTTD), return on investment (ROI) and organization-wide risk reduction over time according to the MITRE ATT&CK framework.

Security Automation Benefits for MSSPs

- Increase SOC efficiency by 60%
- Save 45 minutes per investigation
- Grow business by 30% without adding headcount.
- Reduce cost of good sold (COGS)
- Increase the profitability of service offerings with fast onboarding
- Reduce MTTD and MTTR for clients
- Expand revenue streams with extensible use cases
- Automate low-level tasks to gain virtual analysts
- Establish 24/7 coverage for virtual SOCs

SWIMLANE

MSSP Requirements for Security Automation

Operational Requirements

Operational considerations are arguably the least glamorous or exciting thing when it comes to evaluating which security automation platform is the best fit. As mundane as it may seem, it's also the area with the greatest impact on outcomes.

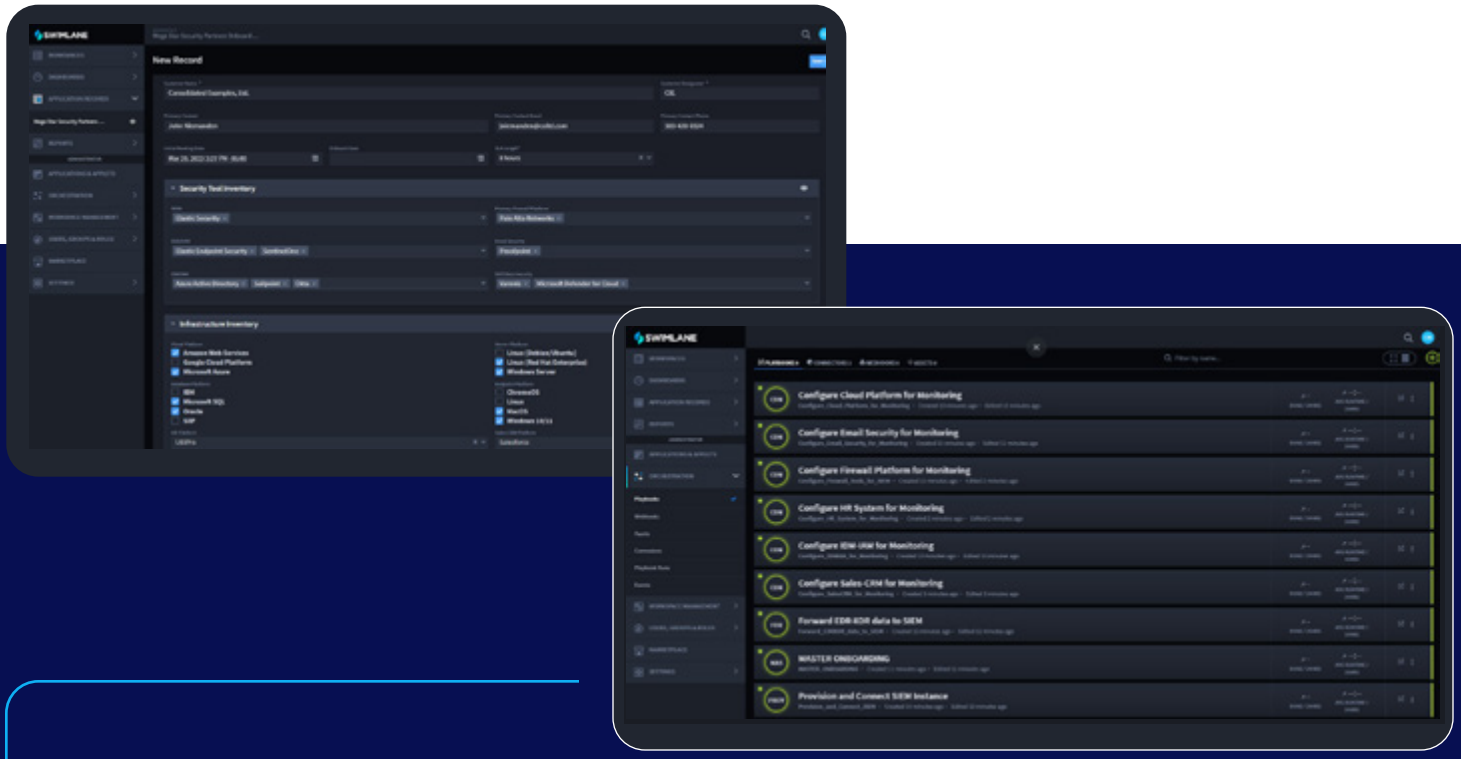
Scalable Client On-boarding

Challenge

The activation time for MSSPs to onboard new customers averages 90-100 days. This is not an acceptable length of time by customer standards, and the resources needed during this time eat into profitability.

Solution

MSSPs who use the Swimlane Turbine low-code security automation platform can leverage pre-built client onboarding solutions to standardize and automate this process. The cloud-native platform can integrate with any API so it's easy for MSSPs to get their customers' credential sources from the cloud and plug them into Turbine in order to configure the solution based on unique customer environments.



Outcome

MSSPs who use automation are able to onboard new clients as fast as 30-45 days. **This time-to-value outcome translates into a differentiator for MSSPs and helps them win new business.**

SWIMLANE

MSSP Requirements for Security Automation

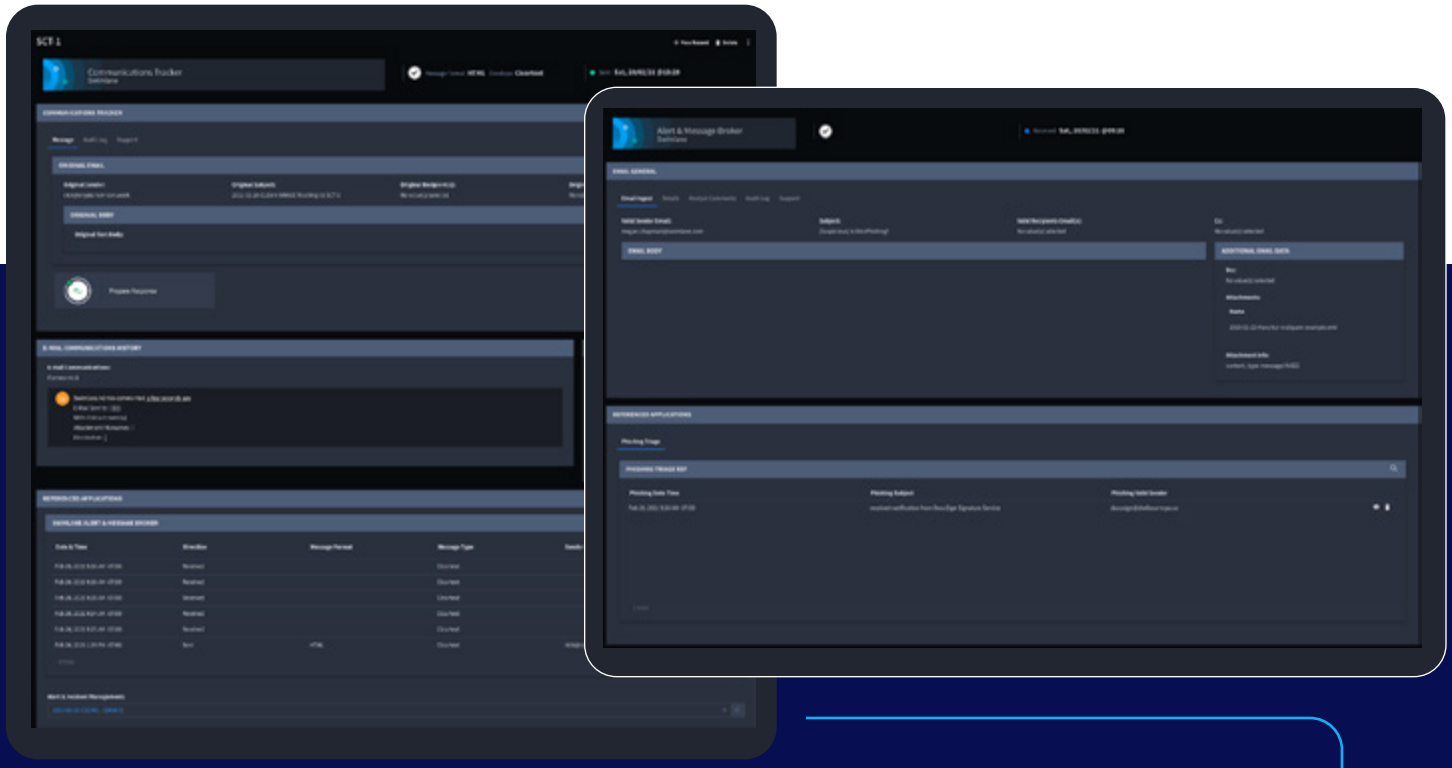
Managing and Tracking Client Approvals

Challenge

MSSPs need to balance urgency with accuracy and client requirements when security incidents and threats occur. It is a challenge for MSSPs to manage and track client approvals due to diverse requirements across their client base, a lack of standardized frameworks, stakeholder communication silos and security or confidentiality concerns.

Solution

Swimlane Turbine has purpose-built communication tracking applications for MSSPs. It integrates with email and documents client communication history and attachments directly in the platform. Alternatively, Turbine can integrate with Slack or Microsoft Teams to offer flexible communication options that fit the culture and individual preferences.



Outcome

Using Turbine to track client approval helps MSSPs bring their customers into the loop of automation in an efficient and effective way. With this solution, when an alert comes, it's easy to collaboratively vet and add to a customer built “approve list” or mark it as malicious for preventative threat hunting.

SWIMLANE

MSSP Requirements for Security Automation

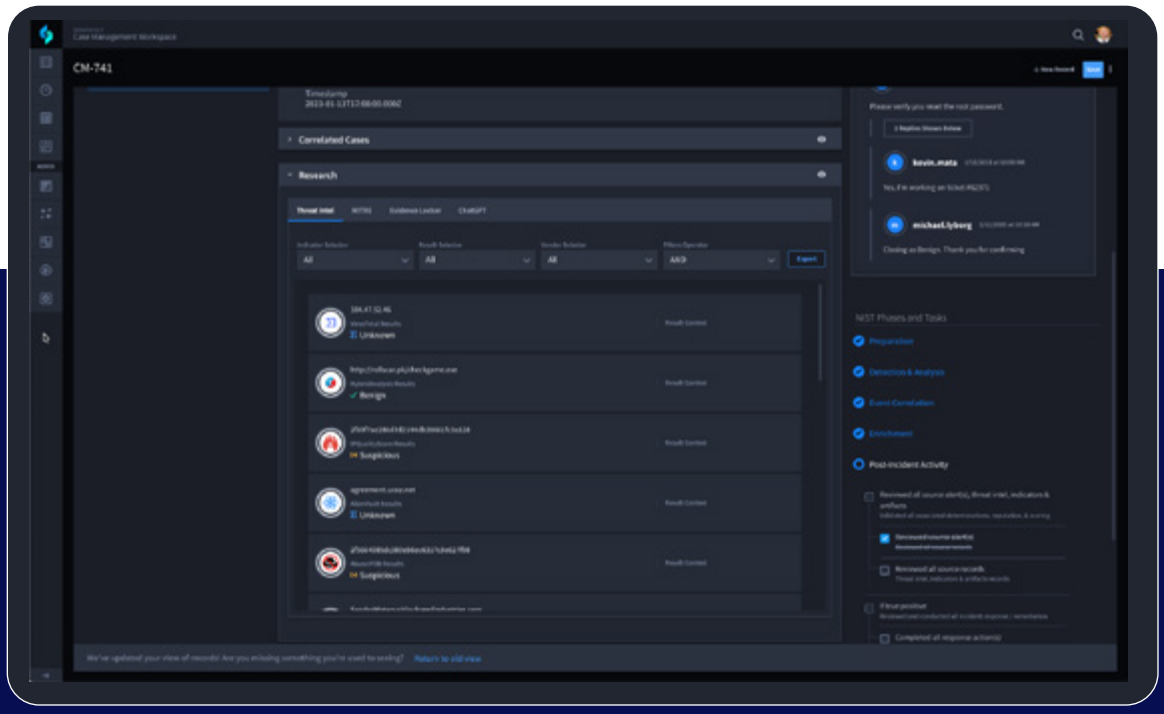
Easily Customize Detection and Response Processes

Challenge

No two organizations operate the same or have the same environment. This means that MSSPs need to adapt their detection and response workflows in order to suit each individual client's requirements. Without low-code automation, this is a manual, time-intensive and costly process.

Solution

Turbine delivers unified automation that is flexible enough to extend beyond the SOC. MSSPs can leverage Turbine's case management capabilities or order to build highly customizable user interfaces for each of their clients.



Outcome

The highly composable nature of Turbine helps MSSPs build more diverse and complex use cases like domain squatting and threat hunting. As a result, **MSSPs increase revenue streams and grow their business faster**.

SWIMLANE

MSSP Requirements for Security Automation

Compliance & Regulatory Support

Challenge
MSSPs who serve customers in healthcare, finance, energy or government sectors need to be experts in the industries' compliance measures and regulations. Knowing the regulation is one thing, but operationalizing security controls and processes to ensure continuous compliance is another.

Solution
A Swimlane MSSP customer who specializes in securing critical infrastructure and operational technology (OT) environments, deployed Swimlane on-premises with a custom hardened appliance to meet CIS level 1 benchmarks automating and provisioning TSL certificates. Turbine dashboards are highly composable, making them a great tool for MSSPs to provide clients with CISO level visibility to help ensure that compliance controls are in order.

Outcome
The MSSP is able to offer its customers a simple, secure and scalable automation solution to help ensure continuous North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements. After the MSSP built the first hardened appliance they were able to replicate the solution for new customers in **15 minutes or less**.

SWIMLANE

MSSP Requirements for Security Automation

Technology Requirements

Active Data Sensing, Enrichment, De-duplication and Correlation

Scalability and performance are critical capabilities for MSSPs. Swimlane Turbine's Active Sensing Fabric uses webhooks and remote agents to ingest data from broad and hard to reach telemetry sources. It enriches, de-duplicates and correlates data at enterprise–scale This ensures that MSSPs can speed the MTTR for their customers by taking action the moment threats occur - not after the detection, aggregation and manual alert triage cycle.

Multi-Tenant and Multi-Brand Infrastructure

In order to speed client onboarding times and keep pace with their customers' ever-changing environments, MSSPs need cloud-native automation platforms. Turbine cloud's multi-tenant capabilities provide MSSPs with the flexibility needed to configure distinct tenants for development and production environments, segmentation for multiple brands, as well as greater control over their environment.

Dynamic Remote Agents

MSSPs can differentiate their service offerings by using remote agents to collect and take action on hard-to-reach telemetry for their customers. Remote agents are highly secure restless sensors that connect Turbine to internal systems without the need for MSSPs to configure complicated networks or multiple VPNs.

Generative Artificial Intelligence

MSSPs are increasingly using generative AI for language models. Turbine offers a pre-built ChatGPT connector in its in-app marketplace. This integration can be used to summarize alerts, query the internet or Swimlane documentation for help answering questions.

Ecosystem-Agnostic Integrations

Inevitably, every organization has a unique tech stack and therefore diverse integration requirements that their MSSP provider must accommodate. This includes a variety of IT service management (ITSM), email, Slack, MicrosoftTeams and other tools, beyond the conventional SOC tech stack. Turbine uses connectors to deliver real-time integration with any REST API. Pre-built connectors can be browsed through an in-app marketplace, and Swimlane builds new connectors on-demand at no cost to customers.

continued ⇒

MSSP Requirements for Security Automation

Technology Requirements

Community-Sourced Threat Intelligence & Enrichment

The ability to centralize threat intelligence for effective detection and response is a core tenant for any MSSP. Unlike XDR technologies that are built around vendor-specific threat intelligence platforms, Turbine integrates with any external threat intelligence repository (even home-grown repos). MSSPs can use Turbine's threat intelligence app to ingest, enrich and correlate IOC data across their entire customer base or multiple EDR sources. This improves investigation speed and accuracy because customers gain a community-sourced knowledge base of threat intelligence.

Highly Composable Reporting & Analytics

The ability to report on KPIs and results is critical to any MSSP's success. In order for MSSPs to prove the return on investment that they deliver to their customers, they need robust reporting and analytics capabilities. Turbine combines human, machine and controlled artificial intelligence to generate performance metrics, incident response times, automation efficiency and other KPIs.

Unlimited Users and Role-Based Access Controls

To get the most out of automation, MSSPs need the ability to collaborate with a wide variety of customers and stakeholders in a controlled environment. Swimlane offers MSSPs a value-based pricing model that allows unlimited users to contribute to automation. Role-based access control (RBAC) like custom user roles and elevated account admin privileges help ensure secure automation development. to internal systems without the need for MSSPs to configure complicated networks or multiple VPNs.

Security Automation Capabilities for MSSPs

- Best-in-class performance at Fortune 50 scale
- Alert correlation across instances and environments
- Environment-agnostic integrations
- Robust case management
- Personae-driven reporting
- Automated event and incident report generation
- Community sourced and enriched threat intelligence
- Human-readable KPI and SLA tracking
- Communication and collaboration resources
- Low-code visualization and orchestration studio

SWIMLANE

MSSP Requirements for Security Automation

Business Outcomes

The benefits of automation for MSSPs is easy to see, but don't take our word for it. Hear from Swimlane MSSP customers about how they have improved their business with low-code security automation from Swimlane.

NTT DATA

"Our customers have changing environments. They might change their SIEM system, or email system – for the analysts, it has to be exactly the same system. For us, Swimlane is the main interface that we're using…and that gives us a great advantage. Not just for us, when we serve our customers, but also for the engineers on our customers' side that have changing environments."

1898 & CO. PART OF BURNS & MCDONNELL

"Before automating this process, the energy company's security team was spending 1 hour manually looking up IOCs. Now, the query happens automatically and is complete in minutes saving roughly 45 minutes per investigation."

Softcat

"Swimlane's automation, intuitive dashboards, and reporting have helped Softcat reduce the cost of acquiring a new customer. They've been able to grow their business by 30% without increasing their headcount."

DIGITAL INVESTIGATIVE GROUP

"In the beginning, from our first initial call and set up, it was only a week and we were already processing through our data. Getting some of that information processing done first – this allowed us to take that time savings from phishing to build our SIEM solution. So, within the first couple of weeks, we had Swimlane up and processing our data, and adding the value of time savings to our business. It was fast."

LUMEN

"We have actually overachieved what I started off with as the KPI, and that's a great success in my opinion," commented Cheah. "Swimlane has become an essential core component of our SOC. It's part and parcel of our SOC operations today, and I would say that it's almost impossible to do without Swimlane."

ProCircular SECURITY. PRIVACY. TRUST.

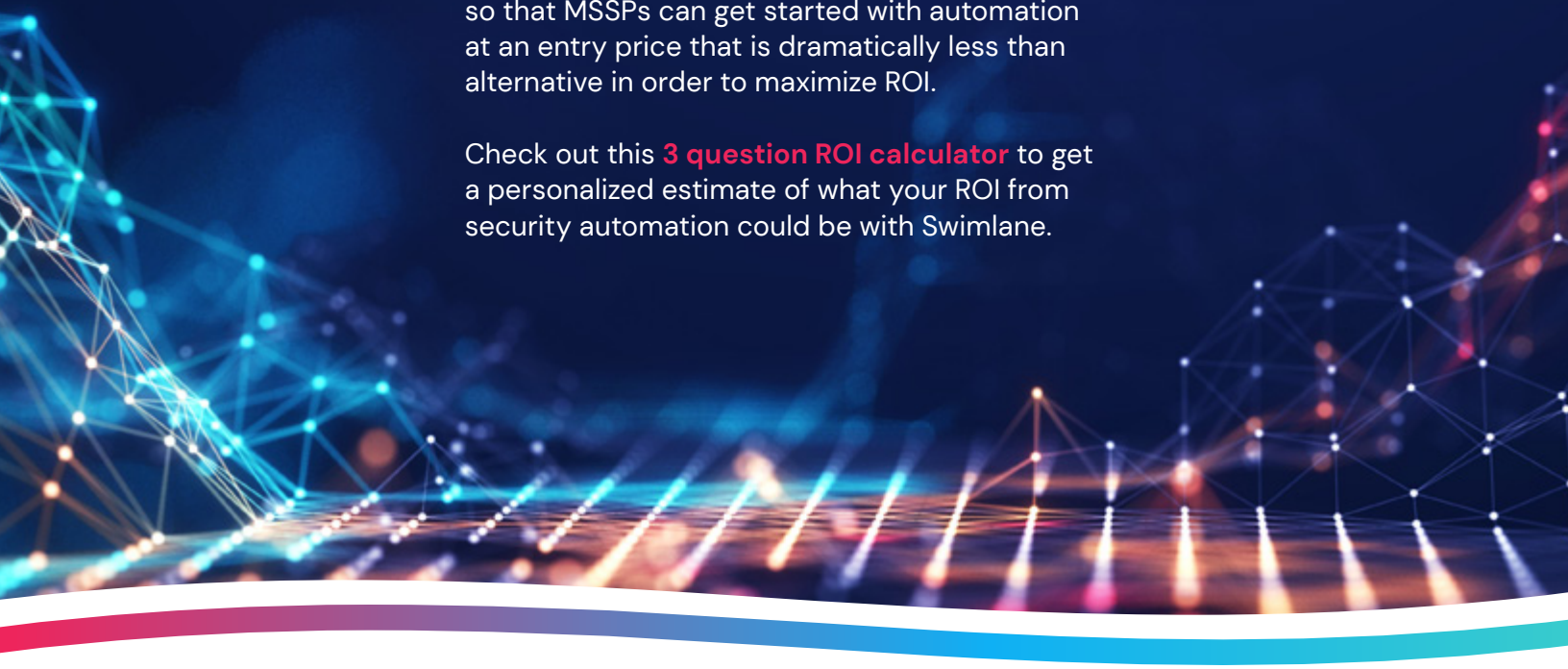
"In order to do this much work, we would've had to add an additional three or four analysts immediately to handle the amount that we're handling. With Swimlane we've been able to add more clients strategically without expanding our cost with additional staff or reducing the quality of our service delivery."

SWIMLANE

Calculate your own ROI today

MSSPs who leverage security automation are in a position to expand their customer base and increase profitability without adding headcount. Swimlane's pricing model offers unlimited users, use cases and connectors at a predictable price point. This value-based pricing model has variable pricing terms with quarterly payment options so that MSSPs can get started with automation at an entry price that is dramatically less than alternative in order to maximize ROI.

Check out this **3 question ROI calculator** to get a personalized estimate of what your ROI from security automation could be with Swimlane.



About Swimlane

Swimlane is the leader in low-code security automation. The Swimlane Turbine platform unifies security operations in-and-beyond the SOC into a single system of record that helps reduce process and data fatigue, while helping security leaders overcome chronic staffing shortages and more easily quantify business value and the efficacy of security operations.

Learn more at **swimlane.com**.

SWIMLANE