How Automation and Orchestration can Help Bridge the IT Security Skills Gap

By Paula Musich
An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report Summary
August 2020

Sponsored by:

SWIMLANE

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

How Automation and Orchestration can Help Bridge the IT Security Skills Gap

Executive Summary

The shortage of skilled information security practitioners continues to grow around the globe. In the US, for organizations with at least 500 employees, Enterprise Management Associates found in a June 2020 survey that the average number of open positions enterprises are trying to fill is 1,324. For the largest percentage of respondents in this EMA survey, that number increased between 1% and 25% over the last year, although that increase is higher for large enterprises.

With the unemployment rate for skilled IT security practitioners at zero, it's no surprise turnover is a significant issue for many, but especially for midmarket organizations with 500 to 999 employees, with the largest percentage of those seeing annual turnover rates of between 20% to 30%. On the bright side, midmarket companies and very large enterprises are not seeing an increase in the amount of time it takes to replace lost expertise. On the not-so-bright side, the struggle to attract and retain cybersecurity talent increases the amount of time it takes to remediate a threat, and large enterprises are unable to adequately manage all the security tools they use.

It's not surprising, then, that automation within security tools has become a major selection criterion in adopting new tools or replacing existing ones for 98% of all respondents. Among 13 different classes of security tools in use, those that respondents indicated gave their organizations the biggest productivity boost include IDS/IPS, digital threat intelligence management, and deception technology. Security orchestration, automation, and response (SOAR) platforms dedicated to streamlining security threat and risk management workflows were ranked somewhere in the middle, most likely because of the level of effort required to operationalize them.

Which of 15 discrete security-related activities offers the greatest productivity improvements with automation? It varies according to the size of the organization. Automating ticket/incident/case tracking initiation offers the greatest improvement for large enterprises with 5,000 to 19,999 employees, while small to medium enterprises (SMEs) with 1,000 to 5,000 employees saw the greatest value in automating vulnerability remediation. Midmarket organizations with 500 to 999 employees see automating patch management as offering the greatest productivity boost through automation.

The benefits that organizations enjoy as a result of security automation frequently vary by the size of the enterprise. Both very large enterprises and SMEs view the top benefit as improved protection, while midmarket companies view better compliance as the top benefit. Meanwhile, large enterprises see improved architectural resiliency as the primary benefit.

Although SOAR technology has not yet reached mainstream status in the Security Operations Center (SOC), there is great interest in it as a means to streamline workflows and improve efficiency. For prioritizing the handling of more business-critical security incidents, 83% of respondents rate SOAR technology a 1 or a 2 on a scale of 1 to 5, with 1 being the most effective. Among those using SOAR products, 30% believe it has reduced their security teams' mean time to respond to a security incident from between one to four hours down to 30 to 60 minutes. At the same time, 45% of SOAR users reported that it saved three to four hours per day per analyst.

During the global COVID-19 pandemic and the resulting widespread shift to working from home, automation became all the more important as security teams adjusted to protecting more far-flung access to corporate resources. Fifty-three percent of respondents said one result of this shift is that it has significantly increased the amount of time it takes to perform vulnerability scanning on endpoints, and another 45% said it made the process of deploying patches and updates much more difficult.

Automating Activities

There are a range of security-related activities that can be automated to some extent across multiple functions. Those include risk and vulnerability management, including patch management, incident handling or threat management, compliance management, data security, information sharing, and more. While automation levels vary according to the vendor and the technology type, organizations in general see greater value in increasing worker productivity through automation with different classes of technology. Out of 15 discrete activities carried out within most information security programs, EMA asked respondents to select the top three activities that offered the greatest value in productivity improvements made possible through automation. The answers varied to some degree by the size of the organization the respondent represented. For example, automating ticket/incident/case tracking initiation and/or updates provides the greatest value for organizations with at least 5,000 employees, while small to medium enterprises with 1,000 to 5,000 employees are seeing the greatest value in automating vulnerability remediation. Midmarket organizations with 500 to 1,000 employees see automating patch management as offering the greatest value through automation. In this case, the size of the organization really does matter, given the requirement to track hundreds of thousands of incidents or cases for the very largest enterprises. At the same time, large or very large enterprises most often charge other non-security-focused organizations with the task of managing patches, while security practitioners in smaller organizations are forced to wear many hats and take responsibility for a wider range of activities. Still, the value of automating vulnerability remediation is commonly viewed as quite high across three out of four organization sizes, with enterprises with 5,000 to 20,000 employees placing greater value on automating compliance audit scans or auto-enforcing actions based on risk or threat assessments from multiple data sources.

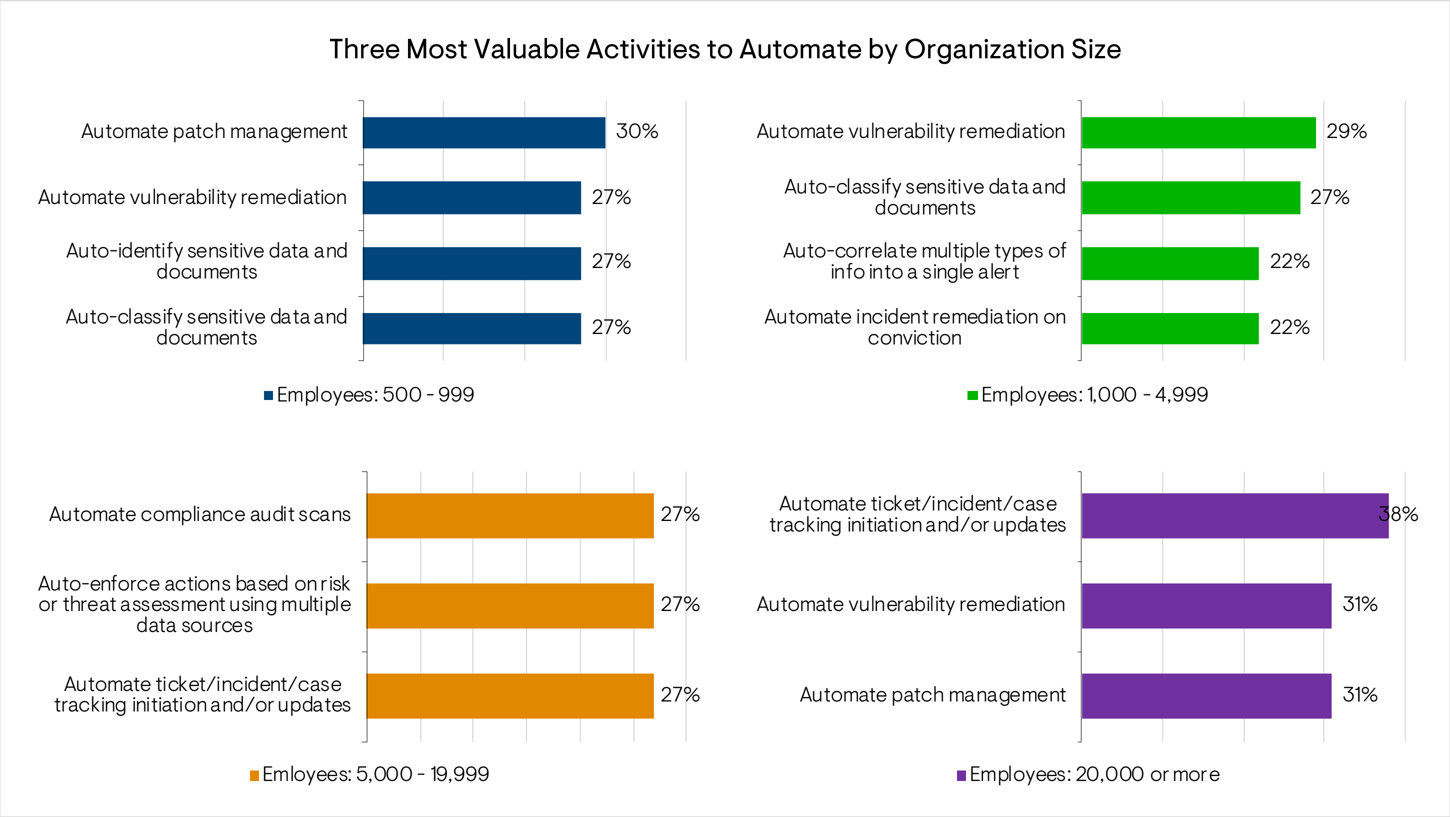


Figure 1

When it comes to threat hunting and automation, there is a range of tasks that can be fairly time-consuming to execute, especially when done manually. These tasks range from correlating threats with high-value assets and common vulnerabilities and exposures, searching the historical record of each threat within a network, reverse engineering of file-based threats, and more. The tasks that are most important to automate vary from one organization to the next, but when asked to rank 5 different activities on a scale of 1 to 5, with 1 being the most important to automate, the largest percentage of respondents selected continuous 24x7 threat hunting. On the other side of the coin, reverse engineering of file-based threats saw the smallest percentage of top ranking for priority in automation. To be fair, continuous threat hunting includes a range of activities, rather than representing a single task. At the same time, fully automating threat hunting is more of a wish than a possible reality. Automation can help a skilled security hunter more quickly find and convict an actual threat, but it still requires experience, knowledge, and good judgement to execute properly. Manually reverse engineering a file suspected of being malicious can take up precious time that many security teams don't have, and there are few options available for automating that task. For the largest percentage of respondents, it takes between 7 and 8 hours to manually reverse engineer a single file to determine whether it is malicious. This was reported by 33% of respondents, with another 27% indicating that it took five to six hours to reverse engineer a suspect file. It's likely that more organizations would attempt it if automation made the exercise faster and easier to conduct.

In the context of digital transformation initiatives and the fast-growing adoption of more modern application architectures, priorities on which threat analysis activities should be automated reflect the new requirements that come with these new ways of interacting with applications. Reliance on more traditional web application firewalls is giving way to other forms of threat analysis. For the largest percentage of respondents, the most important threat analysis activity to automate is the analysis of threats accessing software supply chain vectors, followed closely by analysis of web application file uploads.

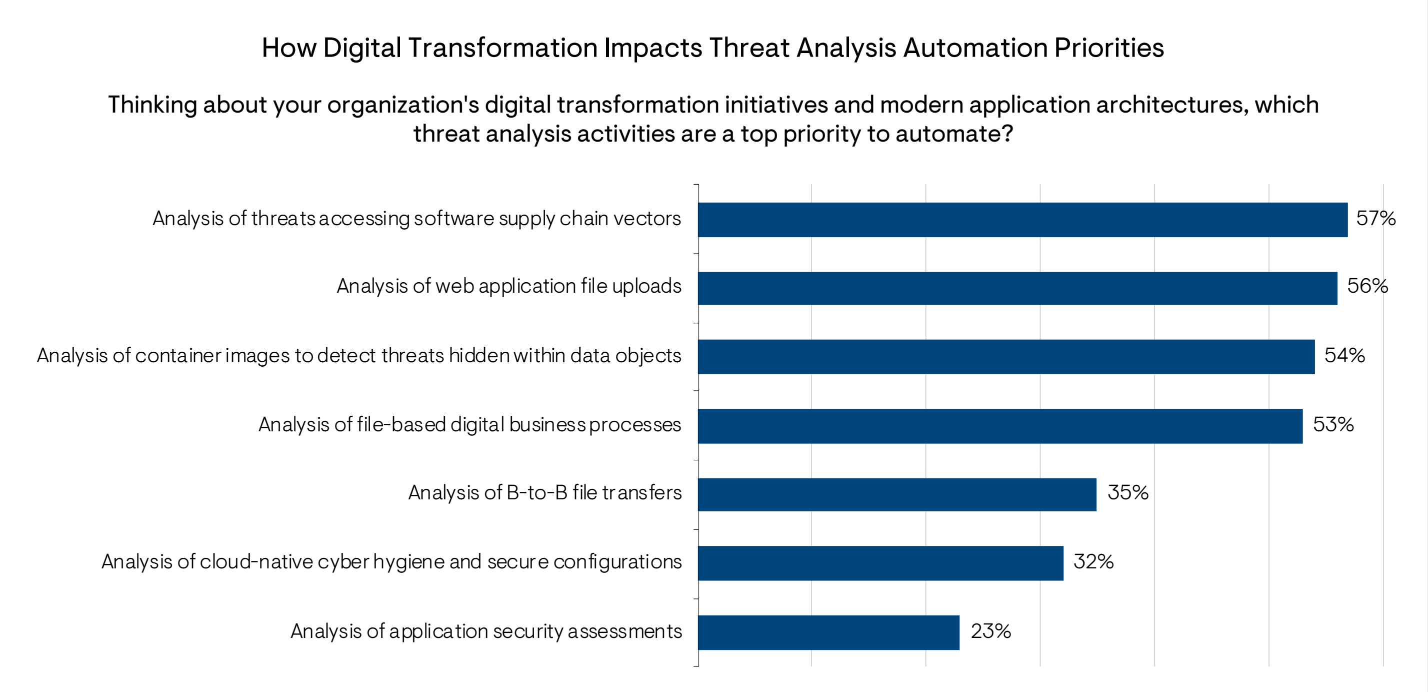


Figure 2

Benefits That Come With Automation

Beyond understanding organizational priorities around task automation, the research also sought to gain greater insights into the benefits organizations are realizing through the automation of discrete security tasks. What do organizations view as the primary benefits of automation? Of ten different benefits organizations gain, including not only better protection against threats or improved compliance but also improved security practitioner morale and application security, the top three benefits once again depended on the size of the organization. Both very large enterprises and SMEs view the top benefit as improved protection. However, midmarket respondents indicated better compliance was the top benefit their organizations enjoyed, while respondents at large enterprises cited improved architectural resiliency as the top benefit of automation. Still, better protection and improved compliance were both common benefits listed in the top three among three out of the four different organization classes. Beyond that, other benefits varied between these groups. It's clear that differently sized organizations face different challenges, and the benefits of automating security tasks vary according to those different challenges.

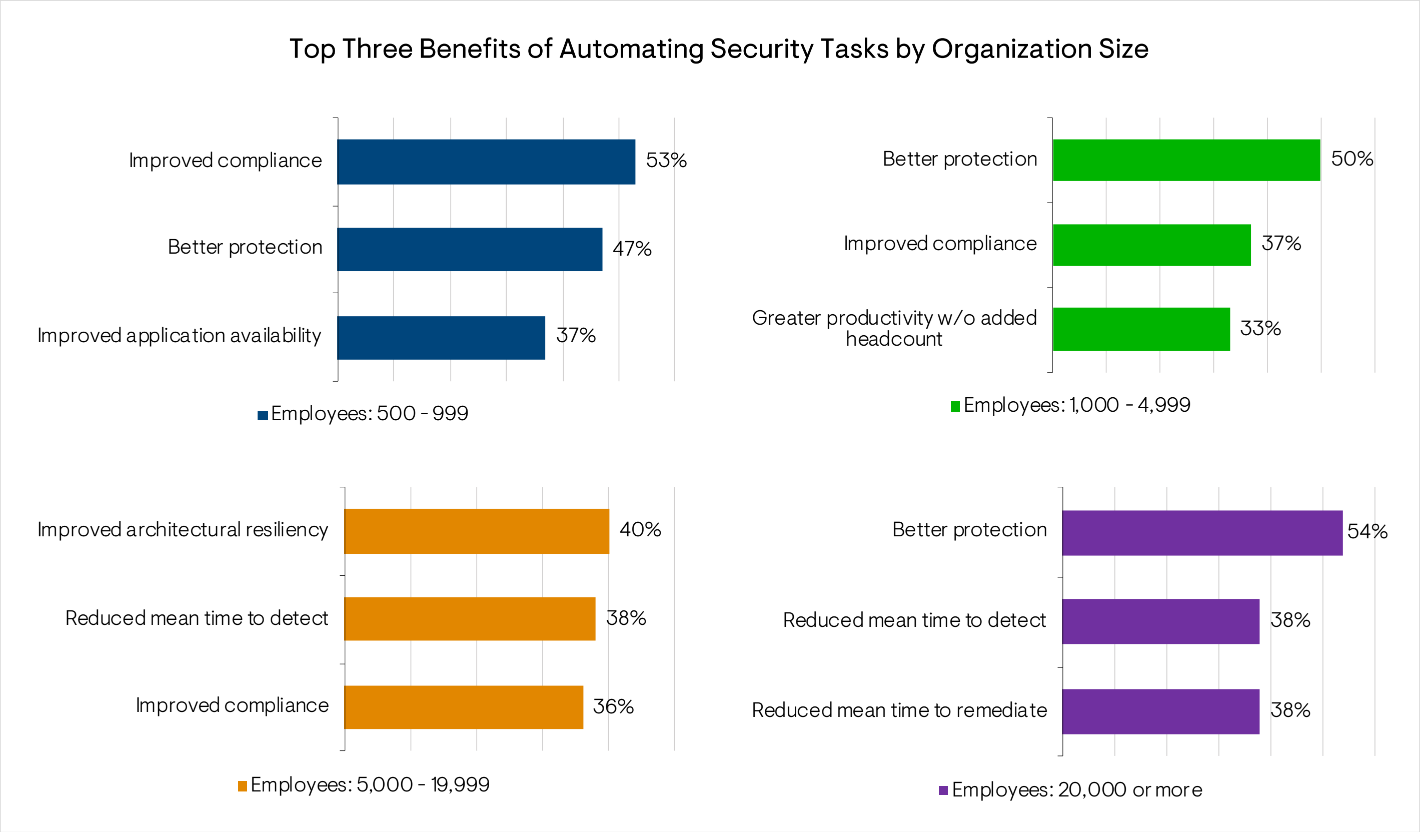

Top Three Benefits of Automating Security Tasks by Organization Size

Figure 3

Another benefit that organizations can potentially realize by leveraging automation to streamline IT security processes and procedures is to free up highly skilled security analysts to focus on more proactive or strategic initiatives that can advance the maturity and improve the security posture of their organization's digital footprint. The additional use cases on security executives' wish lists vary from one organization to the next, but there are some common themes. EMA asked respondents which use cases, if any, their organization enabled security analysts to focus on as a result of the time freed up through security automation. Not surprisingly, the top pick for the largest percentage of respondents was to focus on securing IoT devices at 62%. This was a top pick for all four organization size ranges. Just under half of all respondents also indicated their analysts were able to focus on monitoring and securing cloud workloads, which was a consistent theme across all four organization size ranges. Network traffic analysis was another priority for respondents.

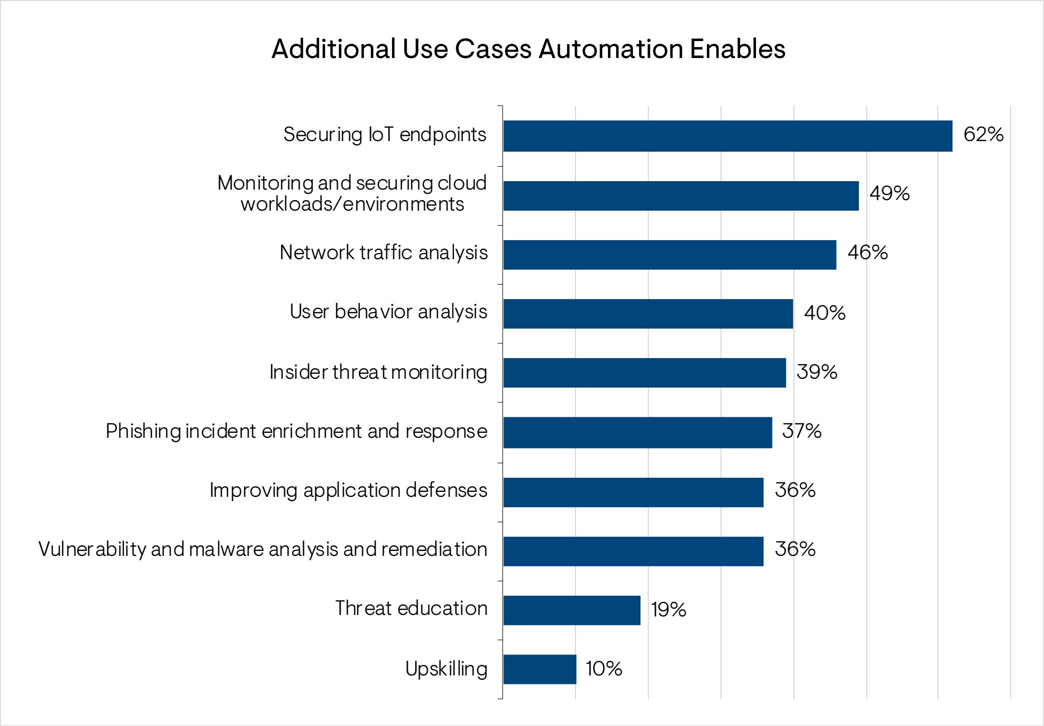


Figure 4

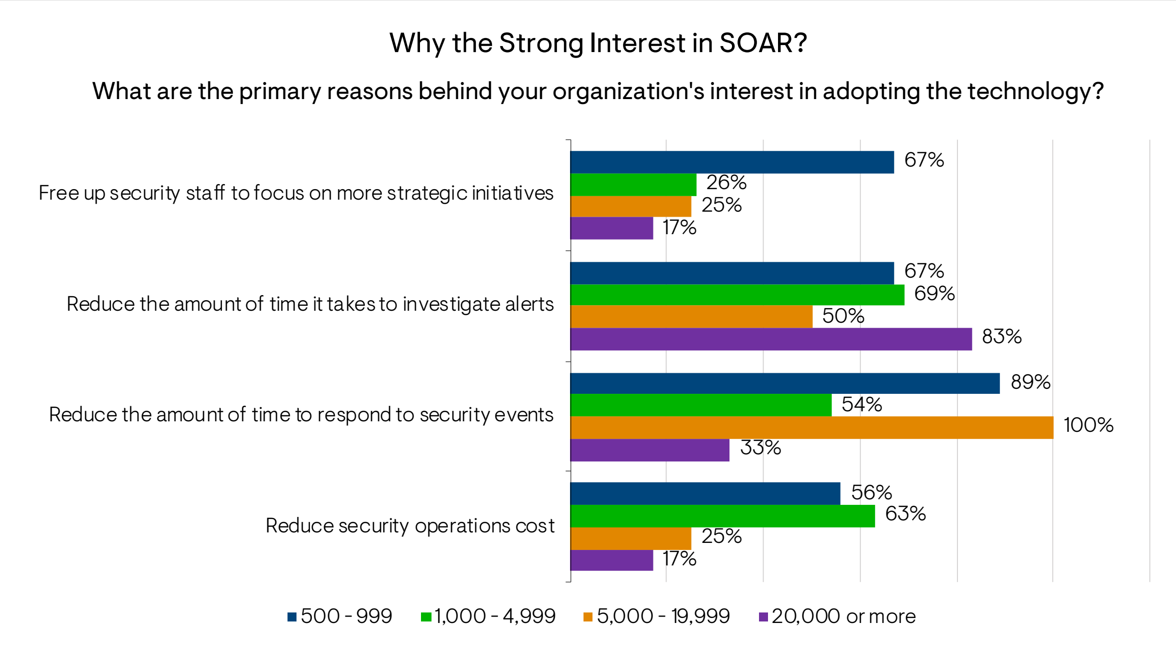
SOAR: Too Soon to Tell if it's a Silver Bullet or Something Else

The centerpiece of a growing number of organizations' efforts to streamline and mature their security programs is the use of SOAR technologies. In addition to automating task-oriented work typically done by security practitioners, SOAR products also weave together multiple automations to complete a set of tasks aimed at a particular outcome. Such orchestration relies on integrating a range of different security products or technologies. Responses such as data gathering and analysis of a detected incident are also automated. Although still relatively new in the threat management market, interest in SOAR products is quite strong. This research found that a surprisingly robust 71% of respondent organizations were already using a commercial SOAR tool. For those respondents whose organizations were not using SOAR technology, 93% said their organizations were evaluating or considering adopting SOAR products.

What's Behind the Strong Interest in SOAR?

For respondents whose organizations were looking to adopt SOAR technology, a critical selection criterion in evaluating the offerings was that it helps to ease the shortage of skilled security practitioners within their organization. For those respondents, that evaluation criterion was either important or very important.

To put a finer point on it, the research sought to understand how these potential SOAR users thought the technology might help them accomplish that goal. For the largest percentage of all those potential SOAR users, the top answer is that they were looking to reduce the amount of time it takes to investigate an alert, followed by reducing the amount of time it takes to respond to security events at 69% and 61%, respectively. It's also interesting to note that another 54% indicated that their organizations were looking to reduce the cost of their security operations. However, in looking at the motivation to potentially acquire SOAR technology according to organization size, some interesting differences in rationale came out. For literally all large enterprise respondents (and almost 90% of midmarket organizations), the primary motivation to adopt SOAR technology is to reduce the amount of time it takes to respond to security events. For SMEs, however, the top motivations were split between reducing the amount of time it takes to investigate alerts and reducing the cost of their security operations. These organizations suffer the most from the constant poaching of security expertise and struggle to keep up with their larger, more deep-pocketed rivals.


Why the Strong Interest in SOAR?

What are the primary reasons behind your organization's interest in adopting the technology?

Figure 5

Despite its status as an emerging market, there is some evidence that replacement opportunities are already starting to open up. Many of the SOAR user organizations indicated that they had a SOAR product but were also in the market for an alternative. Why? The top reason given was that their organizations acquired more than one SOAR product through a merger or acquisition and they were looking to standardize on a single product. That was especially true for respondents representing the largest organizations with over 20,000 employees, although they were a small part of the sample base. That was also the top answer given for respondents whose organizations had between 1,000 and 4,999 employees, which made up over half of all respondents. Other reasons given include the existing product not meeting requirements or missing key features.

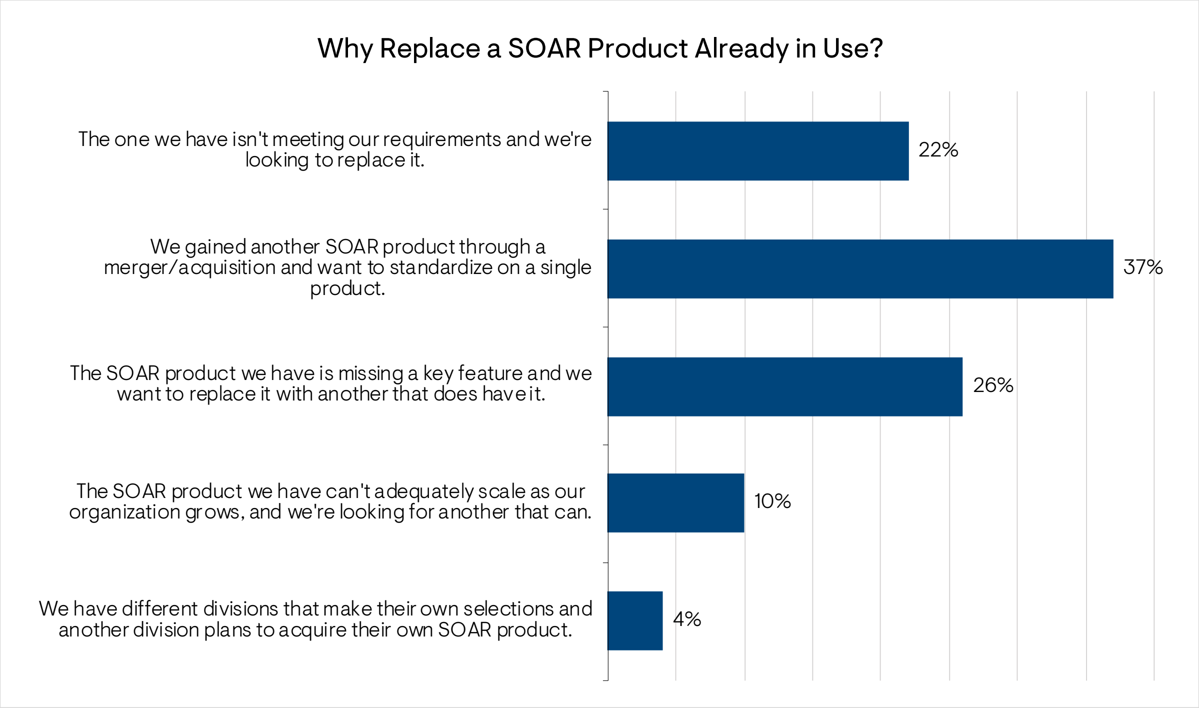


Figure 6

What's so Great About SOAR?

With a deluge of information being showered on security operations centers in the service of detecting, convicting, and remediating malicious attacks, one of the biggest struggles for security teams is determining which incidents should be prioritized. At this point in the evolution of cyber attacks, nearly all security teams believe their networks and other assets are infected with all sorts of different malware, but they want to know which ones they need to prioritize according to the level of threat they pose for the organization. EMA asked all respondents to rate the ability of security automation and orchestration technologies according to how well they think they can help security teams better prioritize handling more business-critical security incidents and/or vulnerabilities. On a scale from one to five, with one being the most effective and five being the least, 83% of respondents gave the technology a one or a two. Clearly, respondents put a great deal of faith—or hope—in the capabilities of these tools.

SOAR technology can bring greater structure and coherence to a chaotic security program and allow organizations to streamline their security operations through a wide range of functions. It allows organizations to automate manual processes, theoretically making them more efficient—that is, if the processes being automated are not in themselves broken. But which of the various features do users of the technology, as well as those evaluating it, find most compelling? To put it another way, which automation, integration, or workflow features are most promising to help reduce the most critical issues security programs face? Just over half of all respondents indicated that submitting data to threat intelligence platforms for analysis was most compelling, followed by 48% who said it was automatically quarantining infected devices. Given the speed with which attackers can strike once they've gained access to critical assets and the amount of damage they can potentially do, especially with regard to ransomware attacks, using automation to reduce the amount of time it takes to convict a suspicious file or activity and move infected devices out of harm's way is paramount. Two other top features that just under half of all respondents noted are a scripting language for custom application integration and submitting attachments to a sandbox for further analysis. With regard to the latter, 60% of large enterprise respondents indicated that was one of the most compelling features. The largest percentage of both midmarket respondents and very large enterprise respondents selected submitting data to threat intelligence platforms for analysis as one of the most compelling features, while just over half of SME respondents selected quarantining infected devices as most compelling.

Most Compelling SOAR Features

Which of the following automation, integration, and workflow features do you think could help best in reducing your information security program's most critical issues?

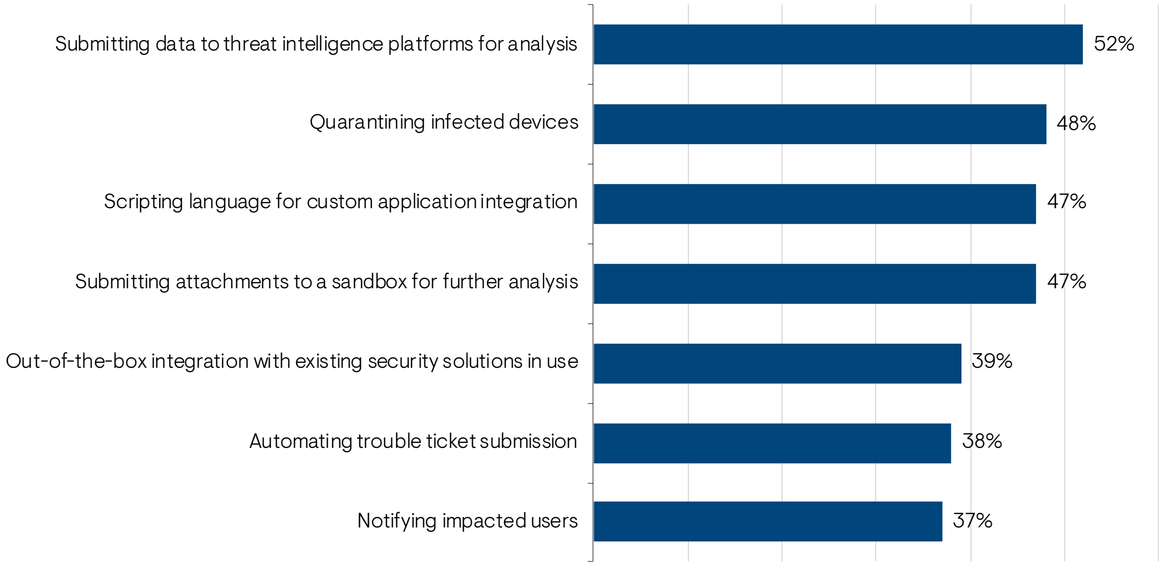


Figure 7

SOAR Proves its Worth

Two widely used metrics to determine how quickly IT security teams can identify and then shut down malware and bad actors within their infrastructure include mean time to detect and mean time to respond. The former measures the amount of time it takes to discover a potential threat. The latter measures the amount of time it takes to control, remediate, or otherwise eliminate a threat once uncovered. As security teams look to ratchet down the amount of time it takes to respond to an ever-increasing number of security events, this tried and true measurement of success can be applied to SOAR tools. To gauge how well SOAR tools score on that metric, EMA asked SOAR user respondents to estimate their MTTR before and after their organizations fully deployed their chosen SOAR solution. For the largest percentage of SOAR user respondents (30%), their security teams' MTTR was between one and four hours. After full SOAR deployment, the largest percentage of users at 27% indicated an MTTR of between 30 and 60 minutes. It's interesting that it appears a handful of SOAR users saw an increase in their MTTR at the longest time intervals. Commercial SOAR tools take a significant amount of time to deploy properly before they can deliver value. It's possible that those SOAR deployments were not properly scoped out, or those organizations had not yet fully deployed their SOAR tool to realize its full value. This may also explain why a handful of respondents indicated they were looking to replace an existing SOAR tool.

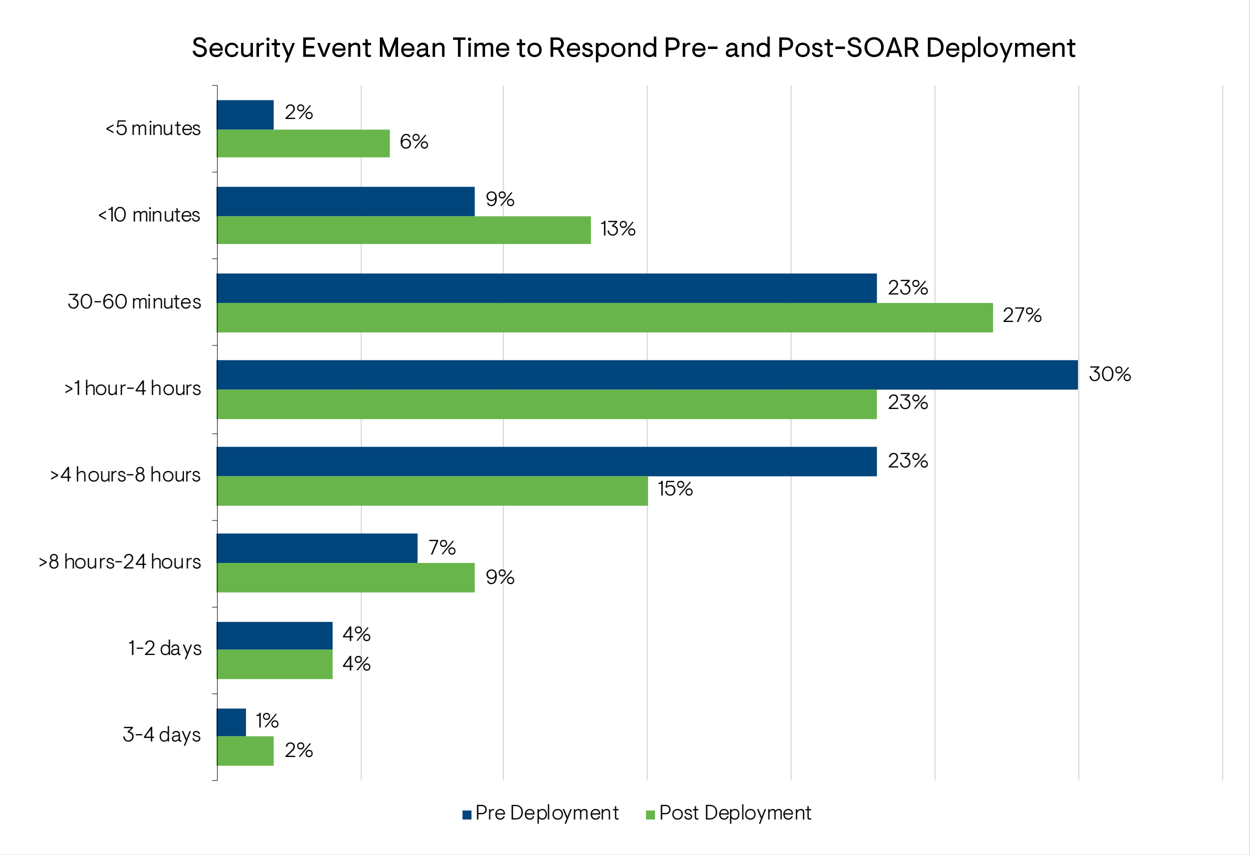


Figure 8

One other efficiency metric worth noting is the amount of time saved per day/per security analyst at organizations that deployed a commercial SOAR tool. For 44% of those SOAR users, that time savings ranged between one and two hours per day. For another 45%, the time savings was three to four hours per day.

Another factor that contributes to the difficulty in retaining existing security expertise is the level of burnout that exists in many security operations centers. In addition to the higher levels of stress associated with IT security, the repetitive nature of manual correlation of threats across domains, manually investigating a sea of false positives, and the complexity of trying to master a wide variety of security tools can send stressed and bored analysts running for the exits. This is especially true at the Tier 1 level for junior analysts who have scant independent decision-making powers and little opportunity to try new ideas. Earlier EMA research on SOAR usage and its benefits documented a perceived increase in the skill level of security analysts who used SOAR tools. Enabling security practitioners to grow their skills is a key factor in keeping burnout at bay. But can the adoption of SOAR technology directly impact staffing levels and job satisfaction? The short answer given by the SOAR users in this study is yes. Of those, 74% indicated that they believe that as a result of their commercial SOAR deployment, their organization lowered security analyst/staff turnover. Only 21% said no and 5% weren't sure. For those who believe their organizations saw lower turnover, the largest percentage felt it was in the ranges of 21% to 30% or 31% to 40%. Finally, when SOAR user respondents were asked to rate their organization's security analyst job satisfaction before and after deployment of the SOAR solution, the percentage of very satisfied answers jumped from 40% to 60%.

SOAR Deployment Contributes to Lower Turnover

By how much do you believe your organization has lowered security analyst/staff turnover as a result of deploying your commercial SOAR solution?

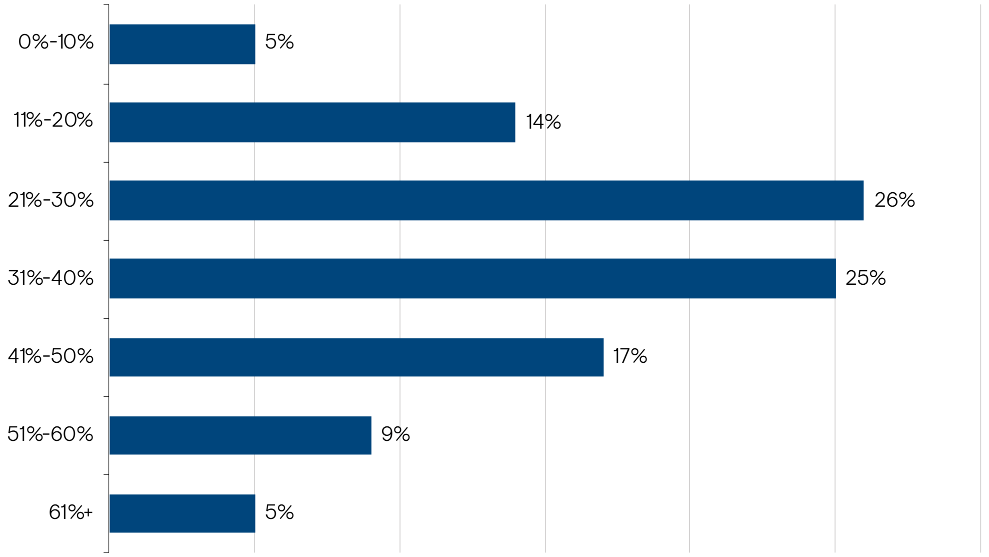


Figure 9

Security Automation and the COVID-19 Pandemic

With the sweeping changes happening in the workplace as a result of the COVID-19 pandemic and the resulting increase in working from home, IT security teams are relying on the automation delivered through SOAR and other security technologies like never before. Of the respondents using SOAR technology within their organizations, 94% reported that their SOAR platforms were either very or extremely valuable in enabling security teams working remotely to coordinate security workflows. At the same time, 85% of these respondents reported that their security teams relied either very or extremely extensively on their SOAR platforms to respond faster to security incidents and alert triage during this time.

More broadly speaking, the pandemic is having an outsized impact on the day-to-day activities of IT security teams. For example, 53% of all respondents in the study reported that as a result of the dramatic increase in remote workers, it has significantly increased the amount of time it takes to perform vulnerability scanning on endpoints. This is especially true for midmarket organizations, in which 60% of those respondents indicated this was an issue. In addition, 45% of all respondents indicated that the pandemic and resulting increase in work-from-home activity made the process of deploying patches and updates much more difficult. This was a bigger issue for large enterprises, with 53% of those respondents indicating that result. For 42% of all respondents and 62% of respondents at very large enterprises, the pandemic introduced new threat vectors into their environments that are harder to secure. Also, for 42% of all respondents, the pandemic and the organizational changes it brought resulted in a significant increase in the number of endpoint alerts security analysts need to investigate. Only 8% of all respondents reported that it had no impact.

As employees are forced to collaborate remotely instead of meeting in person due to social distancing initiatives, organizations have seen a dramatic increase in the volume of communication and sharing of a variety of different file types or formats. Whether it's engineers sharing new product designs, accountants sharing billing data in spreadsheets, or other documents containing sensitive customer information, this increase in communication of different file formats can increase the risks that security teams need to address. EMA asked all respondents which file formats their remote workers increasingly shared and found that the largest percentage indicated they were documents at 80%, followed by email at 76%. Unfortunately, these are the file formats that also pose the greatest risk to respondent organizations.

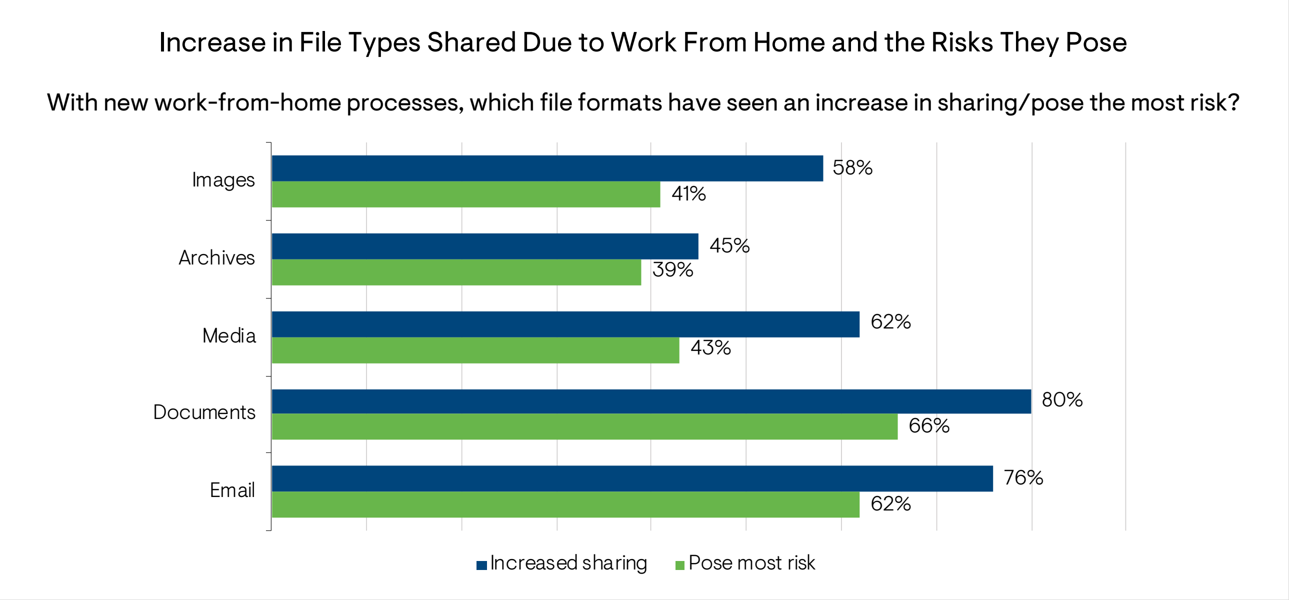


Figure 10

With these additional risks heaped on top of the security teams' plates, and the eagerness of attackers to exploit these new threat vectors that have opened up, it's no surprise that organizations have had to pour more resources into their IT security programs. Whether that involved shoring up remote access controls or expanding the use of encryption or endpoint protection, respondents indicated that their IT security budgets by and large saw healthy increases. For the largest percentage of respondents, that increase ranged from 10% to 25%, with 38% of respondents indicating that range. Another 32% said their IT security budgets saw a minimal increase of under 10%. A surprising 17% indicated that the pandemic had no impact at all on their organizations' security budgets. Unfortunately for the organizations hardest hit by the economic fallout of the pandemic, 11% saw a decrease in their IT security budgets.

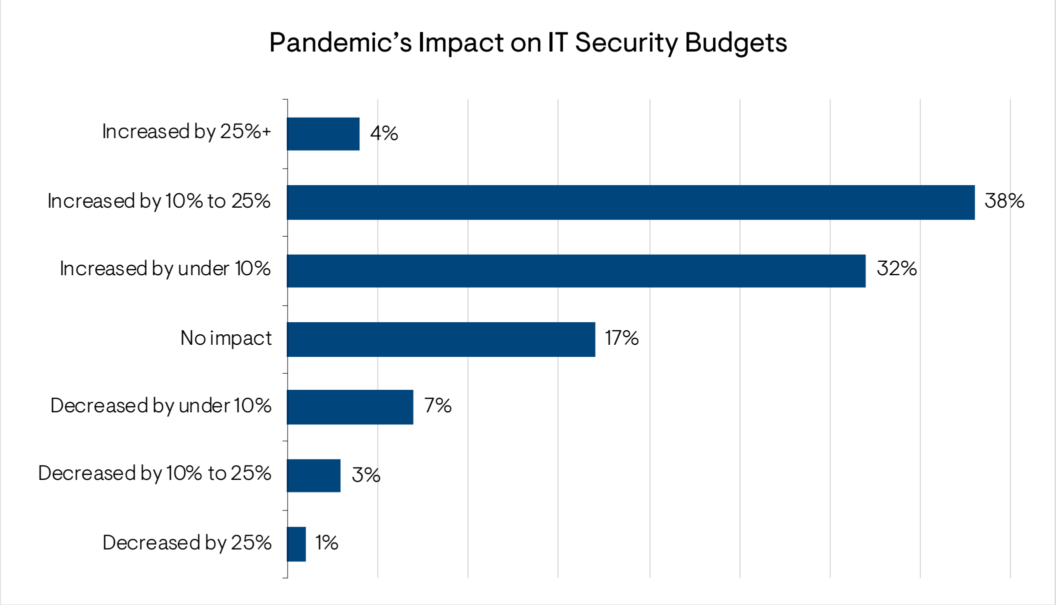


Figure 11

Conclusion

As more and more enterprises seek to improve the maturity of their security operations, the automation of routine activities and the enablement of more streamlined workflows are taking center stage in that journey. Driving demand for greater levels of automation in security tools of all stripes is the unyielding cybersecurity skills gap, which continues to widen with time. It's not only SOAR tools that organizations are turning to for help with that effort. They are looking at many, if not all, of their new tool purchases (and replacements) filtered through the lens of efficiency and automation gains.

The benefits they are seeking (and achieving) include better protection of their critical assets, better compliance, and improved architectural resiliency. For SOAR users specifically, this is accomplished through faster time to respond and resolve security incidents and several hours each day in time saved for security analysts. Saving time for skilled security practitioners allows them to focus more of their efforts on more proactive and strategic security initiatives, which ultimately allows security teams to get ahead of the threat curve.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
www.enterprisemanagement.com
4024.081920