White Paper

An Origin Story: The Role Security Orchestration, Automation, and Response Tools Play in Initiating and Maintaining an Elevated Security Posture

Sponsored by: Palo Alto Networks

Michelle Abraham Christopher Kissel
November 2021

EXECUTIVE SUMMARY

Right now, the expectations for vendors of security orchestration, automation, and response (SOAR) platforms are unusually high. As businesses undertake their digital transformation journey, a journey that was in many ways accelerated by the onset of COVID-19, mounting IT and security problems visible from afar become far more pressing. Businesses have had to — and continue to — deal with the following issues:

- **New architectures facilitating remote workers.** As the pandemic caused a diaspora of remote workers, new connectivity options to VPN, logical business segmentations, and multitenant workflows had to be created on the fly.
- **New surfaces to defend and observe.** Straight-to-user SaaS applications and IoT/OT convergence occurred more rapidly.
- **Limited personnel both an ephemeral and a long-term problem.** If an IT or security operations center (SOC) specialist leaves a company, other team members temporarily fill the void until a replacement is found and trained. Often tier 1 security analysts assume more of a tier 2/3 threat hunting role. IT and cybersecurity workers are in short supply anyway, with estimates of a global shortage of roughly 3 million workers.
- **More sophisticated attacks.** Last, and truly the scariest, is that attackers are more automated now than ever, and the only way to defend from machine attacks is to build your own machine speed detection and response capabilities.

All these problems bring us back to SOAR solutions. SOAR has a profound effect on cybersecurity on the troika of "people, processes, and technology." On a high level, SOAR products create the connective fabric between point products and platforms and aggregate alerts in such a way that redundant alerts are weeded out, and in the investigation process, the analyst works with enriched and contextualized data. Ultimately, playbooks help guide the security analyst through the first steps of suggested remediation to the termination of the ticket.

If SOAR sounds heady and disruptive, it is. Orchestrating workflows between multiple systems and solutions is an engineering feat. Highly sophisticated playbooks can be developed, accounting for minute and specific instances as well as for multiple contingencies. In addition, SOAR provides a centralized investigation platform for incidents and alerts for security analysts rather than requiring them to swivel between multiple systems. Last, with the proper automation, the response process

begins with everything from isolating the endpoint to dynamically creating new playbooks and dynamically refreshing firewall rules.

That leads us to the most important thesis of this paper. Because SOAR can produce so many sophisticated workflows and outcomes, there is a misimpression that SOAR tools can only be used by the most sophisticated SOC teams. Untrue. The benefits of SOAR can be realized by small, less technically savvy IT/security teams with many out-of-the-box functionalities providing immediate impact. Security teams may use the integrations that are part of the SOAR platform to orchestrate actions such as distributing alerts to other teams for case management automation. Response workflows can be created by chaining actions within multiple toolsets to increase team efficiency. Further, SOAR tools can be used to help facilitate collaboration and real-time chat features. SOAR tools are also designed to be self-iterative (i.e., as practitioners become more proficient with SOAR, the practitioner builds better processes). Last, not only does SOAR provide an immediate benefit to an organization but the use of SOAR can serve as a guide to a company in its security maturity evolution.

There is a misimpression that SOAR tools can only be used by the most sophisticated SOC teams. Untrue.

In developing this white paper, IDC talked to several SOC teams about their security orchestration and automation strategy, including Palo Alto Networks' own SOC team. From this, we designed the white paper to illustrate the most acute problems that SOAR helps solve, how organizations beginning with a SOAR platform derive value, and what the best practices are to move SOAR capabilities from beginner to intermediate and then to advanced use cases. Finally, we describe expert use cases and the types of efficiencies that can be gained in more mature SOCs.

What Cybersecurity Teams Are Up Against

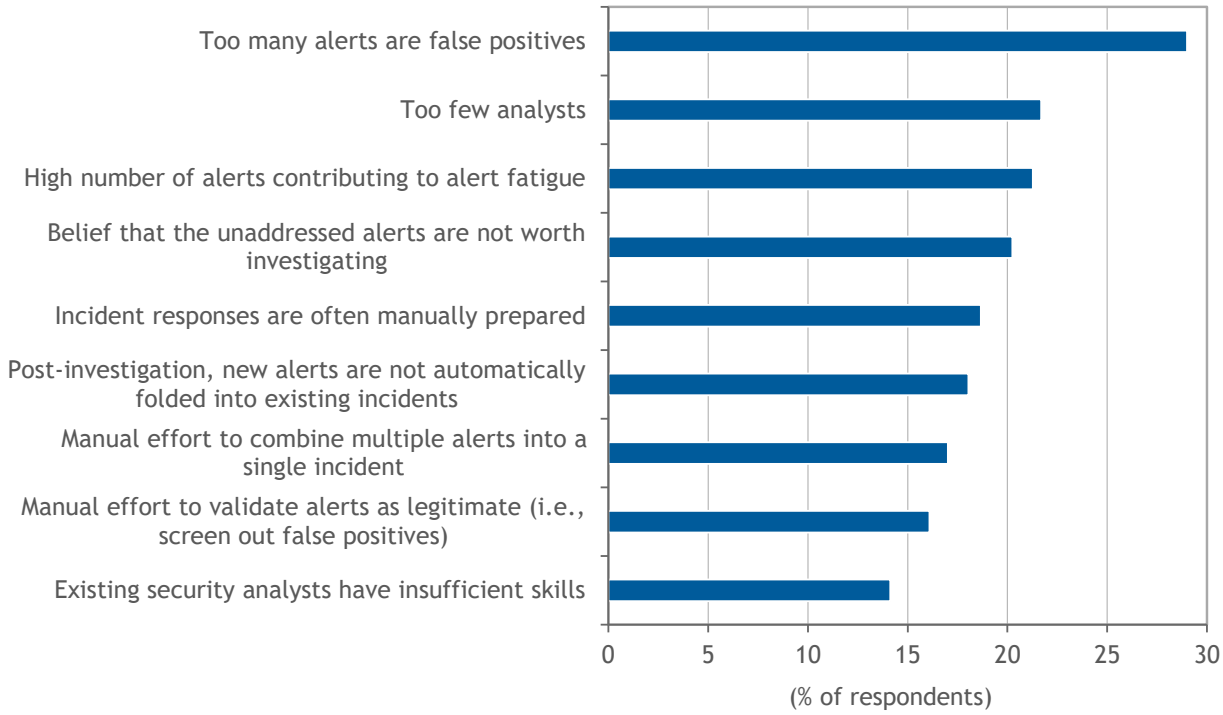
We mentioned the problems of new architectures, expanding surfaces, and qualified personnel. However, there is a cultural transition happening in the approach to cybersecurity that processes (and tools) are having trouble making headway against. Traditional thinking has been to add defense in depth. If there is a visibility gap between machines or zones, simply add another firewall. If an IT team needs more control, just drop another agent on a machine. Naturally, data is its own discrete problem, so products offering better data loss prevention with encryption are then deployed.

The problem is that with each additional tool, there is a direct correlation between the number of tools deployed and the number of false positives or redundant alerts. There are also more silos of alerts that need to be connected in order to respond in an informed manner. Perhaps it is not surprising that security teams cannot throw brute force at *all* the alerts and are challenged to prioritize the alerts they have. IDC's December 2020 *EDR and XDR Survey* shows the reasons organizations do not respond to all alerts (see Figure 1).

FIGURE 1

Reasons Organizations Do Not Respond to All Suspicious Alerts

Q. What is preventing your organization from investigating and responding to all suspicious alerts each week?



n = 359

Base = respondents who indicated that there were organization alerts uninvestigated each week

Source: IDC's *EDR and XDR Survey,* December 2020

For the moment, let's keep the results of this survey on the backburner. When security teams have inefficiencies (or, more dramatically stated, lose confidence), there are several long-tailed consequences. IDC studies have found:

- 18% of alerts are not investigated *at all.*
- After a tier 1 analyst determines there is suspicious threat activity, 18% of the time, the activity is formally investigated. Another 36% of the time, a security team takes 1-3 hours to investigate suspicious activities. The remaining 46% takes longer.
- Roughly 8-9% of all teams cannot investigate an alert within 24 hours.

There is no chance that organizations, on an industrywide level, sustain these numbers.

You have to walk before you can run. Let's examine the first step toward building an automation-based cybersecurity posture. Remember that while there is a longer objective in mind, SOAR tools help a cybersecurity team out of the box.

The Stages of SOAR

Beginner SOAR

Literally in the last year, SOAR platforms have become accessible to businesses of all sizes and to security teams with varying levels of expertise. SOAR platforms are still available as on-premises enterprise licenses but are also conveniently cloud-based SaaS applications. The migration to cloud-based, SaaS-based SOAR holds additional promise as new user groups can be included and updated playbooks can be pushed dynamically from SOAR vendors to its clients. If a business so chooses, there are no practical limits to the scripts that it can develop or the number of administrators that can utilize the platform. In most cases, businesses using SOAR can buy modules for ransomware, threat intelligence feeds, or risk assessment. However, because platforms are extensible, developers can build customized use cases while not adding costs to the contract with their SOAR provider.

The first integration deployment note about SOAR is an important reminder about cybersecurity in general — a SOAR platform will ultimately be as effective as the greater cybersecurity posture an organization takes. It is up to the organization to determine how it uses SOAR and, in turn, how useful it is to the organization.

The next point is perhaps allegorical. A business deploying a SOAR should talk to its stakeholders and decide its most urgent needs. Ultimately, the SOAR will influence the entire incident detection and response kill chain. However, in the beginning, a company may want to deploy playbooks that have the greatest potential to improve analyst efficiency, have better case management, or reduce man-hours to investigate incidents.

The term for assembling information when investigating alerts is called *triage.* Triage is difficult to do. There may be any number of indicators of compromise detected within a security setting. An alert simply suggests that something is wrong. What turns an alert into an incident worth investigating occurs when several amounts of information are compiled and observed:

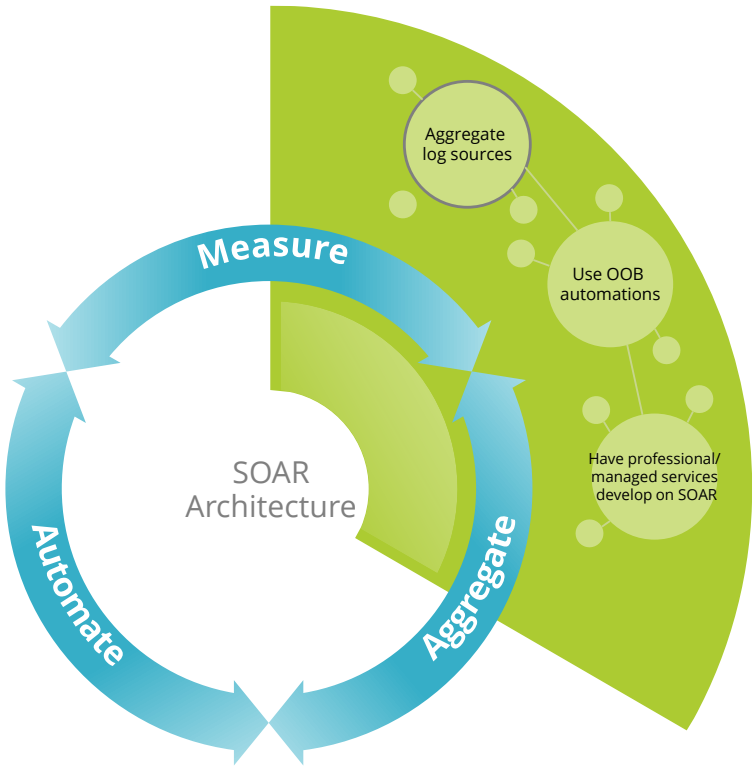
- How can we identify whether the anomaly is a security incident, a false positive, or a networking issue?
- Which machines and user groups are affected?
- If there is a security incident, what is going on (file extrusion, file manipulation, data theft to add from the network, etc.)?
- What is the timeline of events leading to the incident?
- Is there malware associated with the incident, and what can we do to stop the action?

Gathering this triage is often time consuming. By chaining alerts together, the SOAR platform can greatly truncate this process. (Note, the triage process becomes easier as the user builds automations and the platform "learns" the network and the workflows.)

Figure 2 shows the beginner SOAR automation stages.

FIGURE 2

Beginner SOAR



Source: IDC, 2021

The first step in standing up a successful SOAR is to perform log aggregation to know where data is located and what the data sources are and then collect data centrally. Once the logs are collected, an organization will be able to determine which alerts are taking an inordinate amount of the security team's time. It can start to automate the responses to alerts from a single source for an immediate impact. As it becomes comfortable with SOAR, additional categories of alerts provide an easy path to further automation. There will be time to review and tune SIEM rules once playbooks are in place, maximizing the SIEM's ability to detect and alert on the correct events minimizing false positives.

Automating the alerts that generate the most noise relieves the SOC of some basic repetitive tasks, giving security teams time to investigate the more serious incidents. The following is the tactic that Palo Alto Networks used internally:

> We first came up with a priority escalation workflow, making sure that all of the data that we were pulling in was standardized in terms of a mapping and layout perspective, because when you are first implementing a SOAR product, for the first two to three months, it's mostly to be used as a ticketing tool so you want to make sure that you have that usability perspective ready for the end analyst. – Elle So, staff security engineer, Palo Alto Networks

Another smart onboarding activity is to use out-of-the-box playbooks. In the early versions of SOAR, the platforms started with automations for basic tasks, but playbooks have grown in scope to enable much greater automation with more integrations. Over time, the platforms themselves have become easier to use with more playbooks included out of the box, such as directing investigations and ranking alerts. Out-of-the-box playbooks are the first and most important way for analysts to interface with the software.

After taking advantage of the out-of-the-box playbooks and those offered by the SOAR community as much as possible, organizations may use either managed services or premium customer support to develop playbooks for their use.

As the analysts build confidence with the prebuilt playbooks, they should begin to develop their own automations. All of these API-rich and script-heavy playbooks are designed so that analysts can build their own processes using low code or no code. Analysts should use the platform with the objective of automating manual tasks that they would like to eliminate. Schlumberger, for instance, started small by identifying minor things like phishing and a response that could be automated and removed from analyst workloads. Other relatively simple use cases are where automation can connect IT and SecOps user groups for use cases such as active directory and password reset.

Intermediate SOAR

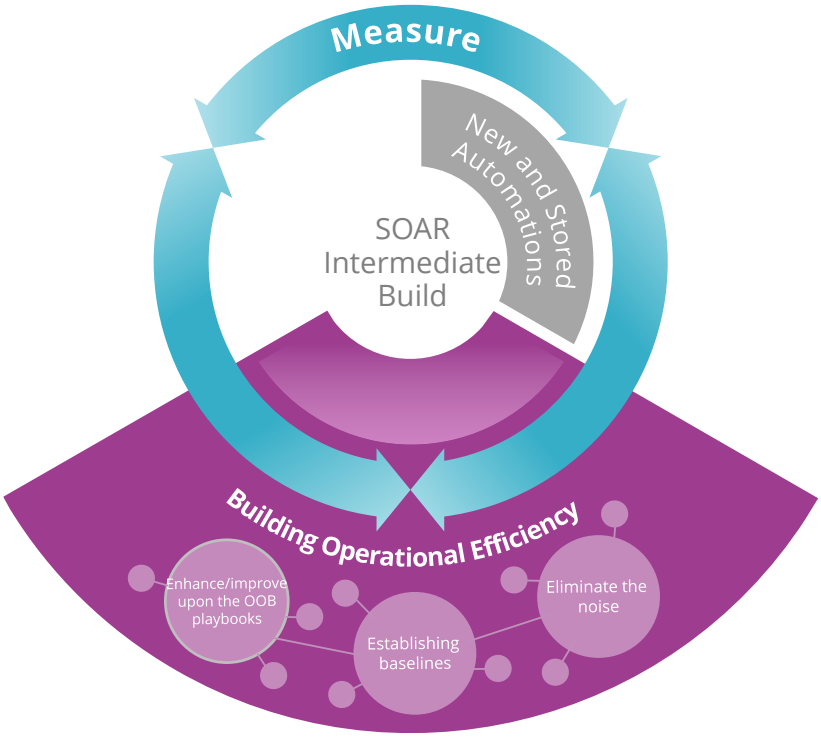
SOAR contains an archive of past incidents that can be queried to show what was previously done. Analysts may collaborate on investigations with all handoffs recorded in the SOAR. The SOAR platform is complementary to the SIEM, able to take the data flowing into the SIEM, enriching the data, and correlating the data to deduplicate alerts, combining multiple alerts into a single incident (see Figure 3):

> Alerts are correlated and enriched in the SIEM, which held everything in the beginning. All network and endpoint logs are fed into the SIEM and aggregated into the SOAR, with analysts consuming data in the console of the SOAR tool. — Diego Santana, cybersecurity operations center manager, Schlumberger

While SIEM and SOAR go well together, SOAR can be a strong complementary tool for endpoint security products, data security, next-generation firewalls, and identity and access management tools. Understand that a proper SOAR tool can not only enhance and contextualize the alerts from disparate security tools but also refine these alerts to reduce the incidents to a "single version of truth."

FIGURE 3

Intermediate SOAR



Source: IDC, 2021

The second effective strategy is to establish a statistical baseline of activities and of performance. Along the lines of collecting multiple sources of data, understanding what is a conceptual "normal" is helpful. In fairness, the SOAR platform is doing this for you dynamically.

Automating to create connectivity fabrics, eliminate noise, consolidate triage, and assign workflows is the smartest way to realize the benefits of SOAR. At this point, it makes sense to address the "response" element in SOAR. The proper response truncates man-hours in the SOC, which Schlumberger discovered:

> About two years ago, Schlumberger had 50-60 runbooks, which has more than doubled since then. Each has a new version and release with continuous review to evolve them. As analysts get better at solving an alert, they build the learning back into the runbook. – Diego Santana, cybersecurity operations center manager, Schlumberger

At this stage, organizations should be adjusting already developed playbooks to their own needs, tweaking them to best suit their products and workflows. The SOAR community and vendor training programs will help analysts learn how to make changes. One security analyst on the team may be

tasked with being an automation champion with a focus on understanding current processes and working with colleagues to best understand where to automate next.

Automated workflows do not need to be built from the ground up; security teams should take advantage of what is already written for the organization's environment. Existing simple automations may be layered into more complex automations so there is no need to start writing each automation from scratch.

The Transition

Pragmatism wins the day. Committing to automation is not just a matter of technology, it becomes a mindset. The shortage of security analysts helps with the mindset since there are not enough people to do all that needs to be accomplished to secure the organization. IDC spoke to several companies, and the following are tactics and attitudes that various companies developed to make greater use of orchestration and automation toolsets:

- **Palo Alto Networks.** Even before Palo Alto Networks acquired and assimilated Demisto, it knew that its internal SOC needed to be highly automated. Palo Alto Networks reconstructed its SOC personnel to include two automation specialists. Predictably, the first automations were not splashy, but in the process, the Palo Alto Networks' SOC began to create better alert enrichments, eliminate its noisiest alerts, and then build stronger and more use case–driven playbooks.
- **Schlumberger.** It was a three-year process of moving to its next-gen security SOC. The planning had to be managed around people, processes, and tools.
- **A lending institution.** The director of security wanted to get rid of the concept of a tier 1 analyst doing enrichment and triage, automating the Level 1 SOC team. The company's goal was to have its analysts essentially be super analysts who focus on cases where there is not a clear playbook on how to respond to a ticket. The value for the platform was that it could take an incident to the level of automation. Still there remained incidents where an analyst needed to apply some human intuition and judgment.
- **A multinational IT solutions company.** One goal was to get useful results when it hired new security personnel. Internally, the company observed that it typically took three to six months to train new analysts on security operations, and it could be much longer before they delivered the value of a more seasoned analyst. With automation, training time was brought down to just four to six weeks. In addition, automated playbooks ensured consistency, so new analysts can act to the same standards as more experienced SOC experts.

To be certain, SOAR platforms, like counterparts SIEM, endpoint detection and response, firewalls, and many other security tools, are impressive engineering achievements. Remember, though, that the efficiency of a SOC is the sum of doing many little things well. Time saved in enriching data allows analysts to act on existing alerts faster and frees them up to look at new incidents. Automated processes reduce the time spent in generating the proper remediation.

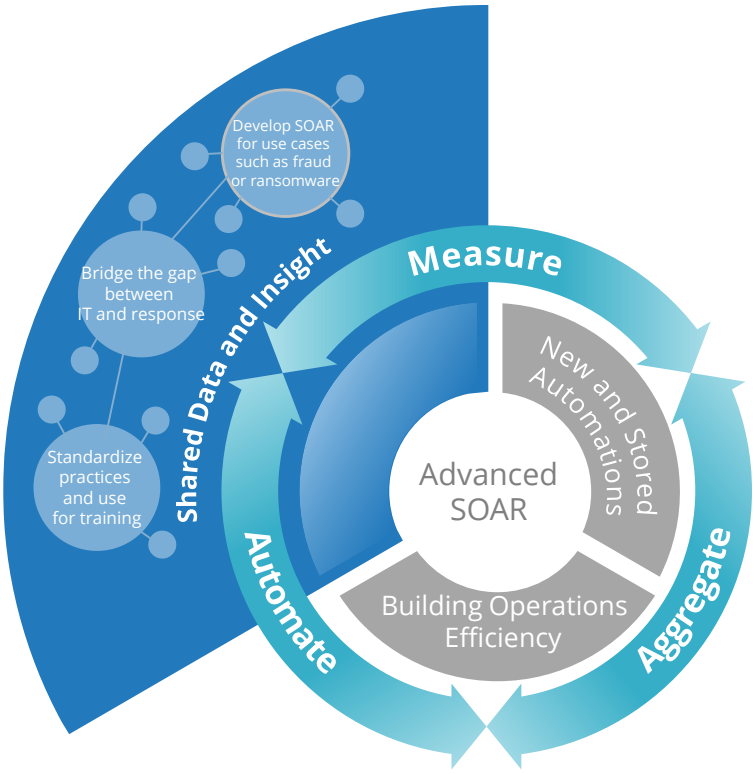
A not-so-small benefit to an automated SOC is that it helps negate burnout. An analyst would often flip through screens and pair time event logs with time stamps and then investigate threat intelligence feeds. When the most onerous manual tasks in the SOC are absorbed in automation, analyst fatigue diminishes and job satisfaction increases.

Advanced SOAR

Make no mistake, if push comes to shove, companies with a security team and even smaller teams are buying tools and creating processes to drive better outcomes. In fact, that is what the fruition of SOAR is (see Figure 4).

FIGURE 4

Advanced SOAR



Source: IDC, 2021

Cybersecurity may be the synthesis of art and science, but ultimately, the sanest approach is to measure what can be measured in the SOC. The most common measures in the SOC are mean time to detect (MTTD), mean time to respond (MTTR), and tickets processed. A properly tooled SOAR provides these measurements of SOC performance. Worth noting, SOAR is an iterative process. The longer the SOAR platform is in place, the more time it has to improve its machine learning algorithms around how to handle incidents, from assigning them to analysts to helping create playbooks.

Another aspect of SOAR is how it facilitates the "fusion center." In large organizations, the SOAR can bridge multiple teams in an organization such as the security team, the IT operations team, the cloud operations team, and the network operations team. For smaller teams, it can bind generalists that pass workloads onto another. In either event, collaboration tools within the SOAR make it easy for the teams to communicate without needing to fire off emails. The context of an alert and all the information relating to an incident and its remediation can be contained within the message.

Quick and actionable response is the most desired outcome in a SOC. There are temporary tactics that can be used to "stop the bleeding" such as quarantining the affected endpoint or revising a firewall rule. The faster this can be done, clearly the better. A more explicit idea of the time savings that can be generated in the SOC by the strategic use of SOAR is provided by Palo Alto Networks:

> The methodology behind automation is we try to automate 70% of every workflow that comes in, so we are automating up to a decision point. For example, with priority escalation, automation is pulling all the data, making sure to enrich all of it and then presenting it to the user with some sort of recommendation. However, that is why we are paying an analyst to manually look over it and use their expertise to decide what type of remediation action should take place. Once that decision point is reached and they have come to a conclusion, we abstract out the actual remediation portion via XSOAR automations as well … we have that decision point where analysts will look at it, hopefully they spend 10-30 minutes doing their investigation based off the data we already provided them, and *then click a button and the system performs whatever remediation action they requested*. — Elle So, staff security engineer, Palo Alto Networks

The SOAR platform may also be used outside of protection and defense-specific tasks. Automation workflows can help train security analysts on how to handle incidents that show up in their queue. The process of automation helps security teams develop a consistent method of working to guide the team in its workflows, helping with both automated and nonautomated processes. Mapping to the MITRE ATT&CK framework helps develop this consistency in building disciplined processes. Workflows may also be set up in the SOAR platform to help with human resources tasks such as user onboarding and offboarding. Again, many of the companies using SOAR reported tangible results:

- **The multinational IT solutions company.** Before implementing automation, MTTR was 4–24 hours, even for a Level 1 incident. With automated playbooks, MTTR numbers have gone down dramatically — often including real-time response.
- **Schlumberger.** The company demonstrated its ROI with SOAR, increasing its SOC performance as the number of incidents per month grew by five times, meaning 20% of the workload is being automated.
- **The lending institution.** When someone applies for a loan, the customer experience matters, and fraud issues can make it harder. A breach of information is a compliance issue as well. By reducing mean time to respond to these incidents, the organization has more available resources to dedicate to preserving a trusted relationship with customers. The lending institution estimates that it takes half the time to investigate a fraud incident now than when it had a less automated response strategy. It built customized workflows tying its own internal tooling with credit rating agencies and third-party software detection platforms to detect and respond to fraud. The in-house Python libraries make it possible to create integrations and build case-specific playbooks extending the value of SOAR.

In 2021, it really is not enough to have a reactive and defensive posture. Security teams should try to spend more time in threat hunting and less time in remediation. A SOAR platform can help with threat hunting by freeing up SOC analyst time for the task as well as providing playbooks for threat hunting exercises. Palo Alto Networks has been able to formally automate the assignment and track threat hunting exercises in the current construct of its SOC. It instituted a threat hunting program where it can assign hunting tickets to analysts on Monday and create a Friday due date. It found that SOAR playbooks and automation were robust enough that it could use the platform to determine which hunts have been valuable with metrics calculated in the SOAR.

There is another outcome when a SOAR is fully utilized. First, all of the analysts that use the platform investigate incidents in a more uniform fashion, making the SOC more efficient. The transition to more skilled threat hunters is more refined and more consistent. Second, the SOAR is something of a teacher; new analysts can use existing playbooks to uplevel their skill sets.

CONCLUSION

Security orchestration and automation are not "nice to have" concepts in a healthy cybersecurity posture — they are now "need to have." The sophistication of the adversary requires the most rapid response possible. New security surfaces and a more remote workforce require new observability and connectivity fabrics. The SOC analyst is subject to burnout, and automating as many repetitive tasks as possible while empowering them to make decisions instead of just gathering data will make for a more dynamic work environment.

It is also possible that the road to automated processes holds value as much as the fruition of the journey. By committing to automation, a company considers what processes need to be harmonized and made more consistent. Last, the SOAR platform enables security teams to build use cases that integrate different assets of identity, IT platforms, and security point products for better data enrichment and streamlined workflows. The dream of breaking down the silo between IT and security is more fully realized by the strategic use of a SOAR platform.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com