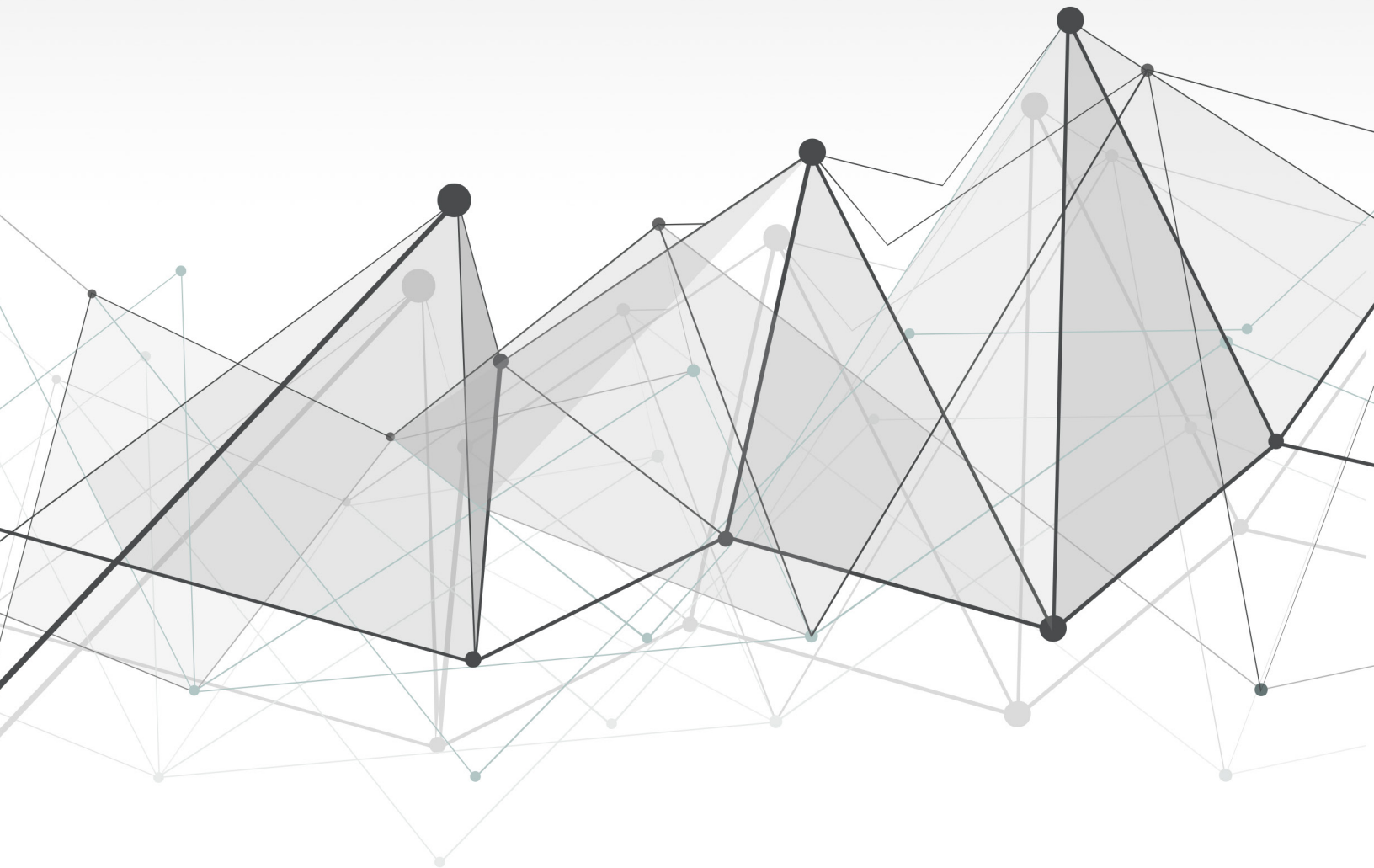
SWIMLANE



Automating Incident Response

How security orchestration will improve your life.

SWIMLANE

Table of Contents

Introduction

Security operations present an escalating series of management challenges. As the frequency and variety of attacks accelerate, even the best teams can get overwhelmed with alerts.

The sheer volume of potential threats often presents teams with the false dilemma of trying to choose which alerts to deal with—often relying on the somewhat arbitrary threat classifications presented by a disparate set of siloed tools. This kind of alert triage creates the risk of missing serious threats. But many teams often feel that they have no choice. Using criteria like an alert's perceived importance or criticality as the decision point to take action is the antithesis of being proactive. There are generally several early lower criticality or priority indicators which suggest a serious attack is underway. Yet, to address every alert would require significantly scaling the incident response team. Even if budget is available, adequately trained staff may not be.

What can be done about these challenges? Security orchestration, automation and response (SOAR) with automated incident response is a solution. This e-book shows how your team can streamline alert monitoring and speed up the incident response process.

Address every alert thereby reducing risk exposure by automating repetitive and time-consuming tasks.

Pressures faced by security teams

Security managers work in a pressurized environment which seems to create new varieties of stress on a regular basis. The overall threat level continues to grow. Beyond that, however, the "surface area" of risk exposure expands over time. In tandem, the number of security alerts increases—creating a situation where staffers and their incident response capacity can become overwhelmed. This reality is compounded by the fact that businesses today are more reliant on IT than ever before. In many cases, IT defines the organization in strategic and operational terms. When a bank essentially becomes an IT entity that happens to lend money, the stakes for cybersecurity become higher than ever.

Increasing attack surface area

Organizations today face new types of threats. Evolving IT platforms such as Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS), coupled with innovations in mobile devices, conspire to increase risk exposure. For instance, the practice of placing data assets and applications on cloud infrastructure expands the security perimeter. The popular trend of hybrid IT, which blends on-premises and cloud infrastructure, results in more—and more diverse—systems to monitor for security incidents.

The growing use of "as-a-Service" solutions, like IaaS and SaaS, now places critical systems outside of the firewall and beyond your direct control. However, data security and incident response are still your responsibilities. For example, with a SaaS solution such as Salesforce.com, an organization generally has its entire customer list in the cloud and accessible by third-party entities and contract-based employees.

In the case of online productivity and file sharing applications—like Microsoft Office 365, DropBox, or Box—the organization may have a wide variety of confidential documents stored on the cloud. While most SaaS providers have excellent security, it is still up to the client's

security team to stay on top of suspicious log-ins, attempts to compromise user accounts and so forth. After all, it's users that are generally your weakest link.

The Internet of Things (IoT) presents a similar but potentially bigger increase in attack surface area. According to Gartner, 43% of organizations were adopting IoT in 2016. Longer term, 64% are expected to adopt IoT. IoT means different things to different organizations, but the impact is the same regardless of how companies are connecting devices to their networks. Whether it's sensors and industrial controls or smart agents monitoring remote facilities, more devices are becoming IP-enabled, exposing organizations to the risks of malware and network penetration. Bottom line: IoT means yet another (potentially huge) set of systems to monitor and patch.

High volume of security alerts

Large organizations are now handling between 10,000 and 150,000 security alerts a day. These numbers reveal the scale of the security workload. The high volume also suggests that circumstances reward cyber crime. Compared to physical crime, where the risk of punishment is high, online crime presents many opportunities including lots of reward but a low risk of being caught and prosecuted. Security teams and their toolsets are all that stand in the way of the malicious actors.

Sub-optimal incident response processes and workflows

We've experienced first-hand many of the pressures security operations teams face today. One thing that we have seen repeatedly, is how a high volume of alerts and security incidents can throw off even the best prepared security teams. A number of factors contribute to this reality:

- **Inconsistent response to critical threats.** Threats tend to manifest in ways that defy the structure of existing incident response workflows. Threats, as well as the systems they target, undergo constant evolution. The amount of threat intelligence also grows constantly. Therefore, it is critical that incident response protocols adapt to the evolving threat landscape.

- **Failure to effectively integrate people, process, and technology.** Cyber defense works best when security toolsets and personnel are aligned around common processes. Many security tools, such as intrusion detection systems (IDS) operate as siloes. This can result in personnel missing important alerts because they're only seeing the impact of an incident on a single system.
  Even with security incident and event management (SIEM) tools, which are designed to correlate security data across multiple systems, there can still be a need for manual research of adjacent event data and so forth—tasks that slow down incident response and potentially overwhelm the team.

- **Staff turnover resulting in loss of institutional/tribal knowledge.** When security analysts leave teams that operate on complex rules and informally defined workflows, incident response suffers. Getting a team member on-boarded and up to speed also requires an investment of time and money. When people leave, that investment is lost.

- **Compliance and regulations affect security policy.** New rules, driven by changing regulations, mean new headaches and more potential missed procedures.

These factors also tend to overlap. The high-turnover security team may experience a lack of coordination between toolsets and personnel. A team that lacks good coordination between toolsets and personnel may experience inconsistent response to critical threats, and so forth.

Overloaded personnel

A workload that involves assessing thousands of alerts every day can become overwhelming. Teams are affected by low morale, burnout and the inevitable turnover of staff. High turnover is exactly the wrong environment for security teams that need to grow to meet an expanding array of threats. Industry research reveals the depth of the problem. According to the 451 Group, as reported in CSO magazine, over a third of security executives surveyed said that a lack of experienced staff was delaying security projects. Another 26% said they were being slowed down by inadequate staffing levels.

Several serious challenges emerge when this happens. It can be hard to recruit qualified people, even if hiring budget is available. Then, if the team starts to assign members to monitor tools they don't fully understand or are properly trained upon, there is the risk of missing important alerts. This, in turn, creates a stressful environment, which results in higher turnover and a difficulty in recruiting staff—and a vicious cycle emerges.

The risks of alert triage and other symptoms of alert overload

The math works against security teams trying to stay on top of alerts. How long does it take to process an alert? That number depends on the complexity level of the alert, how thoroughly each alert needs to be investigated, as well as the nature of the review process. Figure 1 shows a typical event management process. It uses estimated times to respond to a suspicious binary, but of course, actual times will vary. A reasonable estimate, though, is that it might take 40 minutes to thoroughly process an alert on a completely manual basis. Based on our experience, with all the variability in process and circumstances, it's realistic to assume that an average alert handling process will take 5 minutes.

At the rate of ~12 alerts handled per hour, a team of 5 security staffers can get on top of about 500 alerts per eight hour shift. That's a lot of alerts! But, given a workload of 10,000 alerts per day, they're ignoring 95% of the alerts they receive. (Of course, ideally, there should be more than one shift running. However, only 24% of enterprises have 24×7 monitoring in place using internal resources.)

Effects of triage and prioritization

How do most teams handle this overload? They adopt a triage or prioritization approach. The team establishes parameters for which alerts will receive attention and which will be ignored. This is an understandable response to being flooded with alerts, but it's quite flawed.

Manual workflow for a suspicious binary alert

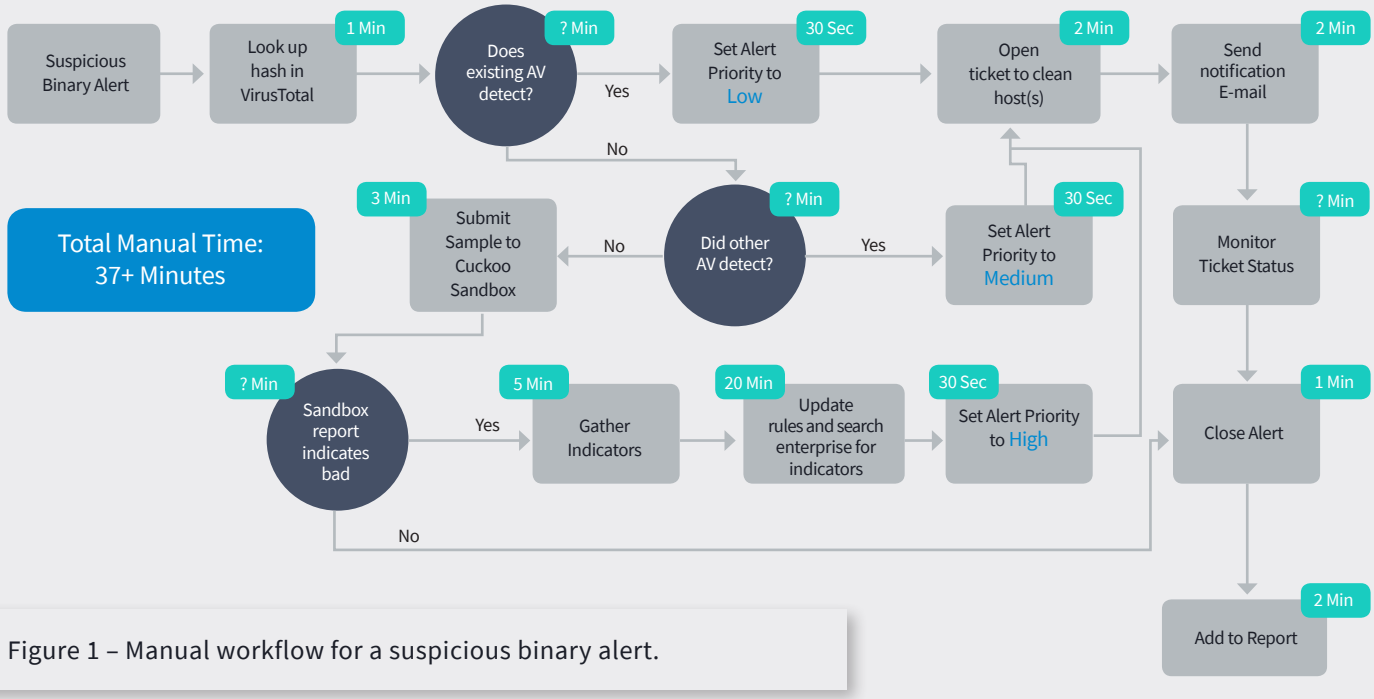


Figure 1 – Manual workflow for a suspicious binary alert.

Triage inevitably leads to missing a real attack at some point. There is no way to skip a major portion of alerts and stay in front of all valid threats. Indeed, a number of major breaches in recent years have been attributed, in retrospect, to seemingly minor alerts being overlooked.

In addition, any process that essentially turns people into machines is going to have consequences for the business. On a practical level, the speed of response is never going to be good enough. Security demands the capability of real-time rapid response. The problem is that humans are incapable of 100%, always on, immediate response. On a personal level, security professionals did not get into security to spend their time performing administrative tasks like cutting and pasting data. Security pros generally want to be involved in challenging security work, but the great majority of security operations in a triage environment are highly administrative. Ultimately, it's a poor use of expensive human capital.

The problem of scaling a sub-optimal alert management process

It is possible to manually scale the alert management process shown in Figure 1. But there are many problems with this approach. It would take a staff of 100 to handle 10,000 alerts per day at the rate of 12 alerts per person/hour. (For a cost perspective, that's an annual payroll of about $20,000,000, based on industry salary data.[1])

Even if it's possible to hire that many people, would it be the right move? Scaling up a sub-optimal process just makes it sub-optimal at a bigger scale. The manual nature of the process (and the tedium it implies) will still result in missed alerts, regardless of how many people are on task. In our experience, the majority of organizations believe they are not doing all that they could, in operational terms. There are many things they know they could be doing but don't, even if they could hire more people. Examples include increasing vulnerability scanning cycles, responding to generally disregarded reconnaissance attempts, and cultivating internal threat intelligence from their alarms and other datasets.

Figure 2 – The alert triage process lets security analysts review alerts selectivity based on criteria that establish the seriousness of the threat.

Automated Incident Response & SOAR

Automated incident response and security orchestration, automation and response (SOAR) helps solve the alert overload problem. What do we mean by SOAR? It is a collection of processes and tools working in concert to automate otherwise tedious and time-consuming security management tasks. As such, SOAR lacks a simplistic, clear-cut definition. By design, it adapts to every organization's unique security requirements. However, most solutions share several common characteristics.

Centralize operations

A solution for automated incident response and SOAR typically offers centralized security operations. It provides a tool for handling tasks that require the use of secondary systems. For example, through a single console, a security manager can monitor and interpret the outputs of SIEM, a monitored phishing email box, and IDS systems. Figure 3 shows an example of this kind of security automation dashboard.

Automate security operations

The solution enables the security team to model its alert response processes and automate them. Imagine that an incident response process calls for a suspicious binary to be manually uploaded into the VirusTotal system for evaluation. An automated incident response solution will handle the VirusTotal submission and data collection steps on its own. It can also automatically open a ticket in JIRA, as shown in Figure 4. These automated steps save a few minutes of work for every alert response. It may not seem like much, but by automating and orchestrating the sub-tasks associated with incident response, the solution can speed up the process significantly, saving time and improving the organization's ability to repond to incidents.

1. Source: According to CIO Magazine, the average security professional earns $116,000 per year. The fully allocated cost of a security staffer is therefore in the range of $200,000 per year, on average.

Figure 3 – Example of an automated incident and security orchestration dashboard.

Time-draining sub-tasks that can be automated and orchestrated include:

- Incident investigation involving log gathering and analysis.
- Review and analyze threat intelligence sources.
- Update tickets, create reports and email alerts (e.g. automatically log into multiple systems systems and entering incident information).
- Understand context and take corrective actions (e.g. implement security controls, update black list, update IDS rule, disable a user account, etc.).

Sample use case

To illustrate the potential of a solution to improve security while enabling 100% of alerts to be addressed, consider the following incident scenario. A SIEM generates an alert based on suspicious firewall log activity. Is it a minor aberration, a meaningless surge of random pings or the start of a massive distributed denial of service (DDoS) attack? The team will have think fast. There are 9,999 other alerts to tend to.

A well configured SOAR tool will instantly evaluate the alarm and then gather related context to the SIEM alert to determine the proper set of actions. It provides context and presents the user with a visual display. The solution may draw security intelligence data from other sources, such as STIX/TAXII or an ISAC.

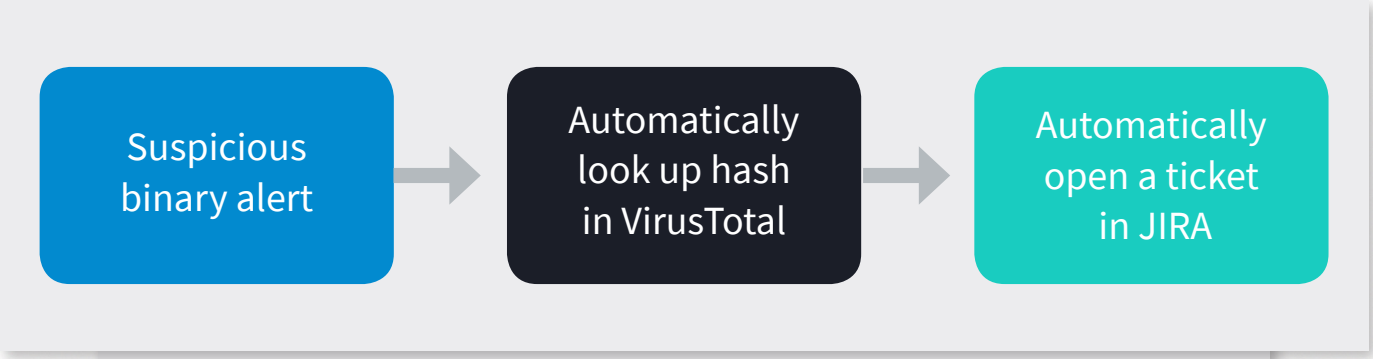


Figure 4 – Sample workflow of automation of two manual incident response processes.

The solution will then automatically open a ticket in JIRA (or another issue tracking software), send notification emails to relevant personnel and create a report of the incident. If the incident warrants changing IDS settings, the automation solution will execute a rules-based workflow to update the IDS. Based on rules and orchestration settings, the solution can change the priority of the alert ticket and notify people by email or text automatically. It will also automatically close the ticket based on rules at a given time interval. Data from the incident will be stored and used to create context for future, similar alerts.

The impact

The use case described above will positively affect security management. The incident response process becomes substantially faster, so the team can handle more alerts in the same amount of time. From there, the solution enables further tuning of security systems so the overall alert level drops.

Automated incident response and SOAR also allows security team members to focus on what matters and get less distracted—and bored or burned out—by routine, repetitive work like sending email updates and changing alert priorities. They can hone their skills and use their training best, leveraging the analytical power of the system to make better decisions about which incidents are serious and which can be set aside.

No incident data is ever lost. The solution logs incidents and can be set up to interpret past events and get better at providing context for new incidents. This is essential for many compliance regimens and systemic data retention policies. It can enable deep analysis and reporting of the security condition of the organization. Analysis and reporting of this type is useful for risk management and planning for future security needs as well as updating security policies.

How it works

Security orchestration, automation and response relies on standards-based software and open application programming interfaces (APIs) to enable broad, easy interconnectivity between security systems.

With a REST-based (RESTful) API and the JSON language (as well as other common open standards like SOAP, XML, SMTP, ODBC), it is possible to integrate security tools with the SOAR platform without the need for proprietary connectors or custom-coding. This is necessary since custom connectors and coding would add so much time, expense and rigidity to the solution as to render it difficult to deploy and maintain. With the flexibility of open standards

and RESTful APIs, the team can simply and quickly connect SIEM, IDS, endpoints, threat intelligence and other security tools with the automated incident management portal and orchestration capabilities—all without creating a maintenance nightmare.

Standards-based orchestration languages complete the architectural picture. As shown in Figure 5, the SOAR solution enables users to model incident response workflows visually. The tooling then makes it possible for the user to easily invoke software—internally and externally – to execute the incident response workflow.

Some automated incident response and SOAR solutions provide recommended automated process (i.e. playbooks) out-of-the-box. From there, it's up to the security team to refine the workflows and analytical capabilities of the solution. This can be helpful for some teams while others may eschew generic responses. In this sense, the solution will only be as good as the people who manage it. However, if properly configured, the solution empowers the security analyst to do his or her best work. The nature of the system allows the analyst's expertise to scale exponentially across the security management process rather than be constrained by an individual's personal output.

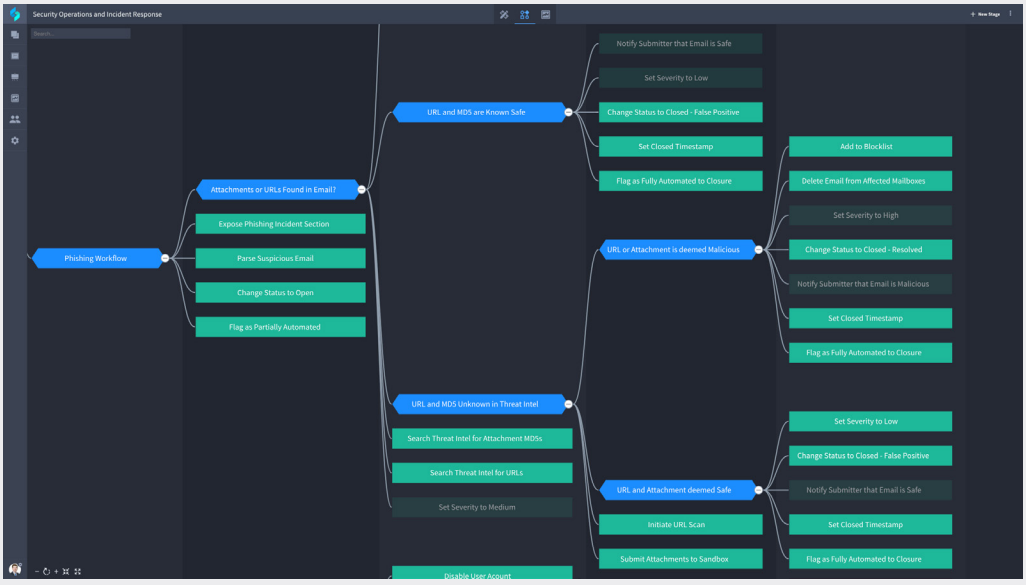


Figure 5 – Example of automation being modeled in a SOAR solution.

Return on investment

Managers can estimate financial benefits or return on investment (ROI) for a SOAR solution in at least three ways. Being able to determine ROI matters because it is important to quantifiably justify the spend by providing relevant success metrics to executive management and boards of directors.

First, there's the basic cost-per-alert metric, which will decrease with the implementation of automated incident response. Thus, if a security team costs $5,000 per day to employ and equip, and they can manually handle 500 alerts per day, the cost to handle each is $10. If it becomes possible to handle 10,000 alerts per day with the same team, the cost per alert goes down to a mere 50 cents.

Second, when the existing team can handle all of the alerts, there is less need for costly staff expansion. If hiring a additional team member will cost $200,000 per year, then a $100,000 investment in automated incident response that avoids the need for that staff member yields a 200% ROI in the first year.

Third, the additional analytical capabilities of SOAR should facilitate better security capacity planning and staffing budgets. The solution's dashboards and metrics usually deliver extensive visibility into the performance, capacity and value of a security operations investment. Avoiding over-provisioning of security systems going forward can significantly contribute to ROI for automated incident response.

Finally, there is the intangible but quite serious value of reducing risk. As recent events have shown, major incidents can be catastrophically costly. Reducing their likelihood is a strong financial incentive.

Swimlane's solution

Swimlane offers a SOAR solution that centralizes security operations activities. Swimlane's solution manages and automates the response to security alerts and incidents identified by existing monitoring and detection systems. The Swimlane approach utilizes automated incident response to replace slow and manual threat response capabilities with machine-speed decision making and remediation.

Swimlane tracks all enterprise security tasks, providing centralized access to cases, reports, dashboards and metrics for individuals and teams. It standardizes incident response and notification processes to mitigate risk, speed resolution and streamline communications. Its automation leverages vendor APIs and Software Defined Security (SDSec) methods to rapidly respond and prevent attacks earlier in the kill chain.

With Swimlane, a security team can capture and standardize its processes. Then, it can use SOAR to scale them. Scalability stems from the ability to expedite information review through centralization. Then, by automating the repetitive aspects of the process, the security team has time to address a larger number of issues. Standardization allows the team to learn and resolve security tasks quickly. The solution also enables staff to resolve incidents using newfound security intelligence capabilities. Visualizing threat intelligence and case history allows Swimlane to provide situational awareness of an incident and potentially related events that may actually be part of a larger attack. The platform provides insight into the specific variables that may be negatively affecting productivity, efficiency and morale.

Conclusion

Staying on top of thousands of security alerts every day is exhausting for a security team. It is nearly impossible to assess every incident manually. However, missing even one incident can contribute to risk exposure.

Automated incident response and SOAR allows security teams to respond to every alert without increasing the size of their staff or increasing staff turnover and burnout. It also crystalizes and documents workflows and security responses to improve institutional knowledge. The SOAR capability delivers a faster mean time to resolution along with greater risk reduction and threat protection. It accomplishes these goals while reducing costs and extending the capabilities of existing resources.

Figure 6 – The Swimlane analyst dashboard.

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 needs, including prioritizing alerts, orchestrating tools and automating the remediation of threats—improving performance across the entire organization. Swimlane is headquartered in Denver, Colorado with operations throughout North America and Europe.

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 email us.