Automating Detection and Response: A SANS Review of Swimlane

Alissa Torres

A SANS Product Review

Automating Detection and Response: A SANS Review of Swimlane

Written by **Alissa Torres**

December 2018

Sponsored by:

Swimlane

Introduction

Most security operations teams are burdened by overwhelming operational tempo and imperfect implementations of technology, people and process. During the past decade, a succession of security solutions packaged as silver bullets has been introduced to harden the enterprise and provide visibility into network and host-based assets. Many organizations sourced and supported these tools from different vendors and introduced them into their systems over many years. These disparate technologies present logistical and financial challenges to seamless security operations detection, analysis and response.

Swimlane, a SOAR (Security Orchestration, Automation and Response) technology, offers integration and interoperability across security teams' tools, providing a centralized user interface for security teams (analysts) to alert on and triage tracking and case management. Certainly, it is reasonable to doubt that the solution to this excessive complexity is YALTS (Yet Another Layer in the Technology Stack). However, SOAR technologies just may be a great solution for integration and interoperability. In addition, SOAR addresses the skilled cyber workforce shortage by acting as a force multiplier, culling the manual, repetitive tasks from daily routines of security analysts. Lastly, the implementation of playbooks (workflows of tasks that follow a decision tree-like format) formalizes triage and response procedures, enforcing repeatable processes that grow teams' efficiency and effectiveness.

The need for an orchestrator that makes all of these security technologies work together for seamless detection, analysis and response is obvious, given that analysts waste large chunks of their work day on tedious tasks such as copy/paste and manual inventory/user queries against internal databases. Swimlane, named as a breakout vendor in the 2017 Forrester report on SOAR technologies,[1] orchestrates this workflow with remarkable ease of use and flexibility.

Swimlane provides centralized incident tracking, data contextualization and workflow for incident triage, escalation and response based on well-defined playbooks. As an automation/orchestration response tool, Swimlane offers a two-prong solution for technology integrations. In addition to addressing the need for weaving current implementations together, it also supports impressive automation of entire components of triage, analysis and response processes. Swimlane delivers considerable value to security analysts by automating manual, repetitive tasks that take them away from triage and subsequent analysis. By freeing work cycles, analysts are able to focus on more in-depth data correlation.

This paper highlights the best-in-breed features of Swimlane: its ease of use, customizability, role-based access control and current technology integrations. We put Swimlane through its paces in a triage of a typical phishing email, applying the concept of componential workflow automation.

Swimlane Terminology

Workspace: Customizable areas within the Swimlane platform where you can organize and access the Swimlane tools and features you use on a regular basis. Workspaces can include applications, dashboards, records, reports and charts.

Dashboard: Visual display of records, reports and charts associated with the applications in the workspace

Card: Individual customizable visualizations that make up a dashboard

Applications: User-defined templates for the collecting, storing and organizing of an organization's data. A collection of layout and field elements, field keys and workflow stages and actions used for record automation and integration activity.

Applets: Preconfigured set of field and layout specifications that can be added to an application

Workflows: Defined process for how an organization handles an event that includes conditions, repeats and actions

Features that Set Swimlane Apart

Swimlane offers a variety of features that distinguish its tool from others. What follows are the most significant ones we identified in our testing.

Ease of Use

Security analysts spend a tremendous portion of their workday navigating through ticketing queues of security alerts. For this reason, logic should dictate that ease of use would fall among the most important features for a SOAR. Our first impression of Swimlane's user interface was favorable. Navigation is intuitive and dashboard tiles called *cards* are attractive. Dashboards are just one component of a Swimlane workspace, which is a customizable container that include applications, dashboards, reports and charts. Figure 1 shows an example of an analyst dashboard, with each of the tiles allowing for interactive drilldown.

Figure 1. Swimlane Analyst Dashboard

[1] "Breakout Vendors: Security Automation And Orchestration (SAO)," www.forrester.com/report/Breakout+Vendors+Security+Automation+And+Orchestration+SAO/-/E-RES136903

Because security operations teams may require unique reporting or data classification features, the Swimlane customized dashboards cater to and support unique experiences for everything from alert queues to categorization of alerts by source. Figure 2 illustrates three customized dashboards within the "Security Operations and Case Management" workspace, visible to my user account.

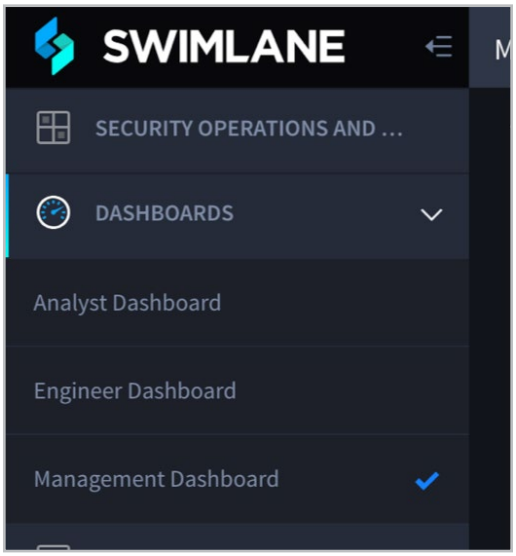

Figure 2. Multiple Dashboards per Workspace

The individual cards (records, reports and metrics visualizations) that make up a dashboard can be tailored to the team member's role. For example, a SOC manager may create and customize a unique dashboard to contain metric visualizations tracking the number of open alerts per analyst, alerts per type, cases per handler and important metrics such as "time to resolution" and "time to escalation." Dashboards can be standardized for a team, a role or a specific team member. Figure 3 shows an example of a full, customizable management dashboard.

One slight issue we noted with the Swimlane dashboard was the truncation of value names with ellipses. Though many field names expanded into pop-up "tooltips" when hovered over, some did not, making for an inconsistent experience. This issue would affect those analysts without multiple monitors and high screen resolution more significantly. Figure 4 shows how the dashboard looks with the ellipses.

Figure 3. Customizable Management Dashboard

Alert Workflow with Dynamic Case Management

If you are new to security orchestration, automation and response tools, it helps to know the initial implementation of SOAR technology focuses on the automation of some routine event types that nearly every security team currently handles. Common pain points most SOAR customers first focus on are malicious binary analysis and phishing email attachments or malicious URL triage. The best way to emphasize Swimlane's strengths in both orchestration and triage simplification through automation is to walk through the workflow based on a very common type of incident encountered by SOC analysts today: a malicious binary download.

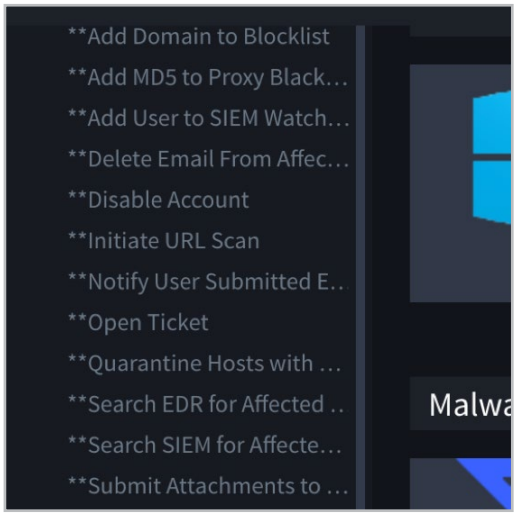

Figure 4. Missing "Tooltips" for Truncated Fields

For a routine alert such as this, a set of actions based on certain conditions can be defined in a repeatable process called a *workflow*. Swimlane uses customized workflows for particular event types within applications, where record layouts and technology integrations are containerized. To maximize Swimlane's robust, dynamic case management, an organization can design its workflows

to draw from data sources and ensure analysts have immediate access to the most relevant data for the specific incident type. Without the integrations offered by SOAR technologies, this type of triage would, for most security operations teams, require several manual and time-consuming tasks to be performed by one or more analysts.

Initial Stage: Alert Generation

Due to tight integration with SIEM technologies in this test Swimlane environment, the alert for binary download was automatically routed to the Swimlane alert queue on the analyst dashboard. As we drill into the case record view of the alert, shown in Figure 5, the internal host **`acme7834`** downloaded **`gamble.dll`** from **`199.7.234.100 port 88`** using **`FTP`**.

Figure 5. Swimlane Case Record View for Proxy Alert

Second Stage: Alert Contextualization

The automated creation of an alert triage record in Swimlane's built-in case management saves the analyst time, and the incorporated alert contextualization provides additional value. Through endpoint detection and response (EDR) integrations, Swimlane displays other affected host systems in this enterprise that it also has identified as containing the suspicious **`gamble.dll`** file.

Security analysts can make more informed decisions based on tactical threat intelligence, information derived from previously identified threat activity and malware. Typical triage of potential malware eats up valuable analysis time because many of the analysis steps are manual and repetitive. Security analysts routinely upload attachments to a sandbox for "detonation" and static and behavioral triage.

Swimlane allows for easy incorporation of these resources through automated file hash reputation checks via VirusTotal and Cymru Totalhash, among others, and automated file submissions to malware sandboxes such as Cuckoo, Cisco's ThreatGrid, Joe Sandbox and Lastline. As defined in our sample workflow, Swimlane automatically conducts a VirusTotal reputation check for the associated IP address and immediately ascertains the known threat of the malware. Based on the ThreatScore shown in Figure 6, it appears our binary warrants further action. Organizations can build automatic containment steps into a Swimlane workflow based on defined conditions or by the analyst.

Figure 6. Sandbox Analysis

Third Stage: System Triage

Swimlane supports host-based triage integrations with endpoint analysis tools, such as Tanium, that remotely acquire process and network connection details for the associated host. Swimlane acquires this information automatically based on the definition of the workflow. In our analysis, the analyst is able to check the process list, network connections and running services of the system as well as pull Active Directory information on the host and associated user. Typically, this type of host triage requires an analyst to run remote collection scripts in a separate tool as well as query AD details through another interface. Swimlane's consolidated interface saves the analyst time, keeps data associated with the alert record in a central location and conducts all of this additional data in a documented, consistent process.

We can see these host details under *Internal Asset Enrichment* in Figure 7. It should be noted that Swimlane is drawing host details from other data sources, so its ability to contextualize relies on the fidelity of its sources.

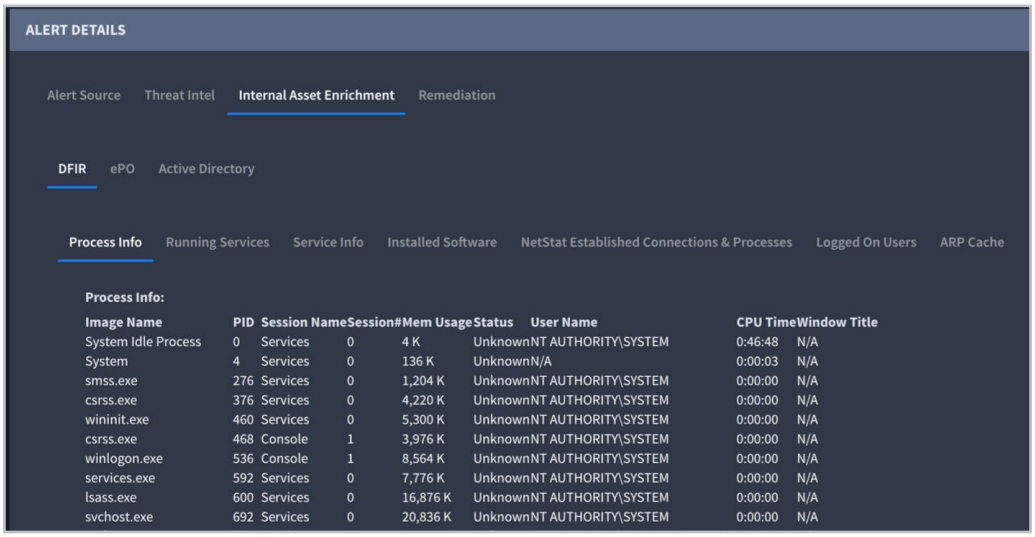

Figure 7. Host-based Triage Data

Fourth Stage: Containment and Remediation Actions

After determining the binary is malicious, the analyst can invoke containment actions through interaction with the Swimlane alert record. Based on the technologies in place, the analyst can invoke EDR capabilities to perform numerous tasks, including gathering more host-based data, deleting malicious files and/or quarantining affected hosts. In addition, he or she can put necessary proxy blocks and firewall changes in place and automatically notify other teams, such as field services, that the systems require re-imaging.

Swimlane's search capability allows the analyst to obtain the history of past incidents involving this same system as well as any further associations between the system's primary user and other assets involved in past compromise. Analysts can perform searches from the "keywords or filter" field, which offers granular filter capabilities based on field parameters. See Figure 8 for an example.

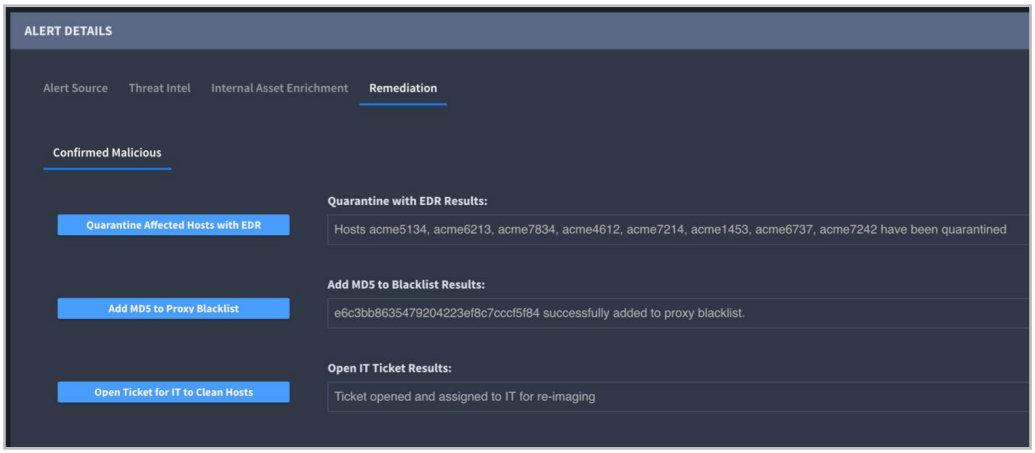

Figure 8. Containment and Remediation Actions

Figure 9 represents the steps we took in the walk-through of the product to show the seven automations that save time.

Final Stage: Case Management and Record Close

Based on the conditions of the defined workflow within the alert triage application, several final actions may take place when the alert has been successfully handled. Should additional notifications be needed, the organization can configure Swimlane to trigger notifications, emailing associated analysts or other relevant teams of the record status. In addition, the alert severity can be adjusted, record status set to closed and timestamps updated to reflect these changes.

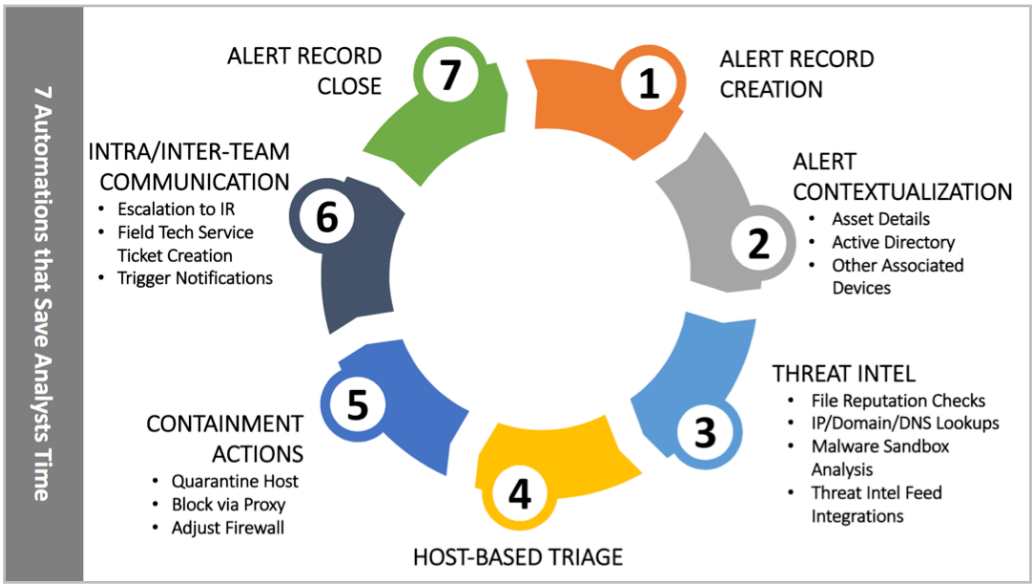

Figure 9. Seven Automations that Save Analysts Time

Figure 10 depicts a sample workflow that aligns with our alert walk-through.

Workflow/Applet Ease of Creation and Reuse

The core element in standardizing the response of a specific category of event is modularizing basic tasks. For example, in the case of a binary download detected by a proxy, one task would be to upload the binary to online or in-house reputation checkers/sandboxes for further analysis. With Swimlane, the "binary analysis" process can be developed into a "plug n play" applet to be reused as a module in other applications, such as SIEM malicious binary alerts and suspicious email attachment detection. Swimlane provides an easy "drag and drop" interface for crafting additional workflows using pre-defined applets that integrate with specific technologies and

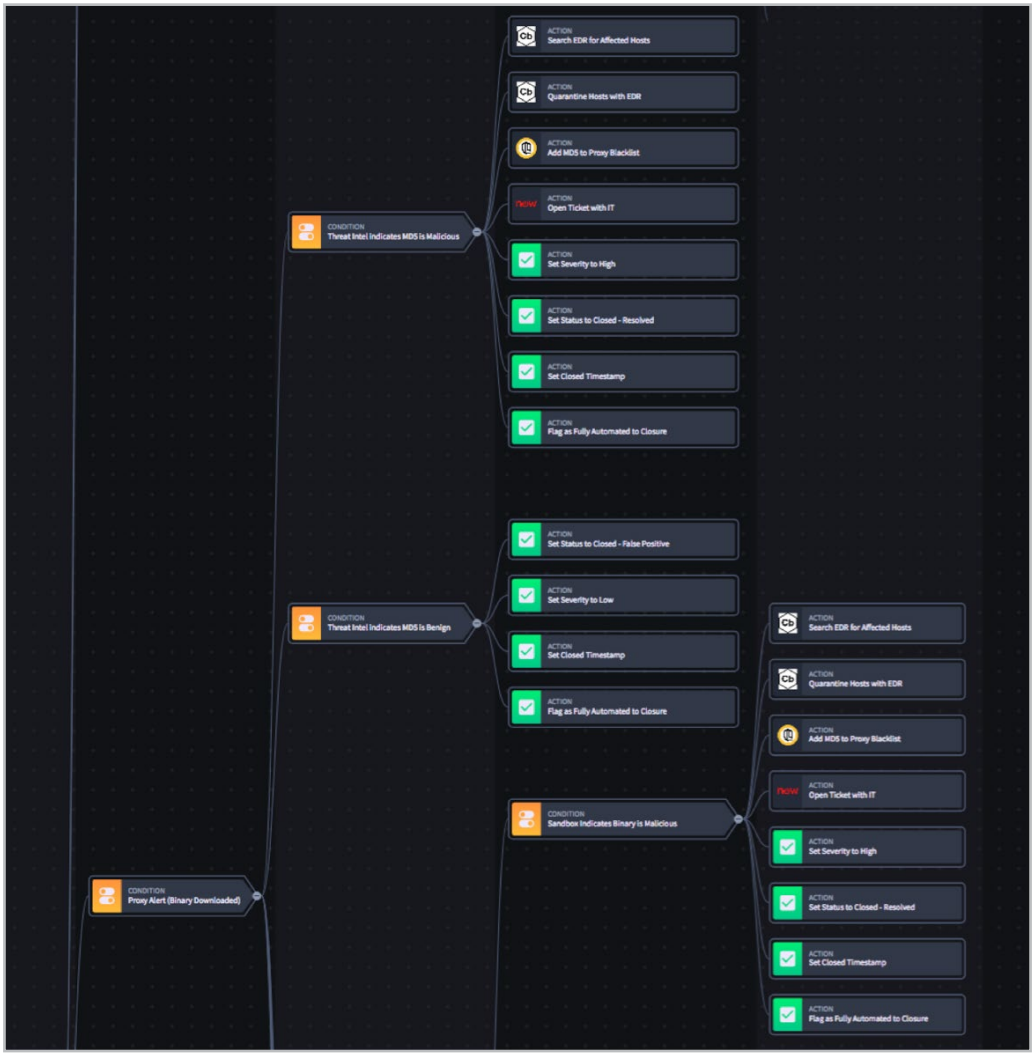

Figure 10. Example Workflow in Alert Triage Application

provide configured field and layout specifications. Figure 11 shows an example of an applet for VirusTotal File Report. In edit mode, you can customize the fields to see data most relevant to an analyst. The analyst can then place this applet in applications as needed as part of a workflow for handling different incident types.

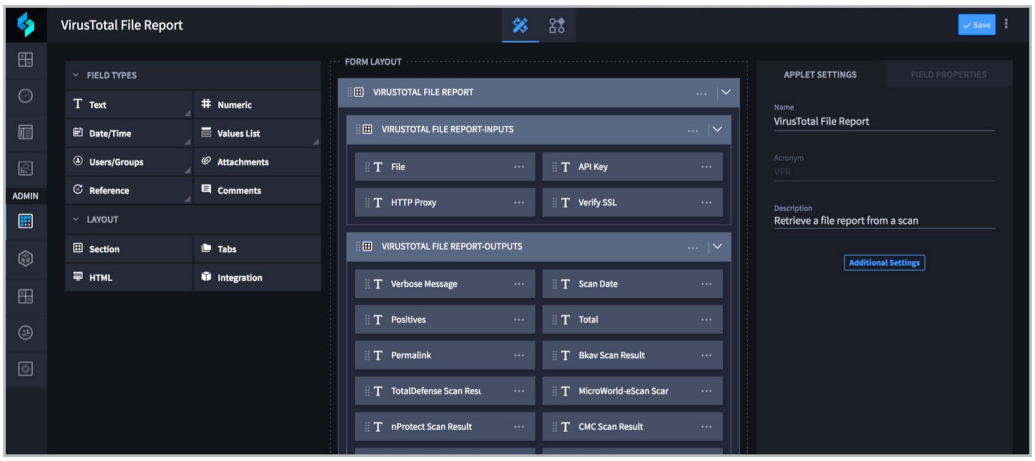

Figure 11. Edit Mode of Customizable Applet

Role-Based Access Implementations

Often when working on incidents, the circumstances of business units, data, systems and people involved are of a sensitive nature. A centralized incident-tracking repository can be ideal for most operational needs, but when it comes to restricting access to current or past cases, "need to know" restrictions become a challenge some SOAR technologies have not yet mastered. Role-based access control is built in to Swimlane and has been a feature since its inception. By using role-based access controls, Swimlane allows whole workspaces or individual components of a workspace to be assigned to or restricted from specific users. Organizations can define unique roles and then grant or restrict access to dashboards, reports, categories of incidents and incident cases.

The demo Swimlane environment to which we were given access did not have an enterprise-level RBAC model rolled out, but we were easily able to start from the ground up and create an "analyst" role. We assigned this role to a group, created an incident record and restricted access to that record solely to include the analyst group. See Figure 12.

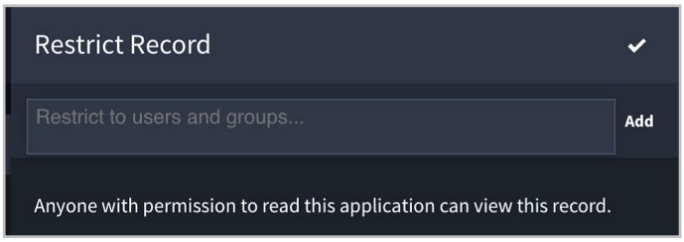

Figure 12. Example of Record-Specific RBAC

As we walked through the malicious binary case study presented earlier, you may have noted there are numerous actions an analyst who is performing manual review may elect to take. These actions depend on technology integrations specific to the customer environment but may include blocking IPs, isolating hosts on the network and blocking MD5s from execution. Some of these actions may not be appropriate for all alert reviewers to access. This points to another use case for RBAC. Containment/remediation action lock-down is easily implemented in Swimlane through assignments directly to the actions as well as through workflow creation. As organizations develop applications, they can define workflows where escalation is required if additional analysis or skills are needed prior to specific action being taken.

Robust Reporting Features

Swimlane supports report creation for any filter or visualization and offers visually appealing reporting capability with numerous table and chart views. The report editing

mode features the query filters of the Open Incident report, which can be customized to bring in any defined data set. Comprehensive prebuilt KPI metrics reports come ready to use with entirely customizable options. RBAC can be applied to reports and the ability to generate them. After they are created, reports can easily be added to dashboards. Figure 13 shows an example of customizing the Open Incidents report.

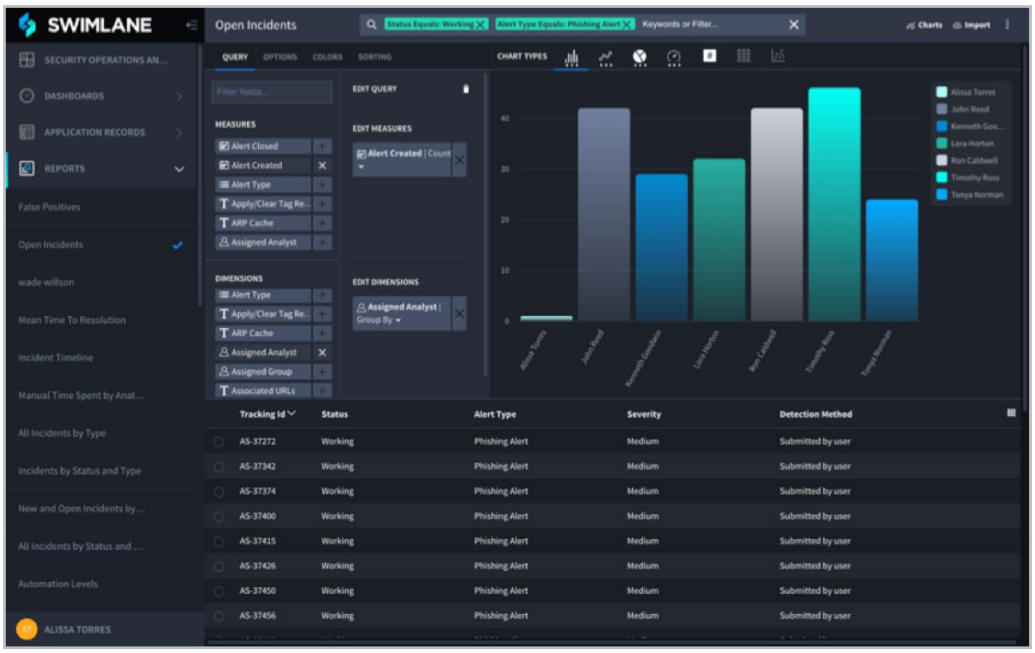

Figure 13. Customization of Open Incidents Report

One of the reporting aspects we found incredibly useful was the ROI calculation based on automated tasks per event record. Not only can Swimlane's value be calculated easily, a security manager can measure the increased efficiency gains over time as workflows are expanded to include more automated tasks and technology integrations are expanded.

Supported Technology Integrations

The true value of SOAR technology hinges on its ability to bring together the numerous technologies that make up an organization's ecosystem to provide an effective, efficient and cohesive platform. Many NIDS and HIDS offer containment and remediation actions, and SOAR technologies should be the sum of all these capabilities. Like the other SOARs, Swimlane offers customizable integrations with a high degree of flexibility, particularly for those skilled enough to grow their own solutions. For those security teams that do not employ a team of integration experts, however, the good news is, at the time of this review, Swimlane currently supports 138 integration bundles "out of the box" and adds new bundles every week. An integration bundle is a proven schema for supporting another technology. The bundles include more than 500 individual actions/integrations. These include integrations with SIEMs, EDRs, threat intelligence platforms, FWs, vulnerability scanners and other security platform categories and related infrastructure.

Some notable technologies that have been successfully integrated in Swimlane customer environments include the following:[2]

Cisco
McAfee ePO
Lastline
CarbonBlack
VMRay
RSA Archer
Palo Alto NAF

[2] Space does not allow us to list all of the integrations available. Also, numerous other integrations are under development.

In our test environment, we had integrations with a limited number of technologies, and most of our interactions were performed with test data. Figure 14 shows the asset integrations that were incorporated into the alert triage workflow for our test lab.

As a Swimlane customer, you have access to the support portal where applet and integration sharing is available, along with customer support from product SMEs and fellow Swimlane users.

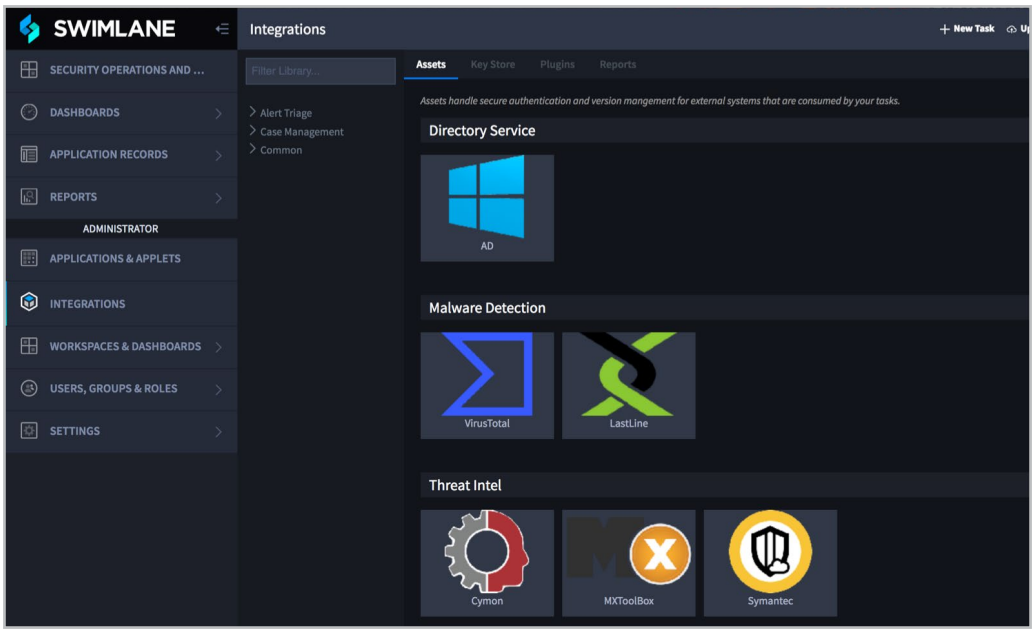

Figure 14. Customization of Open Incidents Report in Bar Chart View

Conclusion

In addition to the well-refined product Swimlane provides, it also has a strong, open collaborative forum in the SecOps hub for information sharing among security professionals. With a growing demand for fast detection and response across all technologies, Swimlane is a well-positioned solution for integration of the technology soup most security operations team find themselves in. With SOAR being such a new and rapidly evolving security product, it will be Swimlane's adaptability and the speed with which it announces partner technology integrations that will ensure it continues as a market leader in this space.

About the Author

Alissa Torres is a SANS analyst and principal SANS instructor specializing in advanced computer forensics and incident response (IR). She has extensive experience in information security in the government, academic and corporate environments. Alissa has served as an incident handler and as a digital forensic investigator on an internal security team. She has taught at the Defense Cyber Investigations Training Academy (DCITA), delivering IR and network basics to security professionals entering the forensics community. A GIAC Certified Forensic Analyst (GCFA), Alissa holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+ certifications.

Sponsor

SANS would like to thank this paper's sponsor:

Last Updated: March 22nd, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Doha March 2019	Doha, QA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, FR	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS Madrid March 2019	Madrid, ES	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FLUS	Apr 01, 2019 - Apr 08, 2019	Live Event
SANS Cyber Security Middle East Summit	Abu Dhabi, AE	Apr 04, 2019 - Apr 11, 2019	Live Event
SANS London April 2019	London, GB	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KYUS	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, SA	Apr 13, 2019 - Apr 18, 2019	Live Event
SANS Boston Spring 2019	Boston, MAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
SANS Seattle Spring 2019	Seattle, WAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
FOR498 Battlefield Forensics Beta 1	Arlington, VAUS	Apr 15, 2019 - Apr 20, 2019	Live Event
SANS FOR585 Madrid April 2019 (in Spanish)	Madrid, ES	Apr 22, 2019 - Apr 27, 2019	Live Event
SANS Northern Virginia- Alexandria 2019	Alexandria, VAUS	Apr 23, 2019 - Apr 28, 2019	Live Event
SANS Muscat April 2019	Muscat, OM	Apr 27, 2019 - May 02, 2019	Live Event
SANS Pen Test Austin 2019	Austin, TXUS	Apr 29, 2019 - May 04, 2019	Live Event
Cloud Security Summit & Training 2019	San Jose, CAUS	Apr 29, 2019 - May 06, 2019	Live Event
SANS Bucharest May 2019	Bucharest, RO	May 06, 2019 - May 11, 2019	Live Event
SANS Security West 2019	San Diego, CAUS	May 09, 2019 - May 16, 2019	Live Event
SANS Perth 2019	Perth, AU	May 13, 2019 - May 18, 2019	Live Event
SANS Milan May 2019	Milan, IT	May 13, 2019 - May 18, 2019	Live Event
SANS Dublin May 2019	Dublin, IE	May 13, 2019 - May 18, 2019	Live Event
SANS Stockholm May 2019	Stockholm, SE	May 13, 2019 - May 18, 2019	Live Event
SANS Northern VA Spring- Reston 2019	Reston, VAUS	May 19, 2019 - May 24, 2019	Live Event
SANS New Orleans 2019	New Orleans, LAUS	May 19, 2019 - May 24, 2019	Live Event
SANS Autumn Sydney 2019	Sydney, AU	May 20, 2019 - May 25, 2019	Live Event
SANS MGT516 Beta Two 2019	San Francisco, CAUS	May 20, 2019 - May 24, 2019	Live Event
SANS Amsterdam May 2019	Amsterdam, NL	May 20, 2019 - May 25, 2019	Live Event
SANS Hong Kong 2019	Hong Kong, HK	May 20, 2019 - May 25, 2019	Live Event
SANS Krakow May 2019	Krakow, PL	May 27, 2019 - Jun 01, 2019	Live Event
SANS Atlanta 2019	Atlanta, GAUS	May 28, 2019 - Jun 02, 2019	Live Event
SANS San Antonio 2019	San Antonio, TXUS	May 28, 2019 - Jun 02, 2019	Live Event
Security Writing NYC: SEC402 Beta 2	New York, NYUS	Jun 01, 2019 - Jun 02, 2019	Live Event
SANS Jeddah March 2019	OnlineSA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced