The State of SOAR Report, 2020

The fourth annual survey on incident response

Table of Contents

Executive Summary

This is the fourth in our annual series of reports on the state of SOAR. As in previous years, we surveyed hundreds of security professionals in diverse roles at large organizations across a range of industries. We asked for their views on the state of incident response (IR) as well as their insights into their current and future use of security orchestration, automation, and response (SOAR) as part of their security strategies and operations.

Here are some highlights from the report:

- **Security analysts are facing an increasingly serious cyberthreat environment**. Attacks are varied and voluminous, with 63% of organizations fighting off attacks originating from suspected nation-state actors.
- **The IR process is overwhelming**. Analysts are required to keep track of an average of 6.8 threat intelligence feeds and manually handle an excessive number of alerts. IR processes originate in a wide array of systems, with an ensuing workflow that crosses many organizational barriers.
- **COVID-19 has made things worse**. The pandemic is exacerbating IR challenges, with new threats to contend with and negative impacts on collaboration between SOC team members. Forty percent of survey respondents believe the pandemic is causing resources to become more constrained.
- **Analysts know what they need to get better at IR**. They want:
  - » More automation to speed up IR and reduce the stress of manual operations. Sixty-five percent of respondents are making IR automation a high priority for the next 12 months.
  - » Integration of SOC tools with third-party systems so they can easily connect with other departments and IR processes. Thirty percent of respondents say they want a common platform for cross-functional team response.
  - » More playbooks, including third-party playbooks and a sharing community, so they can leverage the proven expertise of other teams. Seventy-eight percent of respondents wish there were a common framework and community for sharing playbooks and integrations.
  - » Threat intelligence integrated with SecOps tools to cut down on the challenge of monitoring too many threat intel feeds to stay ahead of serious threats. Fifty-two percent of respondents say their security operations workflows would benefit from more integration of threat intelligence.
- **SOC teams need to reduce alert fatigue**. A tool that can either cut down on alert volume or make the alert management process go more quickly is in demand.
- **SOAR offers a solution to many of these challenges**. The technology is helping SOC teams save time, speed up triage, and reduce the number of steps required for IR processes.
  - » Forty-five percent of SOC teams are using SOAR for detection and response. Other current use cases include vulnerability prioritization (37%), compliance checks (30%), and security audits (30%).
  - » Future SOAR use cases envisioned by SOC teams include IoT management (23% of respondents), Red Team workflows (17%), and cloud security (38%).
  - » Forty-three percent of survey respondents say they plan to increase spending on SOAR tools in 2020. A further 24% plans to implement SOAR in the next 12 months.
  - » The COVID-19 pandemic has led 47% of respondents to increase their use of SOAR.

Introduction

This report presents the findings of an annual survey of security professionals. It looks at trends in incident response (IR) and the potential for security orchestration, automation, and response (SOAR) technology to help with the IR process. Respondents serve in diverse security roles at large organizations across a range of industries.

Security operations centers (SOCs) and the security analysts who work in them need help. As figure 1 suggests, the SOC team is under constant pressure to mitigate a wide variety of attacks. Eighty-six percent of survey respondents shared that they have dealt with phishing attacks in the past 12 months. A further 63% have had to detect and quickly neutralize malware attacks. Password attacks, denial of service (DoS) attacks, and ransomware are active incidents, confronting a further 51%, 39%, and 37% of respondents, respectively.

Indeed, as Gartner shared in its 2020 "Top Security and Risk Management Trends" report, "The velocity and creativity of attacks continue to grow. Attackers will continue to exploit a variety of tools, tactics and techniques against an ever-increasing diversity of targets to achieve a growing range of goals. All of this further reduces the ability to anticipate and prevent security failure."[1]

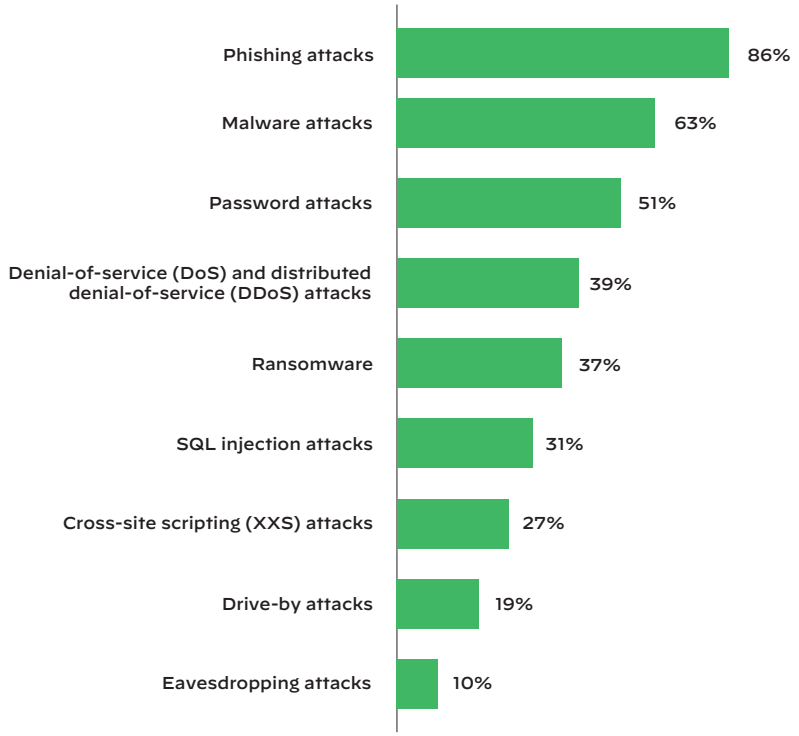

Figure 1: Attacks on respondents' organizations over the last 12 months

A remarkable 63% of organizations surveyed claimed to have experienced a cyberattack launched by a suspected nation-state actor in the previous 12 months. Tactics these powerful malicious actors used included phishing, DDoS, ransomware, SQL injection, and more. The COVID-19 pandemic is also exacerbating the situation (see more in "The Impact of COVID-19 on IR").

An Overview of SOAR

SOAR is a category of security operations technology that enables SOC teams to manage the IR process more efficiently and effectively. SOAR solutions evolved out of attempts to automate IR workflows, which were—and still are, to a great extent—manual in nature. The technology also developed to help SOC analysts orchestrate IR processes that took place between multiple systems, such as security incident and event management (SIEM) solutions, case management platforms, and the like.

SOAR solutions are designed to facilitate faster, more effective IR while allowing for detailed, actionable incident forensics. The technology provides the SOC team with a core set of capabilities:

- **Orchestration** is about linking functions in different systems so they can realize the objectives of the IR workflow. Typically based on standards-based application programming interfaces (APIs), orchestration enables the SOAR solution to generate notification emails, look up threats, start service tickets, and so forth, even though those functions reside in separate systems.
- **Automation** involves configuring machines to perform tasks that used to be done by hand. In a SOAR context, automation is mostly viewed as an enhancement to human beings, rather than a replacement. Automation removes much of the repetitive, boring work that causes burnout for SOC analysts, and it speeds up IR and investigations.
- **Playbooks** are preset sequences of actions the SOC team can deploy in the SOAR solution in response to a given threat. For example, if the team identifies a known Common Vulnerabilities and Exposures (CVE) threat and has a playbook to mitigate that threat, it can run the playbook rather than invent a response from scratch. The result is invariably a faster, more efficient IR process.
- **Reporting and data visualization** in the SOAR solution give the SOC team an intuitive, efficient way to identify, correlate, triage, and document how incidents are unfolding, along with steps in the IR process and their results.

1. Peter Firstbrook, Neil MacDonald, Lawrence Orans, Mario de Boer, Katell Thielemann, Bart Willemsen, Akif Khan, and Michael Kranawetter, "Top Security and Risk Management Trends" (ID G00466211), Gartner, February 27, 2020, https://www.gartner.com/en/documents/3981492/top-security-and-risk-management-trends.

IR: A Choreography of People, Processes, Tools, and Data

Each organization surveyed has its own way of approaching the IR workflow. Broadly, however, the process comprises four elements:

- **Incident ingestion and enrichment**: This is the process by which the SOC gathers detailed information about a security incident and enriches it to better understand what's happening. For instance, if an attack is traceable to a particular CVE, the enrichment process might add detail about the CVE, the systems it affects, how it can be mitigated, and so forth.
- **Case management**: Each incident becomes (or should become) a case to be managed by the SOC and various other teams in the organization, such as IT operations, network operations, legal, and human resources (HR).
- **Incident investigation**: Security analysts must investigate an incident to determine the best way to respond and prevent similar occurrences in the future. Investigation requires knowledge and experience, aided by systems that offer detail about the cause of the incident.
- **Response and enforcement**: This phase of IR involves implementing the mitigation steps determined in the investigation process.

These elements overlap and reinforce one another. The enrichment informs the investigation, which in turn drives response. Case management tools and practices keep the workflow in order and update all relevant stakeholders, at least in theory.

The Impact of COVID-19 on IR

Sixty percent of survey respondents shared that COVID-19 was leading to new work models, including work from home (WFH) for employees and members of the SOC team. Forty-two percent felt the pandemic has increased the need for virtual collaboration, though 40% believed it has caused resources to become more constrained. Perhaps as a result, 24% said COVID-19 is driving an increased need for automation, while 23% cited the adoption of new cloud services as an impact of the pandemic.

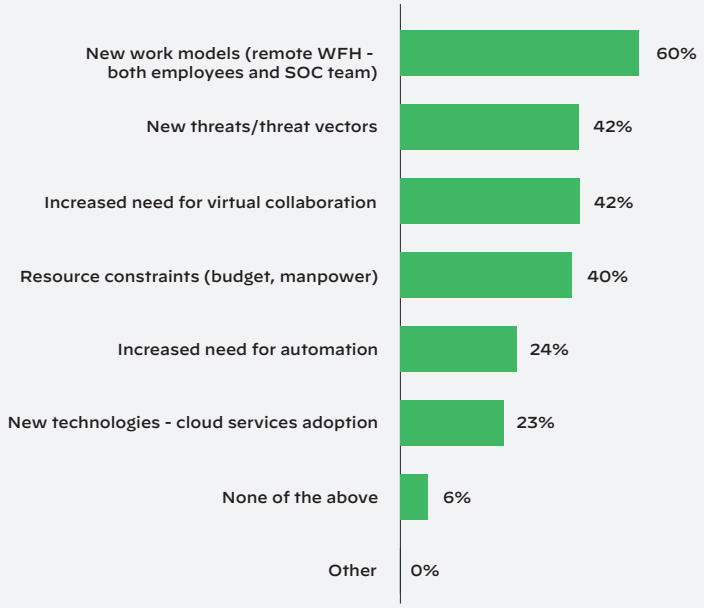

Figure 2: Survey results—impact of COVID-19 on the SOC and security analysts

Security posture and practices were also affected, with 42% of respondents saying COVID-19 was resulting in new threats and threat vectors. In terms of SOAR adoption, COVID-19 had an interesting split effect. Forty-seven percent of respondents whose organizations use SOAR to some extent said that the pandemic would cause their organizations to expand use of SOAR and accelerate its rate of adoption. An equal percentage had the opposite reaction: 47% said COVID-19 would reduce SOAR usage and delay its deployment.

Key Findings from the 2020 SOAR Survey

The 2020 SOAR survey affirmed some of the findings of previous surveys. SOC teams continue to struggle with high levels of alerts. This situation is aggravated by deficits in team member skills, highlighted in Gartner's 2020 "Top Security and Risk Management Trends" report, which noted, "The security skills gap will grow, abetted by the accumulating complexity in IT systems and the rapid pace of change in security tools to protect this rapidly shifting infrastructure."[2]

SOC teams want more automation to cope with these evolving pressures. The survey revealed a clear interest in third-party system integration. SOC teams also seem to want more playbooks, with some expressing a desire to engage with third-party marketplaces and sharing communities. People want solutions, and they are interested in seeing what their peers have come up with to fight the threats they are facing.

IR Today: An Increasingly Complex and Demanding Workflow

Each organization approaches IR in its own way, using its own constellation of tools. The survey revealed that the IR process starts from different interfaces, depending on the organization. As figure 3 shows, more than half of IR workflows start in the SIEM solution while 33% begin in ticketing platforms like ServiceNow® and Zendesk®. Just 6% and 2% start in case management tools and SOAR solutions, respectively.

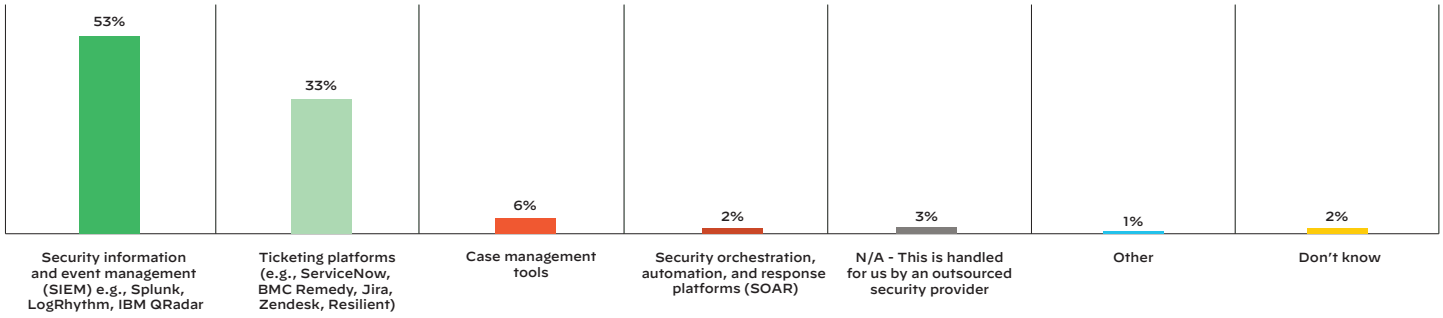

Figure 3: "What is the primary interface from which you start your incident response workflows?"

Outside providers and manual processes shoulder a portion of the IR burden, as figure 4 reveals. Twenty-two percent of IR workflows involve managed security service providers (MSSPs) and managed detection and response (MDR) services. With outside entities doing some of the work, it makes sense that manual processes would be common in the IR workflow. Unless the MSSP or MDR service is integrated with automated IR workflow tools, their engagement in IR will be at least partly manual.

Manual processes account for 38% of incident investigation processes while 35% of processes are manual in response and enforcement. This reliance on manual processes makes sense in the context of the findings shown in figure 3: if 53% of IR workflows originate in SIEM solutions, which are not typically designed with automated IR workflow functionality, then a SOC team member will need to port the case over to the other tools by hand.

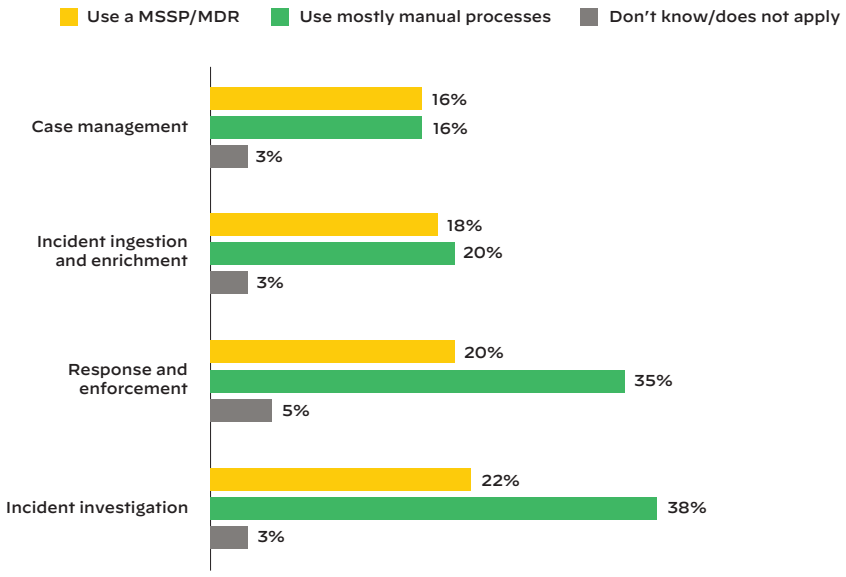

Figure 4: "Which solutions do you use for the following steps of your incident response process?"

2. "Top Security and Risk Management Trends," Gartner, February 27, 2020.

Security Managers Face Barriers to Speed and Scale in IR

Survey respondents shared details about their IR processes that suggest they face barriers to speed and scale in IR. As figure 5 shows, fewer than half of respondents have access to customizable dashboards. Only 40% have real-time and pre-scheduled reporting, while just 15% have machine learning recommendations to improve security operations. These findings point to a SecOps environment where it's inefficient and time-consuming to get things done. If SOC team members have to rely on standardized dashboards that may not reflect an analyst's specific role, and reporting is not immediately available, the work will slow down. The results will also be less meaningful. Machine learning can help, but as the data shows, it's only available for 1 in 6 SOCs.

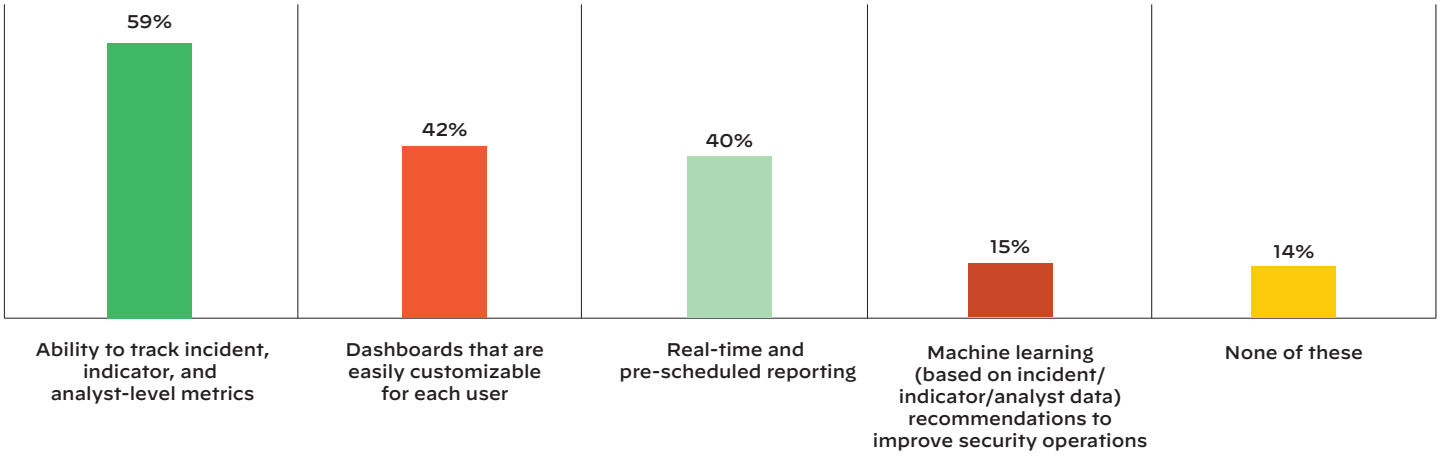

Figure 5: "For incident response and analyst performance tracking, which capabilities do you currently have? (Please select all that apply)"

IR Must Become Less Manual, with Automated Processes and Playbooks

The survey reveals a need for more automation in IR. Survey respondents indicated that 44.7% of their IR processes are automated, which may seem high, but is not enough. While having 4 out of 10 IR processes automated is better than nothing, the prevalence of manual processes still impairs effective and efficient IR. Indeed, a striking 93% of security operations teams say it is a priority to increase automation in their IR processes in the coming year.

Incident Ingestion and Enrichment Only Partly Automated

The incident ingestion and enrichment stages of the IR processes are partially automated. As figure 6 shows, half of data ingestion is automated across multiple sources. Alert prioritization has almost the same level of automation (46%), as does correlation of alerts and indicators across products. Given how stressed and overworked SOC team members tend to be, having just half the ingestion work automated is probably not seen as a great achievement. For enrichment, the number is significantly lower, with just 28% of respondents saying they have automated enrichment processes. Another 30% say they're doing enrichment manually.

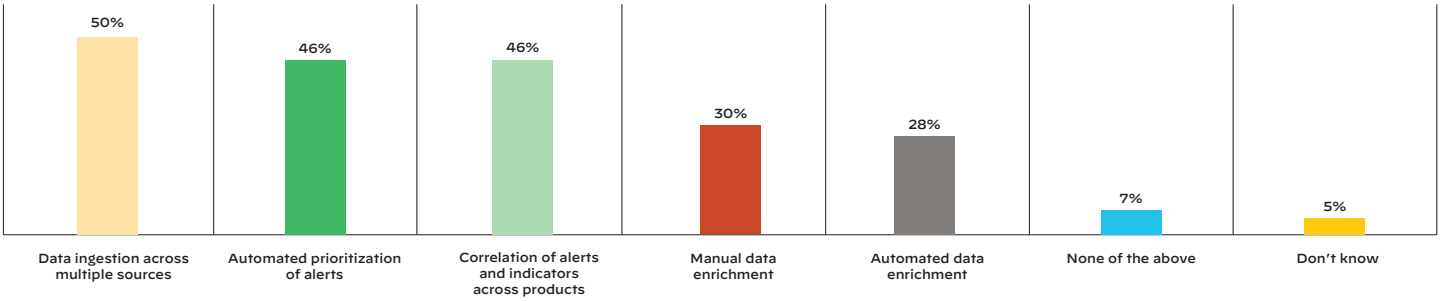

Figure 6: "For incident ingestion and enrichment, which capabilities do you currently have? (Please select all that apply)"

IR Process Implementation: A Mix of Automated and Manual Workflows

IR process implementation, too, is a mixture. Figure 7 shows that 53% of processes constitute a mix of manual and automated playbooks, runbooks, and processes. Just 18% consist of automated playbooks and runbooks. Tellingly, only 6% of processes involve "no playbooks." Playbooks are the way that SOCs are dealing with IR process implementation—and the process is not highly automated.

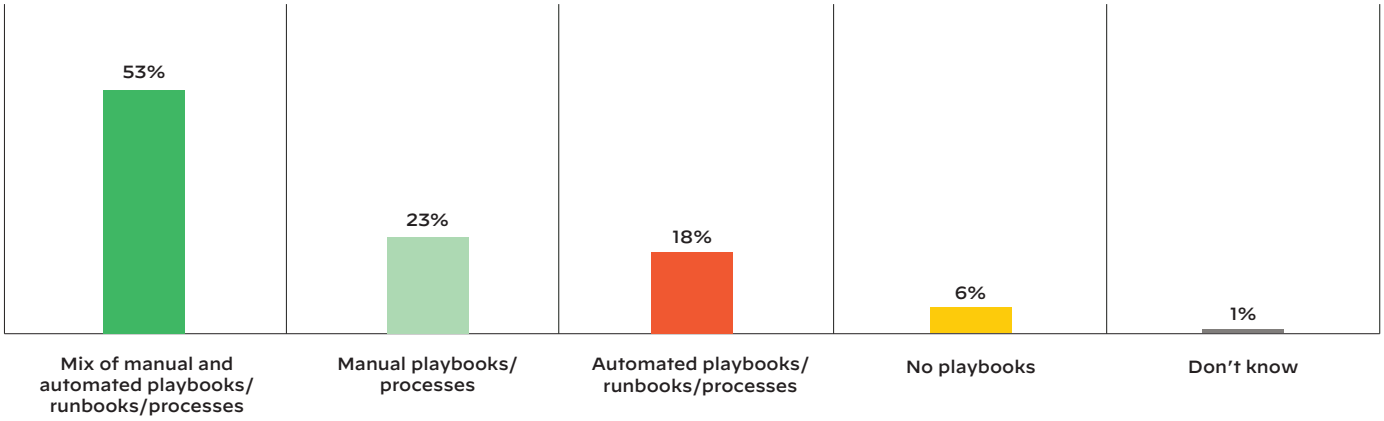

Figure 7: "Which of the following best describes your incident response process implementation?"

Investigation and Post-Incident Workflows Have Limited Automation

The investigation phase of the IR process has some automation, but it is limited. While 37% of execution of remote security tools is automated, 49% is manual. Notably, just 18% of IR workflows feature auto-documentation of investigative actions. This suggests that more than 80% of documentation of investigative actions is done manually or—as is often the case—not at all.

SOC team members are usually too busy to document the steps they take by hand. However, this information is extremely useful in post-incident analysis and improvements for future responses. Having so little automation represents a lost opportunity for IR learning and process improvement. Asked the same question about post-incident workflows, only 23% of respondents replied that post-incident reviews were automatically captured.

Automation Is a Priority for IR Going Forward

Priorities and future plans are revealing, when it comes to IR automation. As figure 8 shows, 65% of respondents are making automation a high priority for the next 12 months in IR. A further 58% have automation as a high priority in threat prioritization, while 46% say the same thing for reporting and visibility across teams. Only small minorities of respondents say automation is not at all a priority—and in the case of IR, just 2% had that opinion.

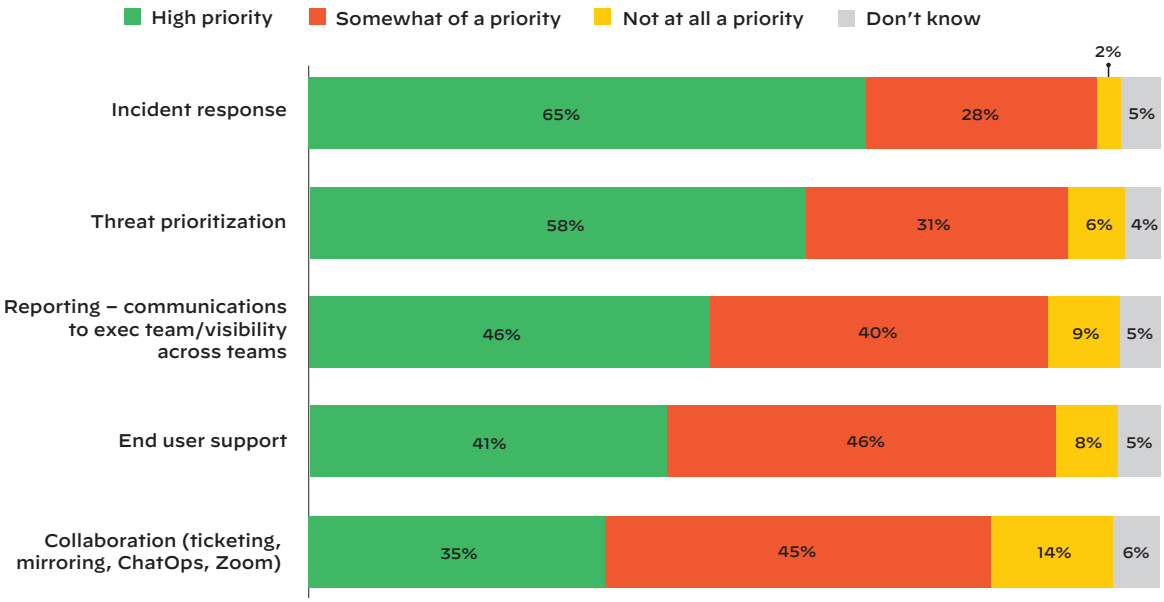

Figure 8: "Over the next 12 months, how much of a priority is it for you to increase automation in the following security operations processes?"

Threat Intel Needs to Be Easier to Manage, Integrated into IR Workflows

As the global threat environment grows more diverse and voluminous, SOC teams need to stay current on threat intelligence. Eighty-one percent of survey respondents say that threat intelligence is critical to their IR processes. To stay informed about threats, companies now subscribe to an average of 6.8 threat feeds. Without coherent, integrated management of these data streams, however, it's easy to lose track of potentially serious threats. Indeed, 62% of survey respondents say using threat intelligence is a time-consuming process.

Integration with threat intelligence thus emerges as the top-rated factor for a new security tool investment. As figure 9 shows, 50% of respondents said that their security operations workflows would benefit heavily from more integration of threat intelligence. Adding in the 46% who said it would "somewhat" benefit their IR workflows, a remarkable 96% of respondents seem to favor integration of threat intelligence.

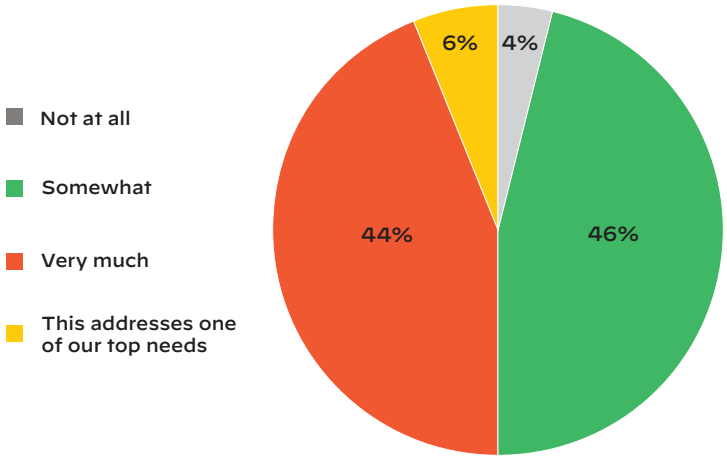

Figure 9: "To what extent would your security operations workflows benefit from more integration of threat intelligence?"

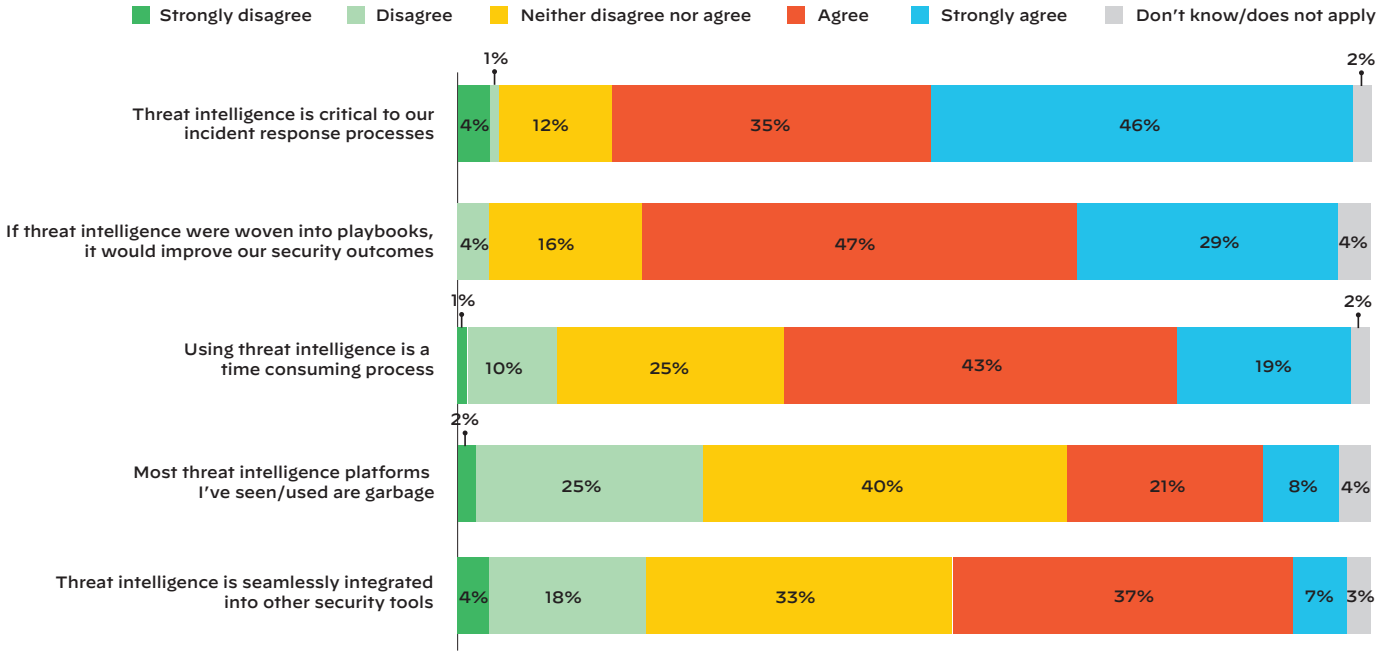

Figure 10: "Please rate your level agreement with the following statements regarding threat intelligence."

That said, the actual rate of integration is relatively low, with 43% of survey respondents agreeing that "Threat intelligence is seamlessly integrated into other security tools." Furthermore, just 28% of incident investigation processes tie into threat intelligence sources.

A number of survey findings offer explanations for the divergence between the desire for threat intelligence integration and the actual rate of integration. One issue is that there are simply a lot of different kinds of people involved in managing threat intelligence. As figure 11 indicates, the work involves security operations, enterprise security team members, IT ops, standalone threat intelligence teams, and others. An additional factor could be perceived quality of threat intelligence platforms. Twenty-nine percent of respondents agree with the statement "most threat intelligence platforms I've seen/used are garbage."

As figure 12 further reveals, the threat intelligence process itself spans no fewer than 12 different systems. The assortment of employees described in figure 11 are doing threat intelligence work on SIEMs, network traffic analysis tools, intrusion monitoring solutions, and so forth. Too many people trying to manage threat intelligence on too many platforms, with too little integration—that's a frustrating formula, for sure.

SecOps Teams Need Fewer Alerts to Review

SOC analysts have too many alerts to process. It's overwhelming. Alert fatigue is a real phenomenon that can drive employee burnout and turnover. There's also a real risk that a serious threat will get missed in all the noise. Moreover, COVID-19 is making things worse. The survey revealed that 47% of companies have seen alerts increase since the start of the pandemic. Companies that experienced an increase in alerts due to COVID-19 saw their alert volume rise by an average of 34.2%.

SecOps Technologies Must Integrate Easily with Third-Party Solutions

IR workflows start in a variety of places, as figure 13 demonstrates. From there, the IR process can jump across multiple solutions and departments. Integration between IR tools and third-party solutions can thus help keep SOC teams productive and able to mount effective response to incidents. The survey found support for this idea, with 30% of respondents saying they wanted a common platform for cross-functional team response. As of the survey, only 32% of respondents have a common platform for cross-team investigation.

To understand the scope of the issue, consider that SOC teams use a variety of tools in each of the four major IR workflow areas. As figure 13 shows, SIEMs dominate, accounting for 69% of incident ingestion and enrichment processes and just under half of case management steps and incident investigations. SOAR platforms are in use in 20% of response and enforcement processes as well as 22% of incident investigations. Threat intelligence platforms (TIPs) are less common, accounting for less than 20% of processes in all four areas.

Figure 11: "Who in your organization is involved in managing threat intelligence?"

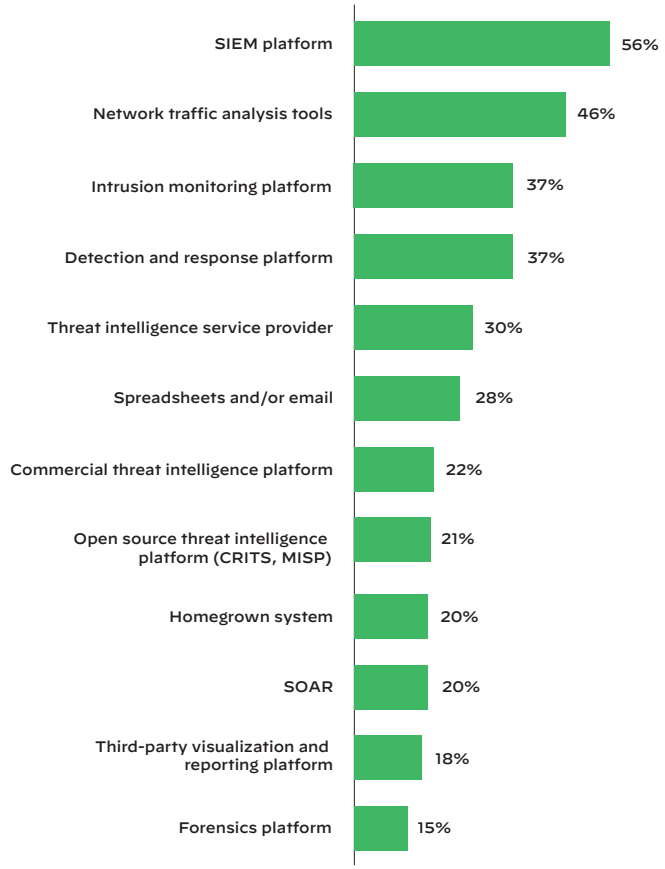

Figure 12: "What kinds of management tools and/or capabilities do you use to aggregate, analyze, and/or present threat intelligence? Select all that apply."

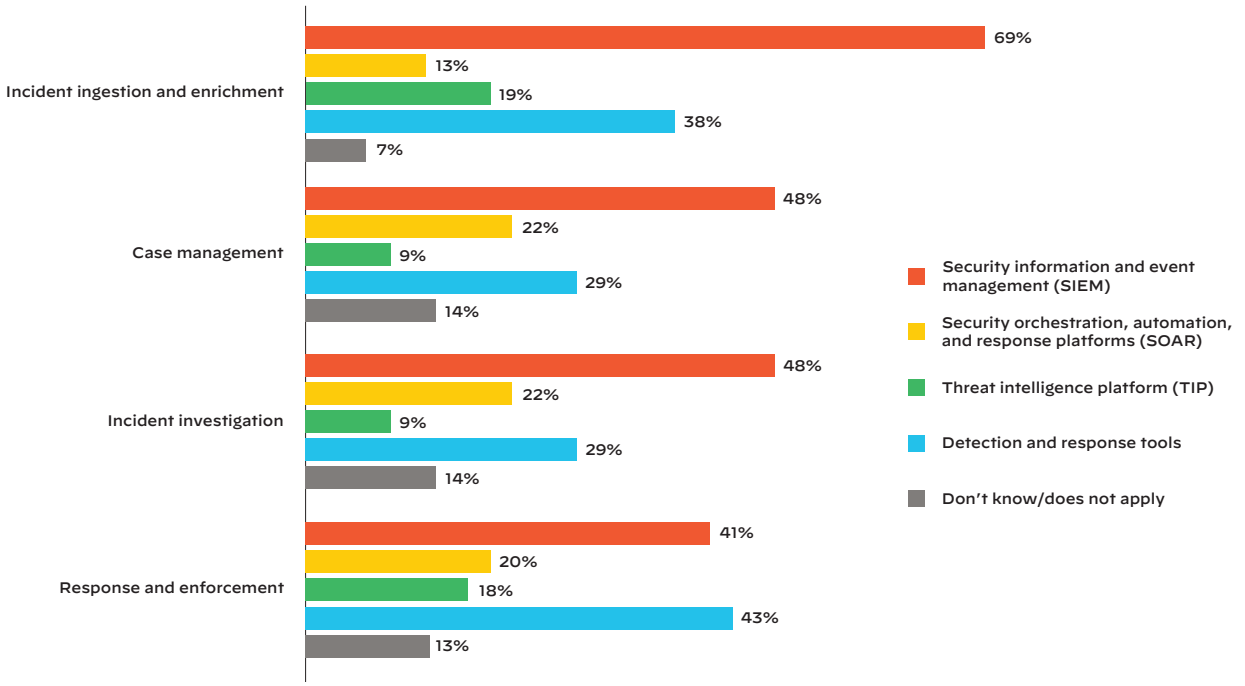

Figure 13: "Which solutions do you use for the following steps in your incident response process (select all that apply)?"

At the same time, the IR workflow cuts across many different corporate departments, though integration between departmental systems is limited. As figure 14 shows, the most integration occurs between IR solutions and those of the IT team, with 23% of systems and processes being described as "tightly integrated." Sharing with the network operations center (NOC) team was tightly integrated just 16% of the time. With HR, 50% of systems and processes were separate. The prevalence of separation between IR and the legal and compliance teams was 48% and 30% respectively.

The response "We share some systems and processes" was true 51% of the time between IR and the compliance team, 56% with the IT team, and 52% with the NOC team. Sharing some systems and processes with other groups occurs less than half the time. The lowest reported integration was between IR and legal, at just 7%. This may reflect the legal department's use of specialized systems for its case management. While not all security incidents are relevant to the legal department, the lack of integration likely results in wasted time and expense as legal and IR people have to coordinate their workflows by hand.

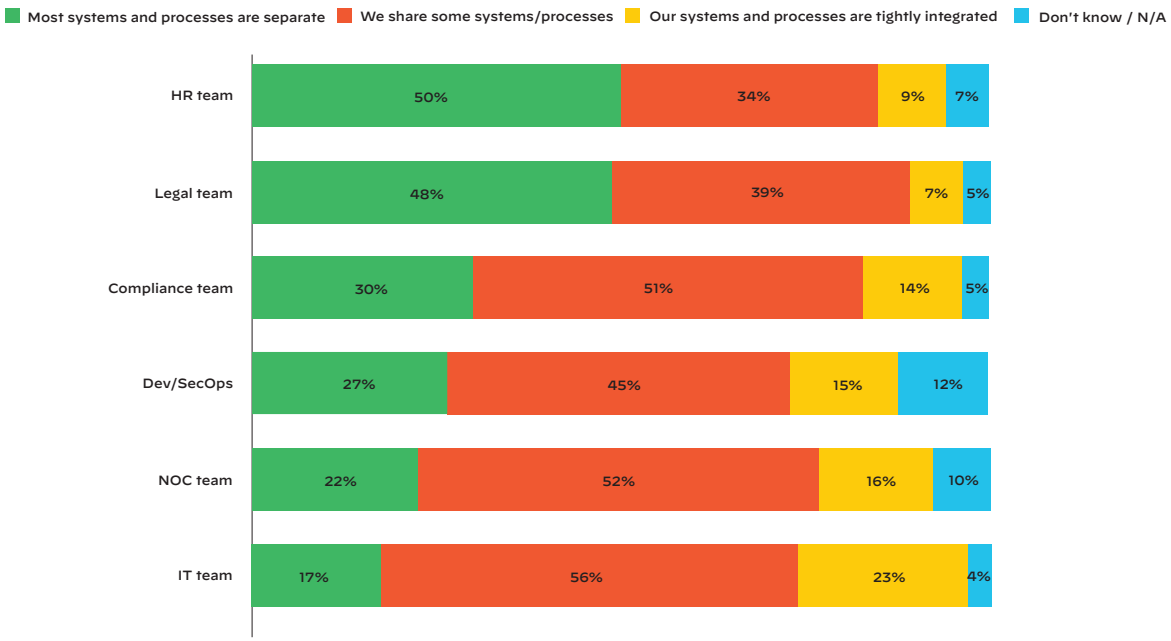

Figure 14: "To what extent do you share tools, processes, systems, and data streams with the following teams?"

Strong Interest in Third-Party Marketplaces and Sharing Communities

The cybersecurity field has a long tradition of people and organizations seeking to leverage the collective wisdom of the community to bolster their security. The origins of this pattern may come from the open source roots of much security and computer technology as well as shared backgrounds of practitioners in law enforcement and the military, where intelligence sharing is encouraged. Though the realities of the work do not always rise to this ideal, there is nonetheless a strong desire for community-oriented sharing of intelligence and best practices.

The survey results bear out this sentiment, with 78% of respondents agreeing that they wish there was a common framework and community for sharing playbooks and integrations. Only 42% felt that they build the best playbooks themselves. In addition to the community, respondents expressed an interest in third-party marketplaces, with 52% saying they were willing to purchase valuable integration with tools from third-party creators. Figure 15 captures the full depth of interest in common frameworks, sharing communities, and third-party marketplaces.

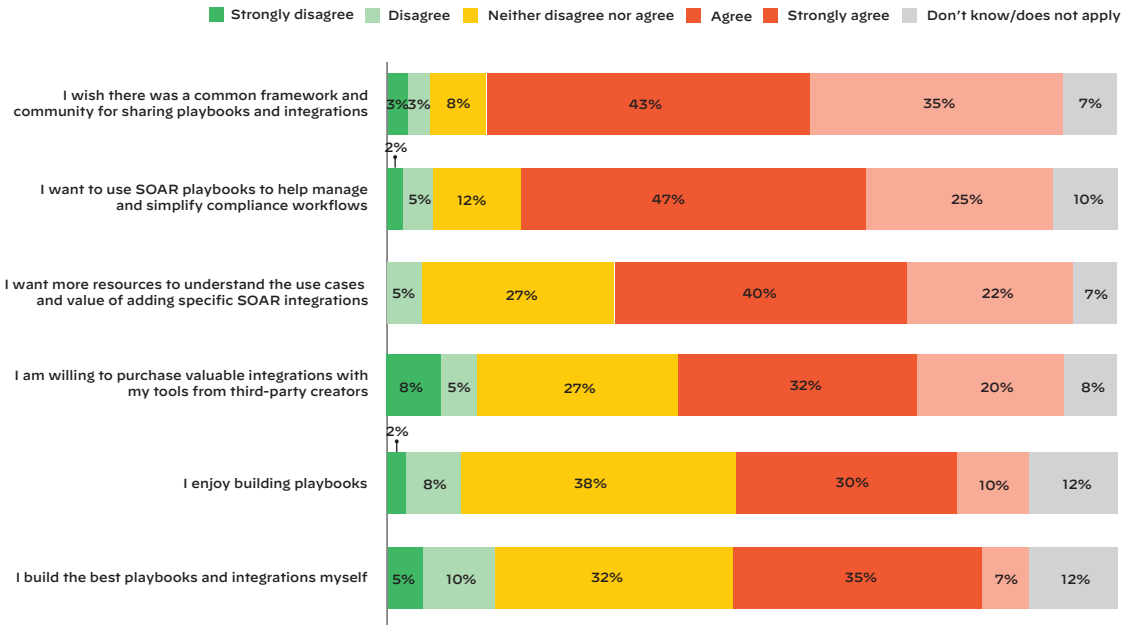

Figure 15: "To what extent do you share tools, processes, systems, and data streams with the following teams?"*

Whom do security professionals trust for playbooks? Figure 16 shows that they trust SOAR vendors the most, with 53% of respondents saying they are most likely to trust vendor-certified playbooks. After that come playbooks they've developed themselves (47%), playbooks created by the SOAR vendor (44%), and playbooks created by an MSSP or other security partner (35%).

Interestingly, while nearly 8 in 10 respondents wanted a sharing community, only 20% are most likely to trust a playbook created by members of the community. This apparent misalignment of interest actually makes sense in the context of 53% preferring vendor-certified playbooks. The results demonstrate the importance of certification.

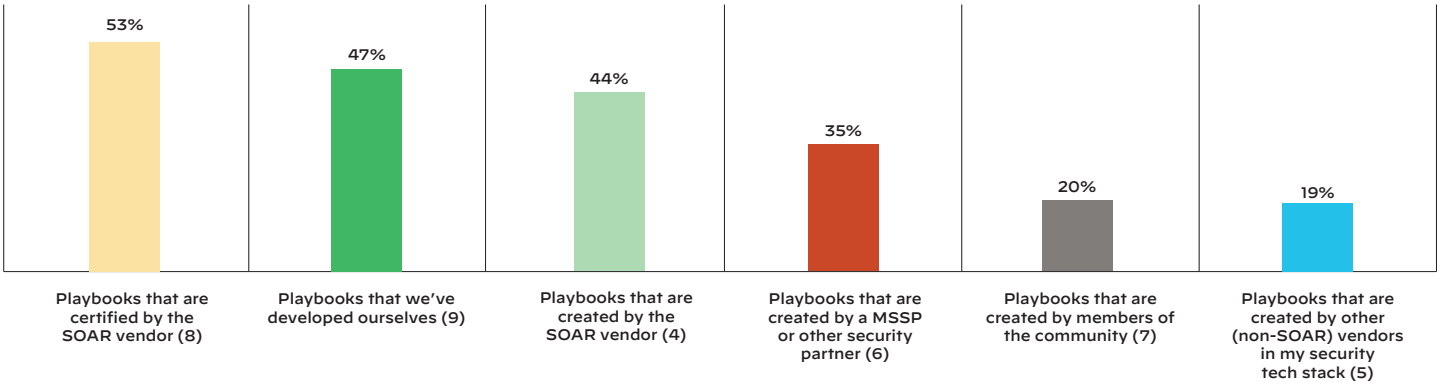

Figure 16: "Which of the following sources of SOAR playbooks would you be most likely to trust? Select all that apply."

* Percentages exceed 100% due to rounding.

The State of SOAR

SOAR offers answers to many of the vexing challenges highlighted by the survey results, including improvements in automation, reduction in alert fatigue, and the like. The survey shows a high level of interest in SOAR, perhaps as a result of the problems it solves. The proportion of respondents who are already using SOAR or interested in implementing the technology in the next 12 months is strikingly high. SOAR is playing a growing role in IR and the broader SecOps environment and seems poised to grow in the coming year.

A Growing Variety of SOAR Use Cases

SOC teams are putting SOAR to work in a variety of use cases. As figure 17 shows, the most popular current use cases where respondents are already using SOAR are detection and response (45%), vulnerability prioritization (37%), compliance checks (30%), and security audits (30%).

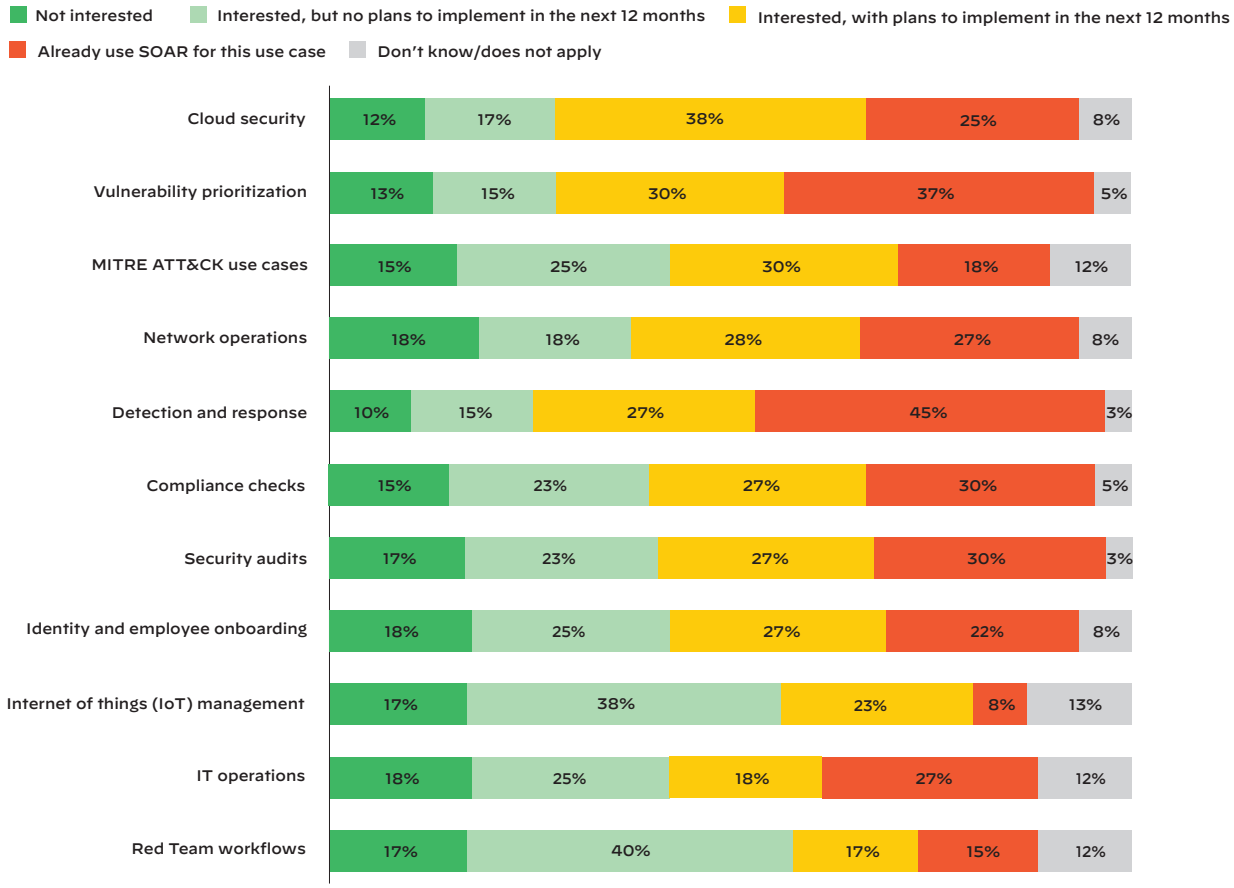

Figure 17: "What extent do you plan to expand your use of SOAR to the following use cases?"

Rates of SOAR adoption are lower in other use cases included in the survey, but the technology is definitely in use, nonetheless. Security teams are working with SOAR for Red Team workflows (15%), IT operations (27%), network operations (27%), and MITRE ATT&CK® use cases (18%). These findings suggest that security teams are interested in SOAR, though they may be slow in the implementation process.

SOAR Gaining a Foothold in Terms of Current Usage

Survey results show that SOAR is gaining a foothold in the SOC, with just under half of respondents (46%) either using SOAR now or planning to adopt it in the next 12 months. Long-term SOAR use is relatively limited, however, with just 7% of respondents indicating they've been using the technology for more than two years. Figure 18 shows the complete breakdown of SOAR usage data. Of note, 41% are aware of SOAR but do not plan to implement it in the next 12 months, and 12% have never heard of SOAR. This last finding, however, may reflect the relatively recent change of the category's name from SAO to SOAR.

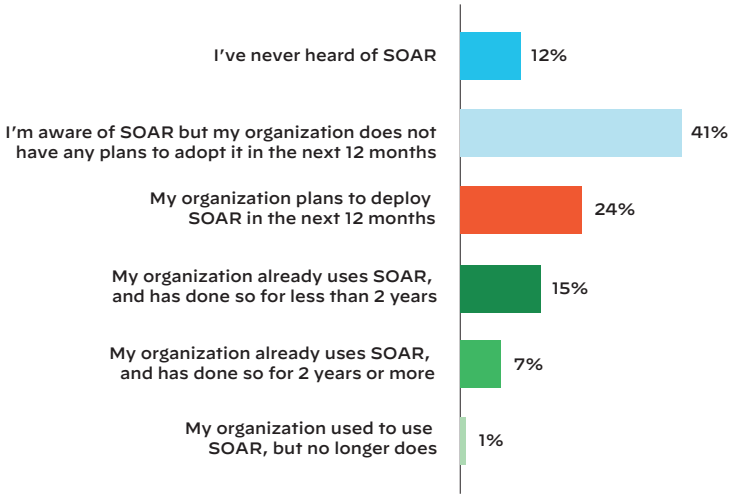

Figure 18: "Which of the following best describes your usage, interest, and familiarity with SOAR tools?"

SOAR Having a Beneficial Impact on IR and SecOps

Multiple areas of IR and SecOps are reaping the benefits of SOAR, perhaps due to SOAR's ability to automate SecOps. As Gartner puts it, "The emerging SOAR technologies promise to bring automation, consistency and efficiencies to security operations centers beyond what is possible in SIEM today."[3]

Among survey respondents who have used SOAR for at least two years, 54% shared that SOAR has saved them time in taking action on incidents. Other improvements include reduction in time to mitigate (51%), reduction in average end-to-end time in incident (47%), and reduction in time to triage (44%). A further 37% said SOAR helped cut down on the number of steps required for IR.

Figure 19 offers insights into just how much SOAR improved SOC performance for this group—namely, that it:

- Made processes more defined (79%)
- Enabled better communication with teams outside of security operations (53%)
- Made SOC teams able to reduce or eliminate unnecessary workflow steps (47%)
- Flattened team structure due to up-leveling of analyst skills (42%)
- Made team able to address more complex security use cases (42%)
- Enabled flattened team structure due to automation of processes (37%)

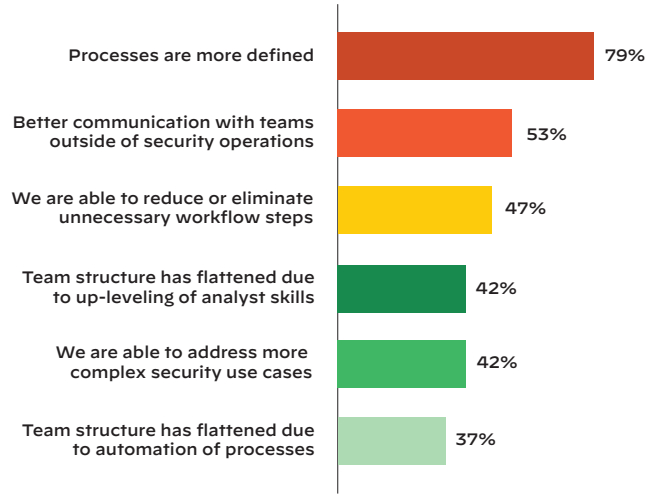

Figure 19: "How has your implementation of SOAR changed your workflows? Select all that apply." Note: N=19

These results suggest that SOAR offers a viable solution for some of the challenges currently confronting SOC teams. Better communication with external teams speaks to the issue raised in figure 14, with SOCs struggling to deal with legal, HR, IT, and other groups. By reducing the time required to manage and resolve incidents, SOAR contributes to potentially reduced stress over high levels of alerts and following too many threat feeds. Faster triage and more productive SOC teams means being able to focus on challenging incidents rather than waste time on low-priority alerts.

3. "Top Security and Risk Management Trends," Gartner, February 27, 2020.

Robust Interest and Purchase Intent

What SOAR plans are security managers making for the future? Forty-three percent of survey respondents—including those who already have SOAR and those who don't—say they are planning to increase their spending on SOAR tools in the coming year.

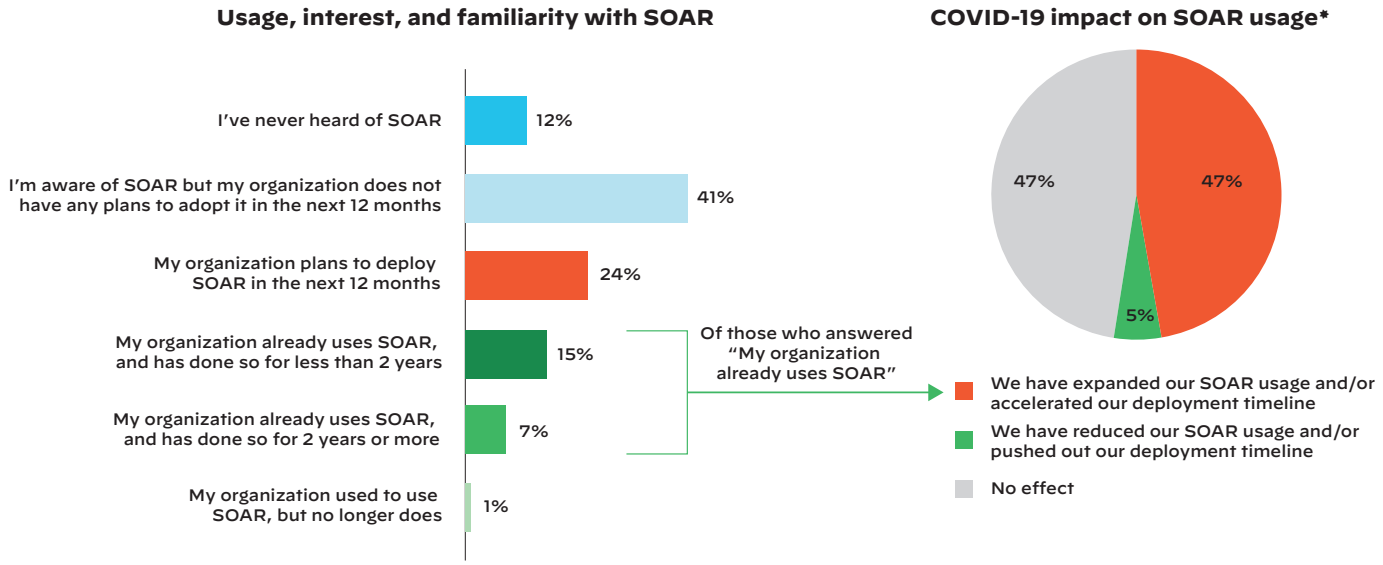

Figure 20: "How has the COVID-19 pandemic influenced your organization's use (planned or implemented) of SOAR?" Note: N=19

IoT, MITRE, and Red Teams Looking to SOAR in the Future

SOAR users have specific workloads in mind as they plan for the coming years. Table 1 breaks down the summary of responses to the question "To what extent do you plan to expand your use of SOAR to the following use cases?" Among organizations that use SOAR, 38% are planning to extend their usage to internet of things (IoT) management use cases in the next 12 months, with another 23% interested in that use case but with no plans to implement it in the next 12 months. When combined with organizations already using SOAR for IoT management, a striking 69% of companies that use SOAR see the technology as an element of their IoT management strategy.

Red Team workflows, cloud security, and MITRE ATT&CK® use cases also had high probabilities of future use, with 57%, 55%, and 55% of organizations, respectively, either using SOAR for these purposes or expressing interest in the use case. Even use cases showing lower levels of interest—such as vulnerability prioritization, IT operations, and detection and response—had current and future interest at 45%, 43%, and 42%, respectively.

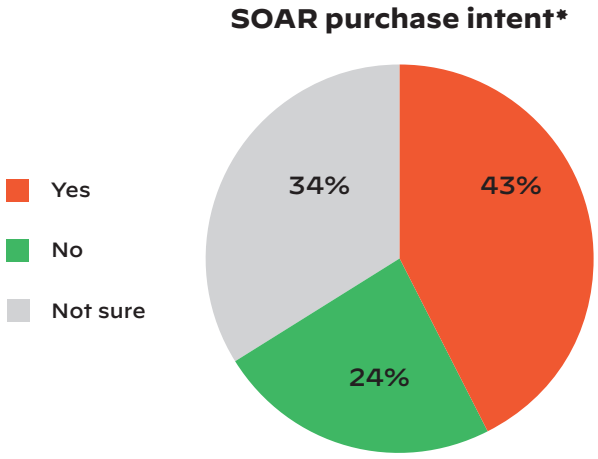

Figure 21: "Is your organization planning to increase spending on SOAR tools in 2020?"

* Percentages exceed 100% due to rounding.

Table 1: Responses to "To what extent do you plan to expand your use of SOAR to the following use cases?"		
	Interested, with plans to implement in next 12 months	Already use SOAR for this use case
IoT management	38%	8%
Red Team workflows	40%	15%
Cloud security	17%	25%
MITRE ATT&CK use cases	25%	18%
Identity and employee onboarding	25%	22%
Compliance checks	23%	30%
Security audits	23%	30%
Network operations	18%	27%
Vulnerability prioritization	15%	37%
IT operations	25%	27%
Detection and response	15%	45%
Averages	24%	26%

How Cortex XSOAR Helps

Cortex™ XSOAR from Palo Alto Networks offers a single platform that orchestrates actions across the entire security product stack for faster and more scalable incident response. It drives the streamlining of IR processes by connecting disparate tools and automating manual, repetitive tasks that don't require human intervention. Cortex XSOAR is the industry's first security operations solution with native incident management and collaboration, security orchestration and automation, and threat intelligence woven into one platform.

Cortex XSOAR helps address the IR challenges raised by respondents to this survey, as shown in table 2.

Table 2: How Cortex XSOAR Addresses IR Challenges		
Challenge/Desire	Needed Solution	What Cortex XSOAR Offers
Too many manual IR processes	More automation to speed up IR and reduce the stress of manual operations	Automation of repetitive actions by coordinating processes across the entire security product stack with playbooks
Lack of third-party integration	Integration of SOC tools with third-party systems so they can easily connect with other departments and IR processes	450+ third-party product integrations to coordinate and automate SecOps
Sharing of community/peer-created playbooks	More playbooks, including third-party playbooks and a sharing community, in order to leverage the proven expertise of other teams	15,000+ peers sharing best practices in an open Digital Forensics and Incident Response (DFIR) community
Too many threat feeds to monitor	Threat intelligence integrated with SecOps tools to cut down on the challenge of monitoring a large number of intelligence feeds and stay ahead of serious threats	Threat intelligence management that lets the SOC take control of any threat intel source by unifying intel aggregation, scoring, and sharing with proven playbook-driven automation
Too many alerts to handle effectively or efficiently	Alert reduction	Up to 95% reduction in the volume of alerts requiring review

Conclusion

This fourth annual State of SOAR Report highlights the rapidly changing nature of cybersecurity. Threats are more serious, with SOCs confronting nation-state actors who are mounting extremely sophisticated attacks. In this environment, despite gains in certain areas of SecOps, analysts are still finding the overall IR process overwhelming. There are too many alerts to handle and too many threat feeds to monitor. Manual processes are still excessive, slowing down responses and pulling people away from alerts that truly need attention.

Security analysts understand what it will take to improve the situation. They want more automation of IR processes and fewer alerts to handle. SOC tools need to integrate with third-party systems. A broader assortment of playbooks, especially those certified by vendors, will further aid in making the SOC run more effectively. Threat intelligence, too, needs to be more tightly integrated with SecOps tools.

SOAR offers a solution to many of these challenges. Platforms like Cortex XSOAR enable SOC teams to save time, speed up triage, and reduce the number of steps required for IR processes. As the survey results reveal, SOAR use is expected to increase in the coming year, with SOC teams planning new, innovative uses for the technology. Even as COVID-19 has made the SOC more stressful, it's an auspicious time to be considering SOAR to improve the efficacy and productivity of the SOC.

Appendix: Survey Demographics

Survey respondents were selected from the Virtual Intelligence Briefings community of more than 150,000 security professionals. Figure 22 captures the sizes of the organizations represented and their proportion of survey respondents. All respondents work in security and compliance roles.

The survey disqualified the people who:

- Work at organizations with fewer than 1,000 employees or that fully outsource security
- Are not sure if security is partially or fully outsourced
- Do not work in a security function or have security in the management chain below them

Industries represented in the survey span financial services (17%), technology and/or technology services (15%), healthcare (13%), and retail and others in smaller proportions. No single industry has more than 20% of respondents. In terms of respondent roles, 24% work in security engineer/analyst roles. A further 17% are managers overseeing a cybersecurity function, and 14% are security architects.

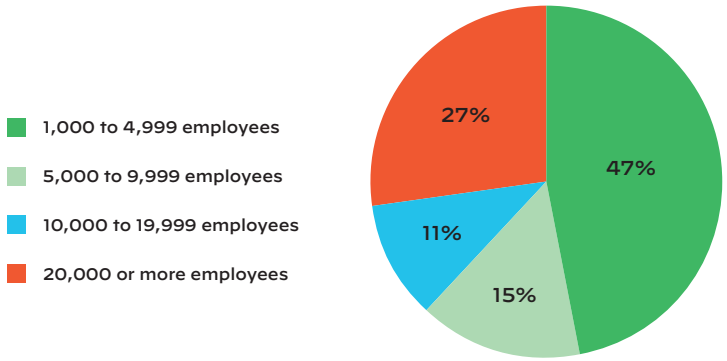

Figure 22: Demographics of survey respondent organizations

paloalto NETWORKS
3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com