SANS

Analyst Program

Survey

SANS 2021 Automation and Integration Survey: First We Walked, Now We Run (But Should We?)

Written by **Barbara Filkins** and **Matt Bromiley**

August 2021

SWIMLANE

Executive Summary

Automating processes and technology—and subsequently integrating them with an enterprise's security posture—is seldom an easy or quick task. These types of projects often take months or years, as organizations test, correct, and adopt at a pace that business operations allow, oftentimes with numerous implementation hurdles. However, in 2020 many organizations were forced to accelerate their automation and integration (A&I) plans by a global pandemic. The COVID-19 pandemic not only sped up various enterprise projects, but also caused long-term shifts in workforce locale and business operations.

In this year's SANS Automation and Integration Survey, we sought to capture both the progress organizations made in the past year and the plans they have for the future. One question was at the top of our minds: When forced to make changes, did organizations automate and integrate where they could, or did they try to rely on the same old techniques? After all, when a pandemic accelerates plans by a few years, that creates opportunities for the organization to hone current implementations and make way for changes.

In our survey, we captured the answer to that question and many more. Some key takeaways from this year's survey include:

- Organizations moved toward more extensively automated security operations, showing significant growth in incident response processing and automated alerting/defensive controls. Planning for automation of key security and IR processes in the next 12 months increased by nearly 30% between the 2020 and the 2021 surveys.[1] While this increase may have been fueled by the pandemic, overall spending projections for 2021 indicate that increased investment in automation will continue.
- Nearly 50% of respondents correlate automation risk with dependency on IT operational processes and tools that can impede key security processes. Inventory management and asset management are key areas to consider because both IT and security operations teams have ownership—from different perspectives—of this area.
- Start simple and build upon success. Nearly 50% of respondents consider the most essential automation requirement as providing "libraries of common practices and best practices that can be used for easy automation."

[1] "2020 SANS Automation and Integration Survey," April 2020, www.sans.org/white-papers/39575/ [Registration required.]

As you work your way through this paper, keep in mind how the results can inform future planning at your organization. We have inserted "Reader Takeaways" throughout the paper to summarize unique results. Consider these points in your mental comparisons, as well as the following:

- Notice the diversity of survey respondents. In this survey we likely have representation of your organization's industry; **how does your organization compare with the results?**
- Our survey respondents provided insight into satisfaction with projects they have implemented. If you have a project in the works or are planning one, **utilize this data for better forecasting and planning within your organization.**
- Many want to automate key security and IR process but are unsure where to start. **Notice where our respondents found success. Can you use that information to help you start?**

As always, our survey captured a diverse blend of industries that utilize automated processes and need to integrate them into security and business operations. Our top industries included cybersecurity, banking and finance, education, and technology. While most respondents have operations in or are headquartered in North America, we also saw responses from Europe, Asia-Pacific, and Africa. As our survey diversity grows each year, we expect our results to continue to display global trends in A&I. See Figure 1.

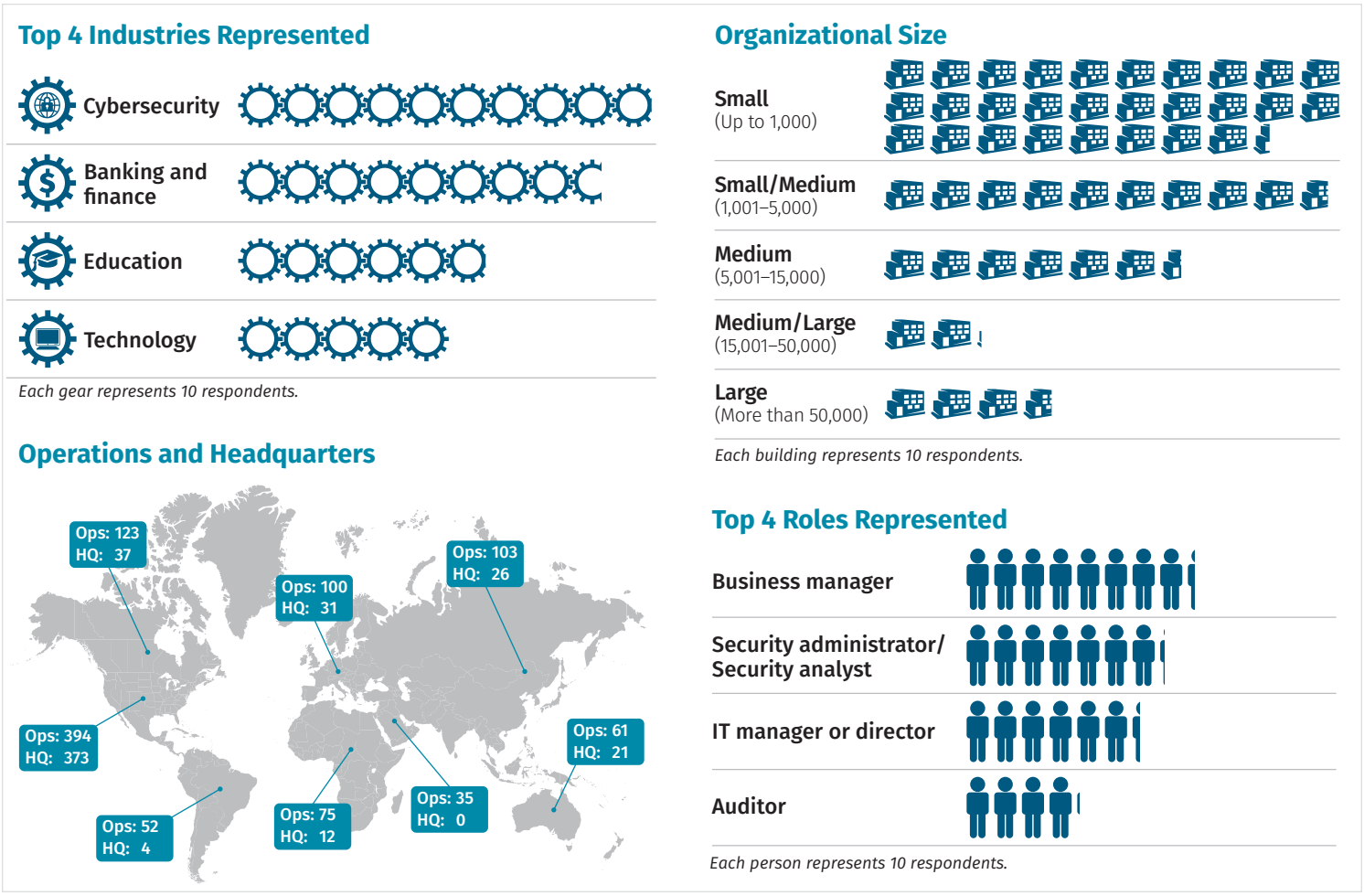


Figure 1. Survey Demographics

This year, in addition to a respondent's geography, role, and employee count, we also asked our respondents for more insight into the size of their organization in regard to endpoints. Figure 2 provides another barometer you can use to evaluate your own organization against our survey results.

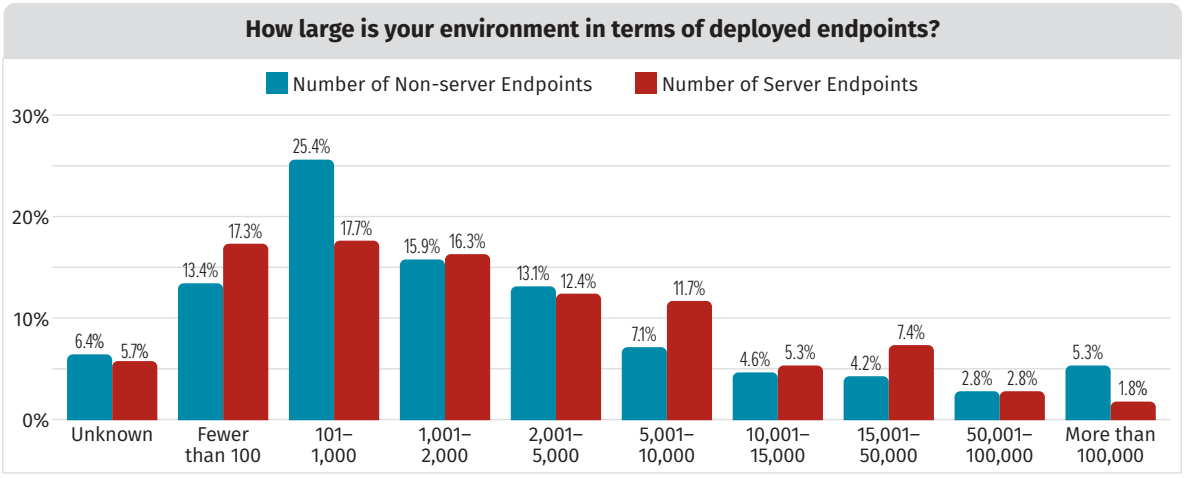


Figure 2. Size of Deployed Endpoints

Most of our respondents (68%) had 5,000 or fewer non-server endpoints, while approximately only 8% had more than 50,000 endpoints. They had similar results for server endpoints, with 64% having 5,000 or fewer server endpoints and 5% having more than 50,000. Deployed endpoint size—categorized as server or non-server in our survey—contributes to the size of an implementation project, as well as how quickly an organization can get that plan into place.

Deployed endpoint size is critical to evaluating A&I implementations, because larger organizations are sure to require larger projects and may achieve the benefits of economies of scale faster than smaller organizations.

We also had a few respondents report that they were unaware of their deployed endpoint size. We always find "Unknown" answers troubling, because visibility into assets within an organization is a foundation of an effective security posture.

What Is Happening Now?

The COVID-19 pandemic disrupted and continues to disrupt business operations. Some organizations are eagerly awaiting a return to a previous state, while many have realized that previously temporary changes are now permanent. In asking our survey respondents how their A&I implementations changed because of the pandemic, nearly one-third (32%) indicated that their plans were accelerated, while approximately 43% experienced some progress even amid slower plans. See Figure 3.

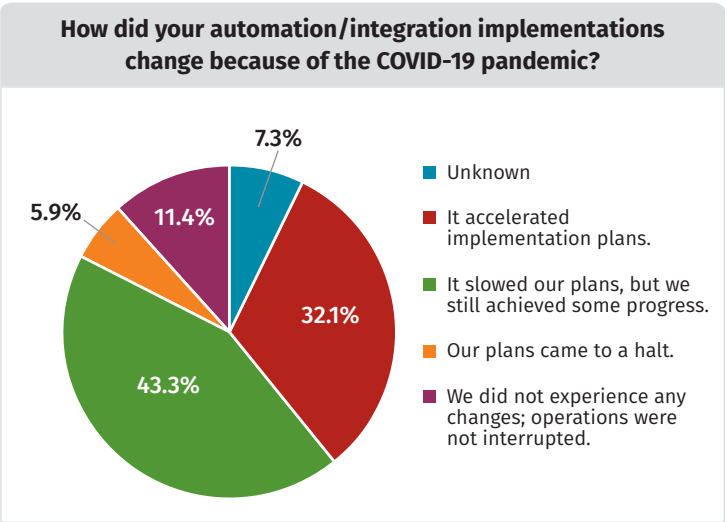


Figure 3. Implementation Changes Due to the COVID-19 Pandemic

Conversely, nearly 6% of our respondents saw their plans come to a halt; while only a small percentage, we expected some of our respondents to express a halt in plans. Organizations that rely on a physical presence or did not find value in accelerating plans during lockdown likely found other ways to cope with the sudden change. Similarly, slightly more than 11% of our respondents saw no changes whatsoever. While we may not see a repeat of this question in the future, we hope that the 11% who experienced no disruption relied on previously integrated automations to navigate the landscape changes.

In the same vein of accelerated implementations, we also saw significant year-over-year growth in the level of automation within organizations. We asked our respondents about the current level of automation within their organization (see Figure 4).

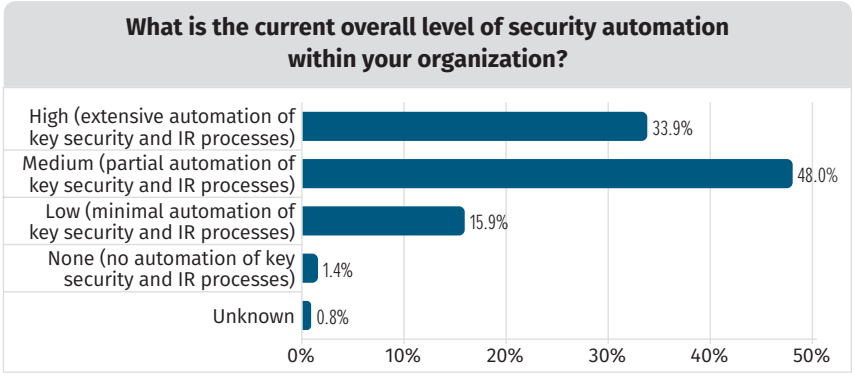


Figure 4. Current Levels of Automation

Approximately 34% of respondents have extensive levels of automation, while nearly half (48%) have partial automation of key security and IR processes. Even more interesting is the growth we saw over the past year. Table 1 compares the data from our 2020 survey with this year's results.

We saw a significant jump in extensive automation of key security and IR processes—nearly 25 percentage points—indicating that organizations are increasingly embracing security automation. Partial automation saw nearly a 10 percentage point increase, again indicating trends toward more automation. Based on these results, we would continue to see an uptick as more organizations drive toward automated security processes and/or technology.

Table 1. Increase in Level of Automation From 2020 to 2021

Level of Automation	2020	2021	% Change
High	9.0%	33.9%	24.9% ▲
Medium	38.3%	48.0%	9.7% ▲
Low	44.2%	15.9%	-28.4% ▼
None	5.0%	1.4%	-3.6% ▼
Unknown	3.5%	0.8%	-2.7% ▼


Organizations are increasingly moving toward extensive automation. We are taking this as a sign that the technology is now capable and certain processes are ripe for A&I.

Looking at these results, we were curious about which processes respondents' organizations were investing in. After all, a "key" security process is likely to be subjective to the organization, depending on its maturity, size, or current posture. Figure 5 identifies three key areas and their level of automation among our respondents.

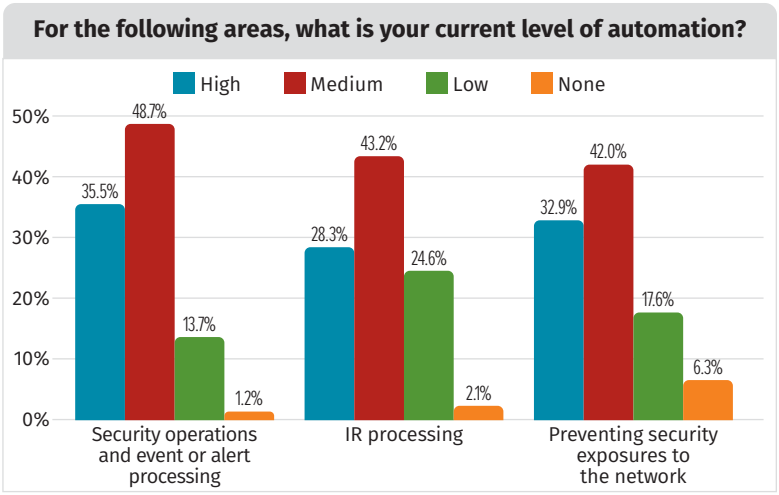


Figure 5. Key Areas of Security Automation

Each key area shows a healthy representation between high (extensive) and medium (partial) automation, with each area being extensively automated nearly a third of the time (ranging from 28% to 36%). As expected, extensive automation is our most significant growth area year-over-year, with each area experiencing double-digit growth, and incident response (IR) processing seeing 18 percentage point growth. See Table 2.

Table 2. Changes in Three Key Areas of Automation From 2020 to 2021

	Security Operations and Event or Alert Processing			IR Processing			Preventing Security Exposures to the Network		
	2020	2021	% Change	2020	2021	% Change	2020	2021	% Change
High	24.5%	35.5%	11.0%▲	10.5%	28.3%	17.8%▲	19.7%	32.9%	13.3%▲
Medium	50.3%	48.7%	-1.5%▼	37.7%	43.2%	5.5%▲	37.0%	42.0%	4.9%▲
Low	24.0%	13.7%	-10.3%▼	41.4%	24.6%	-16.8%▼	31.3%	17.6%	-13.7%▼
None	1.3%	1.2%	-0.1%▼	10.5%	2.1%	-8.4%▼	11.9%	6.3%	-5.7%▼

We suspect that the growth in IR automation is largely due to improvements in detection and response technologies found in many organizations. Endpoint detection and response (EDR) and network detection and response (NDR) technologies are more capable than before. We hope that organizations are taking advantage of these improvements.

While partial automation saw minimal growth over the past year, it still represents the largest grouping of each area of security automation. We suspect that the changes we see year-over-year are representative of two changes:

- As organizations and technology mature, organizations are sliding from the low to high category by slowly increasing automation within their environment.
- An immature organization can quickly jump from low to high with implementation of a new technology, such as an advanced EDR or NDR platform.

It is likely that organizations experienced one or both of these changes, highlighting the growth needed to increase the use of automated and integrated technologies.

Key areas for automation include alert handling, incident response, and mitigating exposure via the network. If you are wondering where to focus efforts next, consider how your organization stacks up against these results.

What Is Happening Next?

An overwhelming number of respondent organizations are considering automation for the future, with 85% planning on automating key security and IR processes in the next 12 months alone. See Figure 6.

This represents an increase of 27 percentage points over FY 2021 and, while this may be due to the pandemic, this growth will likely continue into the future, based on overall automation spending projections.

Do you plan to automate any key security and IR processes in the next 12 months?

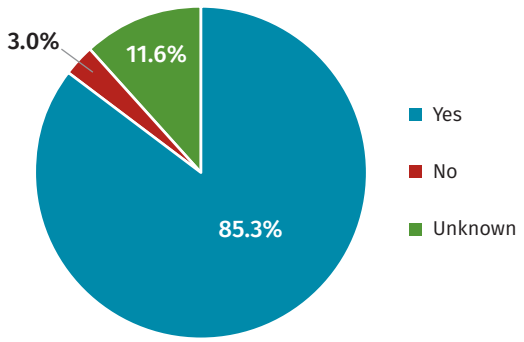


Figure 6. Plans for Automation During Next 12 Months

Overall Spending Trends: A Telling Story

Let's next step back and look at what respondents reported as their current and planned investment in security automation, based on the percentage of the current security budget. Comparing results from FY 2020 (Figure 7) with those for FY 2021 (Figure 8), three things really jumped out at us:

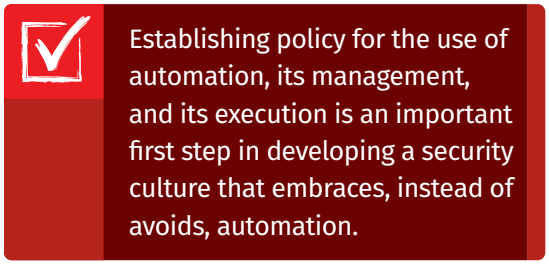
First, respondents are aware of where the money is going! This is a pleasant surprise, indicating improved understanding as to what automation can offer. In 2020, more than 40% reported that they didn't know the current investment in automation versus 9% in 2021. Similarly, in 2020, 44% did not know about the next year's investment, whereas in 2021 this percentage fell to 11%.

Second, the current 2021 investment in automation is substantially greater than what was projected in 2020—with the exception of those spending more than 10% of the security budget on automation—indicating that most organizations recognize automaton as a solid part of their security outlay.

Finally, the 2021 results indicate that investment in security automation will continue at solid levels into the next 12 months.

Placing the Emphasis

The leading factors in FY 2021 that affected organizational decisions to support the current level of investment reflect two key enablers for automation success: establishing effective policy around the use of automation, and ensuring interoperability across the various tools and technologies in use within the enterprise. See Figure 9.



Establishing policy for the use of automation, its management, and its execution is an important first step in developing a security culture that embraces, instead of avoids, automation.

What is the current investment in automation, based on the percentage of your present security budget? What percentage is planned for the next 12 months?

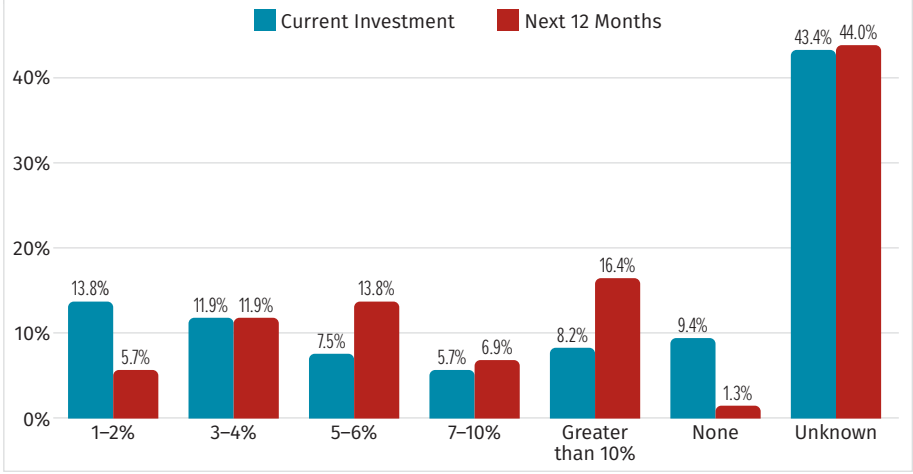


Figure 7. Spending Trends for 2020

What is the current investment in automation, based on the percentage of your present security budget? What percentage is planned for the next 12 months?

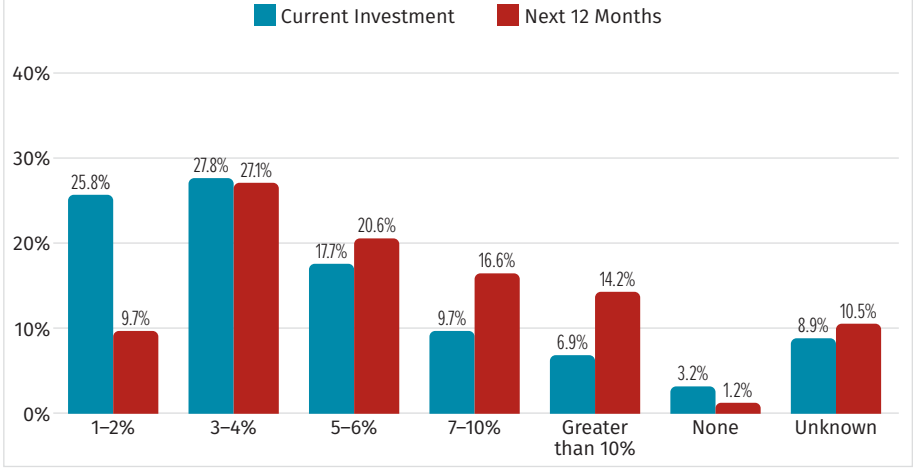


Figure 8. Spending Trends for 2021

What factors affect your organization's decision to support that level of investment? ***Select your top three in no particular order.***

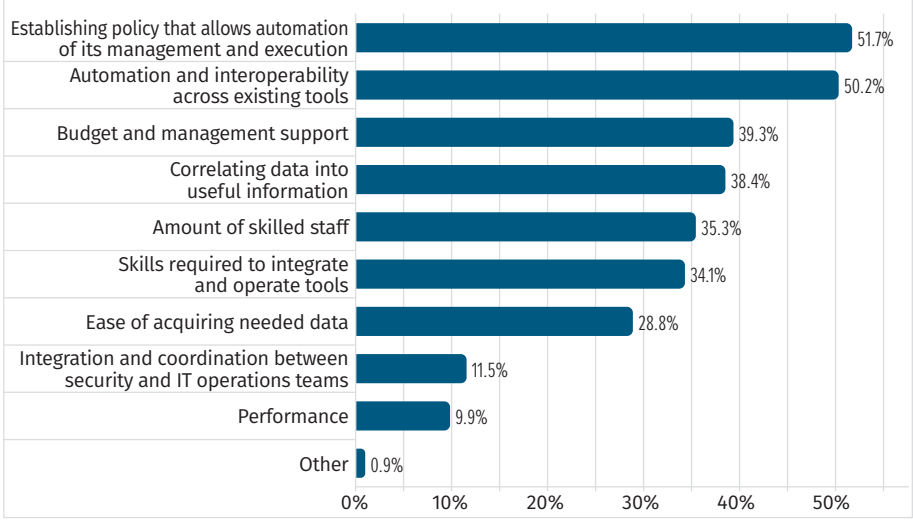


Figure 9. Investment Factors

The second factor is improving automation and interoperability across existing tools, rather than trying to acquire new tools or services, to replace or augment existing capabilities. Security professionals are increasingly depending on open source frameworks and tools such as Python to achieve needed interoperability.

In developing your automation strategy, take the time to first evaluate the capabilities of the tools you already have and how they can interface in order to achieve your initial automated framework. Once you have this baseline, then evaluate what additional tools and techniques you may need to achieve even better interoperability.

This factor is reflected in a significant change from last year regarding organizations' approaches to automation tools. Tool acquisition has given way to a preference for integrating existing tools through in-house efforts, as well as by leveraging tools through the services of a managed security service provider (MSSP), a natural approach given the lockdown-imposed transitioning to cloud-based infrastructure to support a remoted workforce. See Table 3.

Table 3. Changes in Tool Acquisition

Tool Acquisition Approach	2020	2021	% Change
Both acquiring dedicated automation tools and integrating existing tools	38.1%	9.3%	-28.8% ▼
Integrating existing tools through in-house integration and orchestration efforts	28.5%	35.5%	7.0% ▲
Leveraging the tools through the services of an MSSP	11.4%	28.0%	16.6% ▲
No automation or orchestration tools currently in use	10.0%	13.1%	3.1% ▲
Acquiring dedicated automation tools from an independent software vendor	9.6%	13.1%	3.5% ▲
Other	2.5%	1.0%	-1.5% ▼

Project Experience: An Important Factor

Practical experience is an important factor when evaluating the success of any initiative, security-related or otherwise. Table 4 summarizes various goals that respondents strove for as they implemented an A&I project and their level of satisfaction as to how achieving that goal improved the performance of their security operations/IR.

Table 4. Goals and Satisfaction

Goal	Very Satisfied	Satisfied	Overall Satisfied	Not Satisfied	No Opinion
Achievement of continuous monitoring	25.3%	49.6%	74.9%	15.2%	6.1%
Improved visibility and monitoring infrastructure	26.7%	43.8%	70.5%	19.6%	5.0%
Improved early detection of threats through integrated threat intelligence feeds	23.7%	44.6%	68.3%	18.2%	11.6%
Utilization of current enterprise security tools already in place	22.9%	45.2%	68.0%	21.2%	8.5%
Better prioritization of security operations activities	22.3%	45.5%	67.8%	19.8%	9.1%
More efficient and effective routine security processes	24.8%	42.1%	66.9%	22.6%	7.4%
Automated security workflows (such as for detection, remediation, and follow-up) that can be systematically updated as best practices emerge	30.9%	35.8%	66.7%	20.4%	11.0%
Alert monitoring and prioritization	24.8%	41.6%	66.4%	22.6%	8.3%
Improved collaboration between team members working together on incidents	24.5%	40.2%	64.7%	22.0%	12.1%
Better definition of processes and owners	22.3%	42.1%	64.5%	19.8%	12.4%
Reduced response time for detection, response, or remediation	23.7%	40.2%	63.9%	23.4%	9.9%
IR procedures that can be consistently and precisely executed	24.5%	38.0%	62.5%	22.9%	11.8%
Improved handling of insider incidents	21.5%	39.4%	60.9%	23.7%	12.1%
Elimination of alert fatigue	20.7%	37.5%	58.1%	26.7%	10.2%
Other	12.9%	18.5%	31.4%	9.1%	17.9%

Interestingly, most respondents report satisfaction with goals that are usually considered difficult—such as continuous monitoring and improved visibility—lending credence to the perception that organizations need automation to achieve some of the demands for modern operational security.

Pay attention to the leading causes of "Not Satisfied" in Table 4. These exemplify the human side of the security equation, such as alert fatigue and handling of insider incidents. If these (and other human-related) factors aren't accounted for in how you automate, they will continue to be sources of incidents and possible breaches.

Don't neglect the human element in automation design. Remember: Automation is only as good as its design—and automation is designed by humans!

But there is still room for improvement. We also asked what goals organizations needed to address or update to improve the performance of current security operations and IR, couching the response options in terms of respondent confidence that a specific focus would help meet their objectives. In other words, what is the current satisfaction and where do organizations need to focus their emphasis to ensure future confidence in continued or improved project success. See Table 5.

Based on this comparison, both continuous monitoring and improved visibility have room for improvement, being ranked the first and second areas that need continued emphasis for future confidence. Respondents are also interested in an improved capability to be able to systematically update workflows as best practices emerge, accompanied by better prioritization of security operations activities. This speaks, as we shall see, to the top two essential automation requirements discussed in the section "Focusing on the Future."

Table 5. Current Satisfaction vs. Future Confidence for Automation Project Improvement

	Current Satisfaction	Future Confidence
Achievement of continuous monitoring	1	1
Improved visibility and monitoring infrastructure	2	2
Improved early detection of threats through integrated threat intelligence feeds	3	6
Utilization of current enterprise security tools already in place	4	9
Better prioritization of security operations activities	5	4
More efficient and effective routine security processes	6	14
Automated security workflows (such as for detection, remediation, and follow-up) that can be systematically updated as best practices emerge	7	3
Alert monitoring and prioritization	8	5
Improved collaboration between team members working together on incidents	9	8
Better definition of processes and owners	10	11
Reduced response time for detection, response, or remediation	11	7
IR procedures that can be consistently and precisely executed	12	13
Improved handling of insider incidents	13	12
Elimination of alert fatigue	14	10
Other	15	15

Technology Implementation Trends for Automation—Next 12 Months

Figure 10 shows the tools that organizations plan on implementing over the next 12 months. For the most part, respondents have identified specific tools and techniques that, once integrated, provide essential information to support continuous monitoring and improved visibility.

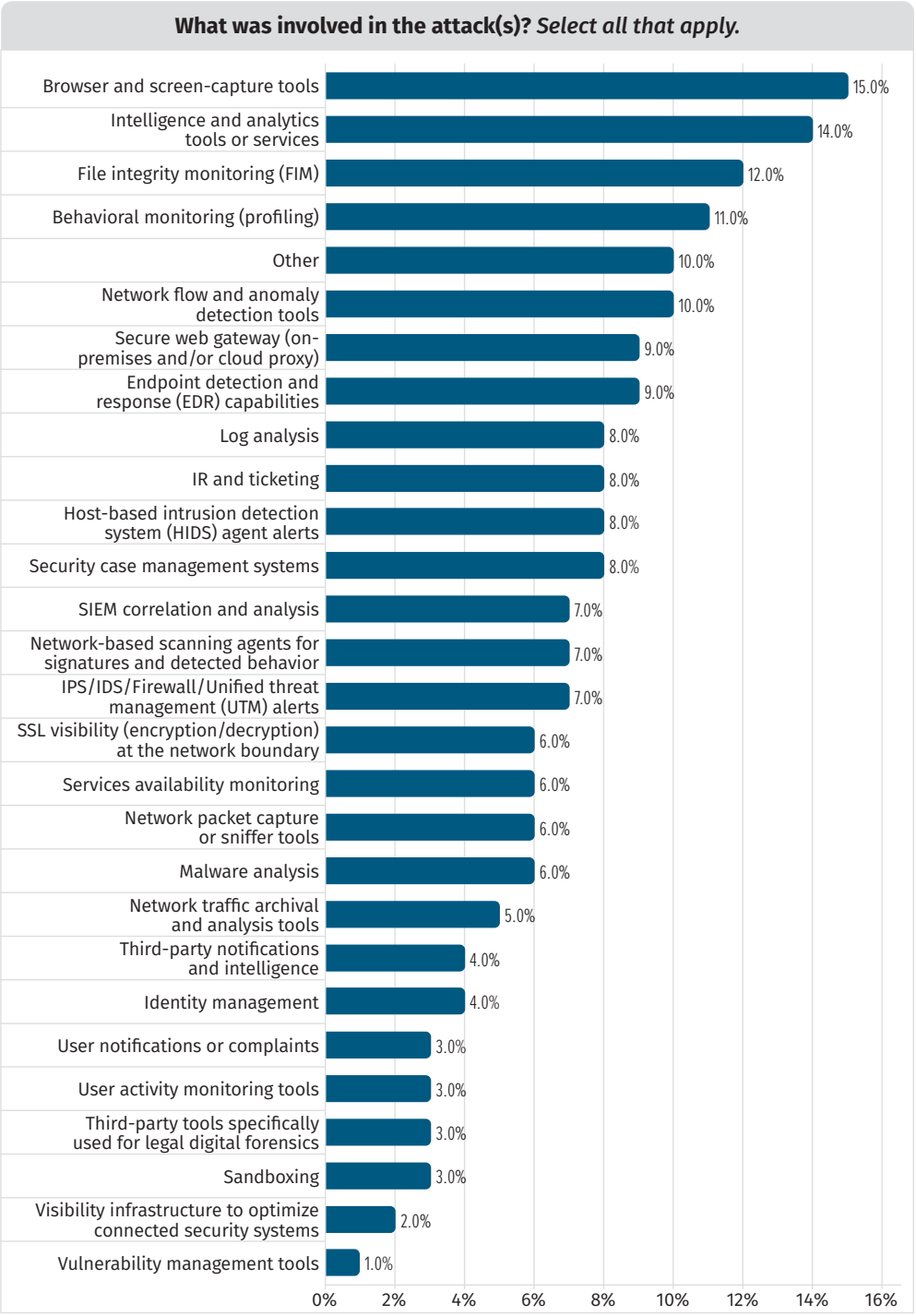


Figure 10. Tool Implementation Planning for Next 12 Months

The Dimension of Risk

Automation is often touted as a way to reduce or mitigate risk: It enforces consistency in repetitive tasks, it can provide unbiased recognition of potentially dangerous trends, and it can process enormous amounts of data faster than a human analyst. But, like any other strategy, automation can also create new risks. Figure 11 exemplifies areas of potential risk due to security automation.

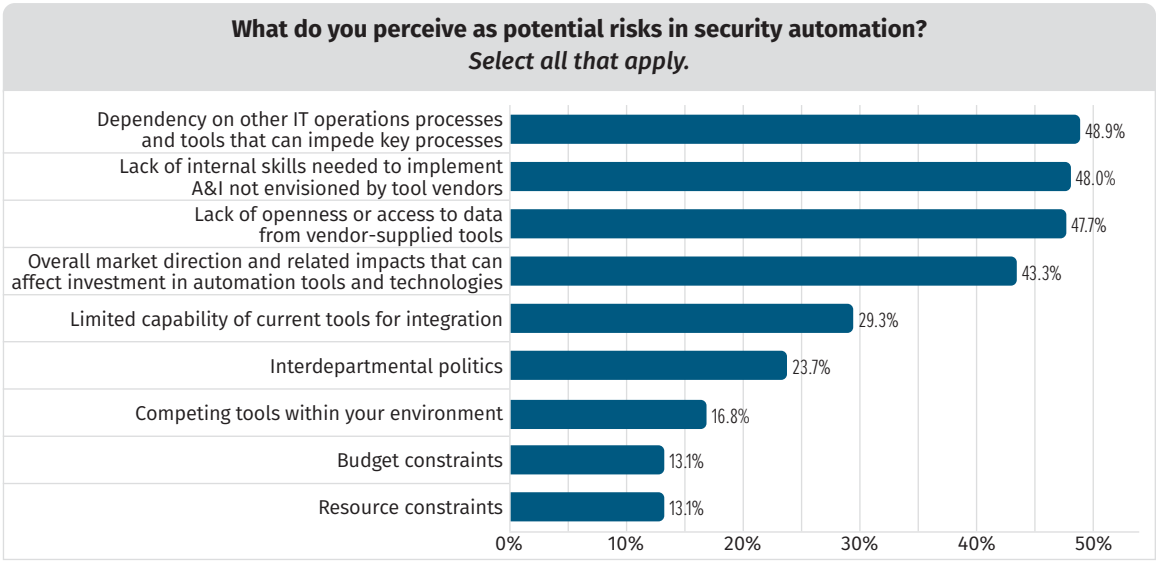


Figure 11. Potential Risks of Security AutomationSecurity Benefits and Capabilities

Nearly 50% of respondents see the leading risk as being a dependency on external factors—IT operational processes and tools—that can impede key security processes. For example, good security should start with good hygiene. Good hygiene depends upon knowing the architecture of the enterprise infrastructure and the important details—what assets are connected to it, how these assets are configured, and who has ownership of and access to key assets—often considered the domain of IT operations. Here operational security may be constrained by IT-owned automated processes, such as asset inventory and management.

Collaboration is key to good automation design. Make sure your operational teams—IT, OT, and security—work together to design the workflows and playbooks for security automation.

The second leading risk has to do with internal skills needed to implement automation. Vendors may help, but they aren't necessarily experts in your processes. While 48% of this year's respondents cite the need for internal skills to implement A&I, hiring staff may not be sufficient for implementation. Figure 12 indicates that most organizations will be hiring during the next 12 months.

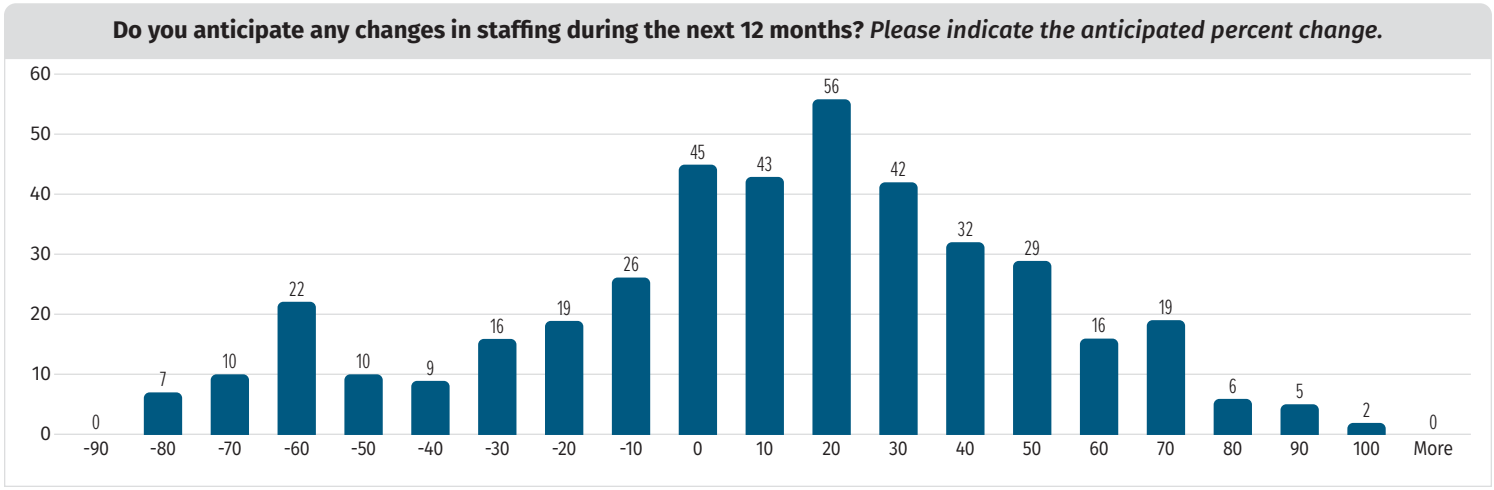


Figure 12. Hiring Trends

Focusing on the Future

Given the increased spending for automation, better integration of tools, and the need to address risk, where should organizations focus in the future? We asked respondents what they consider to be the three essential automation requirements that would improve their organization's security posture. See Figure 13.

The top three essential requirements support the trends identified in the previous analysis and lend themselves to be Reader Takeaways.

What do you consider to be the top three essential automation requirements that would improve your security posture?
Select your top three in no particular order.

Figure 13. Essential Requirements for Automation

- **Provide libraries of common practices and best practices that can be used for easy automation.** In other words, start with you can easily automate, look to what is available in the community, design and implement to achieve success, and then build on your accomplishments.
- **Automate workflows and policy execution around security operations.** Collaborate across your operational teams, keeping in mind that the primary focus should be integrating A&I into your security culture.
- **Support improved exchange of information between operational teams and external stakeholders.** Use automation to improve visibility into security operations, such as real-time dashboards that address concerns specific to the role and responsibility of the stakeholder.

Closing Thoughts

The challenging part about automation, especially as shown in this survey, is that it is not just about technology:

- Understand both what your organization needs and where you want to go with automation. Having a strategic vision is helpful, especially if you are trying to establish a foundation for an enterprise security framework.
- Be realistic. Don't try to meet all your automation goals with your initial project. Start with one that you know will be successful and can, ideally, also be the foundation upon which you can build into the next level of your A&I framework.
- Don't underestimate the need to incorporate automation into your security culture—not only with policy, but also with outreach to and education of your stakeholders. Try to leverage automation to improve visibility and communication across your community as to what security is doing to protect, detect, and respond.

About the Authors

Matt Bromiley is a SANS digital forensics and incident response instructor, teaching FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. He is a principal consultant at a global incident response and forensic analysis company, combining his experience in digital forensics, log analytics, and incident response and management. His skills include disk, database, memory and network forensics; incident management; threat intelligence; and network security monitoring. Matt has worked with organizations of all shapes and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Barbara Filkins, SANS Research Director, holds several SANS certifications, including the GSEC, GCIH, GCPM, GLEG and GICSP, the CISSP, and an MS in information security management from the SANS Technology Institute. She has done extensive work in system procurement, vendor selection, and vendor negotiations as a systems engineering and infrastructure design consultant. Barbara focuses on issues related to automation—privacy, identity theft, and exposure to fraud, plus the legal aspects of enforcing information security in today's mobile and cloud environments, particularly in the health and human services industry, with clients ranging from federal agencies to municipalities and commercial businesses.

Sponsor

SANS would like to thank this paper's sponsor:

SWIMLANE