tines

Voice of the SOC

2023 REPORT

SMART SECURE WORKFLOWS FOR THE WHOLE TEAM tines

2023 Report

Voice of the SOC

Discover insights and recommendations from our survey of 900 security professionals – and the takeaways for leadership.

Contents

A word from Eoin Hinchy

CEO and Co-Founder, Tines

Security teams are getting restless.

Before founding Tines, I spent 15 years in the SOC leading teams charged with protecting organizations from ever-evolving threats. Over that time, the challenge facing SOC analysts became harder, not easier: workloads are increasing, but teams aren't growing alongside them. SOC analysts are burning out as a result of tedious and repetitive tasks. In the best-case scenario, staff will leave in search of new opportunities and leave their previous organizations scrambling to replace them. In the worst case, their burnout will lead to human error that could cost a company millions.

Last year, we examined these issues in detail in our first "Voice of the SOC Analyst" report. Our survey found that while SOC teams were passionate and engaged in what they do, they were plagued by endless manual tasks, inefficient processes, and overwhelming alert fatigue — all preventing them from focusing on high-impact work. The same holds true in 2023.

For the second edition of the "Voice of the SOC," Tines surveyed 900 security professionals. We expanded the scope beyond the United States to include Europe and sought perspectives from security leaders up to and including the C-suite, rather than just analysts.

Like many, security teams have felt the added pressure of economic instability over the past 12 months. They were asked to do more with less, as business leaders scrutinized every line on the balance sheet.

This year's data reveals that overall job satisfaction in the SOC remains high — security practitioners love the work they do. However, burnout is taking its toll. Leaders continue to feel their teams are understaffed and don't have access to the tools that could automate the most mundane aspects of their work. The bottom line: more than half of respondents, across job levels, say they're likely to switch jobs in the coming year.

This should be an alarm bell to business leaders. With both cyberattacks and skill shortages increasing, staff retention in the SOC is mission critical. The following report digs into the factors that undermine morale and offers practical solutions to help alleviate burnout and empower staff to do their best work.

We hope you find it useful in your SOC in 2023 and as you plan for 2024.

Key findings

Here are a few of the insights we learned from the security professionals we surveyed:

#1

63% of practitioners experience some level of burnout.

With more than 80% saying their workloads have increased in the past year, the problem is only getting worse.

#2

55% say they're likely to switch jobs in the next year.

Organizations could increase retention by increasing salaries, supplying modern tools with advanced capabilities, hiring more staff, and investing in solutions that automate tedious, manual tasks.

#3

Spending time on manual work is the most frustrating aspect of the job.

If respondents had to spend less time on manual tasks, they would most likely use that time to research and evaluate new tools, develop more advanced detection rules, and integrate more systems and logs.

#4

There's hope in automation.

Nine out of ten security teams are automating at least some of their work, and 93% of respondents believe that more automation would improve their work-life balance. Respondents expect automation to help their teams increase productivity, save time, and optimize performance and reliability.

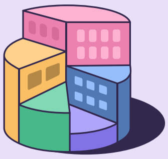
#5

Security practitioners are learning to code.

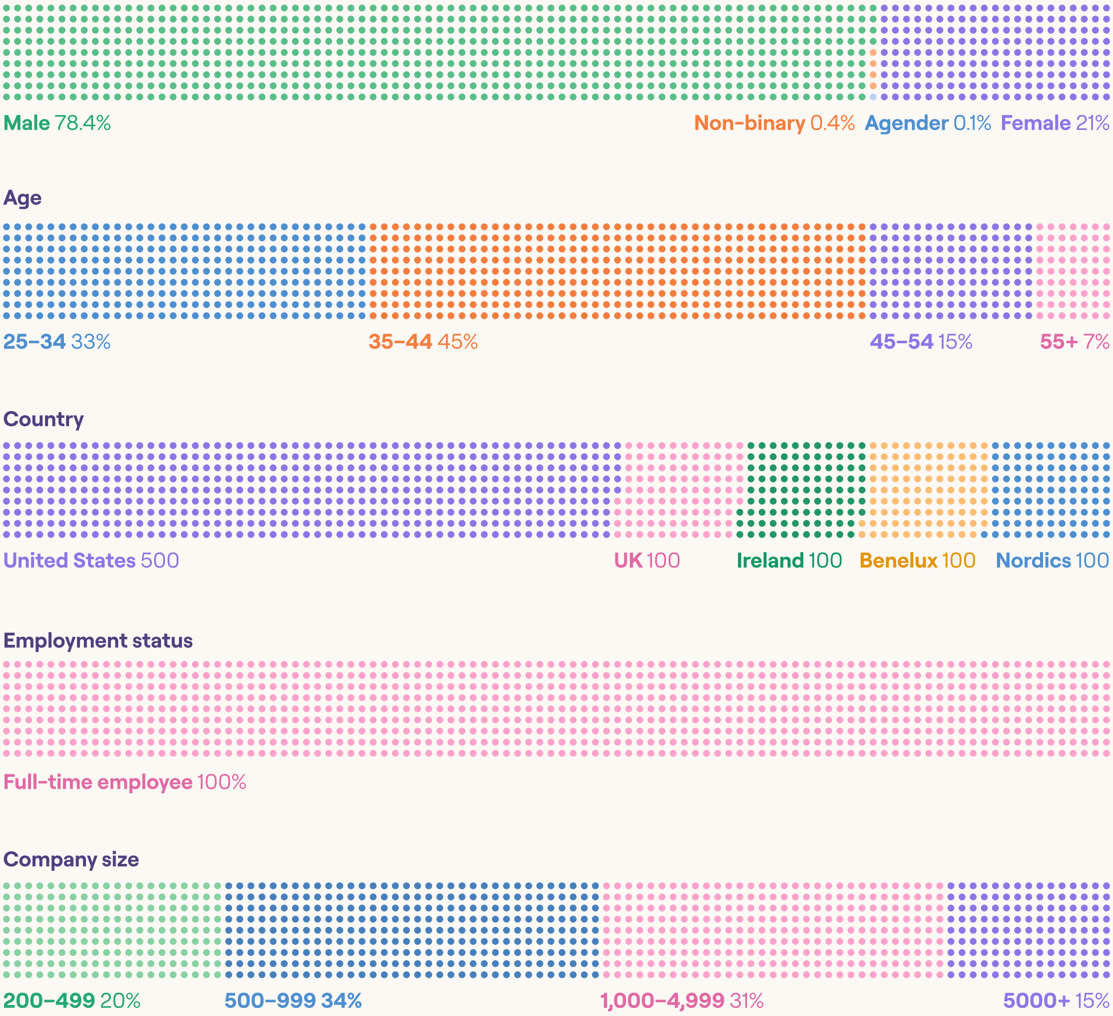
Security teams now consider learning to code — along with computer forensics and malware analysis techniques — most important to succeed, likely because of coding's key role in automation. No-code security solutions could provide similar benefits as organizations automate repetitive tasks.

Methodology and participant demographics

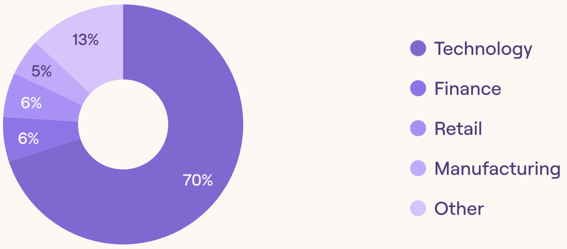
Tines surveyed 900 full-time security professionals from companies with 200 or more employees. Nearly half (46%) work at companies with more than 1,000 employees. There were 500 U.S. respondents, along with 100 each from the United Kingdom, Ireland, Benelux, and the Nordic region. The survey was conducted online by **Sago** (https://sago.com/), a research panel company, in May and June 2023.



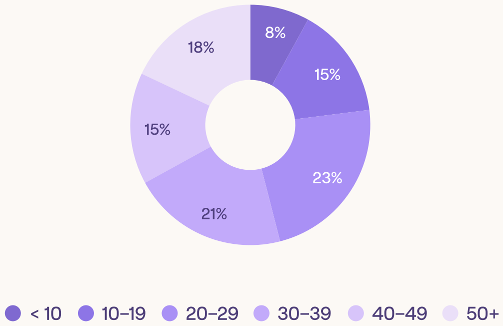
Demographic breakdown



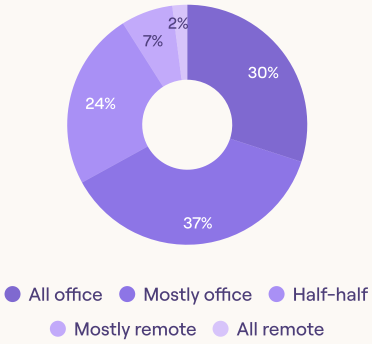
What best describes the industry you work in?



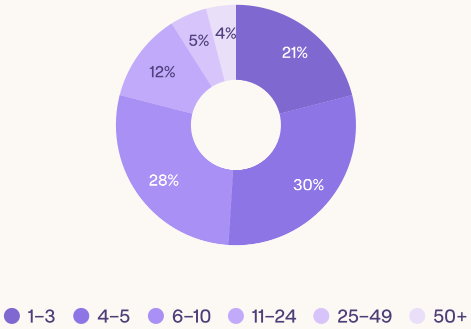
How many people are on your security team in total?



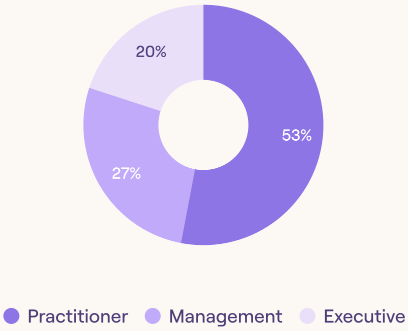
Which of the following best describes your security team in terms of work location?



How many different tools do you use for your security-related work?



Which of the following best describes your title?



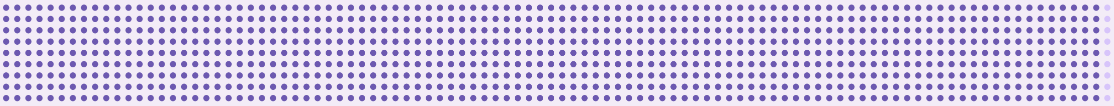
To summarize, our respondents are typically security professionals, the majority of whom work for companies in the technology industry with more than 500 employees. Let's explore their day-to-day experiences in the SOC.

Chapter 1

Job satisfaction and workloads

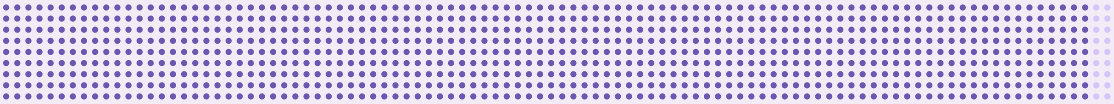
Security teams enjoy the work they do and feel appreciated by the organization. But all is not well in the SOC — burnout and understaffing threaten stability and security. To better understand how leaders can fix the challenges at play, we first must take stock of how security teams are feeling today.

Job satisfaction



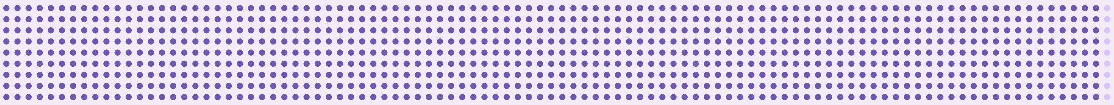
99% are satisfied with their job

Overall job satisfaction is up among security teams this year. The number of respondents satisfied with their current job rose from 88% last year to 99% in 2023. 54% are very satisfied this year.



98% are engaged with their work

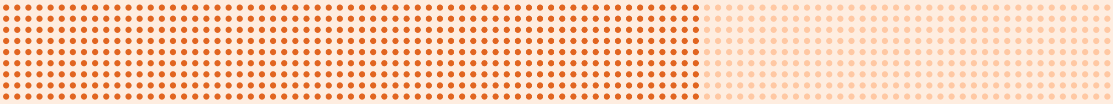
Analysts aren't just satisfied — they're locked in. 50% of respondents are very engaged with their work, and 98% are at least somewhat engaged.



99% feel respected by their peers outside the SOC

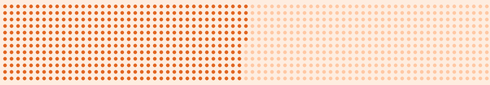
Security teams may sometimes feel like they are working in the shadows as they defend their organizations against threats, but their hard work does not go unnoticed. Almost all (99%) of respondents said they feel respected by their peers outside of the SOC team, and 52% feel very respected.

Workloads



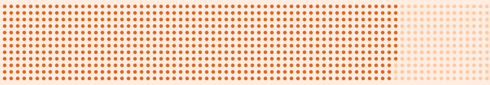
63% are experiencing some level of burnout at work

Despite 99% saying they're satisfied with their job, nearly two thirds (63%) of respondents said they feel burned out at work. One in five feel very burned out. We'll uncover some of the reasons for this shortly, along with ways to help SOC teams join the 37% who say they do not feel burned out at work.



50% say their SOC team is understaffed

Half of our respondents said their team is currently understaffed, and staffing problems are tied closely to burnout. Of those who felt understaffed, nearly four in five (79%) are burned out, compared to just 47% of those who felt they currently have the right amount of staff for their needs.



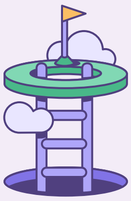
For 81%, workloads have increased over the past year

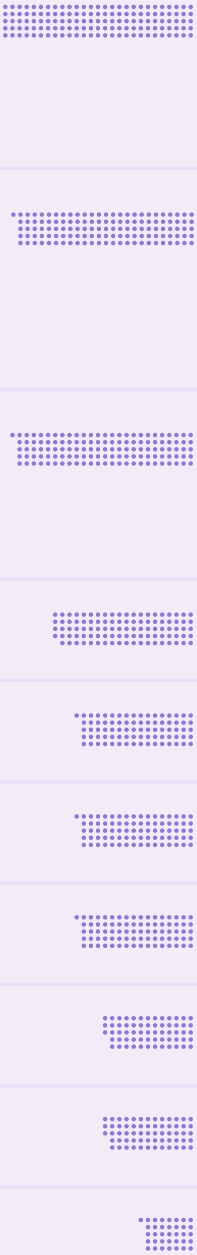
One of the reasons for burnout could be that 81% had more work than ever over the past year. This was particularly true in the United States, where 39% said their workload had increased substantially, compared to 22% in Europe. Just 2% of overall respondents said their workload had decreased.

SOC teams love what they do. The majority of respondents report feeling satisfied with their jobs, engaged in their work, and respected by their colleagues in other departments. They also indicated they are paid what they deserve, with 96% feeling fairly compensated.

However, 63% are experiencing some level of burnout at work, and many security teams feel understaffed and overburdened by ever-increasing workloads. These issues can lead to employee churn, even among those who love their jobs. In the next sections, we'll take a closer look at the factors that have helped retain respondents who would otherwise look for new opportunities.

Top three skills needed to succeed as an analyst





15% **Computer forensics techniques**

Knowing how to recover data from crashed servers and drives after an incident is a key step in uncovering what went wrong in the failure or attack.

14% **Learning to code**

Being able to code can help in task automation, which alleviates some of the most tedious processes. There are also no-code automation options that allow teams to focus on security analysis.

14% **Malware analysis techniques**

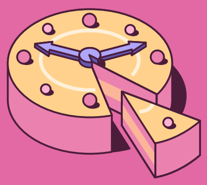
SOC teams must be able to examine malicious software to reveal its purpose and potential impact on their systems.

11%	Threat hunting techniques
9%	Obtaining high-level training and certifications
9%	Operationalizing Mitre ATT&CK
9%	Advanced query language techniques
7%	Keeping up to date on threat actors' TTPs
7%	Learning penetration testing
4%	SOAR integration

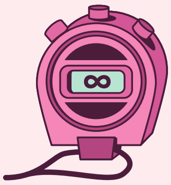
Chapter 2

Where time goes

We know security teams are frustrated by time spent on tedious tasks, and this repetitive work prevents them from engaging in the improvements that will enhance their organization's security posture. In this section, we find out exactly what these necessary but mundane tasks are, and learn more about the internal metrics guiding this time management.



Top five time-consuming tasks



18% **Security orchestration, automation and response (SOAR)**

The number one most time-consuming task is SOAR, likely because nearly every current SOAR tool uses an app-based integration model which relies on limited pre-built integrations and often requires teams to build their own custom apps. Direct integrations can address these challenges.

17% **Troubleshooting system errors/system maintenance**

Troubleshooting and maintenance take up a significant amount of time, preventing teams from doing the proactive work that could improve security postures.

16% **Intelligence (i.e. researching threat actors, TTPs, ATT&CK)**

Teams are also spending time researching threat actors — including their tactics, techniques, and procedures — and operationalizing the MITRE ATT&CK framework.

15% **Monitoring**

Respondents are spending valuable time monitoring for threats and alerts, despite the fact that respondents over the practitioner level should not be doing front-line monitoring.

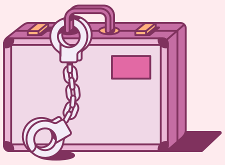
15% **Managing a knowledge base/operational documentation**

Documentation rounds out the top five tasks — ensuring all essential documents are stored, backed up, and eventually discarded when they’re no longer needed.

Lower on the list, you’ll find more proactive, higher-impact tasks like managing IOCs and modifying alert rules — tasks that SOC would likely prefer to prioritize. One task that saw a steep decline this year? Reporting.

13%	Data Loss Prevention (DLP)
12%	Communicating (email, phone, messenger, etc)
11%	Detecting (including intrusion detection)
11%	Responding to security incidents
11%	Vulnerability/compliance scanning (e.g. Nessus) and patching
9%	Malware analysis/forensics
8%	Threat hunting
8%	Evaluating new vendors/products/services
8%	Log analysis
8%	Operations/ShiftOps
7%	Compliance and audits
7%	Managing IOCs
7%	Tracking
6%	Penetration testing, Red teaming, Purple teaming, etc.
6%	Reporting
5%	Phishing triage/response
5%	Recovery
4%	Modifying alert rules
3%	Containment

Top four tasks security teams enjoy the least



18% **Communicating (email, phone, Slack, etc.)**

One of the two tasks which respondents enjoyed the least was communicating. Slack notifications come for us all, but there are ways to automate communications internally and externally and increase transparency on shared projects.

18% **Reporting**

The other top choice was reporting. Reporting matters, but it's reactive — collecting what happened after an incident — rather than proactive. Streamlining the reporting process through automation frees up security practitioners to focus on analysis and increases job satisfaction.

10% **Monitoring**

Monitoring, one of the most time-consuming tasks, is also one of the least enjoyable. Much of this type of manual front-line monitoring can be automated.

10% **Responding to security incidents**

As you'll see below, teams are judged on their ability to respond to incidents. It should be noted that 14% of respondents named this type of response their most enjoyable task — including 22% of VPs and above, suggesting a split between analysts and leaders on the task.

9%	Triaging
9%	Threat hunting
8%	Tracking
6%	Intrusion detection
6%	Detecting
6%	Operations/ShiftOps

Top four key metrics used to measure job performance

What key metrics are used to measure a security team's job performance? In other words, what metrics should SOC teams prioritize to improve team performance?

When we asked this question last year, the top five responses were mean time to investigate (54.1%), number of alerts (43.8%), mean time to respond (40%), time to detect (37.6%), and number of incidents handled (34.2%). Four of those answers cracked the top five again this year, with only the number of alerts falling off — possibly because security teams are learning that an avalanche of alerts is an impediment to success, not a marker of it.

36% **Mean time to investigate (MTTI)**
The average amount of time between when a problem is detected and when the security team begins to investigate it. Successful SOC teams reduce the intervening window.

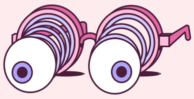
36% **Time to detect**
The time it takes an organization to discover an incident. SOC teams need solutions in place to identify issues quickly and catch zero-day vulnerabilities.

36% **Number of incidents handled**
SOC teams are measured by the amount of incidents they resolve successfully. They can slash this figure by implementing faster and more thorough alert and resolution tools.

36% **Mean time to respond**
The average time it takes to resolve an incident completely. Automation can help security teams investigate and remediate threats and return a system to operation after a failure.

33%	**Adherence to SOW/SOP/KBs (Statements of Work, Standard Operating Procedure, Knowledge Base articles)**
33%	**Percentage of recurring incidents**
31%	**Time to containment**
31%	**Adherence to Service Level Agreements (SLAs)**
30%	**Number of alerts**
28%	**Percentage of escalated events**
28%	**Knowledge base/wiki articles created or enhanced**
28%	**Rules or detections created or enhanced**
26%	**Time to eradication**
25%	**False positives identified and reduced**
22%	**False positive rate**

Where you can find them



As a fun aside, we asked our participants which conferences they're aware of or have attended in the past two years. If you're looking for your peers, your best bet is AWS re:Inforce, followed by Black Hat and AWS re:Invent.

AWS re:Inforce	39%
Black Hat	37%
AWS re:Invent	35%
InfoSec	27%
DefCon	27%
BSides	24%
RSA	13%
None of the above	19%

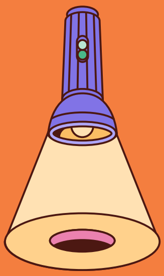
Our respondents reveal that their time is mostly spent on necessary but tedious tasks like operating imperfect SOAR tools, troubleshooting system errors, and front-line monitoring (which is also one of the tasks they enjoy least). Effective automation can help maximize a SOC team's time and improve the metrics — including time to detect, investigate, and respond — that they are measured against.

Chapter 3

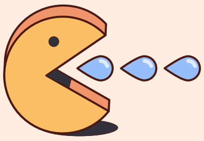
Barriers to good work

Security teams want to do their best work — they're passionate about protecting their organizations and highly engaged in their roles.

Let's take a look at some of the other obstacles that SOC teams encounter.



Top three challenges



We wanted to better understand the primary pain points for SOC teams, so we asked respondents to rank their teams' top day-to-day challenges. The following ranked in the top five most frequently.

37% **Too much data, not enough information**

Security teams are drowning in data but struggle to turn that data into actionable insights.

36% **Time spent on manual tasks**

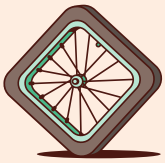
As we've seen elsewhere, tedious tasks — like reporting, monitoring, and detection — are a daily challenge.

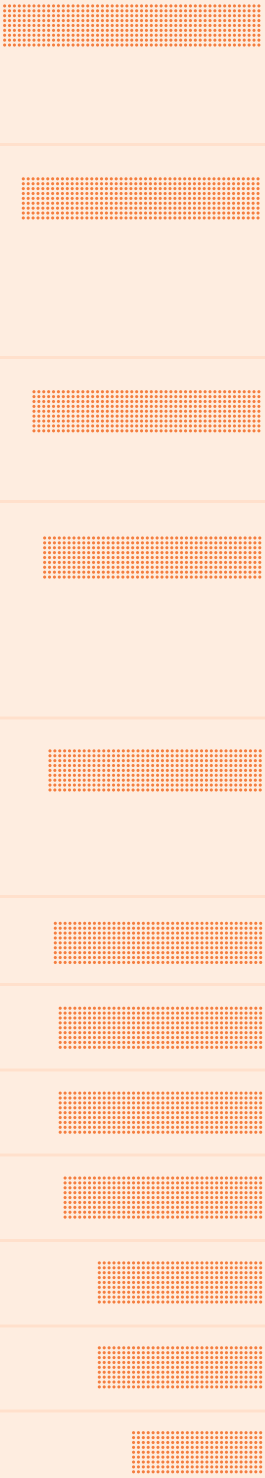
34% **Too many reporting requirements**

Reporting is one of the least popular tasks, likely because of its arduous requirements.

31%	Too many logs
30%	Compliance
30%	Too many alerts
29%	System downtime
28%	High staff turnover rate
28%	Lack of training
28%	Understaffed
26%	Tools don't integrate
26%	Poor processes
25%	Clunky, outdated, or misconfigured tools
25%	Leadership issues
23%	Restrictive SLAs
23%	Teams are very siloed
22%	Poor visibility into our environment
17%	Boredom

Top five things that frustrate security teams the most





53% **Spending time on manual work**

No one likes doing tedious work, and a majority of respondents feel, or their team feels, frustrated by repetitive, manual tasks.

49% **Too many different consoles/tools to investigate incidents**

Tool consolidation was a trend this year across the tech industry, but its effects haven't yet taken hold in security. Fragmented toolsets could lead to gaps in an organization's response.

47% **High cost of security and log management software**

All those tools don't come cheap.

45% **Lack of unified query language to access all data across all monitored systems**

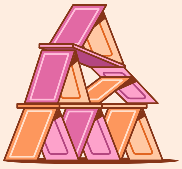
Security teams are swapping screens, tools, and languages to access all their distributed data.

44% **Poor integration of different security tools**

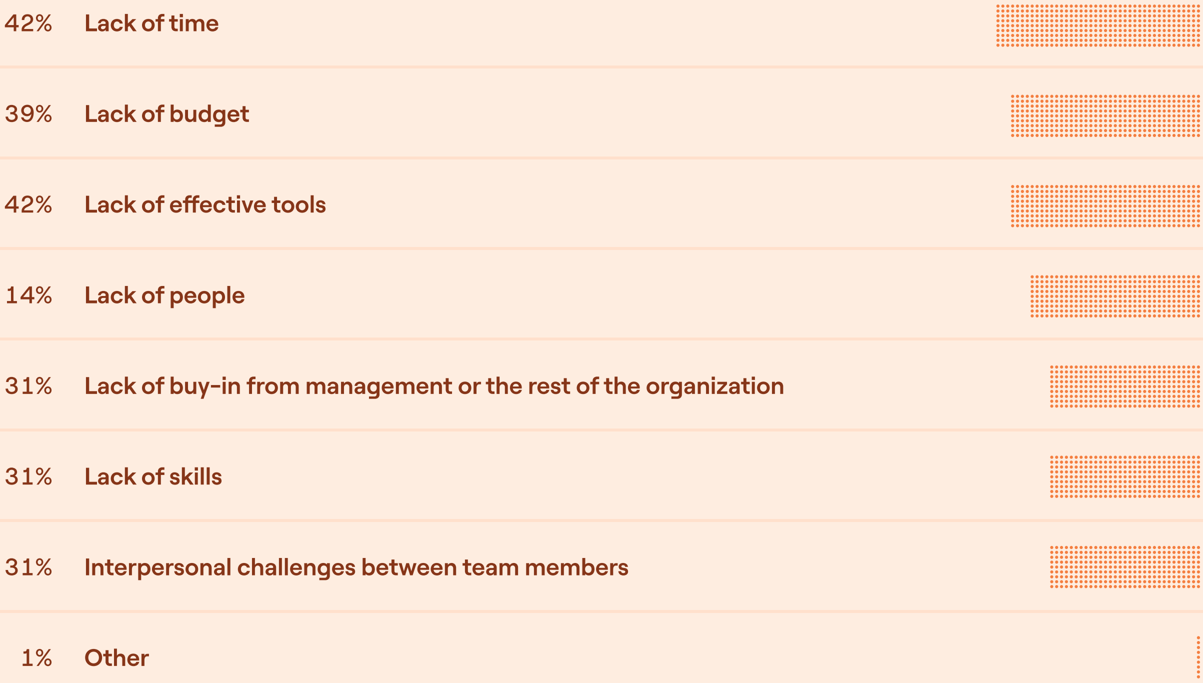
When tools don't integrate well, it creates unnecessary friction within teams and between business units.

43%	Inaccurate or incomplete attribution
42%	High false positive rates
42%	Slow or delayed log file ingestion and processing
41%	Lack of broad support for different log types and systems
34%	Toxic work environment/personnel issues
34%	Lack of space for logs
27%	Our SIEM

Lack of time, budget, and effective tools are inhibiting SOC teams



Overall, what prevents the SOC team from doing their best work? In a word: resources. Our respondents, selecting all that applied, said a lack of time (42%) was the top factor holding them back, followed by lack of budget (39%), lack of effective tools (39%), and lack of people (35%).



42%	Lack of time
39%	Lack of budget
42%	Lack of effective tools
14%	Lack of people
31%	Lack of buy-in from management or the rest of the organization
31%	Lack of skills
31%	Interpersonal challenges between team members
1%	Other

SOC teams identified three clear challenges preventing them from doing their best work: too much data, too many tedious tasks, and too many reporting requirements. These pain points are amplified by a lack of time, budget, tools, and people.

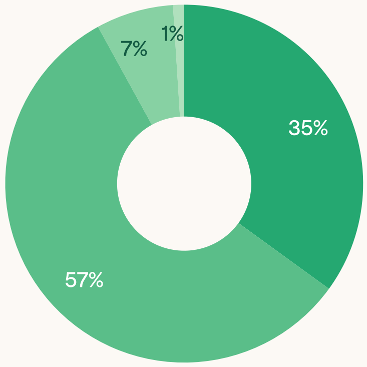
Automation offers a path forward for security leaders to remove obstacles and refocus their teams on proactive, high-impact work. No-code tools can help teams catch up quickly, keeping their organizations safe and possibly keeping their teams intact as well.

Chapter 4

Automation — friend or foe

Business leaders are focused on streamlining processes and achieving operational efficiencies. They've found an effective way to do so in automation. But how do they feel about automation? Are they embracing the technology?

Nearly all security teams have already adopted automation to some extent. This is especially true in Ireland, where 44% of respondents said much of their work is automated, the highest percentage among the countries we surveyed.

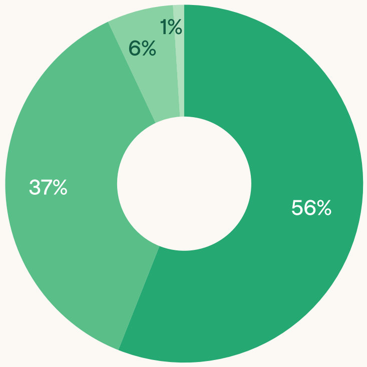


Nearly all security teams have already adopted automation to some extent

This is especially true in Ireland, where 44% of respondents said much of their work is automated, the highest percentage among the countries we surveyed.

What best describes your team's adoption of security automation tools?

- ● Much of our work is automated
- ● Some of our work is automated
- ● Very little of our work is automated today
- ● None of our work is automated

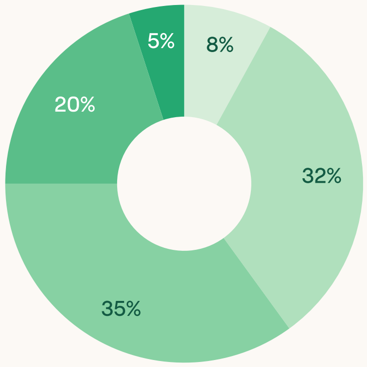


SOC teams are excited about automation's effect on their lives

A stunning 93% of respondents agreed that automation at their workplace would improve their work/life balance.

Please indicate whether you agree or disagree with the following statement: "Automation at my workplace will improve my work/life balance."

- ● Strongly agree
- ● Somewhat agree
- ● Neither agree nor disagree
- ● Somewhat disagree



25% spend more than half their time on tedious manual work

While tedious manual work is still an obstacle for security teams, they are making strides in this area. In 2022, 64% of surveyed analysts reported spending over half their time on such work. This year, that number fell to 25%.

What percentage of your or your teams' time would you describe as tedious manual work?

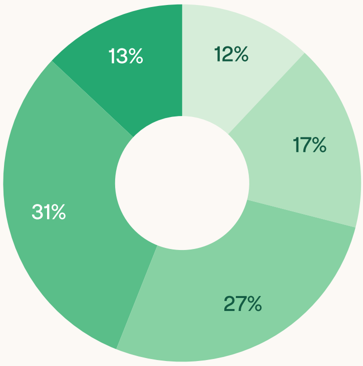
● < 10% ● 10–24% ● 25–49% ● 50–74% ● 75–100%

56% fear automation will eliminate their job

More than half of respondents worry that automation will eliminate jobs in the near future. This figure is down from 69% last year, which may reflect a growing understanding of how jobs could evolve after automating manual tasks.

How worried are you that automation will eliminate your job/your co-workers jobs in the near future?

● Very worried ● Worried ● Somewhat worried
● Not very worried ● Not worried at all

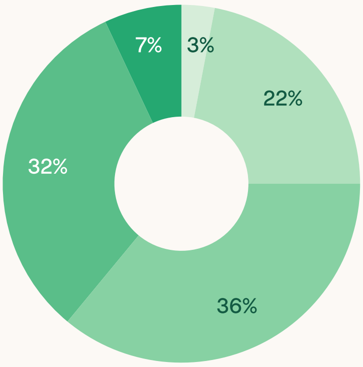


SOC teams recognize automation could have an immediate impact

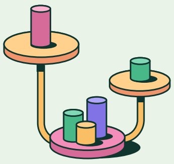
Only 3% of respondents believe less than 10% of security work could be automated by software currently available. More than a third said that half to all of the work could be done by today's automation solutions.

What percentage of your work do you believe could be done/automated by software that's available today?

● <10% ● 10-24% ● 25–49% ● 50–74% ● 75–100%



Top five tasks SOC teams would automate to save time



17% **Intelligence analysis**

The task SOC teams most want to automate would ensure alerts arrive with richer, more actionable context, saving valuable time spent tracking that information down manually.

12% **Threat hunting**

This would automate manual efforts to smoke out hackers or data that indicates a system may have been breached.

11% **Endpoint detection and response**

Survey respondents want to use automation to detect and investigate threats on endpoints.

11% **Risk assessments**

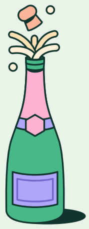
This was the top answer in last year's report. SOC teams would love to automate these assessments rather than manually monitoring for and triaging risk.

10% **Vulnerability management**

This process — identifying, assessing, reporting on, and remediating vulnerabilities — rounds out the top five.

9%	Advanced triage
8%	Email phishing
8%	Attack surface management
6%	Patching
5%	Initial triage
4%	Abuse response

What would SOC teams do if parts of their work was automated?



45% **Research and evaluate new tools**

Respondents welcome the opportunity to spend more time finding the best tools for their teams.

44% **Develop advanced detection rules**

These rules help enhance an organization’s security posture and improve their key performance metrics.

38% **Integrate more systems and logs**

Bringing these sources of data together is a key proactive action with long-term performance benefits.

37% **Research TTPs more/intelligence**

Respondents want more time to dive deep on threat actor tactics, techniques, and procedures.

37% **Update reports and dashboards**

In the absence of manual work, SOC teams would focus on keeping reports and dashboards up-to-date. This indicates they are currently behind, and the first order of business after automation would be catching up.

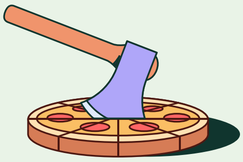
36% Update operational documentation

36% Modify detection and alert rules to reduce false positive rates

30% Threat hunt more

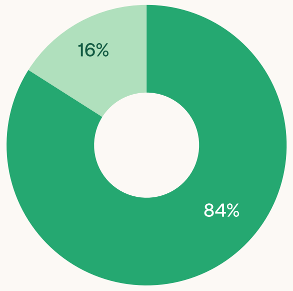
1% Other

SOC teams and their tools



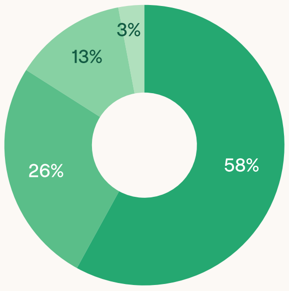
Our respondents would love to spend more time researching and evaluating tools, rather than doing tedious tasks. On the subject of tools, they feel like they have access to the best available — probably because they are involved in the evaluation process. Three out of four respondents have found a security solution and added it to the organization's toolkit.

Do you have access to the best tools possible?



● Yes ● No

How involved are you in evaluating the software tools your team uses?



● Very involved - we have a lot of influence over the process
● Involved ● Somewhat involved ● Not very involved
● Not involved at all - management just gives us the tools (0%)

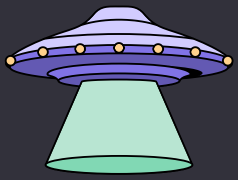
In this section, we learned that nearly all security teams have already adopted automation — and they're excited about its impact on work-life balance. We previously established that the SOC feels understaffed and overworked under a deluge of alerts and manual tasks. Now, we've identified the tasks that security professionals wish they could automate to save time, and the high-impact tasks — like researching new tools and developing advanced detection rules — that they would work on instead if automation was deployed to full effect.

Automate the present tedium, and security teams can anticipate the threats of tomorrow. Given time, they could focus on protecting the business with insights from integrated systems and enhanced research and reporting capabilities.

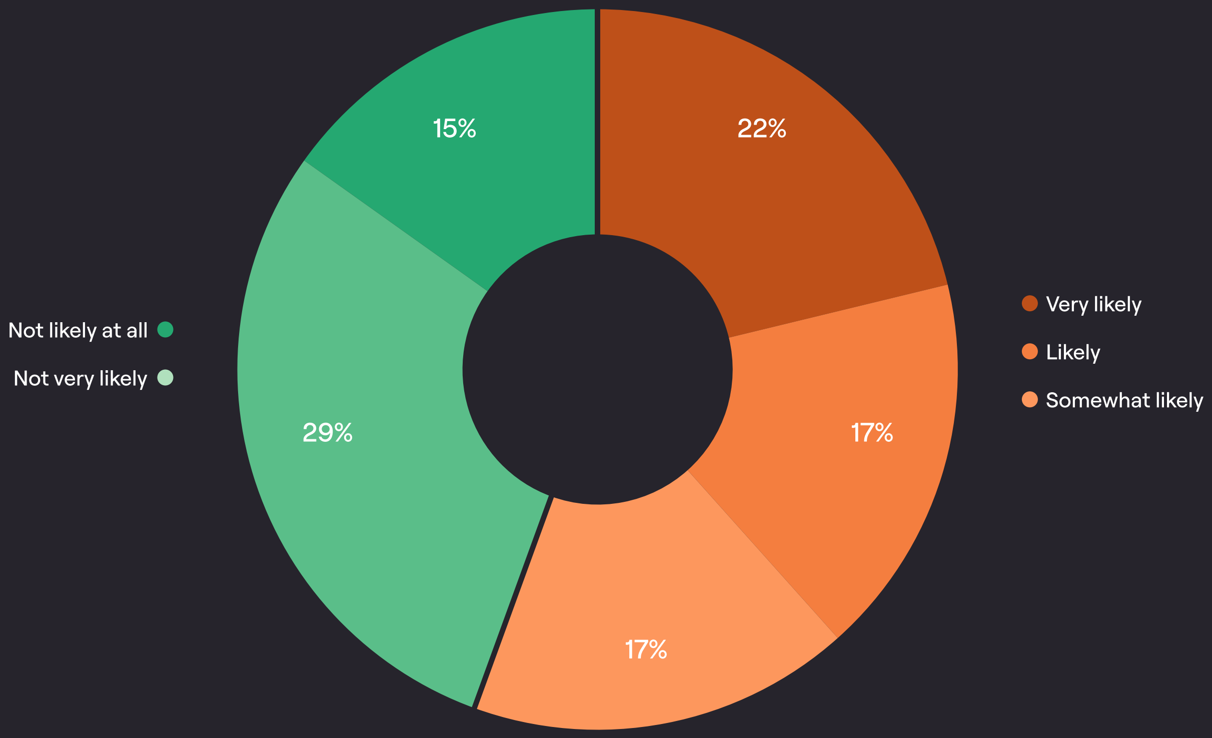
Chapter 5

Improving retention

Burnout is a real issue for SOC teams, and the current economic pressures are only making the job harder. We wanted to know if SOC teams were considering career moves — and what organizations could do to retain them.



How likely are you to switch jobs in the next 12 months?



We know SOC teams are frustrated by manual work and poorly integrated tools, so it's no surprise that more than half of respondents are at least somewhat likely to leave for a new job in the next year.

Top three ways to improve retention

As SOC teams eye the door, we asked our respondents about the actions their organizations could take to keep them on board. The top answer was to simply pay more — no surprises there. Despite over 96% of respondents reporting they feel fairly compensated, they still feel a pay increase would help keep them around. But security teams also pointed to other factors: supplying more modern tools with advanced capabilities; hiring more people; and providing tools that automate the tedious manual tasks that have them looking elsewhere.

What could your current organization do to retain you or your team?

49%	Pay more
42%	Provide more modern tools with advanced capabilities
40%	Hire more people on our team
39%	Provide tools that automate tedious manual tasks
34%	Provide regular training
33%	Pay for industry certifications
33%	Consult security team for security software purchases and upgrades
31%	More favorable shifts
25%	Reduce on-call hours
1%	Other
2%	None of the above

Actionable takeaways for leaders

The 2023 Voice of the SOC found that security teams continue to experience burnout amid relentless cyberattacks, internal pressures, and limited resources. Security professionals want to pursue high-impact work, but they're being held back by growing workloads, shrinking budgets, and a worsening skills shortage. The findings are consistent: regardless of location, company size, in-person or remote, security professionals are feeling the pressure and are looking for an escape hatch. Limited resources and increasing external threats will continue to pose problems for the foreseeable future. To that end, here are four actionable takeaways that can help SOC teams stay ahead of the challenge.

#1

Make more out of your resources

Organizations large and small are facing the pressures of a down economy, with many teams adjusting to hiring freezes or reductions in force. Meanwhile, security threats are only increasing, leaving smaller teams left to tackle a growing problem. There is good news: the most monotonous tasks in a SOC analyst's day are also those that can be automated most easily.

The greatest challenges security practitioners face on a regular basis include too much data and not enough information, too much time spent communicating, and too many reporting requirements. Automation can solve many of the most repetitive and error-prone aspects of data collection, communication, and reporting, including building workflows across systems and business units. Unique workflow builds can automate internal and external communications tasks, as well as data enrichment and reporting, increasing a team's productivity and freeing up SOC analysts to focus on more valuable work.

#2

Tackle burnout at the source

Nearly two-thirds (63%) of survey respondents indicated they were burnt out, and this ongoing problem often leads directly to employee churn. More than half (53%) of respondents said the most frustrating aspect of their work was spending time on manual tasks. Organizations can't afford to ignore the problem of burnout. Otherwise, they'll risk greater consequences when they have to replace valuable team members.

The only way to alleviate burnout is by increasing resources, and SOCs have two options: hire more staff or adopt better tools. Increasing the size of the team will naturally spread out the workload. However, advanced tools and automation can effectively increase the productivity of each employee without having to invest in new hires. If they didn't have to spend as much time on manual tasks, security practitioners say they'd develop advanced detection tools, integrate more systems and logs, and research new tools that could improve their organization's security posture.

#3

Prioritize retention to avoid the skills shortage

The cybersecurity industry continues to labor under a significant skills shortage: there simply aren't enough qualified professionals to meet the needs of today's organizations. Minimizing employee churn is mission critical. If a highly skilled employee leaves, it will be difficult — and expensive — to replace them.

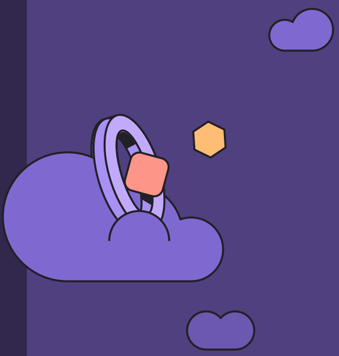
More than nine in 10 respondents (93%) said that automation in their workplace would improve their work-life balance. Whether by paying them more or making their jobs easier, organizations need to do what it takes to keep SOC analysts happy and onboard.

#4

Identify ways to break down silos

Our survey respondents consistently pointed to communication and data collection as pain points in their day-to-day work, and these challenges are exacerbated by silos between departments and business units. Organizations can make life easier for their SOC — and improve security outcomes in the process — by streamlining workflows between departments.

Smart, secure workflow automation can effectively break down silos, simplifying communication and making data easier to access and act on. With simple interfaces and a low technological barrier to entry, SOC teams can quickly adapt to the new platforms and streamline their operations.



Conclusion

The second edition of the Voice of the SOC paints a clear picture of the pressures facing today's security teams. Competitive organizations need to move quickly to address the lack of resources in their SOC; otherwise, they risk significant consequences to their reputation and bottom line.

Smart workflow automation offers a logical solution to many of the challenges outlined in this report. SOC teams at leading organizations are deploying the technology to run mission-critical workflows and achieve greater productivity at scale, all without having to write a single line of code. As a result, security professionals can focus on high-impact work and improve their most important performance metrics.

To learn more about how smart, secure workflows can make a difference in your SOC, visit tines.com.