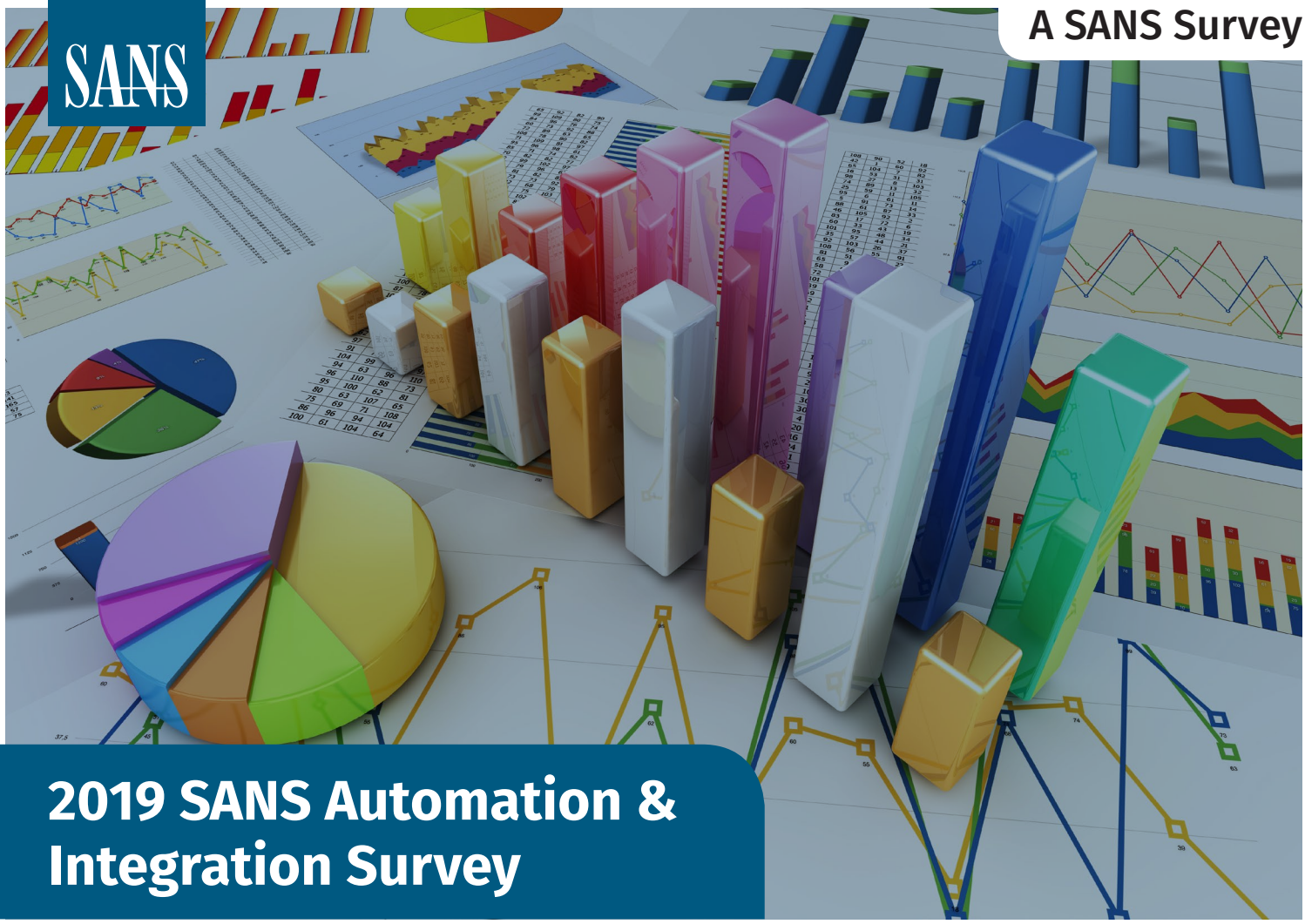
SANS

A SANS Survey



2019 SANS Automation & Integration Survey

Written by **Barbara Filkins**

March 2019

Sponsored by:
LogRhythm

Analyst Program

Executive Summary

Automation balances machine-based analysis with human-based domain knowledge to help organizations achieve optimal workflows in the face of staff shortages and alert fatigue, all caused by an increasing number of destructive threats. Yet, 59% of survey respondents indicate that their organizations use low levels or no automation of key security and incident response (IR) tasks. In this new SANS survey, we wanted to understand and explore some of the misconceptions versus facts around automation and what to do about it.

Automation and its issues—although a relatively new concept for security—have been around for generations, ever since the 1940s in the automotive industry. Unfortunately, broad misconceptions about automation's benefits have arisen that practical experience both negates and, ultimately, results in the failure of the enterprise moving to processes that truly provide a substantial cost-to-benefit ratio.

Accomplishing effective automation means understanding these common misconceptions, determining how to overcome them, taking into account the potential risks, and then working through the resulting challenges. SANS presents several broad misconceptions about automation that have arisen though the years, discussing them in light of our survey results, with the goal of avoidance by the cybersecurity community.

Activities that Depend on Automation

Activities dependent on well-known, structured data sources—such as network packet and flow traffic—should be considered more mature than those that support decision-based analysis, such as remediation or forensics. This reflects directly on the level of automation achieved. See Table 1.

Table 1. Automation Levels

NIST Cyber Security Framework (CSF) Phase[1]	Key Activity	Automation Level	
		Medium	High
Detect	Security monitoring and detection	35.0%	27.1%
Protect	Data protection and monitoring	32.1%	17.1%
Identify	Asset and inventory management	31.4%	10.7%

Misconception #1: Anything can be automated.

Integration requirements across the IT stack today are numerous, broad and complex, making it nearly impossible for operational teams to develop the unique plug-ins needed to orchestrate tasks across all the endpoints and security tools in place within their infrastructure.

Specifically, the IoT revolution limits the capability to provide enterprise automation, given the diversity of endpoints that inhibit interoperability. Given the rapid explosion of these endpoints, there is a need for security orchestration, automation and response (SOAR) platforms that can handle the integration and the numbers. Don't overlook the vulnerabilities these devices and sensors introduce!

Misconception #2: Automation will replace people with machines or robots.

Automation allows security experts to focus on more important aspects of the security life cycle. In this survey, automation doesn't appear to negatively affect staffing. For the most part, respondents see automation as allowing them to explore new areas and to concentrate on more strategic endeavors.

[1] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Misconception #3: Existing tools can be easily integrated to automate anything.

The integration of disparate tools and technologies to achieve crucial interoperability appears to be a more pressing concern for respondents than staffing. This can create risk and possible uncertainty in budgeting for automation, as the specific requirements for interoperability are not well-understood.

Taxonomies are typically applied to data within security technology—this is a much larger issue than it is for automation alone, and there is no standardization in sight. The end customers interested in automation need to know that the tools they use can typically be made to work regardless of the taxonomy, and other complexities around integration—but the benefit may not be worth the effort, and there are solutions with offerings that can help alleviate some of the pain of integration.

Misconception #4: Automation is easy to measure.

Although the use of automation for response is still in the planning stages at most organizations, respondents feel positive about its ability to enhance the performance of SecOps and IR teams, such as improving alert monitoring/prioritization and eliminating alert fatigue. Organizations do, however, need to develop better metrics to visualize and evaluate automation efforts.

Misconception #5: Automation is quick to implement.

Actually, automation takes a tremendous amount of effort to arrive at the point where it makes things look easy. Don't underestimate the resources needed to define the processes—in the light of more effective tools—and close the semantic gaps in the data gathered. Effective automation depends on the integration of people, process and technology. Automation of security processes will face bumps in the road—bumps that organizations can overcome by reaching out to other industry sectors (such as document management) that have embraced automation across diverse platforms and disparate technologies to understand and appropriately apply the "lessons learned."

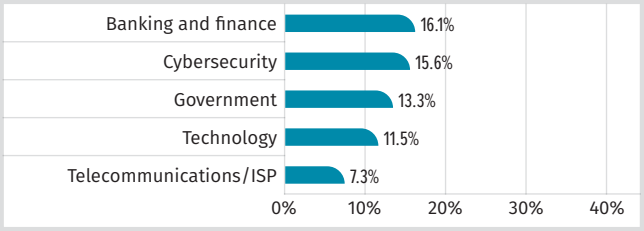
Automation in the Organization

Automation is not a new concept. The term was first coined circa 1946 in the automobile industry. In the late 1980s, the term *workflow* became synonymous with document imaging and management processes. Early workflow automation systems during the 1990s successfully replaced basic paper-based processes with electronic ones. As have other industries, the security community has begun to embrace automation as a solution to handling tedious, repetitive tasks, allowing skilled staff to focus on more strategic and advanced endeavors.

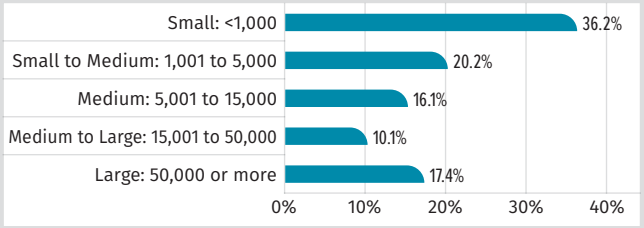
Respondent population:

- **218** professionals, who attested they are engaged in the practice of cybersecurity, specifically in the areas of how security operations should interface with IR
- **70%** security professionals
  - **47%** security analysts, administrators and architects
  - **27%** security management including C-level management roles (CSO, CISO or VP Security)

The top five industries representing enablers of automation are:



Organizational size in terms of its workforce, inclusive of both employees and consultants:



Our survey dataset draws from global sources, weighted toward North America, but with significant operational presence in Europe and Asia.

	HQ	Operations
United States/Canada	64.2%	98.7%
Europe	16.5%	44.5%
Asia	7.8%	35.3%

SOAR, first defined by Gartner in 2015 as "security operations, analytics and reporting," has become a common acronym throughout the security community when referring to automation and integration solutions, with "response" substituted for "reporting."[2] Orchestration actually depends on these two concepts working together to achieve improvements in response, such as efficiency (increased numbers of incidents being worked per analyst) and performance (decreased mean time to remediation from detection). (See sidebar.)

Gauging the maturity of security automation within an organization is difficult; its use within an enterprise tends to evolve organically, a natural extension of individuals and teams trying to do their day jobs more effectively. The Carnegie Mellon Capability Maturity Model Integration (CMMI)—a well-respected approach to assessing organizational maturity in terms of people, process and technology—provides a perfect backdrop for seeing how automation and integration can work together. Figure 1 shows such a road map for security automation.

Key Terms

Orchestration
Orchestration invokes and coordinates functionality across diverse technologies and independent tools to create an overall workflow. Orchestration depends on automation and integration.

Automation
Automation refers to the execution of a sequence of tasks without human intervention.

Integration
Integration allows an automation platform to access the capabilities of other independent tools through a well-defined interface—preferably standards-based (such as a RESTful API or messaging framework), and supporting a common taxonomy for seamless data and process exchange across the connected infrastructure.

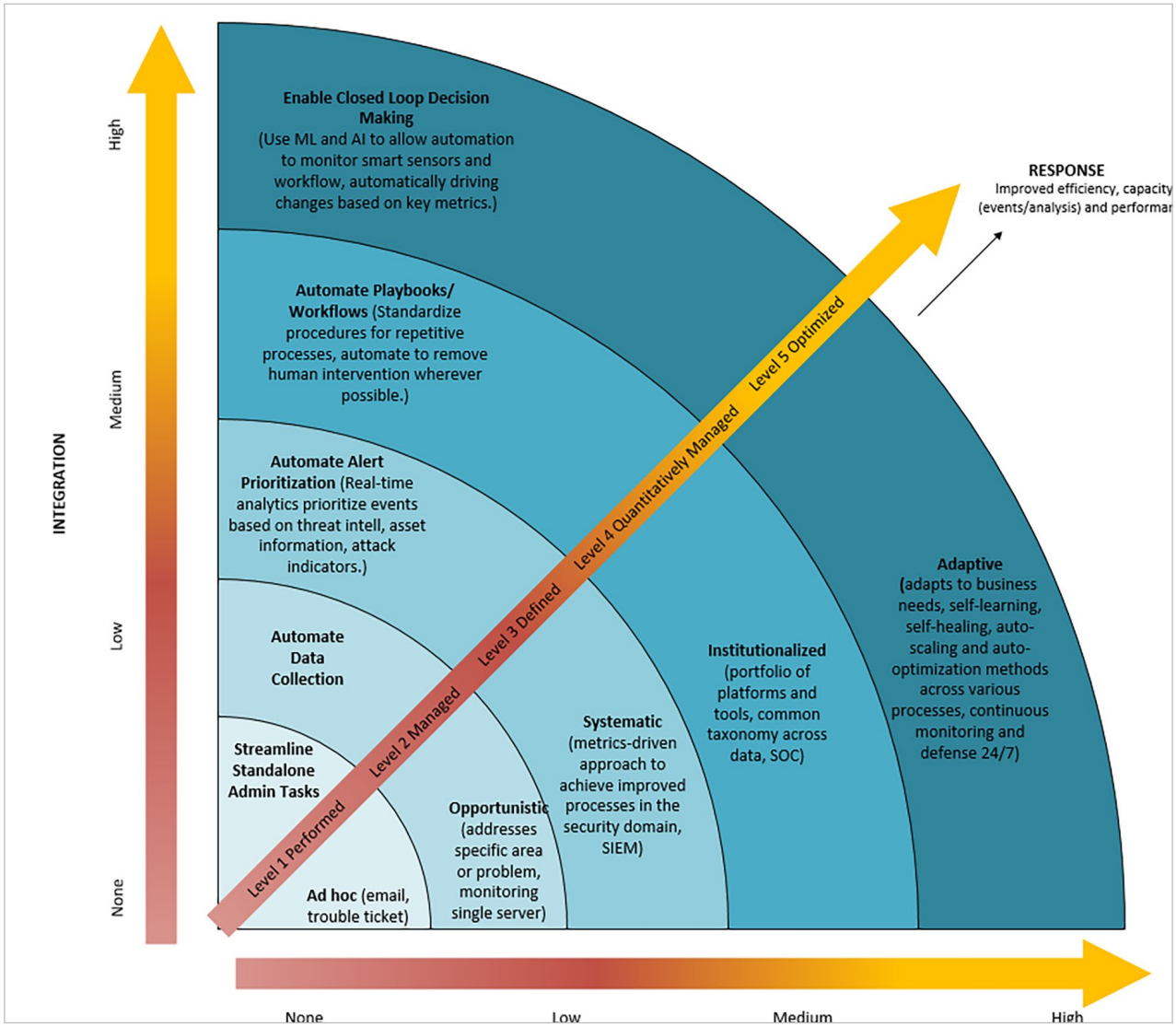


Figure 1. CMMI Applied to Security Automation, Integration and Response

[2] https://www.gartner.com/doc/reprints?id=1-4O4VC17&ct=180109&st=sb

Most respondents (46%) reported having minimal automation of key security and IR processes. This survey explored some of the reasons why this may be the case. See Figure 2.

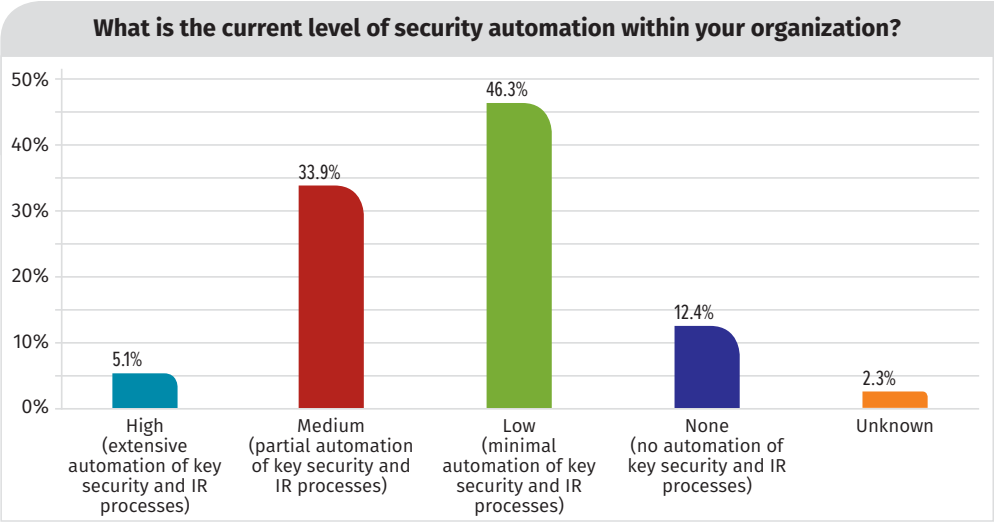


Figure 2. Level of Security Automation

Platforms: Where Is Automation Being Used?

Not surprisingly, most systems subject to some level of security automation are under the direct control of the organization as opposed to systems/assets not owned by the organization. Other systems lacking automation include industrial control systems, IoT devices or sensors, and other examples of operational technology (OT) such as smart sensors and wearables. See Figure 3.

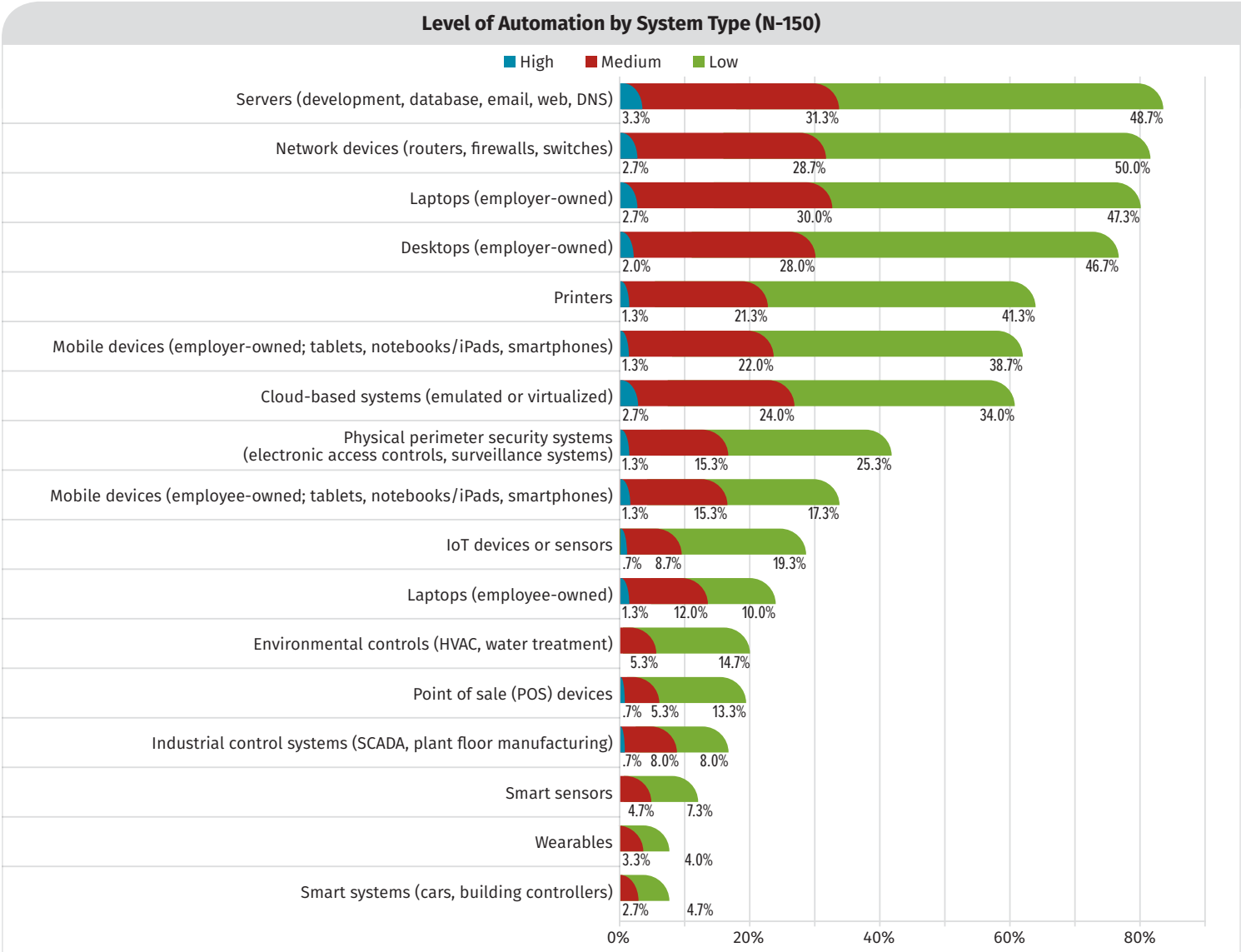


Figure 3. Level of Automation by System Type

In the 2018 SANS ICS survey, SANS noted that diagnostic and prognostic data in OT systems are excellent indicators of normal vs. abnormal processes, indicating expected operational problems (reduced output, intermittent disruptions, premature wear) as well as accidental or malicious tampering or the presence of a threat inside the system.[3] Typically, most automated security tools do not use such process-oriented data to evaluate the security posture of a system and determine whether that posture has changed. Diversity across IoT endpoints—each with its own unique connectivity, APIs and data formats—inhibits the needed interoperability for pervasive automation. Efforts by academia, industry and standards bodies are underway, but a definitive road map to achieving the needed orchestration still remains unclear.[4]

Process: How Is Automation Being Used?

Automation supports numerous key activities that map into the overall security life cycle as defined by the phases in the NIST Cyber Security Framework (CSF). Some activities used in the survey do not map directly to CSF phases. The SANS crosswalk between the CIS Security Controls and CSF[5] was referenced for:

- **Incident response—**Belongs to both Detect and Respond phases
- **Pen-testing and red-teaming activities—**Covered by CIS Control Family 20, mapped to Respond and Recover phases

Table 2 identifies those activities that this survey addressed in bold.

Table 2. NIST CSF Version 1.1 Phases and Categories

Phase	Definition	Associated CSF Categories[6]
1. Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities	**Asset Management (including inventory management)** Business Environment Governance **(including compliance)** Risk Assessment **(including threat intelligence)** Risk Management Strategy
2. Protect	Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services (e.g., supports ability to limit or contain impact of a potential cyber security event)	Access Control Awareness and Training Data Security **(includes data protection and monitoring)** Information Protection Processes & Procedures Maintenance
3. Detect	Develop and implement the appropriate activities to identify the occurrence of a security event	Anomalies and Events **Security & Continuous (24/7) Monitoring** Detection Processes **Incident Response**
4. Respond	Develop and implement the appropriate activities when facing a detected security event	Response Planning Communications Analysis **(includes digital forensics)** Mitigation Improvements **Incident Response** **Pen-Testing/Red-Teaming**
5. Recover	Develop and implement the appropriate activities for resilience and to restore any capabilities or services that were impaired due to a security event	Recovery Planning Improvements Communication **Pen-Testing/Red-Teaming**

[3] https://www.sans.org/reading-room/whitepapers/ICS/2018-industrial-iot-security-survey-shaping-iiot-security-concerns-38505, p. 10.

[4] https://link.springer.com/article/10.1007/s11036-018-1089-9

[5] www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

[6] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Overall, security monitoring and detection leads as the key activity supported by automation (with 35% reporting a medium level of automation and 27% characterizing their automation as high). Monitoring and detection tools, especially in the network realm, have long relied on well-established tools for automated alerting. Data protection and monitoring is next highest, also related to the use of automation for monitoring structured data. Asset and inventory management also shows a definite investment in automation, especially critical for large enterprises. Pen-testing and red-team automation ranked relatively low; surprising, since these activities have very automated toolkits available. See Table 3.

Table 3. Level of Automation by Activity

Manual	Key Activity Supported	Activity Usage	Level of Automation			
			Manual	Low	Medium	High
Detect	Security monitoring and detection	97.9%	7.9%	27.9%	35.0%	27.1%
Detect and Respond	IR	93.6%	27.9%	35.0%	20.0%	10.7%
Recover	Remediation	92.1%	35.0%	25.0%	25.0%	7.1%
Identify	Threat intelligence	90.0%	18.6%	37.1%	22.9%	11.4%
Protect	Data protection and monitoring	90.0%	10.7%	30.0%	32.1%	17.1%
Protect	Security administration	90.0%	16.4%	35.0%	27.1%	11.4%
Respond	Digital forensics	89.3%	42.1%	26.4%	12.9%	7.9%
Identify	Compliance support	88.6%	27.1%	24.3%	28.6%	8.6%
Respond and Recover	Pen-testing	83.6%	27.1%	25.7%	23.6%	7.1%
Identify	Asset and inventory management	82.1%	16.4%	23.6%	31.4%	10.7%
Respond and Recover	Red-teaming	67.9%	30.7%	22.1%	10.7%	4.3%

Digital forensics and remediation activities still depend on manual processes, areas where human insight is still largely necessary. Digital forensics and incident response (DFIR)—a multidisciplinary profession focused on identifying, investigating and remediating computer network exploitation—still relies on tedious processes, such as log and intelligence analysis, where analyst skill could be augmented through automation. DFIR automation is a thing that needs to happen.

Automated remediation tasks introduce risks that not every organization can safely take. Consider, however, the use of automation to expedite investigations and response by enriching data, performing lookups, and to kick off manual remediation assignments by notifying individuals and gaining necessary approvals.

SOC's Impact on Automation

The level of collaboration achieved between the security operations center (SOC) and 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. See Figure 4.

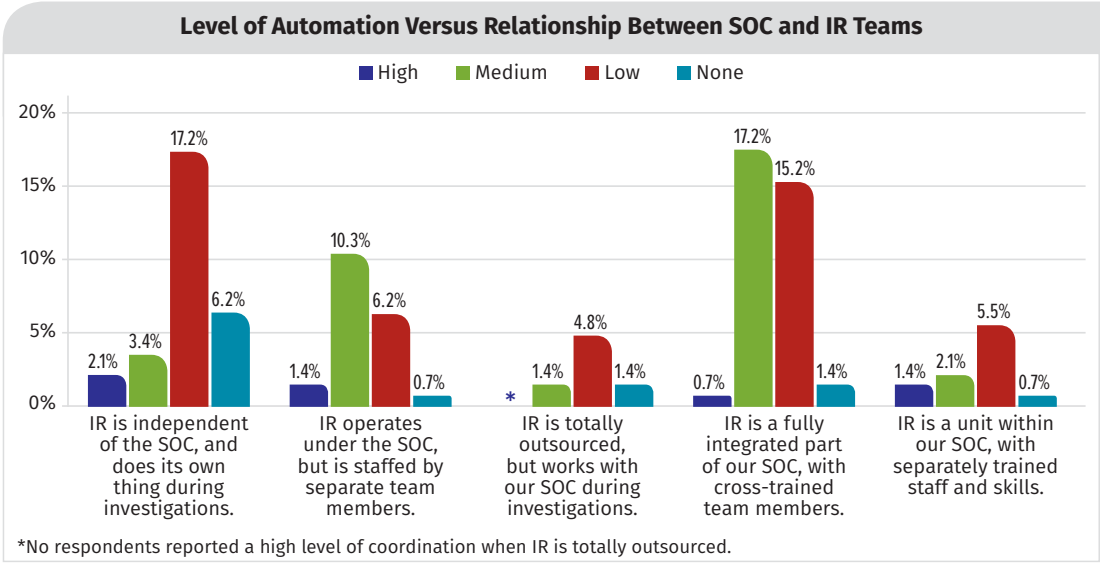


Figure 4. Level of Automation Versus SOC and IR Coordination

How this dependency may affect future automation and integration plans remains unclear. Whereas 52% foresee no change in status during the next 12 months, 25% remain unsure. For the 23% who anticipate change, several respondents noted that they are in the midst of defining the problem.

A significant portion of SOC actions focus on finding and validating security incidents—activities that are also key to IR. Fully integrating the SOC and IR teams can contribute to the success of SOC automation. Consider addressing any cultural issues when starting to consider improving instrumentation—including working to improve relationships between the SOC and IR teams, and removing any silos that stand between these groups.

Defining Automation Efforts

"More information-sharing in day-to-day business, not just during an incident [is needed]. Cross-access to specialized tools [and b]etter, more standardized policy, process and procedure documentation [are also needed] to make cross-training easier."

– Survey Respondent

Platforms: What Are the Leading Tools?

Table 4 shows that alerts and log analysis tools lead the advanced levels of automation. This may be in part due to the fact that the data sources for these tools tend to be better defined (normalized to a given schema) with less variation in understanding both the syntactic (format) and semantic (meaning, definition) constraints than other sources such as user activity monitoring.

Table 4. Level of Automation for Key Tools

		Level of Automation		
	Total Used	Low	Medium	High
Browser and screen-capture tools	48.9%	31.4%	14.6%	2.9%
Third-party tools specifically used for legal digital forensics	50.4%	29.2%	13.9%	7.3%
Security case management systems	51.8%	23.4%	19.0%	9.5%
User notification or complaints	56.2%	23.4%	18.2%	14.6%
File integrity monitoring (FIM)	59.1%	30.7%	19.0%	9.5%
Network traffic archival and analysis tools	59.1%	27.0%	19.0%	13.1%
Behavioral monitoring (profiling)	60.6%	34.3%	19.7%	6.6%
Sandboxing	61.3%	29.2%	19.7%	12.4%
SSL visibility (encryption/decryption) at the network boundary	62.8%	19.0%	21.9%	21.9%
User activity monitoring tools	62.8%	33.6%	15.3%	13.9%
Intelligence and analytics tools or services	65.0%	31.4%	27.7%	5.8%
Services availability monitoring	65.0%	24.8%	22.6%	17.5%
Homegrown tools for our specific environment (e.g., playbooks)	67.9%	34.3%	21.2%	12.4%
Identity management	70.1%	23.4%	32.8%	13.9%
Network packet capture or sniffer tools	70.1%	34.3%	19.0%	16.8%
Host-based intrusion detection (HIDS) agent alerts	71.5%	28.5%	26.3%	16.8%
Network-based scanning agents for signatures and detected behavior	75.2%	22.6%	32.8%	19.7%
Network flow and anomaly detection tools	75.2%	31.4%	23.4%	20.4%
Secure web gateway (on-premises and/or cloud proxy)	78.1%	24.8%	27.7%	25.5%
Endpoint controls (e.g., network access control [NAC] or MDM)	80.3%	19.0%	40.1%	21.2%
SIEM correlation and analysis	83.2%	24.8%	28.5%	29.9%
Endpoint detection and response (EDR) capabilities	86.1%	27.7%	38.0%	20.4%
Vulnerability management tools	86.1%	25.5%	36.5%	24.1%
Log analysis	91.2%	29.9%	33.6%	27.7%
IPS/IDS/Firewall/Unified threat management (UTM) alerts	92.0%	21.9%	40.1%	29.9%

Respondents approach tool integration in different ways, ranging from using no tools (21%) to both acquiring dedicated platforms and integrating existing tools (26%), demonstrating the need to match their approach to technology with staff skills. See Figure 5.

Respondents are looking to leverage existing tools, with 34% involved in in-house integration and orchestration efforts and another 26% acquiring automation tools to aid their endeavor. Here, standard methods for integration, such as standard data formats (JSON, XML and so forth), API functionality and messaging frameworks should be used.

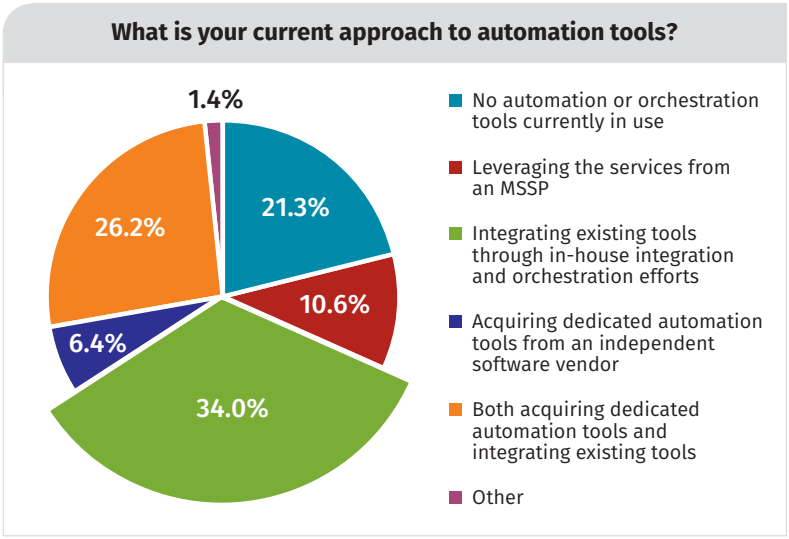


Figure 5. Approach to Automation and Integration of Tools

Something more may be needed as organizations look to institutionalize security automation across their enterprises, as both SIEM and SOAR platforms depend on well-defined interfaces and common data taxonomies. Consider doubling up on using your SIEM schema in deploying your SOAR solution—you have already normalized the data you are collecting into one consistent format.

Open standards are developed and maintained via a collaborative and consensus-driven process to facilitate interoperability and data exchange among different products or services. These 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. The relevant integration standards that have emerged—such as NIST Security Content Automation Protocol (SCAP) 2.0 and OASIS Open Command and Control (OpenC2)—have a relatively low level of adoption, possibly because the automation they define is not a truly machine-definable problem, other than for the threat/response actions. Additionally, commercial vendors are supporting messaging frameworks with a trend to fully use the framework as open source, providing it to the security community without charge to improve interoperability across security products and tools.

If most analysts are good at writing scripts, don't hesitate to develop an integrated development environment (IDE) with a variety of Python, Ruby or other tools. However, if the majority are noncoders, look to leverage the strengths of a SOAR platform that has simple drag-and-drop functionality or even consider completely outsourcing development to a managed security service provider (MSSP).

Growth, Change and Budget

More than 57% of respondents anticipate changes to the focus of their use of automation in the next 12 months, while another 28% remain unsure. The top five industries, all of which significantly influence the security market, show they are definitely anticipating a change in their adoption of automation. See Figure 6.

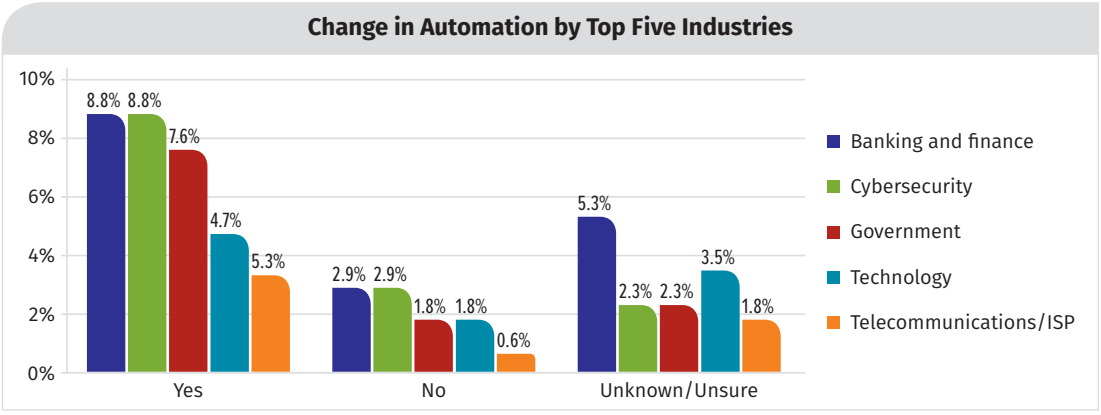


Figure 6. Change in Automation Adoption: The Top Five Industries

This change is undoubtedly due to a growth in automation. Allocations for automation as a percentage of an organization's present security budget for the next 12 months are increasing over current levels, along with the uncertainty. See Table 5.

Table 5. Budget for Automation

	Unknown	None	1–2%	3–4%	5–6%	7–10%	Greater than 10%
Current	37.7%	18.0%	18.0%	6.6%	6.6%	1.6%	11.5%
Next 12 Months	44.3%	6.6%	10.7%	9.8%	9.0%	4.9%	14.8%
Response	6.6%	-11.5%	-7.4%	3.3%	2.5%	3.3%	3.3%

Interoperability
Interoperability is the ability of computer systems or software to exchange and make use of information.

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. See Figure 7.

Indirect factors include the challenges of making tools interoperate in an automated environment; correlating data to obtain useful, actionable information for decision making; and establishing collaboration between the SecOps and IT teams. Understanding these factors allows an organization to develop a solid approach—regarding scope, schedule and resources—upon which the direct factors can be realistically evaluated.

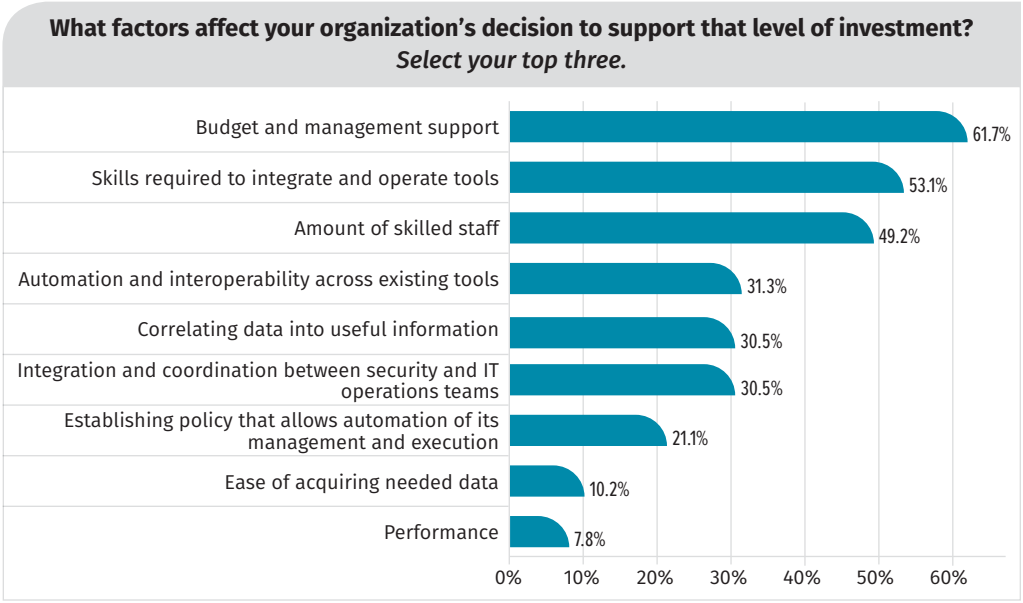


Figure 7. Factors Influencing Automation Investment

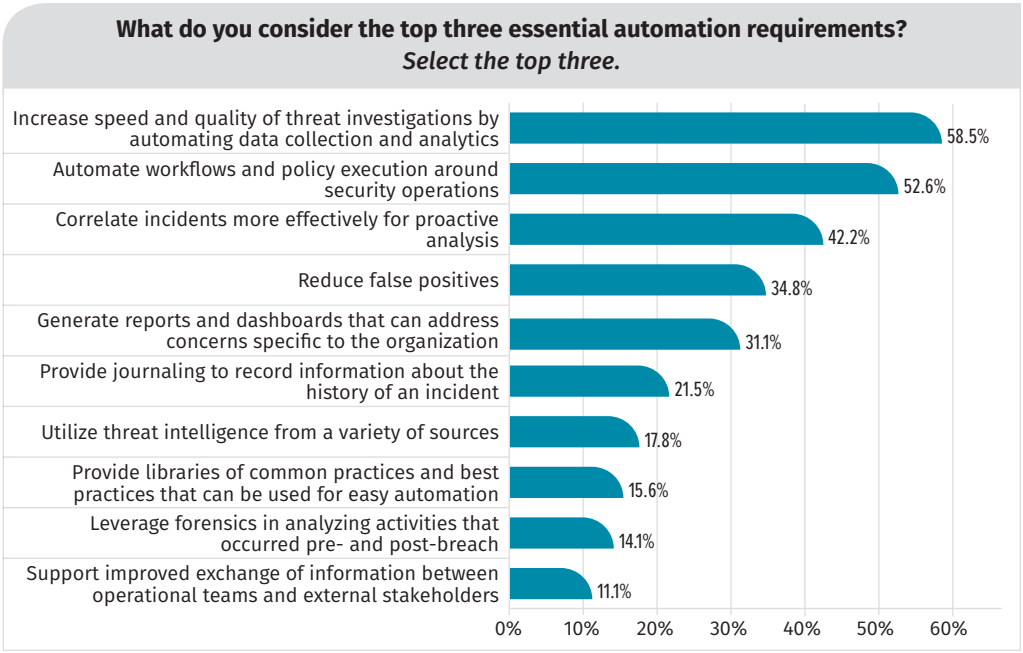


Figure 8. Top Essential Automation Requirements

Perception: What Are the Risks in Getting There?

Most respondents (59%) are looking to automation for improvements in threat investigations, followed by the ability to automate workflows and policy execution (53%) and being able to correlate incidents more effectively for proactive analysis (42%). See Figure 8.

Respondents realize that efficiency comes at a price. An upfront investment of both dollars and resources is needed to reap the benefits of automation. The risks associated with the integration process are also a leading concern, both in terms of overall interface standards and limitations in current tools, as shown in Figure 9.

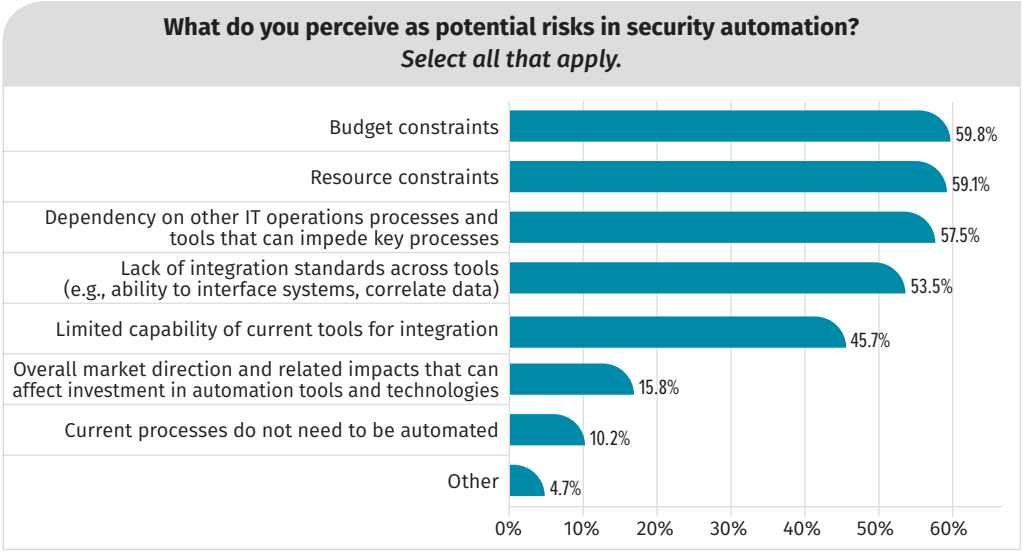


Figure 9. Automation Risks

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 being used to achieve the automation. Accenture Plc, the global consulting firm, took five years to develop the software and services it uses to streamline and automate processes in such areas as finance and accounting, marketing and procurement. The software and services sit on top of existing databases and record-keeping systems. Interestingly, this automation did not result in any loss of employment for Accenture staff; the 40,000 affected workers have been redeployed.[7]

Perception: What Is the Impact on Staffing?

People often view automation with fear: "My job will be replaced by a machine!" However, results show that organizations with medium or greater levels of automation actually have higher staffing levels than those with low automation levels. See Table 6.

Table 6. Level of Automation Versus Staffing (N=142)

	1 or less	2–5	6–10	11–25	Over 25
Medium >	2.8%	7.7%	4.9%	9.2%	9.9%
Low	5.6%	23.2%	9.9%	6.3%	7.0%
Total	8.5%	31.0%	14.8%	15.5%	16.9%

Automation does not necessarily mean a reduction in staffing. It may, in fact, enable existing staff to be more effective, using technology to allow individuals to focus on more important aspects of work and life. Respondents do not appear concerned about automation taking away jobs. Most feel that there will be no change in staffing levels and are actually looking forward to a change in focus—or a new adventure entirely.

Respondents Speak Out on Staffing and Automation

- No change:
  "Do more with the same staff."
- Change in focus:
  "Enable existing staff to spend more time on higher value security activities like threat hunting."
- New adventure:
  "More time to focus more on the 'real' and 'exciting' stuff rather than doing triage monitoring for alerts that might as well be automated."

[7] www.bloombergquint.com/business/accenture-to-sell-software-that-allowed-it-to-cut-40-000-jobs

Implementation of effective automation often requires an initial surge in staff to get the kinks worked out, but it is almost invariably accompanied by a redirection, not reduction, of the existing workforce. The top five industries anticipate hiring in the next 12 months, as shown in Table 7.

Table 7. Change in Security Staffing: Top Five Industries

	Amount of Change (%)	
	Median	Average
Banking and Finance	25%	27.6%
Cybersecurity	50%	36.1%
Government	50%	46.9%
Technology	25%	21.4%
Telecommunications/ISP	25%	29.2%
Overall (across all industries)	25%	27.3%

Making Automation Operational

So, what should organizations be doing as they move forward with automation?

Planning and Preparation

Success starts with planning. Prevention and detection have the highest level of operational automation due to the wide availability of structured logs and the maturity of automatic data collection processes. On the other hand, organizations are focused on planning for automation in the areas of prediction and incident response. See Figure 10.

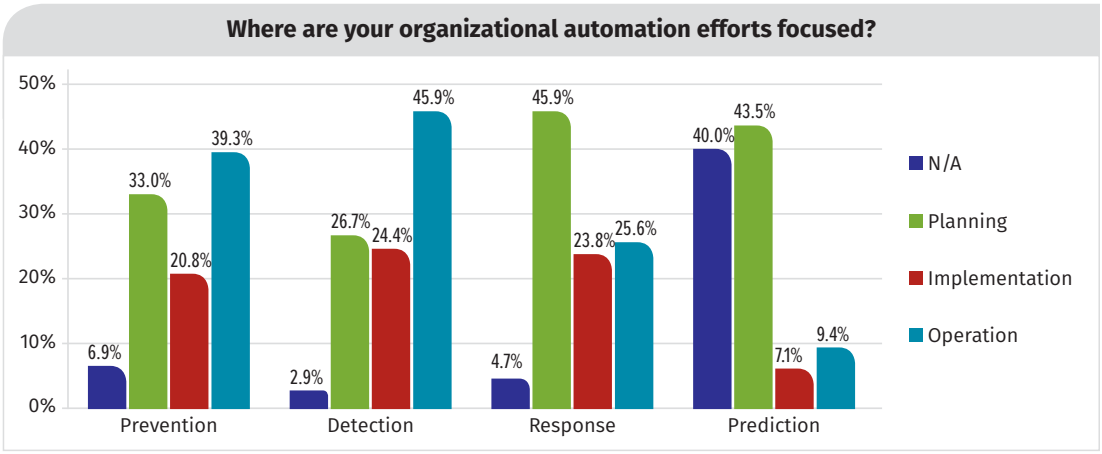


Figure 10. Organizational Focus on Automation

IR is not a leading user of automation for operational processes, as seen earlier (Table 3), but this area is an excellent candidate for its increased use. The overall seven-step response process—preparation, identification, containment, investigation, eradication, recovery and follow-up/lessons learned—contains numerous repetitive and time-consuming workflows where the benefit could be clearly shown.

First, organizations should target a specific business objective within that area, such as the integration of SecOps and IR teams, where automation can possibly demonstrate added value, whether due to greater productivity, better performance or overall better return on investment.

Next, narrow the scope even further by identifying use cases that are readily achievable. Don't overload your team by trying to automate all the processes related to the general business objective at once. Focus on those processes that can benefit from automation, taking the time to tease out and understand current procedural flaws and how automation can help remediate those shortcomings.

Use Case

A *use case* is a set of actions or steps that defines the interactions between an actor—which can be a person, a system or a service—in order to achieve a particular objective.[8]

[8] Don Murdoch, Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases, Notes from the Field, 2018, p. 129.

Respondents feel automation can enhance the performance of SecOps and IR teams in a variety of ways, as shown in Figure 11. This prioritized list of improvements can serve as a starting point as to what types of automation may best support a specific IR use case, such as monitoring privileged user access or responding to a web presence or an end user payload attack.

Remember the toughest, most malicious cases still need the hands-on, critical thinking that can only come from a security analyst. Strive to find the right balance between machine-led and analyst-led activities for a successful implementation.

Figure 11. How Automation Enhances Team Performance

Start with the Playbook

The term *playbook* is perhaps best-known in the athletic arena, where it refers to the compilation of plays and strategies a team has at its disposal. In the realm of security automation, it has nearly become synonymous with workflow—the collection of processes and operating procedures that conform with the policies and culture of an organization to ensure a consistent response to a stimulus or trigger.

When asked what key processes have been automated in their organizations, respondents showed some confusion in their open-ended responses as to what should be considered a process or workflow (automated removal of malicious email post-delivery) vs. an actionable trigger or input for a process (SIEM alert) vs. the actual technology (SIEM).

Understanding how to document workflows and identify improvement is part of *business process management* (BPM), a discipline that uses various methods to discover, model, analyze, measure, improve, optimize and automate business processes (e.g., workflows).[9] As security embraces automation, BPM will become increasingly important in helping identify automation requirements and quantifying the resources needed to achieve the desired goals and objectives.

[9] www.aiim.org/What-is-BPM#

Implementation of an effective automated solution demands analyzing, answering and understanding the answers to three questions:

- What is the existing workflow, even in manual form?
- What are the gaps in the current workflow, such as inefficiencies and bottlenecks, and where should or could potential improvements occur?
- What is the projected (improved) workflow using automation and integration (e.g., SOAR)?

Advice for playbook development includes:

- Look to see which modeling tools you have available. A SOAR platform should include easy-to-use modeling tools (e.g., drag-and-drop) for playbook creation, ideally supporting one of the well-known modeling methodologies, such as UML diagramming.
- Once you have selected a modeling methodology, learn how to really use it—not only for documenting, but also for analyzing the quality of your automated processes.
- Take the time to analyze processes before building playbooks with them. (Note: This can't be said too often.) Automating a bad process makes the bad process more efficient, but it's still a bad process.
- Re-use is your friend. Leverage what others have done. Standard playbooks or templates can be a great way to get started, customizing them as you figure out what works for your particular use case.

A Short Workflow Primer

Workflow—A structured, predefined set of activities that produce a desired result

Workflow Elements—At a minimum, the following are needed to document a workflow:

- **Inputs—**The materials and resources required to initiate a process
- **Actors—**The person(s) or technology responsible for at least part of the work (Here, you need to understand the roles and responsibilities, both of humans and of machines, as they relate to the workflow.)
- **Process—**The action being performed (Consider each process step—taking input, applying a specific set of rules or actions to that input, and providing an output [results]—that can be used as an input to the next process step in the flow.)
- **Outputs and results—**The desired outcome or result of each process step

Documentation Approach—Graphical presentation is a desired aid for stakeholders to visualize an overall process, its issues and the areas of potential improvement. A hand-drawn flowchart is an informal method. Formal methods include modeling methodologies, such as IDEF (Integration DEFinition) or UML (Unified Modeling Language), that capture workflows according to standard terminology and structured rules. Microsoft Visio is a common tool that supports both informal and formal methods of graphically capturing a workflow.

Visibility: Metrics Must Help!

A process without measurement is no process at all! Metrics provide visibility into the state of automation at many levels. Dashboards and reporting, adjusted to the role and needs of the user—analyst, SOC director, CISO—are needed. An analyst may gauge individual performance by the number and types of incidents touched, closed and opened. A SOC director may look at the number of incidents per security analyst to report on the efficiency and behavior of his/her operation.

Management, on the other hand, needs indicators that reflect organizational priorities such as reduced risk and cost, along with increased productivity and improved security posture. Here, individual metrics may feed into KPIs, demonstrating how effectively an organization is meeting its business objectives. To demonstrate cost reductions associated with improved IR, a dashboard may need to have a KPI based on the mean times to detection and remediation, together with the time required to complete the standard and/or tasks involved.

A fairly significant gap still exists between what is actually being used and what is still needed, especially at the management level. See Figure 12.

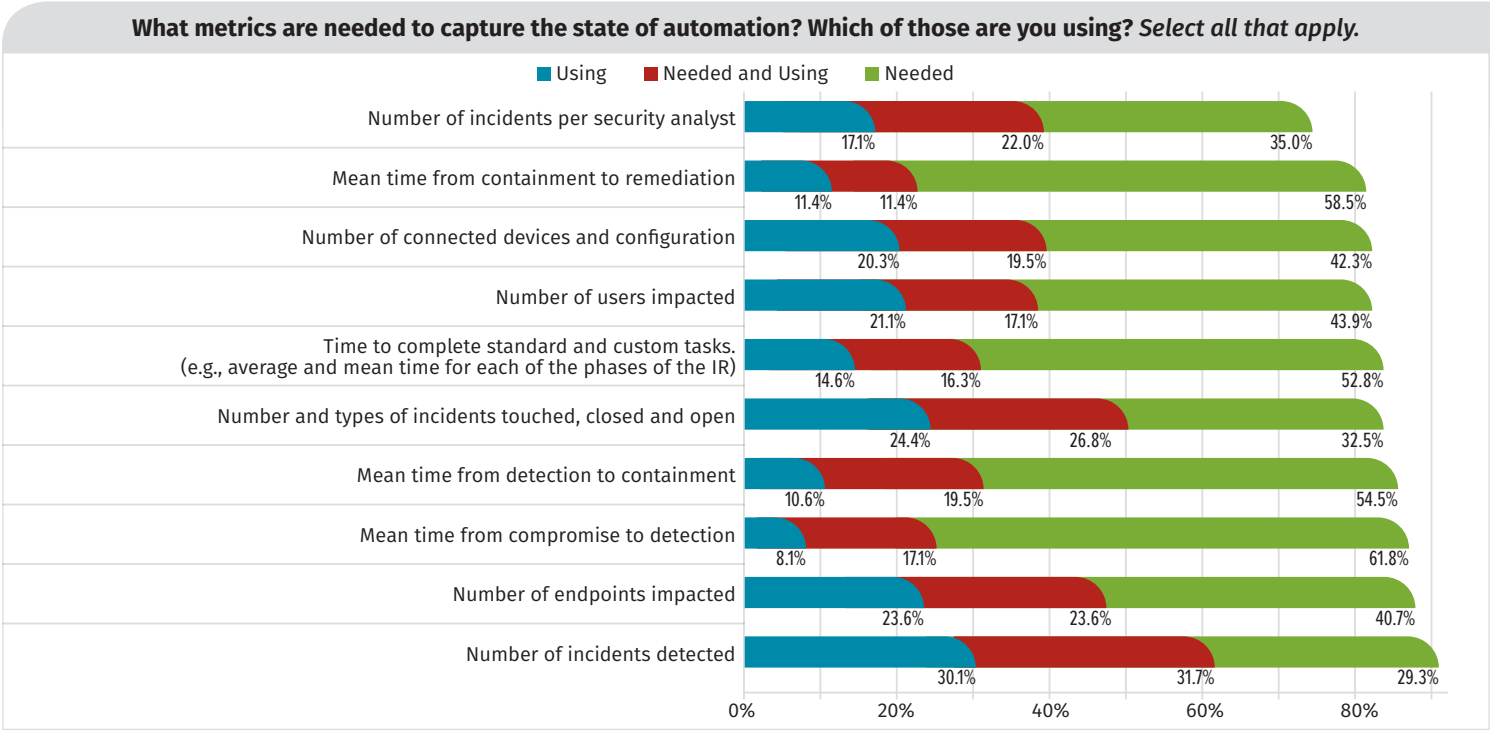


Figure 12. Metrics for Automation

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

First, establish a baseline of what information you need for answering the questions that are most important to your team and your management. The most basic questions remain the same, but there will be some new twists, as well as additional concerns that need to be addressed:

- What are your average/median times for detection, response and remediation?
- How much time are you saving by implementing the new process? Here, automation can help with instrumention that quietly captures statistics throughout the process lifetime, allowing real-time viewing of bottlenecks as well as any changes in the efficiency of the overall workflow.
- What types of incidents are taking the longest? Do you need more training, better tools or improved processes?
- What is the net effect of automation on your security team? How much time does your staff spend doing the specialized security operations you hired them to do versus the more mundane tasks that should be handled by automation?

Gather and analyze your measurements for a period that is long enough to let you determine the ROI of that metric. Don't underestimate the time it takes to develop a meaningful metric. Correct metrics are enablers that help you improve your reponse, make operations more efficient or justify the organizational investment in automation. Eliminate those that are not informative, adjust those that are, and add ones that help tell the story.

Once processes are codified via a SOAR solution, make sure your analysts still monitor, evaluate and improve them to ensure each playbook continues to function at maximum effectiveness and efficiency. SOAR solutions that enable you to run tests and alert simulations on your playbooks can help with this continuous improvement.

Conclusion

Although automation is hailed as an enabler for the future, uncertainty remains about exactly what it can accomplish. This survey identified some of the bumps along the road that may contribute to this vagueness:

- Organizations need to understand that a front-end investment in design, involving all aspects—people, process and technology—is needed to make the operational back end meet the expectations of both the operational teams and management.
- The security community needs to have a deeper understanding of the methods and tools available for playbook development. This represents a relatively new area for most security professionals. Keep in mind the need for initial and continual process improvement. Remember, you can automate a bad process and then, after a substantial investment, realize that you have a more efficient bad process—but it's still a bad process.
- Integration standards for connecting diverse technologies and independent tools to achieve a comprehensive automated workflow are critical. Tools have to talk together across their interface boundaries. The industry must establish standards, whether formal or ad hoc, to help both users and vendors achieve the level of interoperability needed by modern organizations within known constraints.
- Organizations need to develop both KPIs and metrics specific to evaluating the state of automation.

Automation is about bringing people, process and technology together. As one respondent states:

"I don't think even large companies do well with understanding the requirements: people, process and technology. It is a trinity—you can't have one and not have the other two. It is still common to see purchases of one or two—while leaving the third off the list of project completion, [such as] adding more technology but not more staff."

About the Author

Barbara Filkins, a senior SANS analyst, 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 survey's sponsor:

LogRhythm®
The Security Intelligence Company