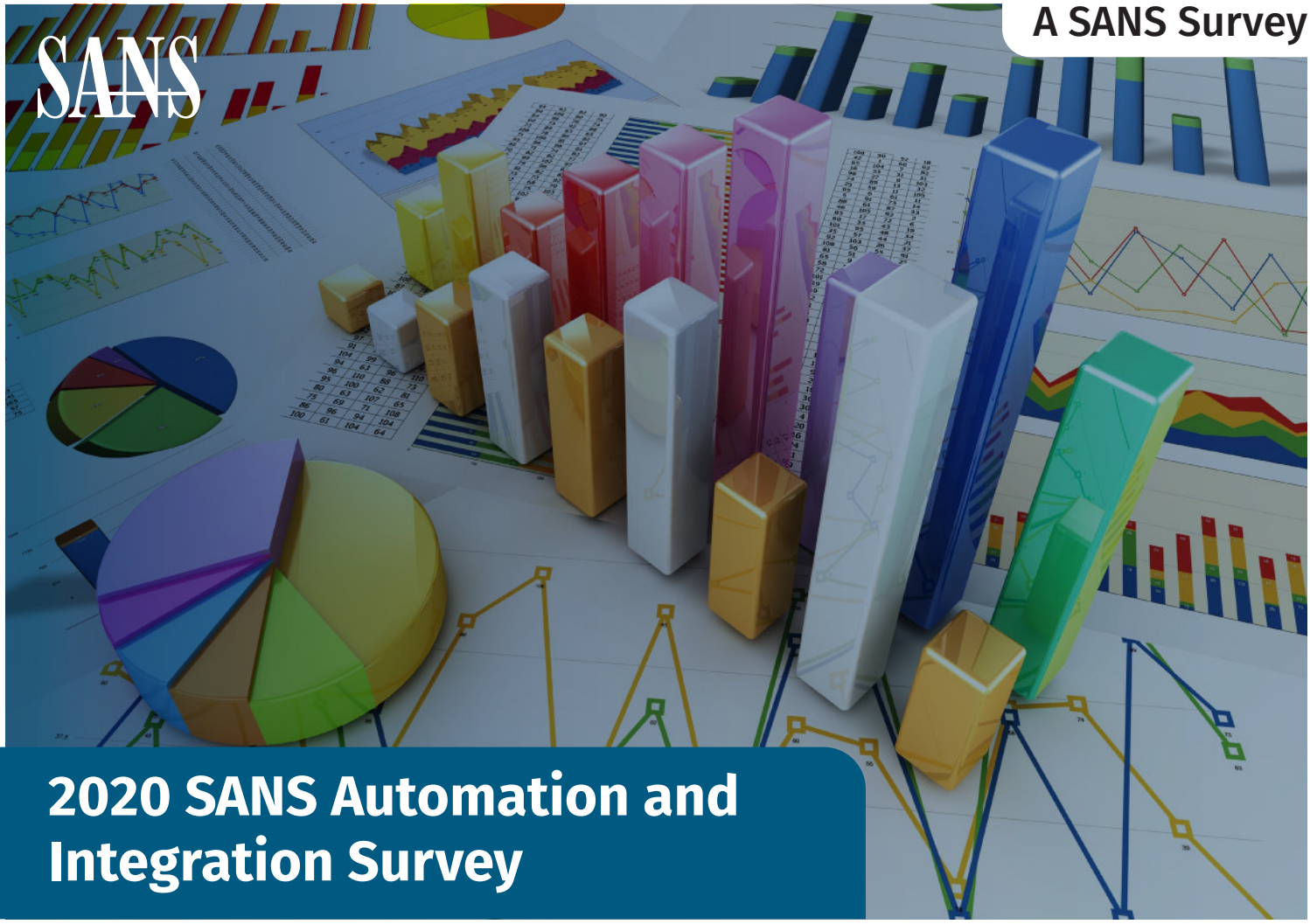
A SANS Survey



# 2020 SANS Automation and Integration Survey

Written by **Don Murdoch**

May 2020

*Sponsored by:*
**DomainTools**

Analyst Program

# Executive Summary

Automation and integration initiatives, projects and solutions balance machine-based analysis with domain-based knowledge to help security teams better support their organizations by achieving a level of optimized workflows and improving the use of security point solutions. Because this is the second year for the SANS Automation and Integration Survey, we are able to gain some perspective on the progress being made in automation and integration. The survey shows that respondents are definitely committing to automation and integration projects, with a primary goal of improving how staff engage with their organizations through improved processes.

Between the publication of the 2019 Automation and Integration Survey[1] and the results of the current survey, several trends are emerging:

- **Increased adoption of dedicated automation solutions in the past year, with an 11.8% increase** in tool adoption, shows a substantial uptick—especially when coupled with increased funding levels of 3–10% above 2019 levels.
- **A gap between current projects and past performance** emerges when comparing lower satisfaction ratings of prior projects with the anticipated higher results of current projects across the same project areas. The average gap is 17%, with a range of 9% to 25%.
- **Organizations are placing higher emphasis on implementing projects that improve security operations, rather than a new IDS or firewall.** Projects such as improving IR command, managing IR and cyber threat integration scored as currently implementing or planning to implement in the next year at 27% to 30%.
- **Automation may not reduce staffing needs.** Some respondents (5%) expect a small reduction in staffing. Perhaps surprisingly, many respondents advised that they expect staffing to increase. For them, the objective is to apply the added staff to more specialized tasks.
- **More security budget is being applied to automation.** The budget picture improved measurably year over year, with increases between 3% and 10% across the board for automation projects and an anticipated increase of 16% next year.
- **SOC and IR will get attention.** The majority of respondents (58%) stated that they plan to automate key security and IR processes in the next 12 months.

Organizations are investing in automation and integration projects, with increased budget to support them. They are giving a higher degree of priority and attention to projects that make staff, security operations and incident response work more effectively and smoothly. These priorities emphasize the "people" part of "people, process and technology." Further, only a few organizations expect a modest decrease in staff—again, emphasizing "people."

[1] "2019 SANS Automation and Integration Survey," March 2019, www.sans.org/reading-room/whitepapers/analyst/2019-automation-integration-survey-38852

The picture isn't perfect, however, as there is a measurable difference in satisfaction with the results of automation projects conducted in 2018, even though there is a much higher degree of anticipated success in current projects. Budget commitment is definitely being applied to this area, showing that organizations are committing to prioritizing automation projects at higher levels in their project portfolio.

## About the Respondents

The 2020 survey had 520 respondents, more than doubling the 2019 sample of 218 respondents. With that growth in participation came a modest shift in the viewpoint of participants. Those holding management roles decreased by five percentage points to 22%, while the group representing security admins, architects and analysts increased to 56%. As a result, the 2020 survey is somewhat more influenced by those closer to the daily workflow than managers overseeing operations.

Figure 1 provides a snapshot of respondents to the 2020 survey.

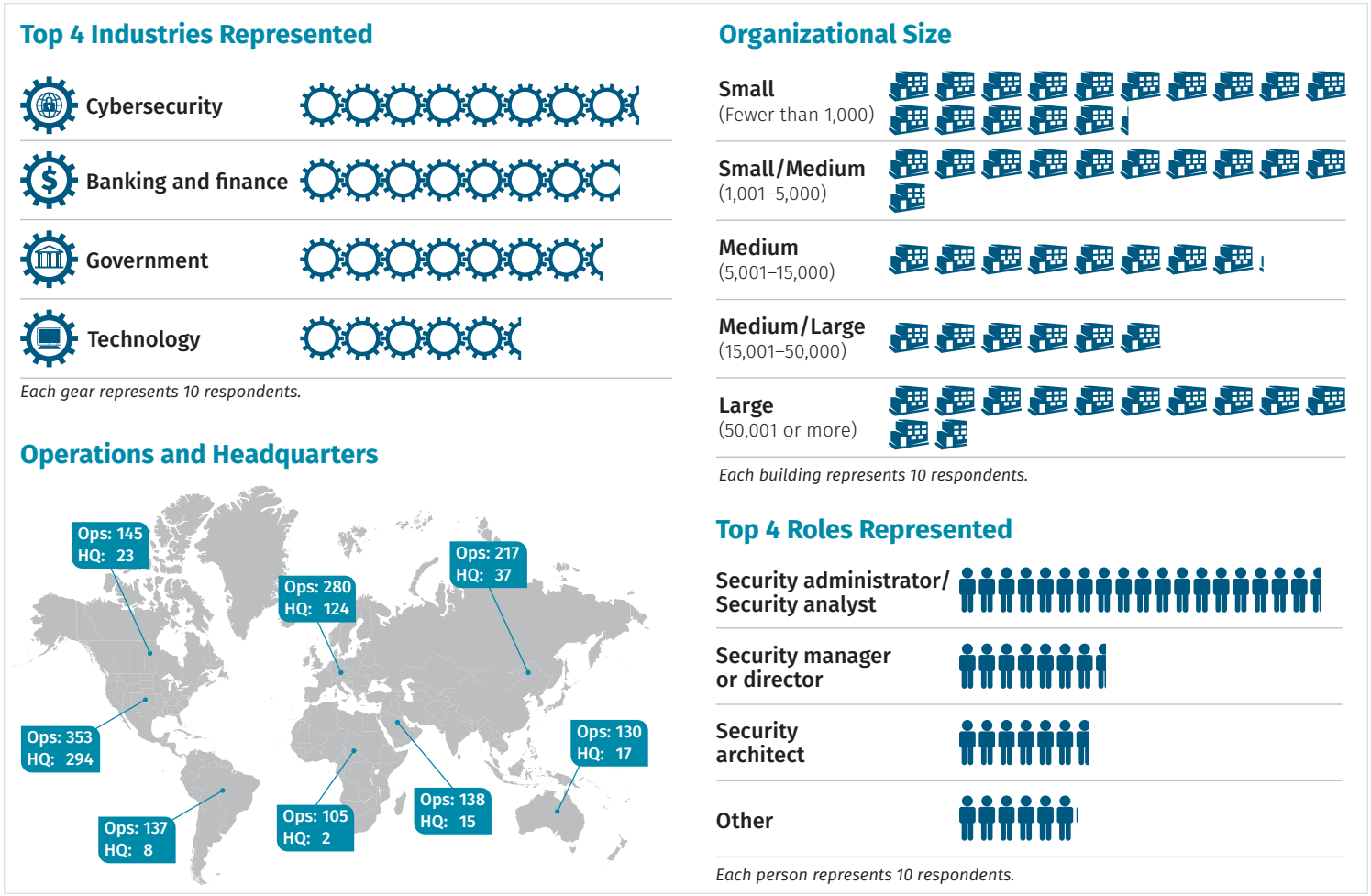



*Figure 1. Key Demographic Information*

Although there were 5% more organizations with more than 50,000 employees and 7% fewer small companies with fewer than 1,000 employees responding in 2020, the three middle groups were very close with respect to the overall percentage of respondents.

# The Evolution of Automation in the Organization

Information technology–focused automation tools and techniques are well known in the IT industry, although examples such as the automatic telephone switchboard, introduced in 1892, predate the first mainframe by more than half a century. In the 1980s, the term *workflow* became a synonym for *automation* with the introduction of document imaging, scanning, routing and management processes. These types of systems replaced paper-based processes with electronic ones in the 1990s. As businesses started using a wide variety of IT systems, it became apparent that repetitive tasks could be automated, and one system could be interconnected with another. In the 1990s, enterprise resource planning (ERP) systems made inroads into businesses by delivering on the promise to improve the performance of internal business processes.

Because the information security community is intertwined with IT systems, the community began implementing automation tools and techniques to handle repetitive tasks by using scripting, programming interfaces, using vendor-designed features or writing their own bridge code. In the mid-2000s, with the introduction of the first SIEM systems—which based decision-making capabilities on event data and action-initiating capabilities that included running scripts, performing lookups and feeding the results back into the system for further action—one aspect of security automation reached the hands of security pros for any organization that could afford the technology.

Network access control (NAC) is another mainstream example of applying automation and integration techniques. NAC is a central control system that monitors the network and makes decisions based on the security posture of an endpoint at its first connection to the network. More sophisticated systems can interact with the endpoint and reassess the posture over time, push agents, communicate actions to operators, and thus react to a change in the endpoint as its security posture changes.

Note that organizations don't need to buy a tool to have automation. They may be underutilizing an existing capability that they can call into action. Or they may be able to build their own automation and integration capability. For example, an organization could use a home-grown identity management engine to poll the HR system once per hour and find that there is a new full-time equivalent (FTE) with a start date within the next three days. The engine would use attributes of the users' names to construct candidate user account names and then create the necessary accounts in various IT systems that the user needs to access, based on their department as defined in the HR system. From there, the engine can email initial credentials to the appropriate onboarding location. The engine could also enable the users' accounts on their start date. The inverse is also true—and another example of automation and integration. When a staff member's termination date and time arrives, the engine disables their accounts across the board and archives their profile, along with any other repetitive actions, to stop other individuals from accessing that user's account.

### Key Definitions

**Automation:** The technology by which a process is executed as a sequence of repeatable instructions or tasks without human intervention or assistance. This process enables systems to perform task-oriented operations.

**Integration:** A process that allows an automation platform to access the capabilities of other independent tools through a well-defined programmatic interface. Examples include a standards-based API such as a RESTful API, message queueing, message sinks and service-oriented architecture (SOA) systems. Successful integration requires a common taxonomy for meaningful and seamless data and process exchange across the connected infrastructure.

**Orchestration:** A method that invokes and coordinates functionality across diverse technologies and independent tools to create an overall workflow. Orchestration depends on automation and integration, and permits systems to work together.

## Level of Security Automation

Survey results demonstrate that respondents who had no automation in place a year ago are making initial efforts to adopt automation and integration at a significant pace. And those who had some degree of automation are not stopping—presumably, they experienced enough of a positive result to continue.

Organizations can apply various levels of automation to improve security operations, posture and incident response. Even the most basic or low-level automation can result in a significant day-to-day improvement. For example, adding a right-click function in a SIEM platform that retrieves an account's properties from the primary directory may take only a day or two to script, but it virtually eliminates transposition errors and can be done without using a secondary application. In contrast, a high degree of automation requires formal requirements, data cleansing and normalization, and thus requires organizational commitment to a robust project that will improve security business processes.

Overall, this year's results show a growing commitment to the increased use of more advanced automation, with increases of 4% at both medium and high levels. Only 5% of respondents reported no automation is in place for 2020, down 7% from 2019. Figure 2 compares automation levels in 2019 with those reported in 2020.

**Low level:** A low level of automation would be implementing a predefined interface, a script that performs data collection or a functional lookup. These items take a few weeks to put in place. Think of these as automating a single task.

**Medium level:** At this level, automation processes start to support decision-making: improving processes by retrieving additional data through complex logic, solving semantic interoperability across disparate data sets and sources, automating one-way data push/pull, and implementing several tasks through a workflow capability. These items take a few months and incorporate formalized test plans, and are highly likely to be subject to organizational IT service management (ITSM) change control requirements. They are likely to require specifying an interface.

**High level:** These processes focus on systems acting on their own and communicating the results through intelligent messaging, should an error be made. Examples include bidirectional data exchange, acting on end system posture, and incorporating complex threat intelligence or analytical processes. Projects in this category require several staff and take many months to complete, and have formal design, requirements, a solid understanding of processes, and formalized test plan documents.

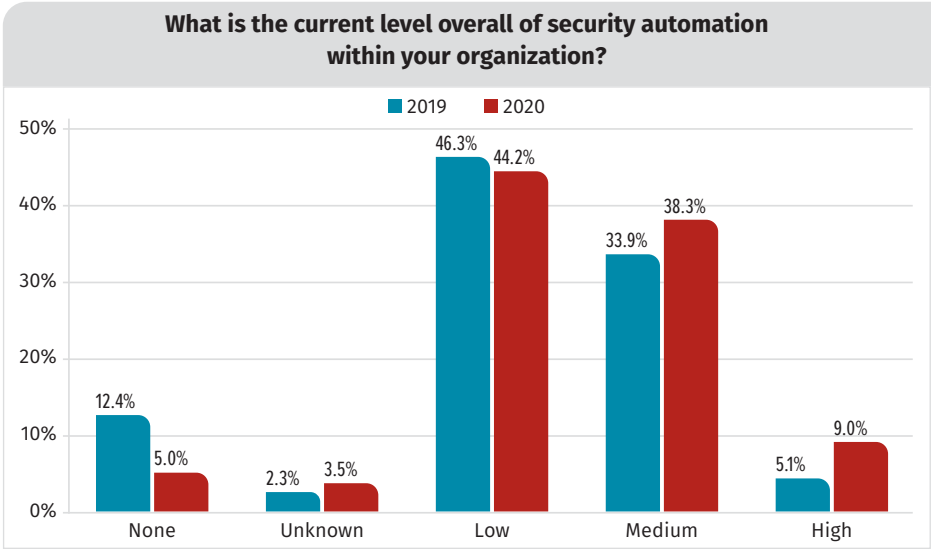



*Figure 2. Levels of Automation in 2019 Versus 2020*

## Automation in Core Areas

In 2020, SANS wanted to get more detail about where organizations are focusing their automation efforts in core areas of security. Nearly 74% of respondents are applying automation at medium or high levels for security operations and event or alert processing, indicating that they are making good use of existing systems. The second highest application of automation comes in preventing security exposures to the network, with 57% of respondents reporting medium or high levels of automation in this area, followed by IR processing, at 47%. (See Figure 3.)

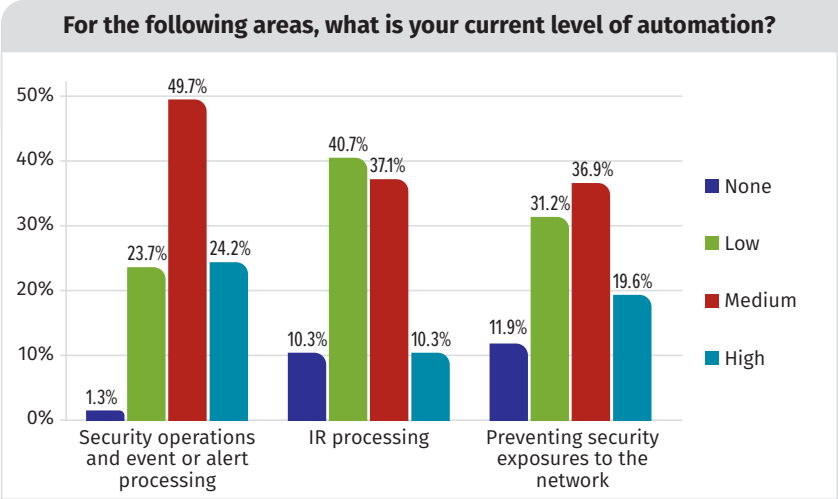



*Figure 3. Levels of Automation in Core Areas*

Event and alert processing remain a core function of security operations teams, especially when enabled by a strong log collection and management posture. Further, event and alert processing are key supports for a threat hunting program focused on proactively searching through data to find indicators of compromise (IOCs). Measures designed to improve alert processing through automation reduce alert fatigue, which is a constant challenge for security operations teams. Measures that apply automation to minimize alerts means that security operations teams can pay more attention to alerts that actually need human intervention to classify them. Measures that identify, manage and reduce exposures that are aimed at preventing exploits from being realized are preventative, which decreases the chance that those exposures can become incidents.

## Changes in Organizational Approach to Automation

In 2020, two dramatic shifts occurred in how respondents approach their use of automation tools, indicative of how organizations are evolving in their use of automation. First, organizations are looking toward the use of automation technology. Those with no automation or orchestration tools currently in use decreased by 11% between 2019 and 2020, indicating that more organizations are adopting automation tools. Second, organizations are investing in dedicated automation tools to augment their integration of existing capabilities (an increase of 12% in 2020 over 2019) as opposed to integrating existing tools through in-house integration and orchestration efforts (a decrease of 5.5%). See Figure 4.

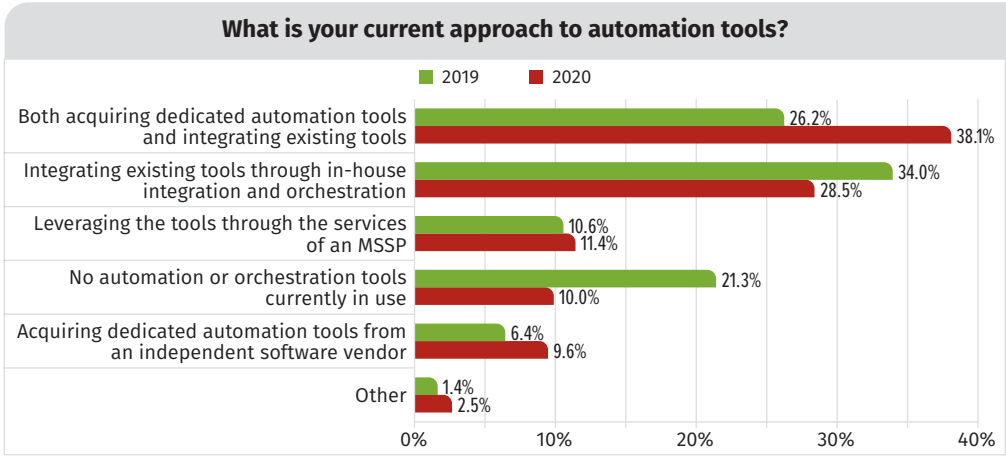



*Figure 4. Comparison of Automation Tooling Approaches Between 2019 and 2020*

SANS encourages organizations to adopt and leverage open standards because they are developed and maintained via a collaborative and consensus-driven process. Organizations will be well served by leveraging data exchanges that utilize known and adopted standards. Open processes facilitate interoperability and data exchange among different products and services. For example, there is a marked rise in data exchanges using JSON, a highly structured and human readable data exchange format. The JSON format easily lends to data extraction, rather than computationally expensive plain text parsing by SIEM solutions, and is rapidly becoming a standard. Open standards can help organizations better understand the risks and work involved in implementation, as well as provide a common framework for vendors to standardize their interface offerings.

### SIEM, SOAR and Automation

SIEM is a mature core technical platform for most security operations teams. Today, SIEM provides many opportunities for automation. Examples include asset and user import, export of alerts into a ticketing system such as Jira or Remedy, and right-click-based lookup capabilities that can short-circuit analyst investigations.

Security orchestration, automation and response (SOAR) platforms are often considered synonymous with automation and integration solutions. The inclusion of threat intelligence and incident response solutions within SOAR shows that the industry is advancing at a rapid pace.

Successfully implementing SOAR has a number of critical dependencies, including:

- Having well-defined use cases with well–thought-out definitions
- Understanding and consensus on the steps in workflow and tooling so that they can deconstruct the tasks
- Having workflow tools and an engine that supports orchestration, scripting capabilities, asset awareness and well-structured data that has meaning within multiple systems

With these elements in place, security operations teams can develop, test and validate use cases.

All of these components must support data exchange so that the back-end engines can integrate data from one system as input to another, make decisions, enrich data and direct downstream actions. In effect, the focus of automation and orchestration is on improving security operations and incident response processes so that they are more effective.

## People, Process and Platforms

Automation is about bringing people, processes and technology together. But these elements are also changing as organizations and their security procedures mature. In this section, we explore these three areas and how they impact automation.

### People: Automation and Staffing Needs

One of the biggest takeaways from this year's survey is that only 8% of respondents believed that they may experience a reduction in staffing levels within the security functional areas. The majority reported a modest reduction of less than 10%.

Only 5% of respondents expect a reduction in staffing as a result of an automation project. However, after an automation project, nearly half of respondents (49%) anticipate an improvement to staff utilization, as illustrated in Figure 5.

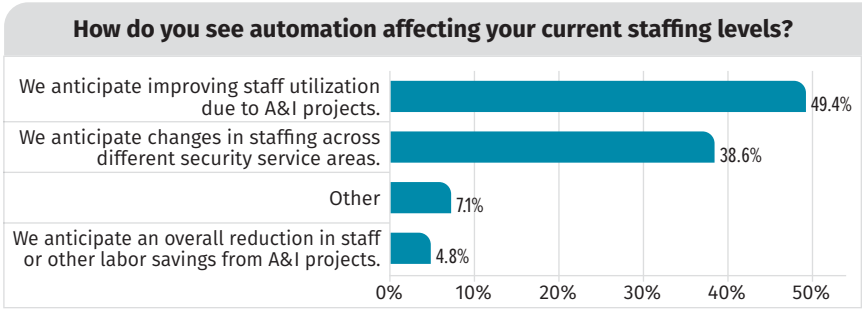



*Figure 5. Effects of Automation on Staffing Levels*

Were respondents confident in actually connecting the dots between automation projects and staffing changes? Not really. Only 17% reported that their proposed staffing changes are in direct response to an automation project; 64% said there is no correlation, and 19% do not know if there is a direct correlation.

## Process: Automation in Use

Respondents use automation to support their key security operations activities and services. More than 80% reported that they support each of the top three areas in use—intrusion detection, vulnerability management, and data protection and monitoring—with at least a medium level of automation. See Table 1.

In Table 1, activities greater than 30% are shown in green, to make it easier to see that several activities include automation. Also for easier identification, the top three activities for each level of automation match the color of their corresponding column heading.

**Table 1. Automation of Key Security Operations Activities and Services**

| Security Operations Activities or Services Supported | In Use | Level of Automation | | |
|---|---|---|---|---|
| | | High | Medium | Low |
| Intrusion detection | 86.8% | 27.7% | 39.3% | 19.8% |
| Vulnerability management | 82.0% | 28.7% | 36.9% | 16.4% |
| Data protection and monitoring | 80.0% | 20.9% | 35.3% | 23.8% |
| Platform health monitoring and support | 79.1% | 25.3% | 30.6% | 23.1% |
| Command function (IR/Analysis) | 73.4% | 14.7% | 31.0% | 27.6% |
| Cyber threat integration | 70.3% | 17.2% | 25.6% | 27.5% |
| Asset and inventory management | 69.9% | 18.2% | 27.6% | 24.1% |
| Initiate and manage incident response | 68.8% | 19.6% | 25.9% | 23.3% |
| Malware analysis | 68.3% | 19.3% | 24.8% | 24.2% |
| Compliance support | 65.5% | 15.7% | 25.7% | 24.1% |
| Audit/Assessment | 64.3% | 13.5% | 25.1% | 25.7% |
| Threat hunting | 57.3% | 10.9% | 23.7% | 22.7% |
| Forensics/E-discovery collection | 56.7% | 12.1% | 22.7% | 21.8% |
| Security posture assessment with a breach attack simulation tool | 44.7% | 6.5% | 16.8% | 21.4% |
| Other | 18.9% | 6.3% | 10.5% | 2.1% |

Consistent with other results, two areas scored well for automation: Vulnerability management (66%) and intrusion detection (67%) scored very well as security operations activities with a medium or high level of automation. These two results were the two lowest manual services as well.

Several of these activities depend on manual processes where automation may be too costly, may not yield results or have a unique characteristic that requires human intervention. It is significantly easier to apply automation that can take action or make decisions which use highly structed data. For example, digital forensics scored among the lowest as an automated process because it depends on manual processes and is an activity dependent on human insight (a forensic investigation seeks to answer a free-form question).

Breach and attack simulation (BAS) tools, a recent entrant in the security pro toolbox, made a good showing in the survey, with 45% showing some level of adoption. This is excellent because it means that nearly half of respondents are taking advantage of a recent set of tools in the IT security toolbox. BAS tools are a relatively low-cost solution set designed to assess an organization's security posture in an automated fashion. For these respondents, even though 41% indicated low or manual automation in this area, they are actively testing posture and are capable of making specific, measured and targeted improvement because of how BAS tools work.

Looking at current and future automation efforts in terms of key processes reveals that three traditional security operations processes lead in the use of automation: intrusion detection systems (61%), followed by vulnerability management (52%) and platform health monitoring and support (51%). These same three items sank to the bottom with respect to planning for implementation, meaning that there are other processes selected for implementation that organizations think will have a higher positive impact

and that focus on processes requiring a higher degree of skill. (See Table 2.)

Respondents are implementing automation in many areas. Two of the top three areas focus around improving how security operations teams manage processes: command functions (IR/Analysis) at 30% and improvements on initiating and managing IR at 27%. One technical system—cyber threat integration—tied with managing IR, at 27%.

**Table 2. Current and Planned Automation Efforts**

| Key Process | In Operation | Implementing | Planning | N/A |
|---|---|---|---|---|
| Intrusion detection | 61.1% | 18.9% | 13.0% | 5.4% |
| Vulnerability management | 52.4% | 22.8% | 14.3% | 8.2% |
| Platform health monitoring and support | 51.2% | 19.9% | 14.8% | 11.5% |
| Audit/Assessment | 39.1% | 18.7% | 19.7% | 20.5% |
| Malware analysis | 38.6% | 17.1% | 18.2% | 25.1% |
| Data protection and monitoring | 38.4% | 25.3% | 24.6% | 10.0% |
| Asset and inventory management | 36.6% | 26.9% | 22.8% | 13.0% |
| Compliance support | 33.0% | 22.3% | 23.5% | 19.9% |
| Forensics/E-discovery collection | 28.6% | 17.6% | 27.1% | 24.3% |
| Cyber threat integration | 28.1% | 26.9% | 26.3% | 17.6% |
| Initiate and manage IR | 27.6% | 26.6% | 27.9% | 15.3% |
| Threat hunting | 25.6% | 24.8% | 26.1% | 22.0% |
| Command function (IR/Analysis) | 23.5% | 29.7% | 28.9% | 15.1% |
| Security posture assessment with a breach attack simulation tool | 17.6% | 15.3% | 27.1% | 38.4% |
| Other | 2.0% | 1.8% | 3.3% | 25.1% |

Two other areas emerged as leaders for current implementation: asset and inventory management (27%) and data protection and monitoring (25%). Certainly, these are top-of-mind topics because, historically, keeping track of assets on a dynamic network can be a challenge. Also, data protection is a prudent preemptive response should an advanced adversary invade the network.

Two processes emerged as leaders in implementation or planned implementation for the next 12 months: command function (IR/Analysis), with 30% currently implementing automation and 29% planning to implement automation in the next 12 months; and initiate and manage IR, with 27% currently implementing and 28% planning implementation in the next 12 months. These results clearly show that organizations are prioritizing automation projects that should help their staff work smarter, improve consistency and standardize the way they handle security incidents.

## Platforms: Leading Tools

In 2020, IPS/IDS/firewall/unified threat management (UTM) alerts retained the top spot for the highest degree of platform utilization. These tools are capable of log analysis, which was in second place in 2019 but dropped to fourth in the 2020 survey, being edged out by EDR capabilities and SIEM correlation and analysis. Because SIEM, inherently, can function as a log aggregation tool, it's important to realize that log management still receives quite a bit of attention. However, even though these technologies changed positions, the difference in the utilization score was less than 3% (see Table 3 on the next page). Note the small percentage of respondents who still use these tools manually. This further illustrates that the core security protection and investigation tools in use today are highly automated.

**Table 3. Tools Included in the Automated Environment**

| Tools Included in the Automated Environment | High | Medium | Low | Manual | N/A | Automation Total |
|---|---|---|---|---|---|---|
| IPS/IDS/Firewall/Unified threat management (UTM) alerts | 35.0% | 33.9% | 20.5% | 5.3% | 5.3% | 89.4% |
| SIEM correlation and analysis | 30.2% | 34.5% | 23.8% | 5.3% | 6.0% | 88.6% |
| Endpoint detection and response (EDR) capabilities | 35.2% | 33.5% | 18.5% | 5.3% | 7.5% | 87.2% |
| Vulnerability management tools | 23.9% | 39.6% | 21.4% | 7.9% | 7.1% | 85.0% |
| Log analysis | 27.7% | 36.5% | 20.6% | 10.6% | 4.6% | 84.8% |
| Endpoint controls (e.g., network access control [NAC] or MDM) | 27.0% | 30.9% | 25.2% | 7.4% | 9.6% | 83.0% |
| Identity management | 23.2% | 31.8% | 26.8% | 10.4% | 7.9% | 81.8% |
| Host-based intrusion detection system (HIDS) agent alerts | 24.7% | 32.5% | 22.6% | 6.4% | 13.8% | 79.9% |
| Services availability monitoring | 23.7% | 30.8% | 25.1% | 8.2% | 12.2% | 79.6% |
| Network-based scanning agents for signatures and detected behavior | 24.1% | 30.9% | 24.1% | 9.9% | 11.0% | 79.1% |
| Secure web gateway (on-premises and/or cloud proxy) | 27.9% | 29.6% | 21.4% | 8.9% | 12.1% | 78.9% |
| Network flow and anomaly detection tools | 19.9% | 28.1% | 28.8% | 13.2% | 10.0% | 76.9% |
| IR and ticketing | 22.6% | 28.3% | 25.1% | 18.7% | 5.3% | 76.0% |
| Intelligence and analytics tools or services | 15.4% | 28.7% | 30.5% | 13.6% | 11.8% | 74.6% |
| User activity monitoring tools | 13.3% | 29.7% | 31.2% | 11.5% | 14.3% | 74.2% |
| Third-party notifications and intelligence | 17.8% | 26.7% | 28.1% | 16.7% | 10.7% | 72.6% |
| SSL visibility (encryption/decryption) at the network boundary | 21.1% | 26.8% | 21.4% | 8.6% | 22.1% | 69.3% |
| Security case management systems | 18.2% | 23.6% | 27.1% | 15.7% | 15.4% | 68.9% |
| Homegrown tools for our specific environment (e.g., playbooks) | 20.6% | 27.0% | 20.6% | 18.4% | 13.5% | 68.1% |
| Network packet capture or sniffer tools | 15.6% | 25.5% | 26.2% | 21.3% | 11.3% | 67.4% |
| Sandboxing | 13.9% | 27.0% | 24.9% | 18.5% | 15.7% | 65.8% |
| Network traffic archival and analysis tools | 14.9% | 23.8% | 26.7% | 14.9% | 19.6% | 65.5% |
| Malware analysis | 19.6% | 23.9% | 21.8% | 21.1% | 13.6% | 65.4% |
| File integrity monitoring (FIM) | 12.4% | 25.4% | 24.7% | 9.5% | 27.9% | 62.5% |
| Behavioral monitoring (profiling) | 11.8% | 22.5% | 28.2% | 10.7% | 26.8% | 62.5% |
| User notifications or complaints | 10.3% | 27.4% | 24.2% | 26.0% | 12.1% | 61.9% |
| Visibility infrastructure to optimize connected security systems | 9.3% | 22.9% | 26.9% | 15.4% | 25.4% | 59.1% |
| Browser and screen-capture tools | 9.3% | 20.6% | 21.4% | 17.8% | 31.0% | 51.2% |
| Third-party tools specifically used for legal digital forensics | 9.8% | 19.9% | 21.0% | 20.7% | 28.6% | 50.7% |
| Other | 4.7% | 11.7% | 5.5% | 4.7% | 73.4% | 21.9% |

The tools that rely on the most manual manipulation are “User notifications or complaints” at 26%, followed by “Network packet capture or sniffer tools” and “Malware analysis,” both at 21%. When it comes to a high level of automation, user notification only scored 10%. These results make sense because automating end user notifications represents a reach-out event—a contact or touch point. It follows that organizations would want to ensure the accuracy of those communication events.

# SOC's Impact on Automation of Incident Response

The level of collaboration between the security operations center (SOC) and incident response (IR) teams appears to be a factor in organizations' adoption of automation. Organizations that have fully integrated their IR team with their SOC show the greatest adoption of medium- or high-level automation, as illustrated in Figure 6. Of that group, 32% of respondents reported that the IR function is a fully integrated part of their SOC and that team members are fully cross-trained.

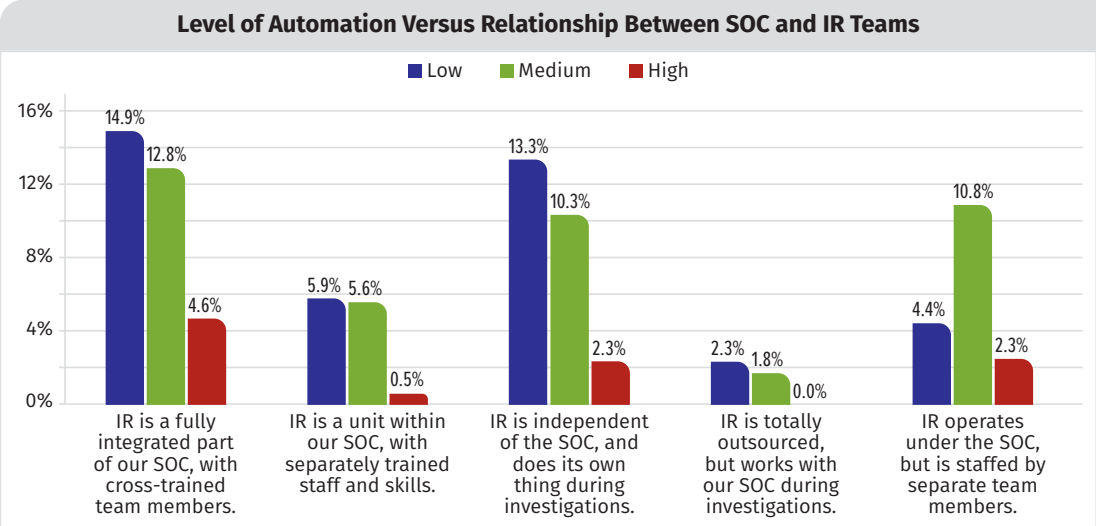



*Figure 6. SOC/IR Integration and Automation*

In most cases, the security operations and IR teams should be close-working partners. Often, alerts that the SOC investigates and determines are real issues are turned over to the IR team. Some of the outputs of mature incident response teams are improved detection techniques or other changes to improve the security posture. Only 26% of respondents indicated that IR and the SOC are not integrated (see Figure 7). In contrast, 32% reported that the SOC and IR functions are functionally fully integrated, meaning that there can be a nearly instant communication between alert analysis and incident response.

To be clear, one should not interpret that lack of integration as a bad thing. Far from it. There are numerous practical reasons for separating IR teams from security operations. For example, the IR function may be primarily devoted to employee investigation, forensics, compliance or possibly e-discovery issues. Many of these areas have a very small circle of trust or communications. In some larger companies, a forensics team may be set up to comply with U.S. Department of Justice lab standards,[2] which have strict access policies.

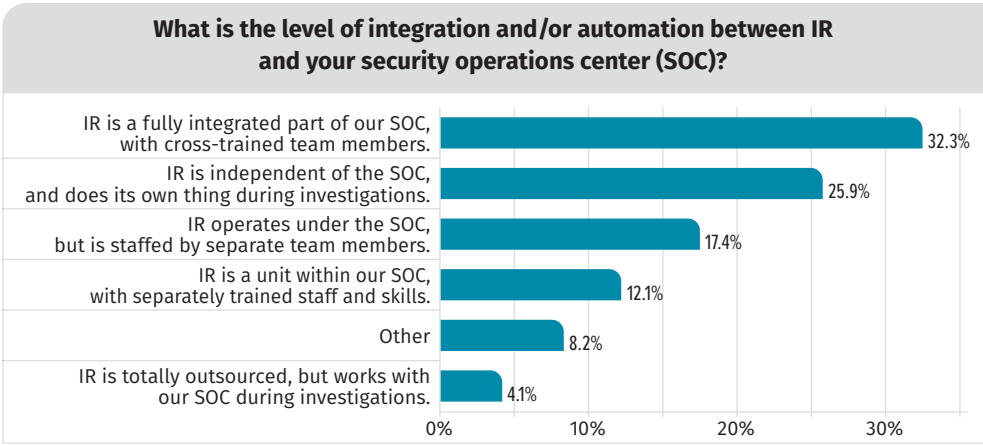



*Figure 7. Integration of IR Teams and the SOC*

[2] www.ncjrs.gov/pdffiles/168106.pdf

# Focusing on the Future

Interestingly, 15% of respondents do not plan to automate any security or IR processes in the coming year. Almost one-third of those respondents provided an explanation of why they weren't planning any automation projects. Budget was a concern for 29%, followed by a prioritization issue (18%) and an internal skills gap (14%). Only 11% said that they do not have a current need for an automation and integration project. Figure 8 provides a snapshot of the reasons given for not pursuing an automation and integration project.

There are many possible reasons for not automating security or IR processing, such as those processes are mature at an acceptable level, other topics are a priority, systems may be undergoing technology refresh, or these processes are outsourced and performing well.

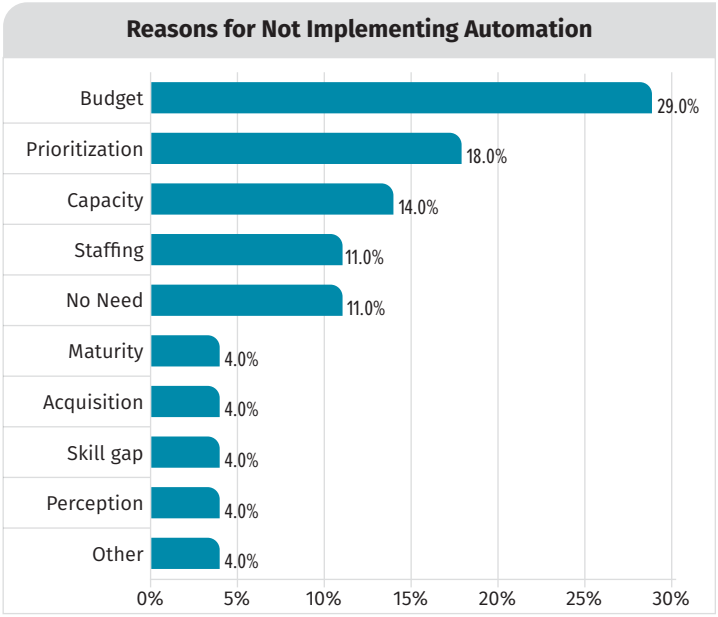



*Figure 8. Reasons for Not Implementing an Automation Project*

## Anticipated Change

Almost one-third (30%) of respondents anticipate some change in the status of automating these processes within the next 12 months, with the remaining 40% not anticipating change and 30% not knowing what to expect. Forty-nine respondents actually explained via open-ended response as to how they anticipate the status to change.

A few key trends emerge from analyzing and grouping these free-form responses (see Figure 9):

- Conduct process improvement—making nontechnical improvements on processes within their security operations and incident response functions.
- Respondents anticipate a significant improvement as a result of an automation project.
- Ensure a successful automation and integration project through anticipation.

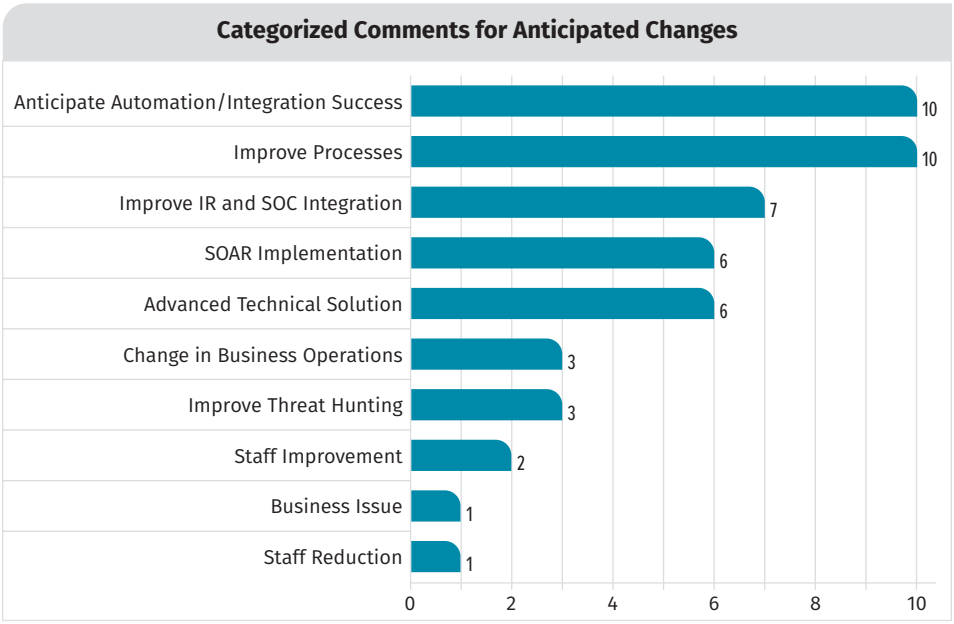



*Figure 9. Explanations for Anticipated Changes*

These responses are closely tied—processes benefit from automation, and a need to improve a process may have prompted an automation project.

After these two items, the next closest category was also people focused: improving IR and SOC. The fourth leading item—anticipated change due to implementation of a SOAR—might signal implementation of additional automation. We counted those responses separately to more accurately reflect respondents' answers and the adoption of this technology stack component.

## Planning and Preparation

The majority of respondents (58%) stated that they are planning to automate a key security or incident response process within the next 12 months. So, what are they doing and how are they doing it?

There is a well-known saying that "If you fail to plan, you are planning to fail," which goes back at least one hundred years. While this phrase may give you flashbacks to formal project management training, it still rings true. Use the following steps[3] to guide your implementation of new automation projects:

1. Determine what you need to automate and where there is an opportunity for improvement, which is often a quality improvement event. Strong candidates for automation include:
    a. Repetitive activities, such as collecting a variety of fact data about an alarm.
    b. Error-prone process supports—when the workflow and steps are understood.
    c. Data consistency between systems—when that data represents different views of the organization. The more teams and their systems have a rationalized view, the less likely they are to make mistakes.
    d. Nearly any form of repetitive lookup activity, effectively eliminating transposition errors and helping to ensure that relevant data is retrieved and available for use.
2. Set your automation requirements and deconstruct the tasks needed to accomplish the automation effort.
3. Learn from the past. Evaluating the automation projects and implementations you have underway can provide important information to assist you in future projects.
4. Plan for the future with confidence. This survey revealed that when comparing past projects to future projects, respondents faced a gap in project performance and achieving a satisfactory result. With this understanding, implementation teams can guard against suboptimal results by knowing which projects performed most poorly.

[3] Several aspects of this section were adapted from a presentation by Mark Orlando at the SANS 2020 Blue Team Summit.

## Automation Requirements

Knowing what you need your automation process to accomplish is key to the planning and implementation of any new projects. Survey results provide guidance from those already involved in implementing automation projects.

For both 2020 and 2019, the same priorities resided in the upper third or lower third, but there were two significant shifts in the results year over year. Two requirements were on top both years. Automating workflows, which retained first place, scored 56% in 2020 and 52% in 2019—clearly an important requirement. However, increasing the speed and quality of threat investigations by automating data collection and analytics, which held second place, lost 11 percentage points, down to 47% in the 2020 data. Another requirement that took a significant dip was generating reports and dashboards that can address concerns specific to the organization, which lost 9 percentage points and fell by 7% from the previous year. Figure 10 illustrates the ratings of automation requirements in the effort to improve security posture.

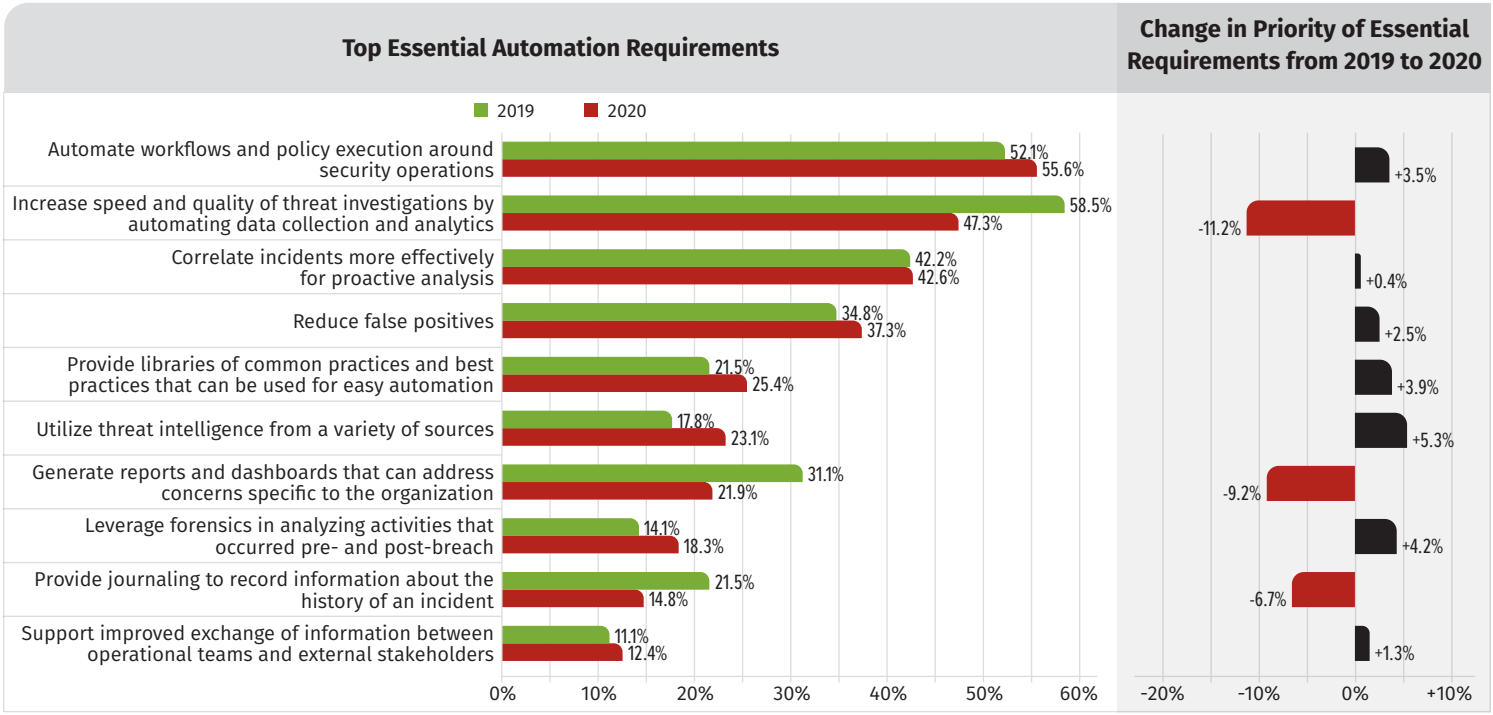



*Figure 10. Top Automation Requirements*

Two themes emerge from respondent data. First, the top three requirements are directly related to improving the handling of alerts and incidents. Automating workflows was the highest at 56%, closely followed by increasing speed and quality of threat investigations at 47% (which decreased by 11% from last year's survey) and improving correlation for more effective analysis at 43%. Second, each of these requirements relates to improving the analyst's ability to have better information available for the alert stream, which will definitely help with reducing alert fatigue.

## Learn from the Past: Automation and Integration Satisfaction

Automation is not new to the information security space. A wide variety of tools, techniques and data exchanges, such as identity management, threat intelligence integration and automatic installation of security focused agents onto domain participants, have emerged and are now well understood. Also, newer systems such as breach and attack simulation (BAS) and user and entity behavior analytics (UEBA) have emerged. Current implementations of these tool sets should definitely apply learnings from the past, taking full advantage of growing pains from the early 2000s. For example, avoid enabling every feature on day one, and instead use a graduated approach.

When it comes to automation and integration impact, the 2020 survey also measured satisfaction with the performance results of various types of automation projects. Some performance issues rates include continuous monitoring, lessening or eliminating alert fatigue, and reducing response time. More than half of respondents rated the processes based on satisfaction. The area in which respondents are most dissatisfied is eliminating alert fatigue, rated as not satisfied by 36% of respondents, with 41% rating the area as satisfied or very satisfied (see Table 4). This common complaint affects many security operations functions.

**Table 4. Satisfaction with Automation Process Implementation**

| Implementation Area | No Opinion | Not Satisfied | Satisfied | Very Satisfied | Total Satisfied |
|---|---|---|---|---|---|
| Improved visibility and monitoring infrastructure | 20.5% | 14.4% | 52.3% | 12.9% | 65.2% |
| Alert monitoring and prioritization | 16.6% | 21.5% | 46.8% | 15.1% | 61.9% |
| Reduced response time for detection, response or remediation | 18.3% | 19.8% | 50.8% | 11.1% | 61.8% |
| Improved collaboration between team members working together on incidents | 21.9% | 16.5% | 49.2% | 12.3% | 61.5% |
| Achievement of continuous monitoring | 21.9% | 19.6% | 47.5% | 10.9% | 58.5% |
| Improved early detection of threats through integrated threat intelligence feeds | 19.6% | 23.1% | 41.9% | 15.4% | 57.3% |
| More efficient and effective routine security processes | 21.8% | 22.1% | 45.4% | 10.7% | 56.1% |
| Utilization of current enterprise security tools already in place | 17.7% | 27.7% | 45.0% | 9.6% | 54.6% |
| Better prioritization of security operations activities | 20.1% | 26.3% | 44.8% | 8.9% | 53.7% |
| IR procedures that can be consistently and precisely executed | 22.9% | 27.1% | 38.9% | 11.1% | 50.0% |
| Improved handling of insider incidents | 30.3% | 23.4% | 37.2% | 9.2% | 46.4% |
| Automated security workflows (such as for detection, remediation and follow-up) that can be systematically updated as best practices emerge | 24.5% | 29.1% | 35.2% | 11.1% | 46.4% |
| Better definition of processes and owners | 25.7% | 29.9% | 36.4% | 8.0% | 44.4% |
| Elimination of alert fatigue | 23.0% | 36.0% | 34.1% | 6.9% | 41.0% |

In contrast, those areas with the highest degree of satisfaction for automation and integration projects (satisfied or very satisfied) include improved visibility and monitoring infrastructure (65%), alert stream monitoring and prioritization (62%), reduced response time all around (62%), and better team collaboration around incidents (62%). These categories demonstrate that organizations are successfully using automation and integration projects to make better use of their security apparatus (which in turn improves the ROI picture) and to make needed improvements.

The story doesn't stop there. In the majority of write-in comments, three themes emerged. A positive attitude toward automation, the importance of use cases, and the need for automation are consistent concerns. Key comments from respondents included:

- **Generally positive attitude toward automation**
  - "All lvl 1 soc analyst operation will be automated so we can train them to do more IR and less triage."
  - "Automation is great for reducing alert fatigue and prioritizing alerts. Integration is more important in my opinion because it help[s] the analyst/responder better make the right decision in a timely manner."
  - "Automation is critical in order to make incident response manageable. Manually responding to, analyzing, containing and remediation incidents is a losing battle."
- **Importance of use cases**
  - "Automation is a journey that should be taken on a bite at a time. Pick good use cases to tackle (such as automating response to user submitted suspicious emails)."
  - "Automation requires to know what you are going to automate and why."
- **Issues of concern**
  - "We lack automation in our environment and are drastically behind the curve when it come[s] to a high-tech environment."
  - "[We need] automation to keep up."

Respondents likely based some of these satisfaction ratings on anecdotal experiences. It is important that organizations use some kind of metric to evaluate whether their automation efforts have yielded positive results and that those results be quantifiable.

## Plan for the Future

Based on respondents' automation requirements and their satisfaction with their ability to improve security operations with automation projects, it makes sense for organizations to consider new projects. Some, but not all, respondents are confident that their current projects will really improve the state of security operations and incident response. The critical lesson here is to avoid overselling automation and integration projects to organizational stakeholders.

The three highest rated projects (rated as confident or higher) that would improve operations included improving visibility and monitoring infrastructure (84%), which has a natural tie in to improving asset management; alert monitoring and prioritization

(83%); and improving the priority of security operations activities (79%). Two of these projects—improving visibility and alert monitoring prioritization—also scored high on satisfaction ratings for previously implemented projects. See Figure 11.

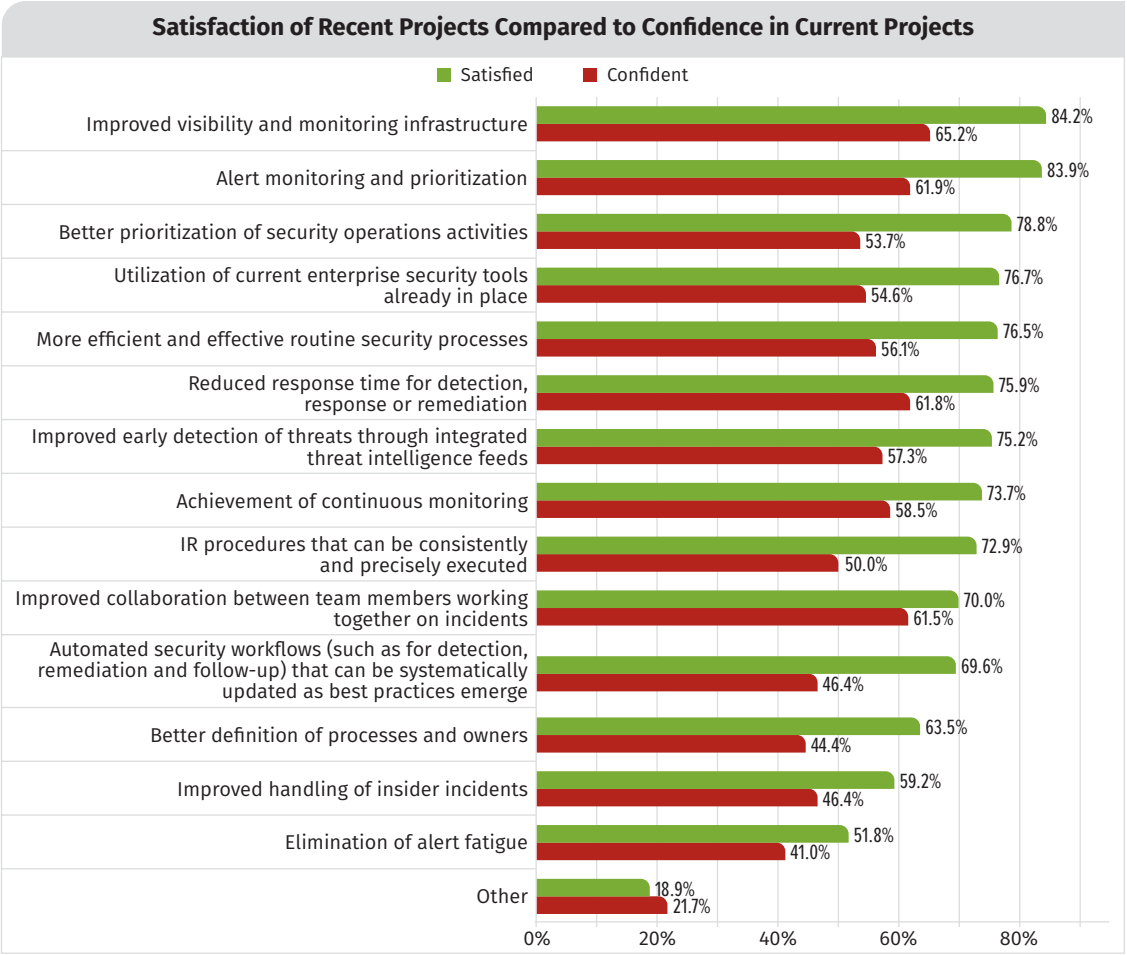



*Figure 11. Current and Past Project Satisfaction Rates*

Unfortunately, analysis of the data also indicated that organizations had the least amount of confidence in "reducing alert fatigue," which had the highest no-confidence score (36%), followed by "better definition of process owners" (28%). These two areas continue to haunt the SOC. Reducing alert fatigue is a common reason to implement automation, yet the data continues to show that this is a difficult problem. Be careful about setting expectations for future projects.

## Metrics: Quantify Automation Results

As the day-to-day practice of security operations matures, senior management starts asking security teams to demonstrate that their budget and activities improve the organization's security posture. Metrics are an essential tool for security pros to understand and demonstrate how their systems and processes support the business—well-designed metrics support data-driven decisions.

Two measures emerged as the most useful and in active use. The most valuable metric was "Number of incidents identified through monitoring program" (57%), followed closely by "Number of endpoints impacted by an incident" (56%). These results show that organizations are measuring the effectiveness of their security spend. When taken together, these top two measures support *impact assessment*—quantifying the impact that monitoring has on identifying a security issue and how it affects the organization's environments.

Figure 12 illustrates respondents' evaluation of various metrics available to them.

Two related metrics also emerged as the most useful in the survey, but not actively in use by respondents: "Mean time from containment to remediation" and "Time to complete standard and custom tasks (e.g., average and mean time for each of the phases of the IR process)," with the latter having the largest gap between active use and not in use. It shouldn't be surprising that these activities are not tracked, but understanding what they measure is desired. To actually collect data to support using these metrics, organizations and staff would need to spend more time discretely tracking the phases of an incident, as well as devise methods to actually track incidents as they are resolved. Given that tracking time detracts from actual incident handling, it logically follows that respondents would prioritize solving for an incident over meticulously tracking time expended in discrete phases.

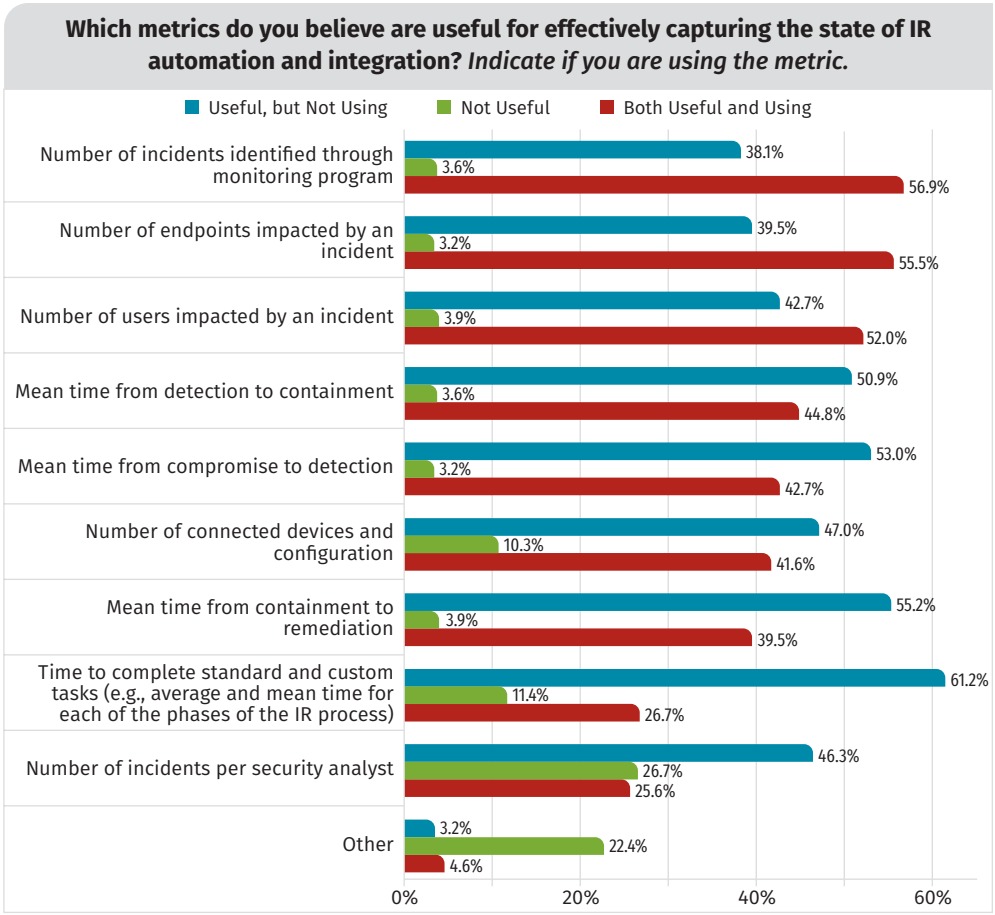



*Figure 12. Metrics for Automation and Integration*

Respondents found "Number of incidents per security analyst" to be the least useful metric (26%), which showed incident volume.

Lastly, a small number of respondents suggested metrics that were not included in the survey. Their examples included comparison measures, such as "time spent on tasks that could be automated" and "approximate time saved by automation (chart by task completed in [K]anban)."

Collecting automation-related metrics is critical to determine the impact of an organization's investment—how effective automation really is, whether the technology performs as expected and management's level of satisfaction with the outcomes. Developing a new strategy for metrics will take time. Make a plan and stick to it.

# Growth, Change and Budget

Organizations are definitely investing in automation and integration, as a percentage of the information security budget.

Budget commitment for automation is on the rise in 2020. Spending increased at the modest spending level of 3–4% and at higher levels of 7–10%, and then took a dip for spending greater than 10%. This amount of change demonstrates that organizations see the value in automation and integration. When looking at planned budget for next year, the picture looks even better, with a *significant increase in spending above 10% of the security budget to an anticipated 16.4%!* Increased spending agrees with confidence in projects that are underway, discussed earlier. (See Table 5.)

**Table 5. Investment versus Budget**

| What is the current investment in automation, based on the percentage of your present security budget? | 1–2% | 3–4% | 5–6% | 7–10% | Greater than 10% | None | Unknown |
|---|---|---|---|---|---|---|---|
| 2019 Investment Level | 18.0% | 6.6% | 6.6% | 1.6% | 11.5% | 18.0% | 37.7% |
| 2020 Investment Level | 13.8% | 11.9% | 7.5% | 5.7% | 8.2% | 9.4% | 43.4% |
| Year over Year Change | **–4.2%** | 5.3% | 0.9% | 4.1% | **–3.3%** | **–8.6%** | 5.7% |
| 2020 Next 12 Months | 5.7% | 11.9% | 13.8% | 6.9% | 16.4% | 1.3% | 44.0% |

Factors influencing investment decisions around automation can be considered as both direct and indirect. Direct factors are the common leading ones: budget and management support along with staffing concerns (i.e., the overall number of staff and how the required skills are being acquired and/or kept current through training and certification).

In 2020, the leading factor that affects the organizations' decision for the level of spending is the amount of skilled internal staff to conduct automation and integration projects (52%). This factor was also the highest in 2019, at 49%. The next two factors scored at the same relative ranking, but were chosen *significantly less often in 2020 than in 2019.* Budget and management support was second in both years. While this factor scored 61.7% in 2019, it scored 50.3% in 2020—a substantial drop of 11.4%. Given that spending increased year over year and future spending is double-digit at the 3% to 6% level, it is clear that respondents are committing budget to automation and integration projects. See Table 6.

**Table 6. Budget Factors for Automation**

| Budget Factors | 2019 | 2020 | % Change |
|---|---|---|---|
| Amount of skilled staff | 49.2% | 52.1% | 2.9% |
| Budget and management support | 61.7% | 50.3% | –11.4% |
| Skills required to integrate and operate tools | 53.1% | 43.6% | –9.5% |
| Automation and interoperability across existing tools | 31.3% | 37.0% | 5.7% |
| Integration and coordination between security and IT operations teams | 30.5% | 32.7% | 2.2% |
| Correlating data into useful information | 30.5% | 31.5% | 1.0% |
| Establishing policy that allows automation of its management and execution | 21.1% | 24.2% | 3.1% |
| Ease of acquiring needed data | 11.2% | 14.5% | 3.3% |
| Performance | 7.3% | 9.7% | 2.4% |
| Other | 4.1% | 4.2% | 0.1% |

# Perception: What Are the Risks in Getting There?

There are definitely risks in any automation and integration effort or project, like any IT focused effort. Recall the essential requirements: automating workflows, increasing the quality of threat investigations by automating data collection and improving correlation. Of all requirements, these essentials were most closely related to improving how security pros make use of event, enriched and alarm data. A well-designed automated workflow reduces risk to the analyst because the workflow performs the same set of actions every time, ensuring consistency. The same applies to automated data collection because an analyst freelancing an investigation, no matter how skilled they are, may miss a critical data element. Or worse, the analyst may be interrupted, and not pick up where they left off. Lastly, improved incident correlation means that the security operations team can connect the dots between a prior case and a current case, meaning that if an issue repeats itself, they should be able to find it while working a current case.

Respondents realize that efficiency comes at a price. Organizations need an upfront investment of dollars, staffing, weighting opportunity costs and resources to reap the benefits of automation. The risks associated with the integration process are also a leading concern. With these factors in mind, the survey directly asked respondents what they believed were potential risks in security automation. Two answers tied for first place at 50%: dependency on other IT operations processes and tools, and resource constraints (see Figure 13).

The top item from 2019, budget constraints, dropped from 60% in 2019 to 39% in 2020, which demonstrates budget was freed up year over year. Thus, budget constraints imposed a 21% lower risk of impact for organizations that are capable of identifying and implementing some degree of an automation and integration project.

**What do you perceive as potential risks in security automation?**
***Select all that apply.***

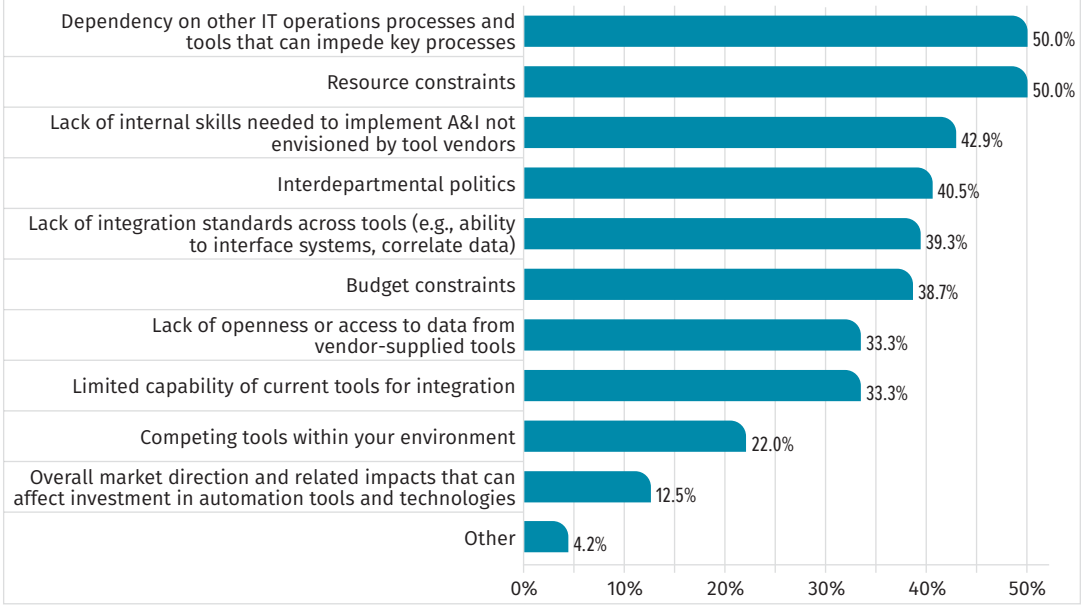



*Figure 13. Potential Automation Risks*

Making things look easy usually takes hard work. Developing and deploying effective automation can be demanding, particularly to get the processes "right" and the interfaces semantically "correct." And it can often take longer than anticipated, regardless of the technology organizations use to achieve the automation.

# Summary

Automation and integration is often hailed as a great enabler for the future. This survey identified how respondents are adopting systems, where their systems currently stand and what is on the planning horizon. Most organizations are focused on making people smarter.

A few key factors, successes and bumps along the road were identified, providing several takeaways:

- Automation requires upfront investment, and organizations recognize this with a move towards increased budgets for tool implementation. If you are implementing an automation project for the first time, be very careful to select projects that provide incremental success, are not overly complex and can work within the constraints of your current data. Don't start the first automation and integration project that requires a software development just to manage the data.
- Close the gap between current projects and future projects. On average, there is only a 17% gap between satisfaction between a prior project and a new one that is very similar. Consider this targeted project management advice: Be sure that you understand why a similar project did not provide the level of expected results from your peers or others.
- Whenever possible, use well-defined standards such as JSON for data or event generation, for your projects. This ensures that consuming the data and information will be significantly easier for your security solution.
- Think hard about how to measure automation and integration projects. The metrics you develop should be purposeful and provide concrete guidance for your security operations.

Automation is about bringing people, process and technology together. As automation projects are devised, funded and implemented, they should improve how staff use systems and improve their security operations practices.

## About the Author

**Don Murdoch** is a SANS community instructor specializing in incident response and security operations. A solutions-oriented IT director and consultant, he has hands-on experience leading software/infrastructure/system development efforts for financial and healthcare systems, including requirements definition, executive-level strategy and communications, solution design, architecture, deployment, production and dissolution. Don is the author of two prominent blue team handbooks: The first focuses on incident response, while the second focuses on SOC, SIEM and threat hunting. He holds the SANS GSE, Cyber Guardian Blue Team and 20 other GIAC certifications, and he is also a certified TOGAF Enterprise Architect and SABSA Chartered Security Architect.

## Sponsor

**SANS would like to thank this survey's sponsor:**

DOMAINTOOLS®