SWIMLANE

Security Orchestration, Automation and Response (SOAR) for MSSPs

Overview

Success and growth in the managed security service provider (MSSP) business requires balancing the delivery on multiple customer service level agreements (SLAs) with cost-effective operations. Costs are high. Competition is intense. Customers are demanding. But, advances in security orchestration, automation and response (SOAR) offer MSSPs a number of ways to meet SLAs, improve response times and deliver better security—all while lowering operating costs and improving margins.

SOAR makes it possible to handle more alerts with fewer people. Automated workflows are faster and more efficient than manual processes. The elimination of tedious manual tasks raises staff morale and lowers turnover. Centralization delivers immediate access to the context necessary for making critical decisions, and the seamless orchestration of various security tools makes it easier to adapt workflows to rapidly evolving threats. SOAR also codifies both formal and informal processes so that important tribal knowledge doesn't get lost when key employees leave.

Table of Contents

Introduction

Organizations are handling security entirely in-house less and less frequently. In fact, it's estimated more than half of organizations outsource at least some of their security tasks to managed security service providers (MSSPs). MSSP revenues in North America are projected to reach $35 billion by 2026.

Brisk sector growth is good news for MSSPs even though it suggests an increasingly competitive atmosphere. To compete, earn profits and grow, MSSPs must operate cost-effectively while adhering to strict service level agreements (SLAs) with multiple customers. Successfully managing an MSSP is a far more people-centric task than many would imagine. Although heavily dependent on technology, the real competitive advantage of an MSSP rests with its people.

Advances in security orchestration, automation and response (SOAR) offer MSSPs a number of ways to meet their SLAs and deliver better security while conserving human resources and subsequently lowering operating costs and improving margins.

By automating various manual security workflows, SOAR solutions make it possible to **handle more alerts and adapt workflows to defend against evolving threats**—delivering better security to more customers with fewer staff resources. SOAR platforms speed up incident response management while reducing the repetitive, manual tasks that can wear out security staff. What's more, by embedding even minute processes and specific client nuances into the software, MSSPs mitigate the risk that important tribal knowledge in the security team will get lost if people leave.

An overview of MSSP business challenges

The core MSSP services are only the starting point for competitiveness. Monitoring and management of security devices and systems are table stakes. The real challenge is keeping up with an ever evolving threat landscape that forces MSSPs to continually update their internal processes. This includes adapting to a proliferating set of specialized security products and a combination of personnel shortages that make 24/7 operations a constant challenge. When employees leave, they take vital procedural knowledge with them.

What it takes to succeed as an MSSP

Succeeding as an MSSP means getting many details right in a complex services-oriented business. It means anticipating and then following through on all the various details of the service agreement. In many cases, the SLA and/or less formal agreements call for client-specific actions and response time–which **often differ significantly from the MSSP's default operating procedures.** This is a potential minefield for staff handling dozens of different client accounts and one of the areas that MSSPs often struggle with as this knowledge is typically unevenly distributed across the MSSP's own staff.

Handling an organization's security is a big responsibility. For example, suppose the SIEM detects suspicious account activity at a client data center. An MSSP has to determine:

- What does it mean?
- Is it a meaningless robotic probe on the client's network or the start of a multi-billion dollar data breach?
- Who needs to be notified?
- Does the incident merit calling the client in the middle of the night?
- Who's the client on-call anyway?
- Does the client prefer email, text or voice?

Client preferences for responses may not match what's in the official SLA. **The MSSP has to think fast and try not to be wrong.**

Every MSSP knows that basic SLA compliance is not enough. The responsibility of an MSSP is to deliver airtight security, and when it comes to preventing a breach, every minute counts in responding to an alert. Technically meeting an SLA but still allowing a breach gets the MSSP nowhere. If the client is breached, the MSSP's ostensible adherence to an SLA might keep them from being sued, but they'll still lose the business.

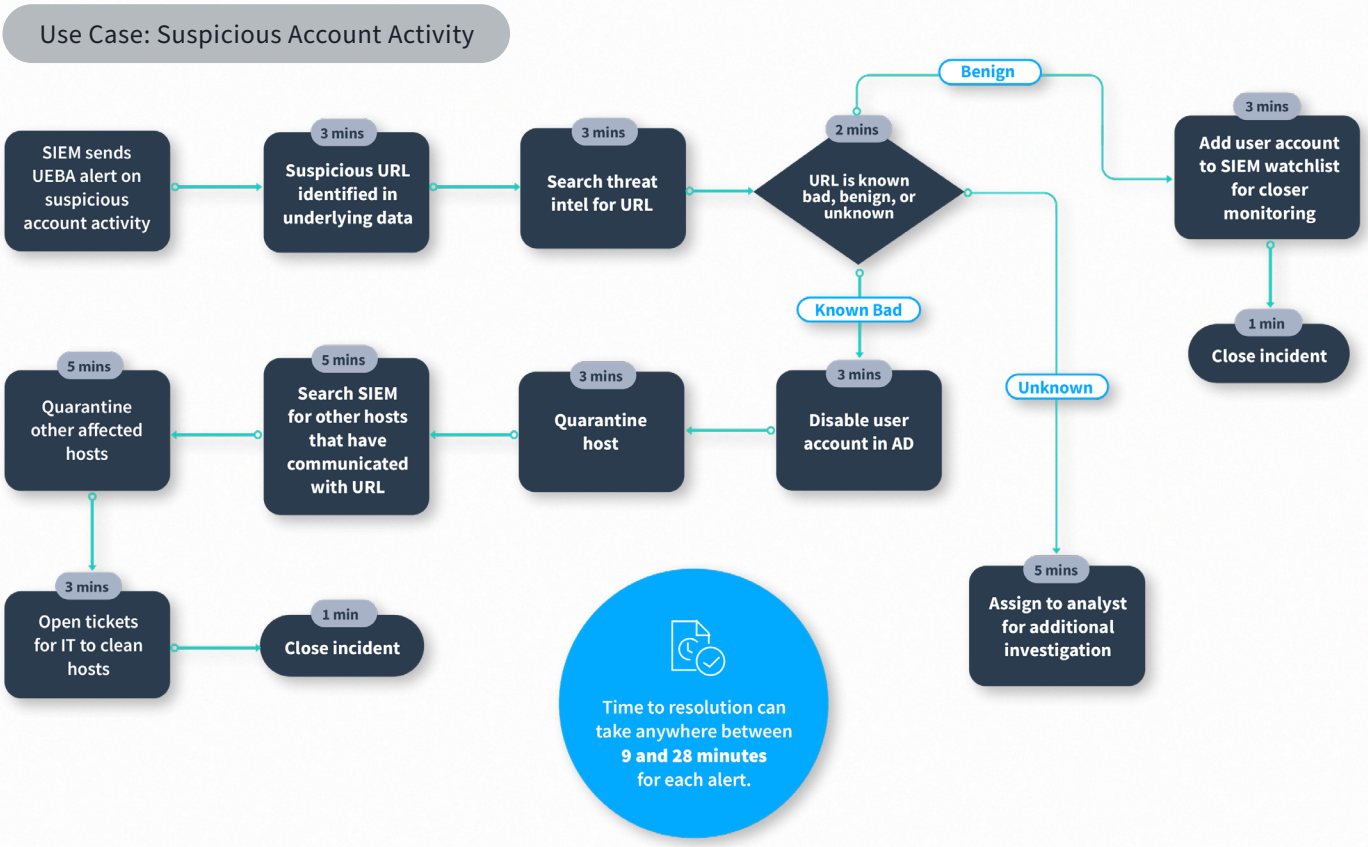
The MSSP-client relationship is based on trust and accountability, factors that cannot be easily captured in a paper agreement. Earning the client's trust by **being accountable, transparent and able to accurately and quickly act on an incident is central to the MSSP's value proposition.**

Balancing productivity with risk

Maintaining a strong track record of trust, accountability and SLA performance is needed for MSSPs to build the customer base necessary for profitable operations. But keeping staff engaged and productive presents one of the largest challenges to meeting this goal. In simple terms, staff productivity involves enabling team members to handle client tasks in a time-frame that makes financial sense. If, for example, an MSSP staff member's fully allocated salary is $50 per hour, he or she must be able to handle significantly more than $50 worth of client work every hour for the MSSP to be profitable.

Imagine that an MSSP client pays $1,000 per month for IDS monitoring and incident reporting services. Let's say there are 100 incidents a month. That's $10 of revenue per incident. If the incident reporting process takes 5 minutes for the MSSP staffer, it will cost the MSSP $4.16, a level of productivity that contributes $5.84 in gross profit to the MSSP's earnings for each incident handled.

So far, so good, but productivity can easily go in the wrong direction. If the time required to process an incident jumps to 12 minutes, the MSSP is now working at break-even. At 15 minutes, the MSSP is losing $2.50 per incident. Then, if the number of incidents swells, the revenue per incident drops. What if the client had 150 incidents per month instead of 100? That would translate into $6.67 in revenue per incident. If the MSSP's workflow takes 15 minutes, the MSSP is now losing $5.83 per incident. It will cost the MSSP $1,875 to handle the client's business for the month, causing a loss of $875.



All this basic math is being played out within the context of several major challenges to staffing an MSSP:

Overwhelmed staff

Staff can get overwhelmed by a spike in incidents. This will affect both productivity and risk. Not only can the MSSP lose money, but it may also inadvertently give too little attention to a serious incident. **A breach due to a missed security alert is a disaster.**

This basic productivity formula gets further stretched by a couple of other realities of the MSSP business. Workstreams tend to be variable. The cookie-cutter example described above was just for illustrative purposes. In practice, specifics in each incident will make the process for any given incident significantly longer or shorter than the average.

MSSPs face a constant challenge balancing productivity, risk and customer service.

Round-the-clock operations

Cyberattacks occur 24/7, so MSSPs must also work around-the-clock. An incident at 2 AM on Sunday needs the same response as one at noon on Tuesday. The MSSP staffers handling it will be different, of course. There can be variations in staff productivity and knowledge on different shifts. **Productivity can thus swing up and down depending on the time of day or day of week.** This is problematic as the bad guys rarely work the same hours as a typical SOC that's not staffed for 24x7 operations.

Informal knowledge loss

In-depth understanding of individual customer requirements fuels MSSP staff effectiveness. For the person responsible for monitoring security systems and executing incident responses, knowing how to handle alerts and incidents can make the difference between profit and loss for the MSSP. If the staffer is unfamiliar with a client's environment and associated incident response workflow, for instance, the process can slow down. Or, worse, if the staffer doesn't have the skill to assess the seriousness of an alert, there might be a lost opportunity to catch an incident early enough to remediate the problem before a breach occurs.

Retaining both formal and informal repositories of knowledge is essential to maintaining productivity and being able to grow profitably. This means retaining people. As with other high-touch, knowledge-specialized industries, the MSSP sector deals with personnel who carry corporate knowledge in their heads and in informal group processes. It can be a veritable tribal situation, where a seasoned team with long-term collaborative relationships can achieve a high level of productivity—but that also exposes the MSSP to **the risk that the knowledge could walk out the door with staff turnover.**

Understanding SOAR

SOAR offers a solution to productivity challenges and other risks to profitability and competitiveness faced by MSSPs. It's a technology category that is adaptive and varied, so it resists simple definitions. In general, though, it refers to processes and tools working in concert to automate otherwise disparate security tasks that can be tedious and time-consuming.

Most solutions share several common characteristics, including the following:

Centralized security operations

Figure 1 – Example of the Swimlane SOAR dashboard.

A SOAR solution provides a **centralized view into multiple security management platforms.** Staffers can use it to handle tasks that require the use of secondary systems. Through a single console, for example, an MSSP staffer can easily monitor and interpret the consolidated outputs of their SIEM, IDS and multiple firewalls. Figure 1 shows an example of this kind of security automation dashboard.

Automated security operations

An MSSP can use a SOAR platform to model and automate its alert response playbooks and workflows. For instance, if the MSSP's incident response process calls for a suspicious binary to be manually uploaded into VirusTotal for evaluation, the SOAR platform can be set to programmatically submit the binary to VirusTotal for analysis, perform data collection, open a ticket in JIRA, send a notification email to the client and alert relevant MSSP team members.

Examples of time-intensive MSSP staff tasks that can be automated and orchestrated include:

- Responding to event data from SIEMs, IDSs, EDRs, UEBA, Advanced Threat Detection tools, sandbox technologies, etc.
- Investigating the incident through log gathering and analysis.
- Reviewing and analyzing threat intelligence sources.
- Updating tickets, creating reports and email alerts. The solution may even be able to log into multiple systems and enter the incident details.
- Understanding context and taking corrective actions (i.e,, implementing security controls, updating a black list, updating an IDS rule, disabling user accounts and so forth).

The potential of SOAR for MSSPs

Given its potential to speed up alert management and incident response, SOAR platforms can help MSSPs in a variety of ways. Deploying SOAR can:

- Increase productivity
- Lower staff turnover
- Enable the use of lower cost resources
- Help provide consistent customer service
- Improve threat intelligence
- Speed up and improve reporting
- Capture and preserve organizational knowledge

Ultimately, security automation and orchestration can **help MSSPs be more competitive.**

Day-to-day benefits

The automation of repetitive, time-consuming tasks improves productivity while reducing incident response times. The solution speeds up the on-boarding process for new clients and staff members as well. It accomplishes this partly through the delivery of prebuilt, automated workflows. Using these as an operational framework, the MSSP team can customize and refine workflows and remedial processes.

SOAR allows for expertise to be scaled exponentially across the security management process rather than be constrained by an individual team member's capacity.

MSSPs also gain productivity from having their operations simplified via the single pane of glass through which a SOAR solution presents a broad range of security operations and procedures. The MSSP can use the SOAR interface to centralize security management. Or, if the MSSP has an existing portal, it can aggregate SOAR information and integrate it into their preferred management interface. With a single console for managing multiple customer SLAs, there is reduced cost in task and customer switching. **Staffers spend less time having to look up what they should do for a particular customer—it's built into the system.** The staffer just follows the process outlined for that customer.

Finally, automated workflows and playbooks can greatly speed up remediation of security problems in three separate ways:

1. The portions of processes that can be automated are obviously faster than their manual counterparts. Typical task automation rates are 80-90%.
2. Centralizing threat data contributes to faster incident response and resolution.
3. The 10x speed increase of the above allows for every alert to be responded to in a more timely manner with less backlog occurring during a spike in incidents.

By radically reducing mean time to resolution (MTTR), SOAR enhances the level of security and service that MSSPs provide their customers.

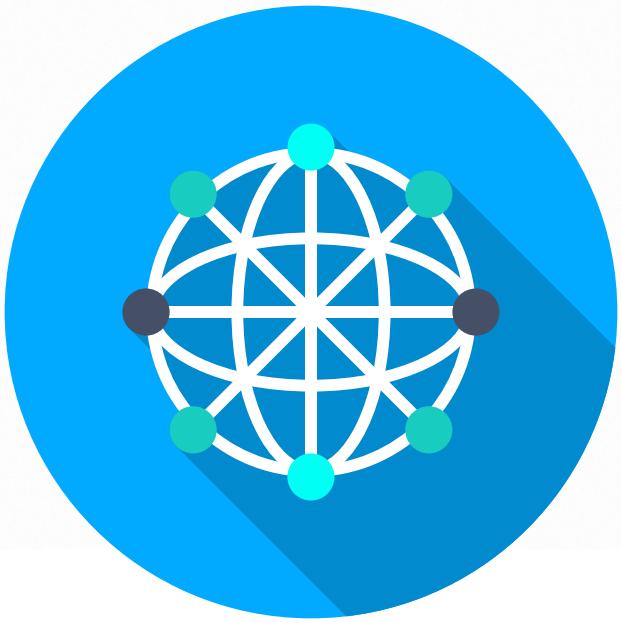
More context

Automating security processes across multiple security systems can lead to better threat intelligence. For instance, a staffer might need to assess the seriousness of a threat by manually comparing SIEM and IDS logs. That can be a time-consuming and error-prone process. Automating that process makes the assessment instantaneous and machine-accurate. Among other benefits, it also **makes it much more likely that these kinds of tedious but valuable tasks will actually be done.**

For instance, SOAR solutions create extensive databases of historical threats and responses across every security tool. That allows threat assessments to be informed by automated rules-based analysis of previous comparable threats. Alternatively or additionally, the system can automatically centralize all of this information for quicker human-based assessment.

Resource optimization and knowledge preservation

Client difficulty in recruiting and retaining skilled security professionals is one driver of MSSP growth. Organizations have trouble staffing their security teams so they outsource the process to companies that have the personnel. But MSSPs also often struggle with hiring and retaining good people. After all, they are in the same labor market as their clients.



It may become quite challenging to arrange for 24/7 staffing of experts in every tool. Using SOAR solutions enable the MSSP to hire security generalists and rely less on people who are primarily expert users of specialized security tools.

Those highly trained staff are hard to keep around. Staff often get poached by other companies or get bored and leave. Repetitive, manual security administrative tasks can lead to burnout, especially among highly skilled employees. With SOAR, team members focus on what matters and get less distracted (and bored/burned out) by routine, repetitive work like cutting and pasting information from one tool into another for analysis, sending email updates and changing alert priorities.

SOAR can have a critical impact on reducing staff turnover.

Security automation solutions also learn to **mimic the procedures and practices of the best members of the MSSP team.** Incident response processes get deliberately and explicitly defined by human users in great detail so the MSSP can automate responses. As a result, the processes for each client are embedded (but still able to be modified) in the solution itself. By remembering how things get done, the tools can mitigate the knowledge loss when people inevitably leave.

Better reporting

SOAR solutions like Swimlane centralize incident data for fast, efficient reporting. The MSSP can use the solution to track key performance indicators, such as:

- Incident response time
- Open tickets
- Resolved incidents
- Resolution categorization

This makes for easy internal and external reporting on SLA adherence and staff performance.

For clients who require maintenance of logs for audit purposes, SOAR reporting offers a cost-effective way to meet this requirement. The MSSP can also generate internal reports that analyze productivity and profitability.

SOAR offers deep analysis and reporting of the security condition of each client. Such insights are useful for the client's risk management program, planning for future security needs and budgets, as well as updating security policies.

Adding revenue streams without adding operating costs

SOAR platforms provide the ability for an MSSP to provide additional services to its customers without adding costs. Expanding the portfolio of service offerings is one way MSSPs can differentiate themselves and increase profits. Offering more than the competition helps attract clients. Upselling existing clients on new services adds to the bottom line without incurring incremental marketing expense or overhead.

Consider the following example:

> An MSSP uses its SOAR solution to easily create a service that automatically updates a customer's web proxy to block newly registered domains for 48 hours. Newly observed domains are a typical tool in phishing or other types of browser-based attacks. Malicious actors like to use a brand new domain that has yet to make it on to a blacklist. The new domain blocker is a good countermeasure to this threat. With SOAR, the cost of creating the service is negligible.

Having the process built into a SOAR platform makes it easier to train staff on new procedures and services.

Swimlane's MSSP-friendly approach to SOAR

Swimlane has an **API-first approach to its SOAR architecture.** It is built using standards-based software and open application programming interfaces (APIs) to enable broad, easy integration with other systems. With a REST-based (RESTful) API and the JSON language (as well as other common open standards like SOAP, XML, SMTP, ODBC, etc.), it is possible to integrate security tools with Swimlane without the need for proprietary connectors or custom software development. You can even fork Swimlane's integration code for rapid customization.

In contrast, custom connectors and coding adds time, expense and rigidity to the solution. RESTful APIs enable MSSPs to simply and quickly connect SIEM, IDS, EDR, threat intelligence and other security tools with Swimlane. You can also **easily connect the Swimlane solution to your proprietary customer-facing portal.**

Swimlane also features a **multitenant architecture**, which is necessary to ensure separation of customer data. Each customer has their own workspace that includes workflows, dashboards, reports and so forth. The multitenant approach is economical. It enables resource allocation and service delivery tracking such as timecards. More importantly, this clear separation of data **ensures one client will never have their data accidentally exposed to another client.**

Scalability is achieved by Swimlane through a MongoDB back-end that uses sharding to allow for infinite horizontal scalability. Individual instances are vertically scalable on a massive level.

Finally, Swimlane offers an **intuitive user experience**. This is essential for delivering the kind of productivity gains MSSPs expect from SOAR. Swimlane's simplified administrative interface speeds time-to-value for the security automation and orchestration solution.

Additional competitive advantages

SOAR tools such as Swimlane provide feature sets that generate further competitive advantages for MSSPs. For example, Swimlane's framework approach helps an MSSP meet a greater number of use cases than it could without this kind of solution. It allows MSSPs to adapt quickly to new customers, technologies (internal and external), emerging threats and so forth. A flexible approach to licensing accommodates individual MSSP monetization structures.

Swimlane is also architected to **massively scale both vertically and horizontally**, fitting the requirements of any sized organization. It also offers flexible deployment options and can be installed on any customer premise equipment or in the cloud. High availability ensures business continuity.

Conclusion

As MSSPs seek competitive strength and better profitability through staff productivity, they should consider implementing a security orchestration, automation and response platform.

Solutions like Swimlane speed up incident response for higher productivity and consistent adherence to customer SLAs. At the same time, the decrease in time spent on tedious tasks lowers turnover and increases morale. The tools even let MSSPs have more flexibility in staffing by making it possible to hire security generalists rather than multi-system experts. What's more, the ability to store preset routines with automated administrative task handling helps retain tribal knowledge when staff leave.

MSSPs can also leverage the toolset to deliver better reporting and threat intelligence while adding new services and revenue streams at very little incremental cost.

In short, SOAR offers MSSPs an **intriguing path to profitability, competitive advantage and growth.**

Maybe you should check it out.

About Swimlane

Swimlane is at the forefront of the growing market of security orchestration, automation and response (SOAR) solutions and was founded to deliver scalable and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages. Swimlane's solution helps organizations address all security operations (SecOps) needs, including prioritizing alerts, orchestrating tools and automating the remediation of threats—improving performance across the entire organization. Swimlane is headquartered in Denver, Colo. with operations throughout North America, Central America, Europe, the Middle East and Australia.

To arrange for a demo of Swimlane or to speak with one of our security experts to see if SOAR would be helpful to your organization, please contact us at 1.844.SWIMLANE or info@swimlane.com.