451 Research

S&P Global
Market Intelligence

Swimlane aims to make it easier to orchestrate and automate security with its low-code approach

Analysts - Jackie McGuire

Publication date: Wednesday, May 11 2022

Introduction

As the security industry grapples with ongoing talent shortages and unmanageable data volume, Swimlane has developed a security orchestration, automation and response (SOAR) offering that features a single dashboard to visualize complex security architecture and help automate alert management and threat response. The company sees low-code development as a "sweet spot" between code-intensive development and less flexible no-code approaches, making its product easy to adopt and maintain as a system of record and central hub for security teams, and making automation accessible to a wider range of nondevelopers.

The Take

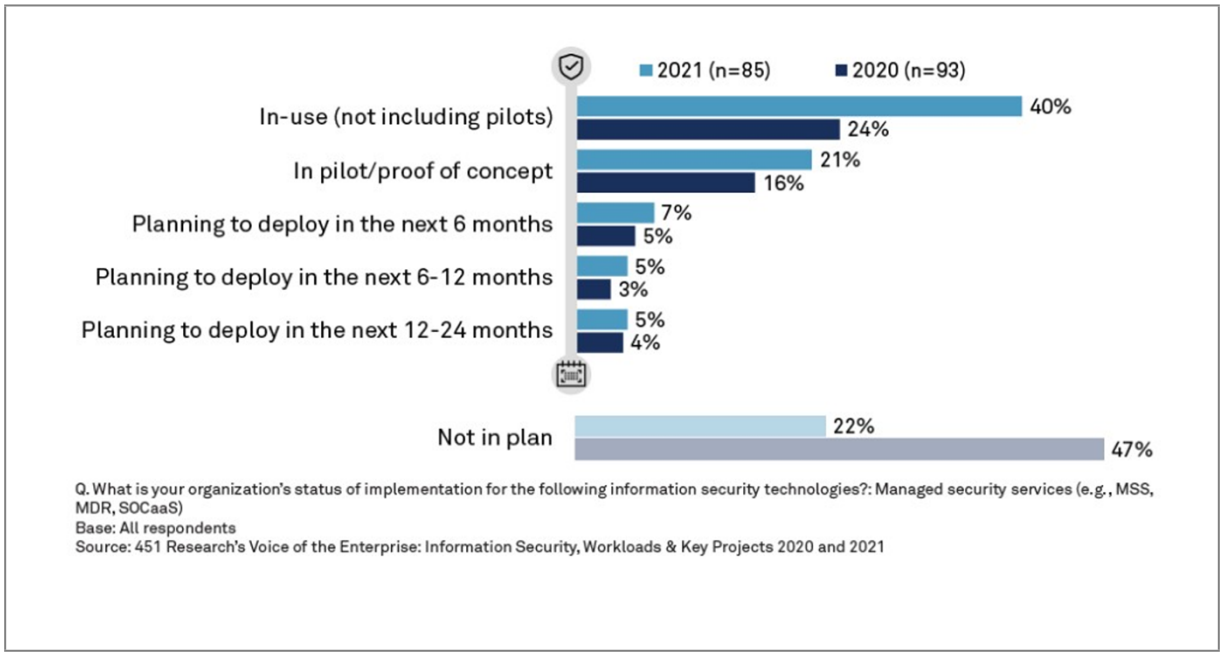
Tasked with managing an ever-increasing volume of telemetry from a range of disparate sources, enterprises and service providers are seeking tools that help them do a better job of managing false positives and repetitive tasks so they can more quickly respond to legitimate threats. Swimlane has invested heavily in low-code automation and workflows, and sees opportunity in removing the technical hurdles to automation development. While many security analysts are developers with some coding background, not all are, and reducing the amount of code to be written or development hours spent on automation will be an important component of easing demands on security teams.

Context

Swimlane has invested in support for granular multi-tenancy, enabling complex organizations to segment their security duties or, more typically, allowing managed security service providers (MSSPs) to service several different clients that all have different systems, without having to replace

large components of a client's existing security infrastructure. This approach expands the company's reach to the many organizations increasingly embracing managed detection and response, as noted in 451 Research's Voice of the Enterprise: Information Security, Key Workloads and Projects surveys in 2020 and 2021, where nearly twice the percentage of respondents indicated managed security services in use in 2021 vs. 2020 (40% vs. 24%). Less than half the percentage of respondents in 2021 indicated that managed security services were "not in plan" compared with 2020 (22% vs. 47%).

Figure 1: Status of Implementation for Managed Security Services



Source: 451 Research's Voice of the Enterprise: Information Security, Workloads & Key Projects 2020 and 2021

Technology

Swimlane's security automation platform is available both as an on-premises offering and, with the release of Swimlane Cloud in October 2021, a cloud-based SaaS product. The vendor calls itself the system of record for security and when fully deployed, enables organizations to document threat alerts, investigation, and response across their entire ecosystem. It has built-in integrations with over 300 security platforms and more than 1,800 integration endpoints, as well as an open API framework that enables integration with nearly any other third-party system.

Once fully integrated, Swimlane enables teams to see all of their security alerts and event data in one place. Events that are part of a broader pattern can be grouped together and enriched with third-party threat intelligence – false positives can be automatically ignored, and the platform can automate response to confirmed incidents by opening and escalating tickets, quarantining emails or files, etc. With a graphical, drag-drop-configure development tool, the company allows users with little to no coding background to quickly build processes and workflows.

The company's dashboards can be configured for different types of users or managers, giving analysts the ability to see individual events, while management can view higher-level response times and event volumes. It also supports multiple users, roles, groups and permissions, as well as granular multi-tenancy, enabling highly controlled access both for complex enterprises as well as MSSPs. Playbooks or workflows built for one use case can easily be adapted for another and the breadth of integrations available make it easy to replace pieces and infrastructure. For MSSPs, integrating a

wider variety of security technology increases their customer base and makes onboarding and management simpler.

Company background

Founded in 2014 and headquartered in Boulder, Colorado, Swimlane has nearly 200 employees with regional offices in London, Sydney, Seoul and Kuala Lumpur. The company has raised a total of $66 million, including its most recent $25 million series B round in November 2020. In January 2021, it welcomed new CEO James Brear, moving founding CEO Cody Cornell to chief strategy officer. Brear joined Swimlane after serving as CEO of Veriflow, which was acquired by VMware Inc. in August 2019. The vendor reports that it has 100-200 customers.

Competition

As one of the few remaining pure-play SOAR providers, Swimlane contends not only with direct rivals like D3 Security but also – and more so – with vendors in the security information and event management (SIEM) sector. Additionally, it contends with the expansion of security operations (SecOps) technology in the extended detection and response (XDR) segment, which has grown considerably over the past year. A tidal wave of M&A activity in the security market over the past several quarters saw Alphabet Inc.'s Google, Sumo Logic Inc., Palo Alto Networks Inc., Splunk Inc. and, most recently, Sophos acquire companies with integration or automation functionality to further their XDR ambitions. Many of the vendors that Swimlane integrates with are beginning to offer automated response, playbook and workflow capabilities. This may very well make Swimlane an attractive target for the few remaining large players in the space that haven't yet invested in automation or extensive integration.

Many of Swimlane's competitors have not reached the level of integration or interface maturity that it has, but are actively working toward it. Despite expanded offerings, some customers have shown a persistent reluctance to consolidate onto singular security platforms, prompting many of these organizations to adopt a more open, integrated approach to multivendor and cloud support. Many have either bought or built additional third-party integrations and support as well. It remains to be seen whether the platform approach to security will work, but if it does, it would introduce further challenges for Swimlane.

SWOT Analysis

Strengths	**Weaknesses**
Swimlane makes automating some or all of the event management and response process easy and supports integration with a wide variety of security tools. These features, along with its comprehensive multi-tenant capabilities, make the company a single point of entry for analysts learning or managing complex IT and security architecture, as well as service providers managing numerous different clients.	As a single-product company, Swimlane has few directions to pivot, should overlapping features from adjacent vendors significantly impact its SOAR business. The company is also reliant on other providers for its data, so its efficacy is subject to the quality and availability of that data.
Opportunities	**Threats**
While many of its competitors in the XDR space have or are working on managed services, Swimlane has invested in supporting MSSPs. Its platform's support for these providers and ability to integrate with a wide range of tooling and easily replicate workflows across different systems give it an edge over rivals weighing building out multi-tenant support and contending with their own	Nearly all large SecOps vendors are offering or developing some type of integrated automation and response functionality, whether under the moniker of SOAR, SIEM or another acronym. Most of these have multiple features and capabilities that rival Swimlane's SOAR. Although not all fully mature now, with such a focus in the area, rivals will continue to advance, and competition will remain high for

managed offerings.	the foreseeable future.

Source: 451 Research