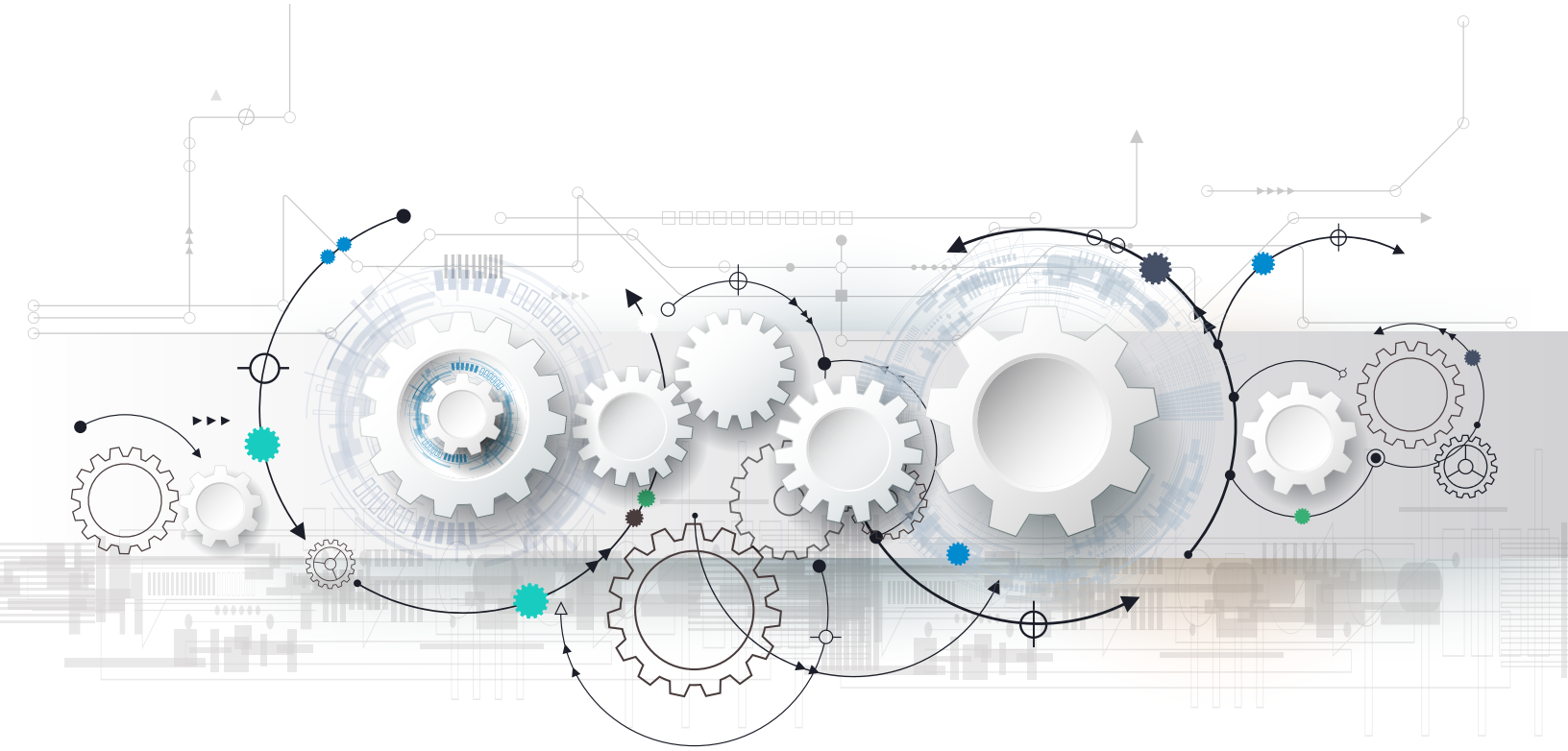
SWIMLANE



Security Orchestration, Automation and Response (SOAR) Capabilities

Abstract

Security orchestration, automation and response (SOAR) solutions help security teams manage a growing volume of alerts and incidents more efficiently by automating manual response workflows. Specific platform preferences may vary for each organization, but there are certain critical capabilities that a SOAR platform should embody. This e-book reviews what it takes for SOAR success and highlights how Swimlane's SOAR plaform meets and exceeds the criteria for effective SOAR. SOAR needs to offer a comprehensive function set in a single platform. An enterprise-ready architecture should be based on APIs, with simple integration, extensibility and scalability. The user experience is paramount. Both end users and administrators are best served by SOAR that enables maximum productivity.

SWIMLANE

Table of Contents

Introduction

Cybersecurity is a high-wire act, with significant challenges tied to both technology and operations. Protecting digital assets requires the right tools and processes for the security team to handle the workload efficiently. This is becoming a greater challenge as the volume and seriousness of threats continue to grow.

Security teams are frequently overwhelmed by the manual review of security alerts and coordination of multiple security systems. Sifting through the high volume of false positives is a resource drain, but as previous breaches have demonstrated, the potential impact of missing a real attack makes it a necessity. So, how can a security team offer the most robust protection and efficiently react to serious threats, despite being inundated by false alarms? This is the realm of security orchestration, automation and response (SOAR).

SOAR overview

SOAR employs a combination of technical capabilities and built-in processes to automate previously manual and time-consuming security management tasks. A SOAR platform delivers centralized security operations by orchestrating incident response tasks through two-way integration with a broad range of third-party security tools. For instance, using a SOAR solution, a security manager can view a single console to monitor, interpret and respond to data generated by a broad range of platforms including SIEMs, IDS/IPSs, FWs, EDRs, UEBAs, malware and sandbox analysis, and others.

SOAR solutions enable the security team to automate its existing alert responses by modeling and orchestrating the workflow steps across multiple tools. For example, an incident response process might call for a suspicious binary to be manually uploaded into a malware analysis system for evaluation. The SOAR platform will automate the submission step on its own and centralize the results to initiate additional actions, like opening a trouble ticket and/or quarantining an infected endpoint without requiring human intervention.

Benefits of SOAR

SOAR speeds up alert response workflows by automating and orchestrating time-consuming and repetitive tasks, such as updating tickets, creating reports, logging into multiple systems, entering incident information and sending email alerts. SOAR also includes workflows, like incident investigation involving log gathering and analysis, and can review and analyze threat intelligence sources. By automating these tasks, SOAR solutions allow analysts to focus their full attention on more advanced security threats.

In addition to automation, SOAR provides context and takes corrective actions based on rules, meaning busy analysts don't have to micromanage their systems. A SOAR solution can implement security controls like updating SIEM watch lists, disabling user accounts and so forth. Because of these capabilities, SOAR helps reduce tedious busy work and frees up security professionals to solve problems that require real expertise.

Swimlane SOAR plaform overview

Swimlane's security orchestration, automation and response solution centralizes security operations (SecOps) activities. It manages and automates the response to security alerts and incidents identified by existing monitoring and detection systems. Swimlane standardizes response and notification processes to mitigate risk, speed resolution and streamline communications through a purpose-built SecOps management dashboard. A single interface enables the consolidation and visualization of threat intelligence and provides access to cases, reports, dashboards and metrics for individuals and teams.

Requirements of a SOAR solution

A truly effective SOAR plaform must incorporate the following critical priorities:

- A comprehensive function set in a single platform.
- An API-first architecture and support simple integration.
- Architecture built for extensibility and scalability, including HA/DR.
- A user experience that ensures both end users and administrators are set up for maximum productivity.

Comprehensive Functionality in One Platform

An effective SOAR solution offers a comprehensive set of functionality in one platform. These include:

- **Automation** – The ability to execute a sequence of tasks related to a security workflow without a human user (i.e. automatically opening a ticket upon the receipt of a security alert, followed by sending out automated ticket status emails or tasks to relevant stakeholders). Automation can be more advanced, executing preset workflows according to extensive "playbooks" based on security team rules and procedures.

- **Orchestration** – The invoking of functionality from multiple, independent security systems to execute a security workflow (i.e. the SOAR solution receives an alert from a SIEM solution, which it then forwards to a malware analysis tool for assessment).

- **Case management** – A centralized capability for managing all aspects of a security incident or alert. This includes a user interface with a complete view of all aspects of the case. The analyst accesses a single screen that enables dynamic interaction with all data and critical components related to the incident—as opposed to toggling between screens to handle a case. From this interface, the analyst can execute an array of incident response actions specific to the case (i.e. seeing the details of a phishing email header that is forwarded to the analyst without requiring the analyst to open the email in a second program). Dynamic case management speeds up investigations, enforces process compliance, and makes it easy to close more security alerts.

- **Reporting and analytics** – A built-in, or integrated, third-party tool that enables the security team to report on incidents or cases in progress, alert levels, threat intelligence and so forth. The capability should go beyond basic reporting to include robust analytics.

API-Centric, Scalable Architecture

Delivering a comprehensive set of SOAR functionality in a single platform requires easy integration across many separate systems using standards-based APIs such as REST. Standards-based APIs make it simple to link applications so they can easily exchange data and procedure calls. Swimlane is compatible with multiple standards-based APIs, and in most cases a RESTful API is the best choice. For example, with an API and corresponding standards-based web service, the SOAR solution can be configured to insert security alert ticket data into Jira without the need for proprietary application integration tools or custom coding. The integration is both quick to implement and simple to modify.

Vertical and horizontal scalability are also necessary. As organizations grow and evolve, SOAR has to keep up. Threat loads can spike, as might happen with a government agency during an election season. The security team's SOAR tools need to be capable of handling such surges in volume.

Every organization is different; therefore, SOAR platforms must be flexible enough to meet whatever deployment requirements an organization may have. It's critical that options exist to meet both current and future needs, which is why Swimlane is flexible enough to be deployed on an organization's own hardware, a virtual machine or the cloud. A smaller organization might want a simple cloud deployment, while an entity with strict compliance guidelines related to data retention may require a SOAR platform to be on its own hardware and deployed in the country where the organization's data originates. As organizations grow or decline and security policies change, Swimlane can be redeployed onto another platform to meet an organization's needs. Swimlane will adapt to each organization's requirements, rather than requiring customers to change their processes to fit platform restrictions.

Attackers operate around the clock, and given its criticality for security, SOAR solutions should as well. For organizations that need 24/7 automation and orchestration, Swimlane offers high availability with automated failover for uninterrupted security. This service also provides a full disaster recovery capability.

A Focus on Usability

One of SOAR's main value propositions is making security teams more productive. This means that usability is a major factor in the success of a SOAR solution. The best SOAR platforms are easy to deploy and manage, with a simple, intuitive user experience for administrators and users alike. Ideally, the user interface (UI) and user experience (UX) is flexible to suit the work styles of a range of users, including power users, security analysts and executives. Since each user type has different requirements, an adaptable UI/UX will make the solution as beneficial as possible to each kind of user.

The Difference Between SOAR and SIEM

SOAR platforms and SIEM solutions perform critical functions for enabling security operations. And while they are complementary technologies, they aren't interchangeable.

Knowing the difference between SIEM and SOAR helps organizations properly assess their organizational requirements and understand which solutions will deliver what capabilities. SIEM solutions detect suspicious behavior by analyzing high volume log and event data from multiple sources. SOAR solutions interoperate with the entire range of security platforms, including SIEM, while orchestrating the incident response process. While SIEM is a critical component of a strong security program, SOAR makes it more effective by cutting down on the volume of alarms and automating time-consuming, repetitive tasks.

SIEM

- SIEM systems typically generate hundreds or even thousands of alerts per day. They do this by ingesting and analyzing a large volume of raw log and event data from across the IT infrastructure. SIEM requires heavy configuration and tuning to reduce false positives.
- Because there are so many alerts, SIEM users are usually only able to investigate a small percentage per day. Users are dependent on risk-based scoring to triage alarm response.
- SIEM usually has limited orchestration and automation capabilities when compared to dedicated SOAR.
- SIEM is primarily a one-way technology, harvesting inbound communications from other security products. Case management in SIEM is primarily a one-way collection of event evidence with limited options for dynamic interaction.
- SIEM workflows are often limited to one or more actions in response to a single alarm.

SOAR

- SOAR solutions gather alarm data from integrated platforms. They place them in one location for additional investigation.
- SOAR case management is dynamic, in contrast to SIEM's. The SOAR approach allows users to research, assess and perform additional relevant investigations from within a single case.
- SOAR is a two-way technology, delivering faster results and facilitating an adaptive defense. Swimlane establishes integration as a means to accommodate highly automated, complex incident response workflows.
- SOAR solutions include multiple playbooks in response to specific threats. Each step in a playbook can be fully automated or set up for one-click execution from directly within Swimlane, including interaction with third-party products.

Orchestration

The purpose of orchestration in SOAR is to provide interoperability and coordination of activities, such as those needed for incident response. Incident response involves SOAR working with third-party platforms. In the incident response context, three main processes dominate orchestration with systems that handle specific tasks such as threat intelligence, case ticketing, email, security analytics, network forensics and endpoint detection and response.

1. **Collecting and centralizing relevant event data.** To manage the incident response workflow and sustain a productive overview of the case, users must have centralized event data at their disposal. SOAR solutions use orchestration capabilities to ensure that any information needed to handle the incident is available to the workflows.

2. **Presenting consolidated incident response context.** Context is important for efficient and effective incident response. If a suspected bit of malware is, in fact, well known and relatively benign, then SOAR solutions can help avoid excessive use of time and resources by immediately revealing that insight to security managers. On the other hand, if a threat is actually part of a broader pattern that is affecting cybersecurity worldwide, such as new rapidly spreading ransomware, then it's imperative that the SOAR solution have orchestration with threat intelligence services that can identify the problem and facilitate a prompt course of action.

3. **Initiating actions on third-party systems.** Orchestration enables the SOAR solution to invoke procedure calls on other systems. For incident reponse, this may involve initiating threat detection and prevention. The solution might also request that a third-party system, like an IPS, conduct monitoring of threats. SOAR workflows may then initiate the remediation of problems, such as quarantining infected devices, disabling compromised user accounts, adding malicious URLs to proxy blacklists, etc.

Swimlane's SOAR solution uses security orchestration to replace slow, manual threat response workflows with machine-speed decision making and remediation. This is made possible by an API-first approach to integration. API-first is a development strategy that emphasizes API creation and awareness of developer interests as the first priority. The application itself is then built on the API-first foundation.

Proper implementation of an API-first approach leads to pervasive, seamless integration for security automation and orchestration. The use of the RESTful APIs and standard network protocols facilitates simple integration with multiple device types—PCs, mobile devices, back-end systems, database servers, and beyond. Then, leveraging the API-first approach, Swimlane has out-of-the box integrations with the majority of enterprise security tools, such as IBM QRadar, Splunk, FireEye, Palo Alto, Carbon Black, RSA Netwitness, JIRA, McAfee ESM, and many others. Combining RESTful APIs with out-of-the box integration connects Swimlane across a full industry spectrum of solutions.

Swimlane's API also enables relatively streamlined creation of new integrations with solutions for which there is no out-of-the box connection. The API is designed for bi-directional communications with third-party and proprietary systems. It can send and receive data and procedure calls.

Swimlane orchestrations provide complete event context for users. Coupling full integration with workflow automation, case management, and a simple UI/UX, the Swimlane orchestration capabilities accelerate time to value for SOAR.

Automation

There is more to automation than simply laying out an ABC set of steps and instructing the solution to execute them. A SOAR solution ought to drive playbook execution of security response workflows to reduce time and overhead. In that sense, the automation capabilities need to be smart. They need to be able to adapt to how the best team members handle security challenges and then mimic the response through an automated sequence of tasks. For medium- and large-sized security organizations, it's especially critical that they are not forced to rely on generic "templates" but are able to build highly customized playbooks that document and replicate their exact workflows to fit their existing people, processes, and technologies.

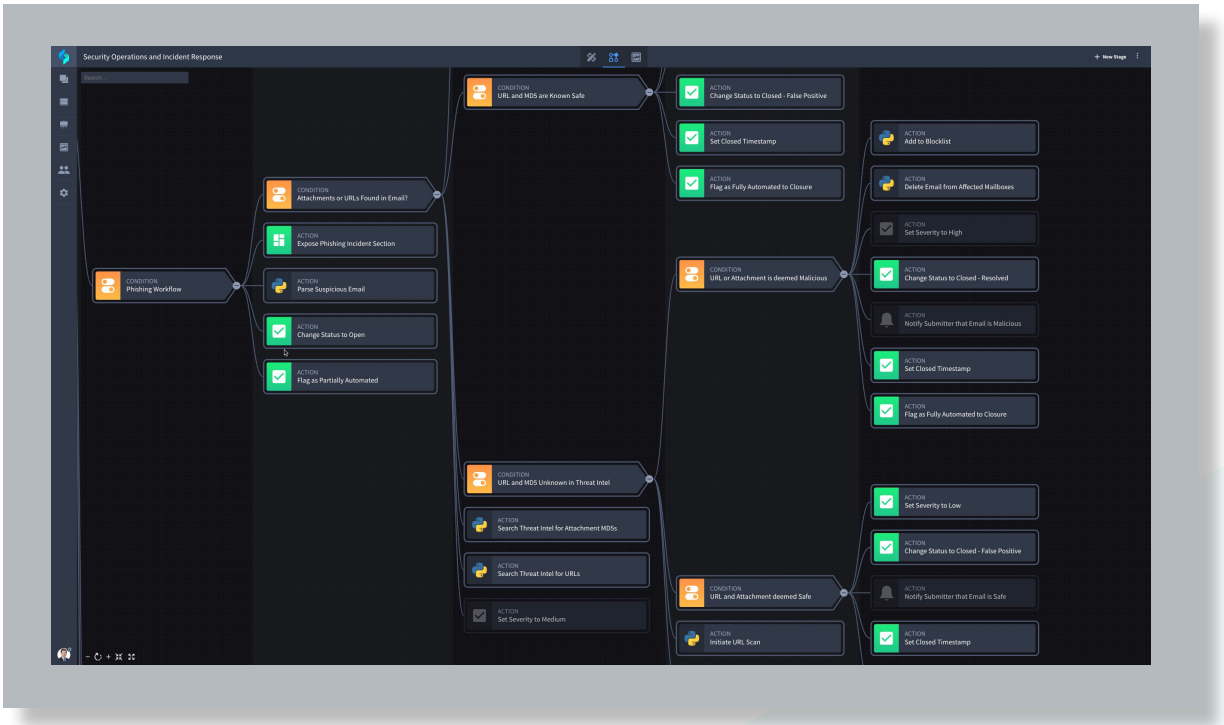
A SOAR solution's automation capabilities can (and should) go beyond preventive measures. Security benefits from automated triggering of additional investigative measures. Similarly, some SOAR solutions can update monitoring platforms on an automated basis.

Swimlane's automation is designed to capture security best practices from its user team. The resulting standardization enables the team to learn and resolve security tasks quickly.

Automation allows Swimlane to scale and execute pre-approved processes without human intervention. The security operations team can leverage automation to triage alarms more efficiently and respond to critical events faster. Automation allows SOAR to integrate existing security solutions into a more efficient and comprehensive security program.

Swimlane's automation leverages vendor APIs and software-defined security (SDSec) methods. With SDSec, Swimlane can rapidly respond to and prevent attacks earlier in the kill chain. For example, consider how an IT organization builds cloud-native applications. After code gets checked into the repository, tests are automatically run in a lab environment within minutes.

Using APIs, Swimlane allows for one-click automation. The user can enact an automation routine without going into any third-party systems, enabling the playbooks and workflows needed for the team's unique incident response processes. Each threat gets a quick but consistent response, and each automation routine can be performed independently at each stage in the playbook. Manual steps, if required, can also be prompted by Swimlane.



Case Management

Case management is where the potential of a SOAR solution comes to life for a security team. Effective case management requires centralizing, tracking, managing, and reporting on security alerts. This is an area where Swimlane is distinctive. Cases in Swimlane can be managed based on defined, repeatable processes to deliver consistent management.

Swimlane is able to capture relevant, real-time, and enriched incident data to drive case management. Effective case management speeds up investigations and enforces process compliance. It gets easier to close more security alerts. The user can perform extensive case management without leaving Swimlane even if the process involves the use of third-party systems. Swimlane case management is fully interactive and tightly integrated with workflow. This ties the entire incident response process with ongoing case management, resulting in a dynamic defense that can adapt to address an infinite number of relevant use cases.

Architecture

Swimlane's API-first architecture was built from the ground up to integrate with an extensive array of IT security and operations platforms. It can scale horizontally, adding capacity where needed across extended enterprises. It can also scale vertically, allowing for intense concentration of processing power in designated areas.

Swimlane features a multi-tenant architecture. This design offers flexible configuration options for enterprises and providers. Highly configurable role-based access control (RBAC) can restrict access down to the field level, ensuring that multi-tenant architectural requirements are met. In this way, access to Swimlane can be carefully governed in adherence to an organization's compliance and security policies.

Swimlane's integration framework is designed to be powerful but easy to use. The API-first approach makes it simple for third-party tools to share data and procedure calls with Swimlane. It also streamlines data ingestion by Swimlane from outside systems.

Swimlane uses a Python-based builder and was designed to make easy customizations using Python and/or Powershell. And to further simplify the process, customers can also fork Swimlane code directly inside of the platform.

Developers can use a familiar language and format to create integrations with Swimlane. For example, whether an organization uses an Eclipse-based Java integrated development environment (IDE) or is a "Microsoft shop," it can still easily write code to speak to the Swimlane API. In the Microsoft case, Swimlane supports Windows PowerShell.

Usability

A simple, powerful UI is one that can be easily customized for different types of SOAR users. Flexible data presentation lets each user create a work environment for his or her particular needs. A security analyst, for example, can customize the UI to expedite automating repetitive tasks like data gathering, reporting and responding to false positives. That way, an analyst can spend more time on higher-priority and skill-intensive tasks. Alternatively, a security manager can create a custom dashboard to help measure, compare and improve the performance metrics of a security team. And a CISO can leverage a SOAR dashboard that demonstrates which key security metrics are being attained and where there are organizational gaps.

Usability is a big part of SOAR's administrative story. The return on investment comes partly from administrative productivity. If administration is excessively time consuming and difficult, it will negate much of SOAR's value to the organization. As a result, the solution should feature a user-oriented administrative experience.

This is the Swimlane approach. Swimlane designed an administrative UI/UX with the goal of lowering administrative overhead and speeding time to value for SOAR. Swimlane offers dashboards displaying security management metrics. The Swimlane administrative UI delivers significant visibility into the performance, capacity and value of an organization's security operations investment. The platform provides insight into security management variables that drive productivity, efficiency and morale.

Conclusion

The design of a SOAR solution is critical in determining its value.

To make it possible for a security team to thrive and be productive despite a rising tide of alerts, a SOAR solution must have comprehensive functionality in a single platform. An API-centric architecture is the key enabling factor. The solution must offer streamlined case management and integration with multiple systems, scaling both horizontally and vertically. Usability is key for maximum productivity.

Swimlane's SOAR solution embodies this criteria. Built with an API-first multi-tenant architecture, it offers seamless integration for security automation and orchestration. It features out-of-the box integrations with major enterprise security tools as well as simple creation of new bidirectional integrations.

As an automation tool, Swimlane leverages vendor APIs and SDSec methods so it can rapidly respond to and prevent attacks earlier in the kill chain. Swimlane captures relevant, real-time, and enriched incident data for efficient case management. Its UI/UX, including extensive, customizable dashboards, is able to lower administrative overhead and speed time to value.

About Swimlane

Swimlane is at the forefront of the growing market of security automation, orchestration 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.

To arrange for a demo of the Swimlane solution or to speak with one of our security architects to see if security orchestration would be helpful to your organization, please contact us at 1.844.SWIMLANE or email us.