SANS | Research Program

Survey

The State of Automation in Security Operations: A SANS Survey

Written by **Mark Orlando**

June 2024

CORTEX
BY PALO ALTO NETWORKS

Introduction

As security operations centers (SOCs) evolve as a set of continuous detection and response capabilities, so too does the volume of data and number of operational tasks included in SOC charters. This expanding scope and increase in workload have necessitated a variety of automation solutions such as security orchestration, automation, and response (SOAR) platforms; custom tools; and, more recently, artificial intelligence to help limited staff scale their expertise. Although automation has long held the promise of increasing SOC capacity and expertise without increasing staffing levels, many teams struggle to realize this benefit even after investing in SOC automation.

The SANS Institute conducted this State of Automation in Security Operations survey to better understand automation use cases, benefits, and priorities, and to explore ongoing challenges in realizing the benefits of automation in security operations. In this paper, we share the results of our survey and highlight important takeaways such as key drivers of automation in security teams, the role of automation in security operations functions and team collaboration, and ongoing barriers to realizing the full potential of automated security workflows.

Key Takeaways:

- **Cybersecurity spending may be slowing, but security operations scope continues to grow for most teams. Defending a growing and changing attack surface was cited by approximately 53% of participants as their biggest challenge, indicating an ongoing need for automation.**
- **Cost is both a significant decision criterion for automation solutions and a barrier to adoption. Approximately 47% of participants cited software costs as one of the most challenging elements for their SOAR, highlighting the importance of a robust support ecosystem and pre-built playbooks and integrations.**
- **Phishing, vulnerability response, and data enrichment are popular targets for automation, with most respondents targeting 50–75% of their incident response to be handled through automation.**
- **Engineering effort required to deploy and maintain automations is the most common challenging attribute of SOAR for approximately 68% of respondents, making ease of integration a key factor in selection of SOAR platforms.**

Demographics

Figure 1 presents survey participants and their organizations. Multiple industries represented here are subject to cybersecurity regulations, which may explain a focus on automation to improve process maturity and incident response. Similarly, most participants work at organizations with less than 1,000 employees, which suggests a need to maximize SOC capability and capacity while keeping headcount relatively low.

Top 4 Industries Represented

- Technology
- Government
- Cybersecurity
- Banking and finance

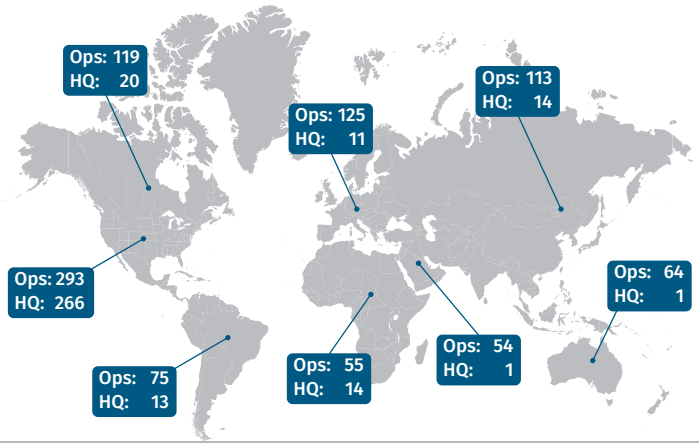
Each gear represents 5 respondents.

Organizational Size

- **Small** (Up to 1,000)
- **Small/Medium** (1,001–5,000)
- **Medium** (5,001–15,000)
- **Medium/Large** (15,001–50,000)
- **Large** (More than 50,000)

Each building represents 10 respondents.

Operations and Headquarters



Top 4 Roles Represented

- Security administrator/ security analyst
- Security manager or director
- SOC analyst
- Security architect

Each person represents 5 respondents.

Figure 1. Key Demographic Information

Background

We asked participants a series of questions about their own environments, SOC challenges, plans for automation, and barriers to automating SOC functions such as detection and response. The results of our survey offer insights into decisions and challenges faced by organizations looking to automate security functions. With so many industries and geographies represented, we encourage you to consider these insights in the context of your own organization. Surveys are invaluable reference documents in predicting outcomes and obstacles in implementing organizational changes, particularly when budgets and capacity must be used judiciously.

Automation is not a tool or technology or even a single initiative; it is an approach to process improvement in which an operation may be completed with little or no input from the operator. In the SOC, these improvements may be achieved by automating operations at a team level or user level, and that automation may take one or more forms:[1]

- *Externally maintained, system-specific automation*, such as a local script running in a user's home directory
- *Externally maintained generic automation*, such as a centrally hosted script or automated playbook in a SOAR platform
- *Internally maintained, system-specific automation*, where a product ships with its own automation features such as endpoint detection and response (EDR) with automated remediation capabilities
- *Fully autonomous systems* that require no human interaction to perform a task or workflow

Just as there is no single solution for cyber defense, there is no single correct method of automating defensive tasks. As Charles Kettering once said, "A problem well stated is a problem half solved."[2] In this survey, we have attempted to better understand "the problem" as it relates to automating SOC functions.

[1] "The Evolution of Automation at Google," https://sre.google/sre-book/automation-at-google/

[2] Charles Kettering was the head of research at General Motors from 1920 to 1947.

Security Operations Challenges

Monitoring security across a growing and changing attack surface was cited as the most significant security operations challenge by approximately 53% of participants (see Figure 2). This response tracks with the significant technological and organizational changes brought on by the COVID-19 pandemic and various IT transformation initiatives underway in many organizations. Other challenges at the top of the list were making time for process improvements and automation, detecting and responding to incidents in a timely manner, and keeping up with the volume of security alerts. Participants also cited operationalizing cyber threat intelligence, maintaining consistent processes across staff and/or shifts, and lack of visibility and unified security analytics as areas of potential improvement. Notably, the lack of visibility cited by approximately 21% of participants focused on cloud-based workloads, applications, and SaaS infrastructure. The cloud theme emerges again when participants list cloud security issues as among the most time-consuming alert types to resolve.

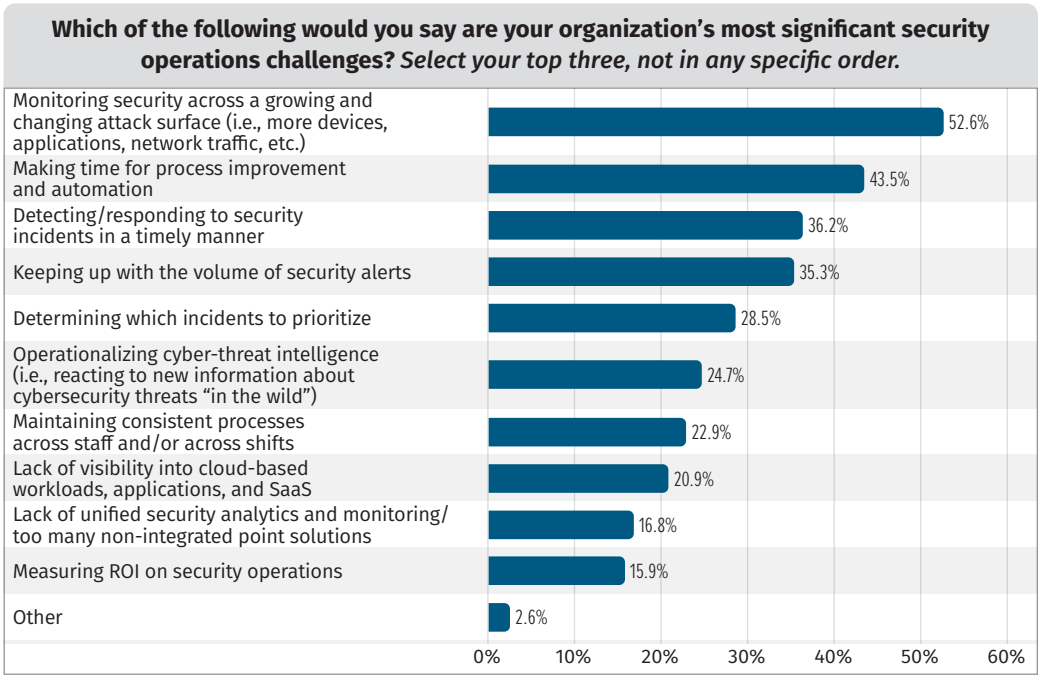


Figure 2. Most Significant Security Operations Challenges

Big Toolsets, Bigger Scopes, Limited Resources

Integration of features and data across security tools continues to be important among most teams. As shown in Figure 3, approximately 59% of organizations participating in the survey use more than 10 security tools. More security tools means more effort required to perform analysis and response across datasets and interfaces, which increases the likelihood of delayed response times or defects in the response process. Utilizing these toolsets might be a more urgent challenge in 2024 and beyond as budgets become tighter.

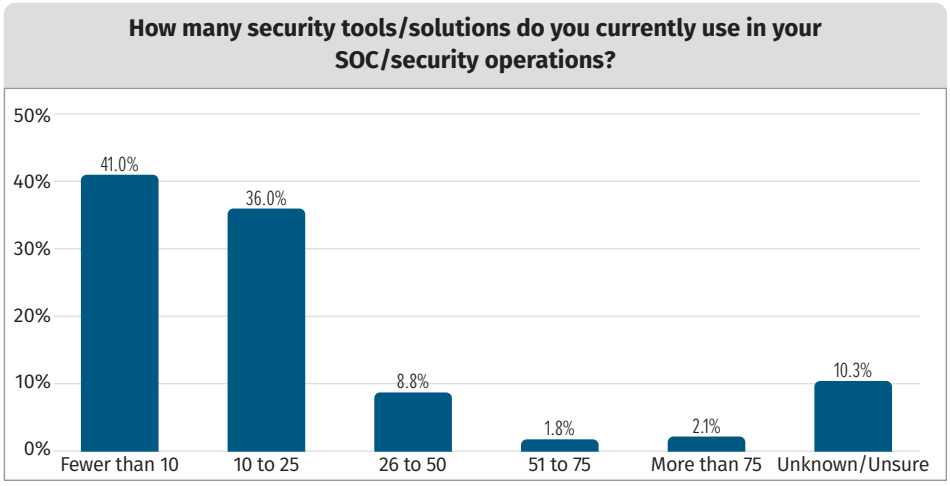


Figure 3. Number of Security Tools and/or Solutions Currently Used in SOC/Security Operations

Research published last year by the Institute for Applied Network Security and Artico Search found that security spending slowed in 2023, with more than 33% of organizations freezing or reducing their annual cybersecurity budgets.[3] Survey participants also cited total cost of ownership as a key factor in selecting automation solutions and a major barrier to implementing automation products.

In any case, the scope of the average SOC has not experienced any such reduction, as echoed in responses regarding major security challenges. It seems clear that the expectation continues to be that security teams do more with less. We might conclude that the need for automation is stronger than ever, but that those automation solutions must provide the right features, the right support, and enough pre-built content and integrations so as to demonstrate clear value. Because making time for process improvements is also a significant challenge for SOC teams, organizations should consider dedicated resources outside of detection and response staff to deploy and maintain much-needed automation.

In Alerts and Investigations, Context Is Key

When asked which alert types take the longest to triage and investigate, matches to indicators of compromise (IOCs) ranked the highest with approximately 37% of responses. These answers underscore the frustration felt by SOC teams investigating IOC-based alerts with little or no context and often with few actionable conclusions. Cloud service provider alerts, network security alerts, and identity/authentication alerts rounded out the top of the list from most to least time-consuming. It is notable that the most popular security operations challenge cited by participants was defending a changing and growing attack surface. We might infer that a lack of asset and/or user context presents a significant challenge in alert triage that is not consistently addressed in point security tools. This might also be a good argument for SOAR solutions that incorporate threat intelligence platform (TIP) features so as to reference key contextual information in detection and response playbooks.

The most time-consuming incidents to remediate, according to survey participants, are cloud security issues followed by data exfiltration and identity attacks. The continued popularity of cloud environments and identity and access management systems as attack targets adds an urgency to these responses that demands a more rapid and efficient response.[4] Many SOC teams have had cloud infrastructure added to their detection and response scope without sufficient training, visibility, or context to make sense of the alerts they see. Similarly, SOC teams may still struggle to collect and interpret telemetry from enhanced identity protections whose adoption has surged in recent years.

[3] "2023 Security Budget Benchmark Summary Report," www.iansresearch.com/resources/infosec-content-downloads/detail/2023-security-budget-benchmark-summary-report (Registration required.)

[4] "M-Trends: 2024 Special Report," Mandiant, https://services.google.com/fh/files/misc/m-trends-2024.pdf

Choosing the Right Solution

When most practitioners think of security automation, they think of SOAR products (or SOAR capabilities in their toolset). But not every organization has invested in SOAR or even in premium SOAR features of their SIEM or incident management system. We wanted to understand the key drivers for automating security operations and the criteria that organizations are using to select automation platforms.

The main drivers for automating security operations functions include reducing manual tasks and other causes of burnout (around 31% of responses), scaling operations, dealing with excessive alerts, and technology consolidation. Anecdotally, participants also listed supplementing in-house knowledge, expediting incident response, and improving consistency. Here is another area where we see alert handling and incident response take center stage in automation use cases. These responses also underline the importance of automation solutions that are easy to deploy and easy to integrate with multiple point security tools and reference systems. The responses also indicate that automation solutions such as incident response may be better employed across functional teams because many of these processes are supported by multiple groups inside and outside the security operations team.

The most common criterion for selecting automation solutions to address these issues was total cost of ownership. The second most common criterion was interoperability with other tools, followed by a well-populated application/integration marketplace, prebuilt use cases or playbooks, and advanced/generative capabilities. Common themes here are speed to implementation for both platform deployment and new integrations as well as total cost of ownership.

Automation Focus Areas

Survey participants were asked which of their security operations processes they have already automated, as well as which processes they plan to automate within the next 18 months (see Figure 4). Approximately 52% of participants cited phishing response as a process they have already automated, followed by vulnerability management, data enrichment, and user onboarding and offboarding.

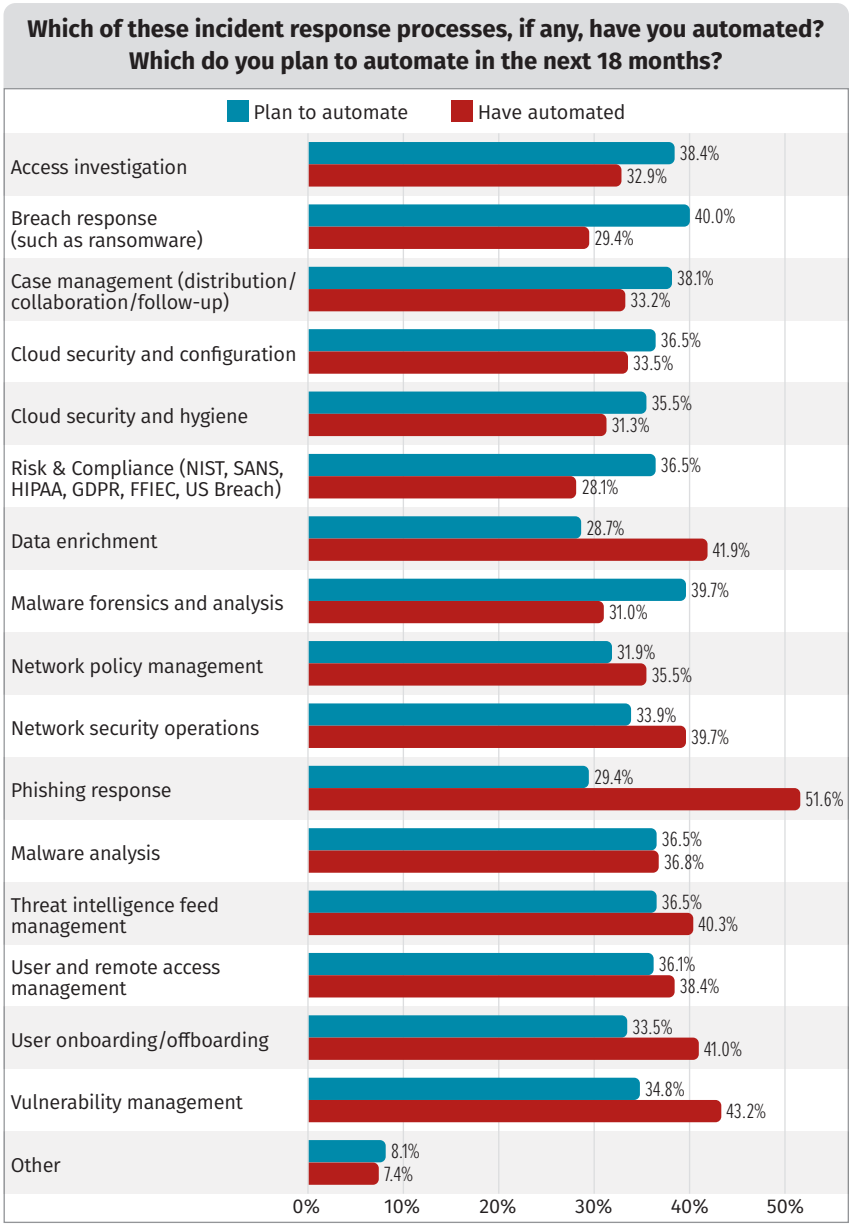


Figure 4. Incident Response Processes Already Automated and Those That Will Be Automated in the Next 18 Months

Among response processes that participants have prioritized for future automation, breach response (such as in ransomware attacks) was most referenced. Other automation priorities included malware forensics/analysis, threat intelligence, user and remote access management, case management, and cloud security and configuration. Again, we see a significant focus on detection and response, and on reducing an ever-changing (and often growing) attack surface. In the next section, we'll look at specific incident response areas cited by participants.

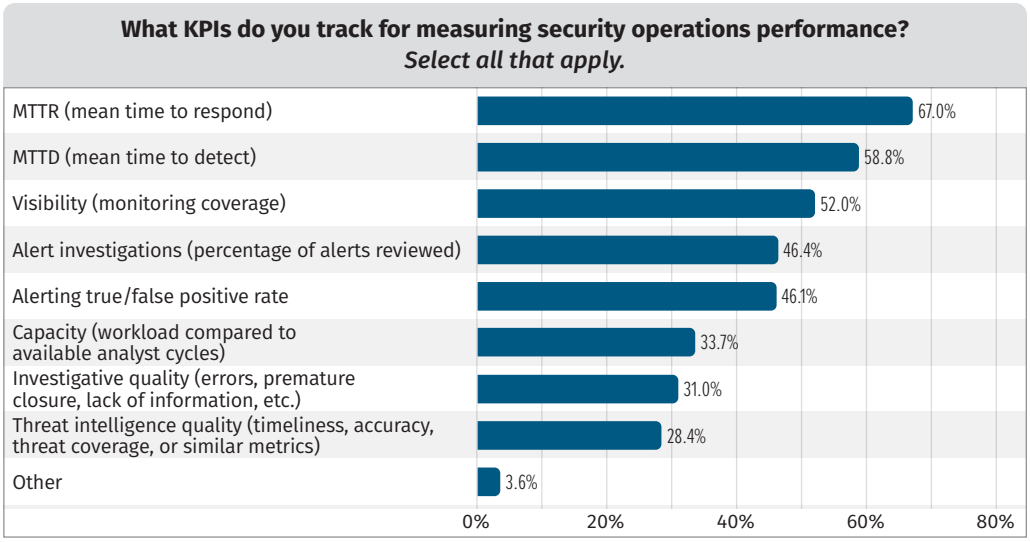


Figure 5. Key Performance Indicators Tracked to Measure Security Operations Performance

Key performance indicators (KPIs) used by participants for measuring security operations performance align closely with incident response measures (see Figure 5). Mean time to respond (MTTR), mean time to detect (MTTD), and monitoring coverage were the top three KPIs selected by respondents. Other KPIs selected by respondents included alert and investigative quality, threat intelligence quality, and team capacity. These responses reflect a focus on incident response and alerting as the primary use cases for automation, but they may also expose an opportunity to focus on more general toil reduction (manual, repetitive tasks) across all SOC functions in the future.

Despite ongoing challenges in automation response tasks, confidence in the impacts of automation remains high. Approximately 45% of participants said that they were aiming to automate responses for at least half of their incidents, and another 35% of participants expect to automate at least 75% of responses. A substantial majority of participants said they expected quicker response times with the implementation of SOAR, more time for alert investigation and/or hunting, more time for improvement initiatives, and more consistent workflows. We can conclude that although humans should remain in the loop for many of these functions, we can use automation to streamline a wide variety of processes and recoup analyst time for more creative tasks.

Automation Challenges

As Figure 6 shows, when asked about challenges in implementing automation, almost 68% of respondents pointed to the engineering effort to deploy and maintain automation. This would naturally include engineering resources and personnel costs. Other major factors included software costs, immature or poorly defined processes, and lack of interoperability with point security products. Whereas these challenges are primarily focused on practical concerns about implementation and ongoing management, the *promise* of automation appears well-understood, with fewer respondents citing lack of usability, lack of adoption, and poor visibility into automation efficiencies as challenges.

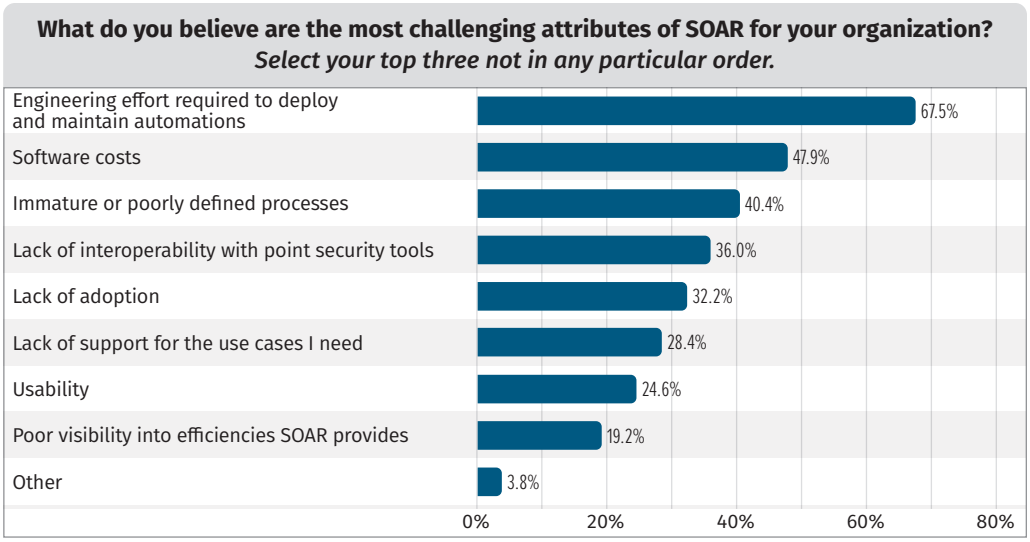


Figure 6. Most Challenging Attributes of SOAR

Cost and engineering complexity as major themes are repeated in questions about why participants may not implement automation at all, with approximately 42% of responses indicating a lack of budget and 41% citing lack of the requisite technical skills to manage automation solutions (see Figure 7). Other participants responded that their workflow needs are already largely met by SIEM products or other existing processes. Only about 29% of participants cited a lack of management support or understanding of where to start as a reason they wouldn't deploy automation in their security operations.

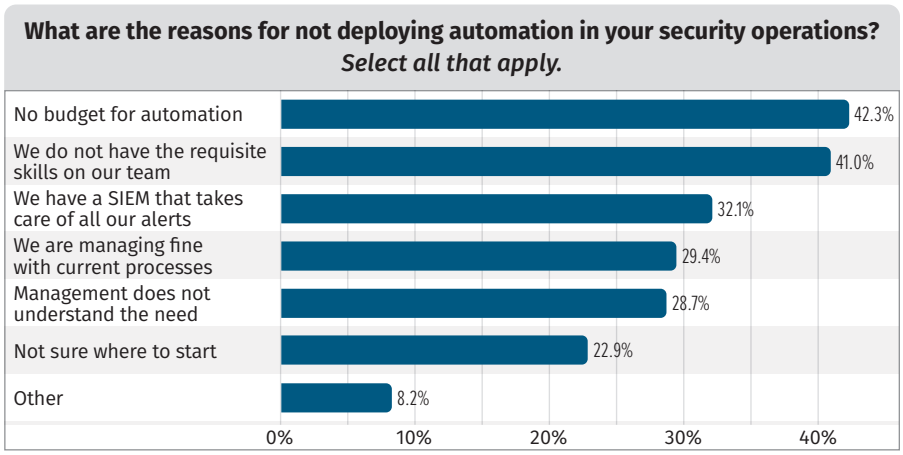


Figure 7. Reasons for Not Deploying Automation

In summary, security automation is still a growth area despite a well-understood need, management support, and measurable security gains to be had from deploying automation. In the next section, we'll consider larger trends and future considerations for security automation.

Trends and Predictions

Analysis of survey responses reveals some predictable trends and some surprising ones. Organizations have the most success automating processes that are mature and well understood, which we can observe in phishing and vulnerability responses being most improved by automated workflows. Total cost of ownership as a major consideration is also something we might have expected. At a macro level, we can discern a requirement for expert assistance via automation platforms to streamline processes and speed up response in addition to simple process automation via low code or no code means.

It seems that SOAR has not yet democratized automation as much as we might have anticipated, with cost and management complexity continuing to be a major concern for already overworked SOC teams. It is also interesting that the most popular methods of measuring automation in the SOC focus on incident response outcomes, which may also be influenced by a variety of organizational factors outside of the SOC. SOAR can help teams find efficiencies in a variety of operational tasks, but recognizing those efficiencies requires accurate metrics (i.e., measuring reduction in manual, repetitive tasks). Some teams appear to be moving in this direction with metrics on team capacity, for example. Automation solutions that can highlight improvements such as headcount reduction, fewer incidents, or quicker response times will be the most compelling for leadership looking to streamline costs.

Although we may not be able to predict cybersecurity spending with any certainty, we can guess that purchasing managers will continue to be cost-conscious when equipping their teams. We also know that the wide range of infrastructure, data, and user types in scope for SOC teams is unlikely to change anytime soon. Therefore, we can expect that SOAR platforms capable of operating across teams and offering a wide variety of analytic features are likely to be the most popular with security teams in the future. Advanced automation capabilities such as artificial intelligence, which are already starting to emerge as features in detection and response products, will help reduce the engineering effort required to define analytic logic. The challenge will be realizing the full potential of this kind of assistive or cognitive automation *without* having to burn more analyst time building playbooks or training AI models.

Transparency will be another important theme in the more streamlined, automated SOC of the future. This applies not only to AI and other automation solutions but also to the security functions we intend to automate. Measuring SOC functions is a major challenge due to the unpredictability of alerts, incidents, and special requests routed through the SOC every day. This is why human creativity and flexibility are a necessary part of standard operating procedures, but it is also why defining those procedures to the level of detail required for automation is difficult. SOAR platforms *must* provide flexible capabilities that work in tandem with humans.

Conclusions

Human judgment and decision making are cornerstones of any security operations center, but the expanding scope of services and volume of data to be reviewed make it difficult to scale that expertise. SOAR is a key component in scaling efforts to process threat intelligence, review alerts and new vulnerabilities, and respond to incidents in a more consistent and scalable way. Cost and management complexity are key considerations in selecting the right technology. As scope continues to expand and budgets tighten, finding solutions that require minimal configuration and ongoing management will be key in finally bringing automation to the forefront of security operations. However, if implemented correctly, SOAR can be a powerful ally in increasing capacity, reducing response time, and improving quality in the pursuit of a more automated SOC.

Sponsor

SANS would like to thank this paper's sponsor: