tines

2022

Voice of the SOC Analyst

No-code automation for security teams

Read online
tines.com/soc

Voice of the
SOC Analyst

A word from Eoin Hinchy

CEO & Co-Founder, Tines

> Security teams are being prevented from doing their best work.

While under-staffing and low budgets have always been challenges for any type of team, security teams are uniquely affected by repetitive, manual tasks, which in turn keep them from working on higher-impact projects that contribute to their organization's overall security posture.

In my fifteen years of being a security practitioner, working on incident response and leading security teams, I witnessed over and over again that in the SOC, there's too much work and not enough staff. More specifically, I saw overworked analysts so consumed with tedious, repetitive tasks that it led not only to burnout, but to human error that could cost a company millions.

The analysts I worked with weren't the only ones facing these challenges, and I wasn't the only security leader trying to find solutions to help my team do their best work.

While we generally know the day-to-day struggles analysts face, there's a lack of current data to give us a clear picture of what it's like to be an analyst today. So we conducted a survey that aimed to understand them better: "Voice of the SOC Analyst."

We found that while SOC teams are passionate and engaged in what they do, they're challenged with endless manual tasks, understaffed teams, inefficient processes, and too many alerts — all preventing them from doing more high-quality work.

Our goal with this project is to help security leaders recognize what they can do to streamline their processes, decrease burnout, increase retention, and create better overall work environments for their analysts.

We hope you utilize these findings and data as you make your way through 2022.

Key findings

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

1

71% of analysts experience some level of burnout.

This could be due to the fact that 69% are understaffed, and 60% have seen increased workloads over the past year.

2

Reporting, monitoring, and detection are top tasks consuming an analyst’s time.

Additionally, reporting and monitoring are also two of the top tasks analysts enjoy the least.

3

Spending time on manual work is an analyst’s top frustration.

64% are spending over half their time on tedious manual work.

4

However, 66% believe that half of their tasks to all of their tasks could be automated today.

If they could automate their tasks, analysts would use the time to update operational documentation, develop advanced detection rules, integrate more systems and logs, focus more on intelligence, and modify alert rules to reduce false positives.

5

64% say they’re likely to switch jobs in the next year.

However, organizations could retain them by providing tools that automate tedious manual tasks, providing best-in-breed tools with advanced capabilities, and hiring more people to the team.

6

Coding is the top skill needed to succeed as an analyst.

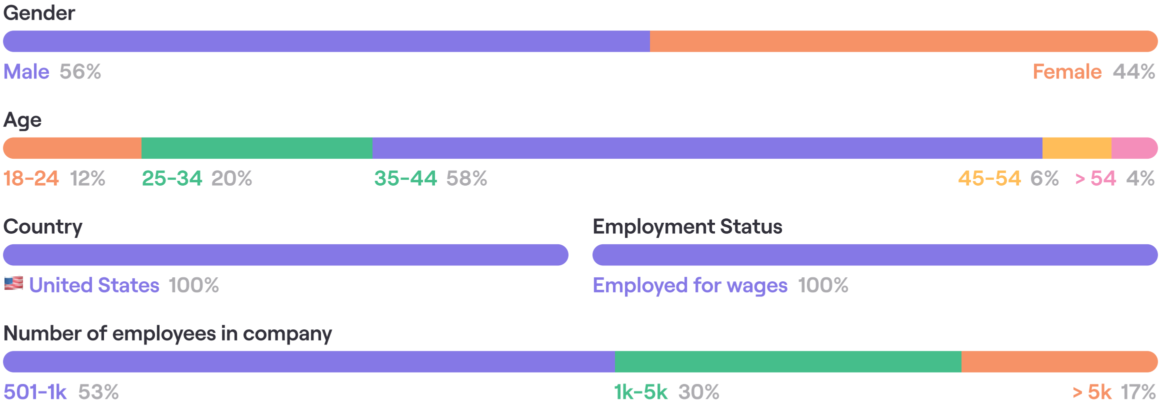
This is likely due to the need to know code to automate processes. Other top skills our respondents say analysts need for the future are knowing computer forensics techniques and knowing how to operationalize MITRE ATT&CK.

Methodology and participant demographics

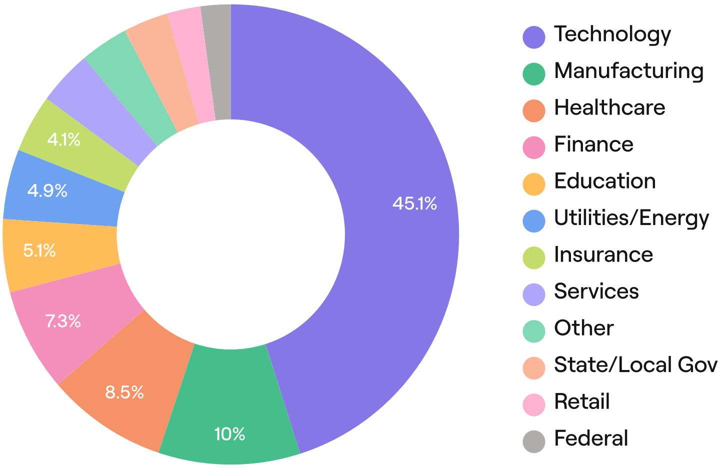
In order to provide greater context around these findings, here are more details on who we surveyed and the methodology used. Starting on December 9, 2021 we surveyed 468 full-time security analysts in the United States who worked at companies with 500 or more employees. The survey was conducted online via Pollfish using organic sampling. Learn more about the Pollfish methodology on https://www.pollfish.com/methodology/.

468

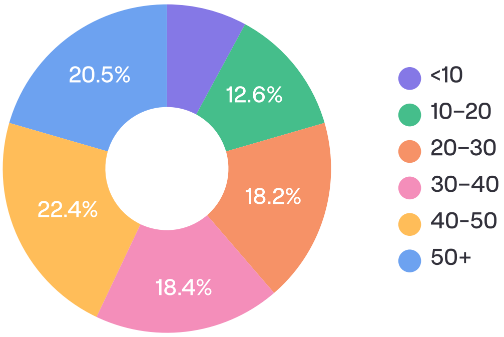
full-time security analysts



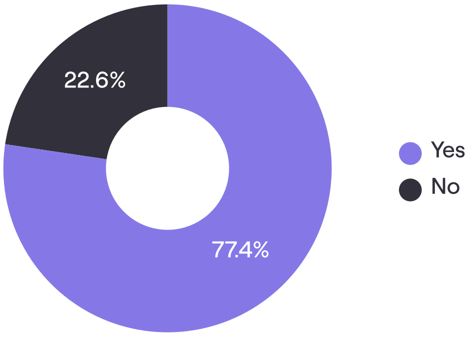
What best describes the industry you work in?



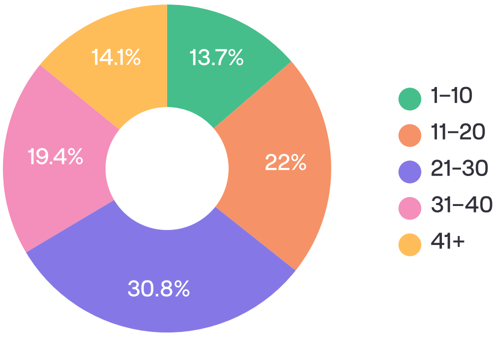
How many people are on your SOC team in total?



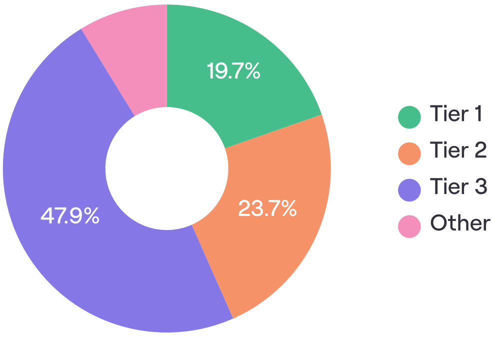
Is all or part of your SOC team remote?



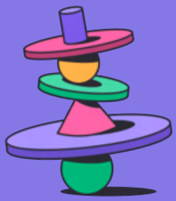
How many different tools do you use for your security-related work?



What tier/level of analyst are you?



Now that we know a bit more about our respondents — security analysts, the majority of whom are Level 3 and work in the technology industry — let's explore their day-to-day experiences on their SOC team.



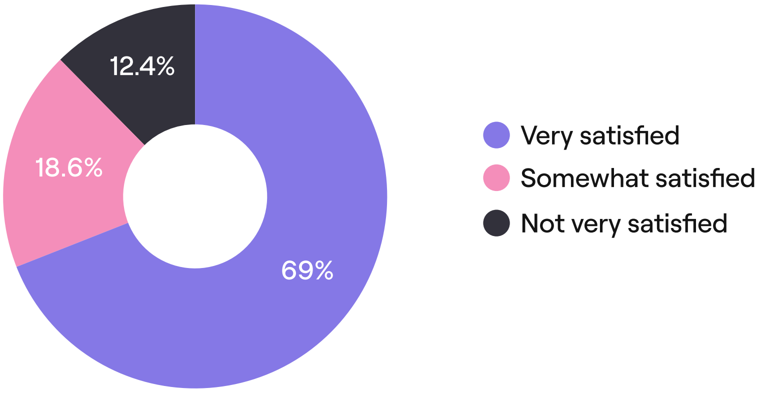
PART ONE

Job satisfaction and workloads

Security analysts play a vital role in ensuring that their organizations stay safe and secure. But barriers to their work, like a lack of staff, overwork, and tedious tasks are causing frustration and burnout. In order to understand better how security leaders can solve their team's pain points, we first have to start with a baseline of how analysts are faring today.

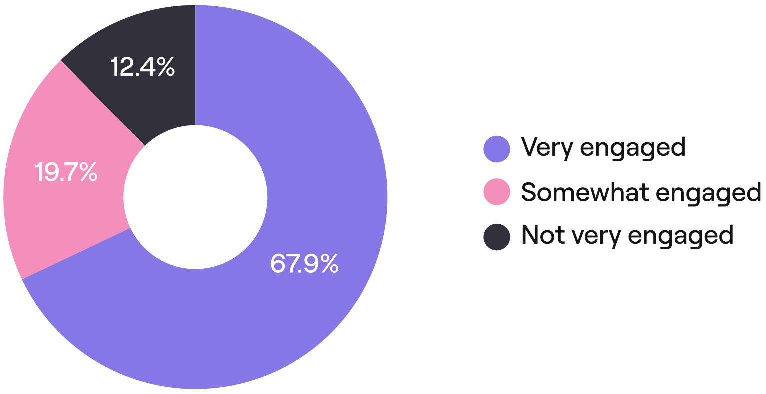
69% of analysts are very satisfied with their job

When it comes to overall job satisfaction, 69% of analysts replied that they are very satisfied with their current job. However, 18.6% replied that they are only somewhat satisfied, and 12.4% are not very satisfied.



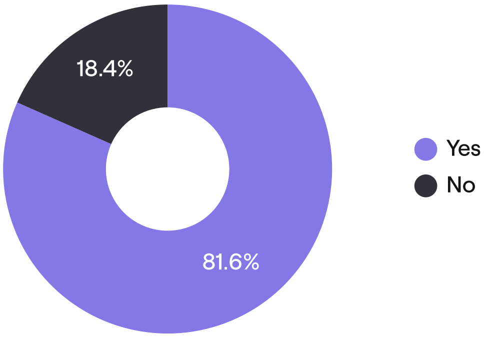
68% of analysts are very engaged with their work

Not only are a little over two-thirds very satisfied with their job, 67.9% say they're very engaged with the work they do as a security analyst as well. 19.7% replied that they are somewhat engaged with their work, while 12.4% say they're not very engaged.



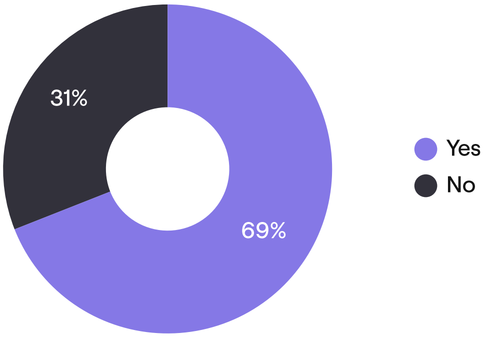
82% feel respected by their peers outside the SOC

Having a hand in the day-to-day protection of their organization means that analysts are aware of the actions that the rest of their organization may not be aware of. Fortunately, 81.6% replied that they do feel respected by their peers outside of the SOC. However, 18.4% say they do not, possibly suggesting that others in the organization simply aren't aware of the amount of work security analysts do.



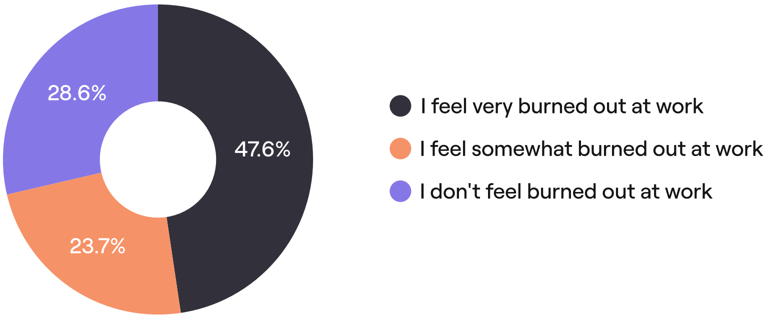
69% say their SOC team is understaffed

With a known cyber security talent shortage, it's no wonder that 69% of analysts say their team is currently understaffed. However, this could also mean that teams are being overwhelmed with mundane, repetitive tasks that are taking their time and skill away from other high-impact projects — making them feel understaffed as well. 31% replied that they currently have the right amount of staff for their needs.



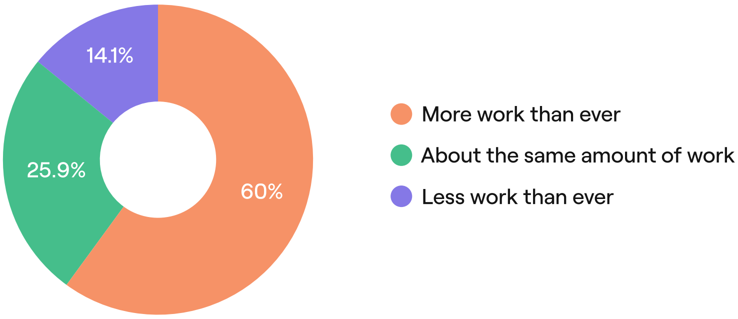
71% are experiencing some level of burnout at work

Despite 69% saying they're very satisfied with their job, nearly half of the analysts who replied (47.6%) said that they feel very burned out at work, with an additional 23.7% saying they feel somewhat burned out. What's important to note is that analysts are passionate about and engaged with the work they do, but other factors like long hours and not having the right tools are causing them to lose their zeal and motivation, and face mental and physical exhaustion — a big driver of analyst turnover. We'll uncover some of the reasons for this later on, and hopefully, find out how we can get more analysts to join the 28.6% who say they do not feel burned out at work.



For 60%, workloads have increased over the past year

One of the reasons for burnout could be that 60% of analysts have had more work than ever over the past year, which could be due to a number of factors: being short-staffed, the added challenges of working remotely during the pandemic, or more alerts and threats due to vulnerabilities caused by remote work. 25.9% say their workload hasn't changed over the past year, while 14.1% say they have less work than previous years.



Summary

SOC analysts love their work: the majority are very satisfied with their jobs, very engaged with their work, and feel respected by their peers. At the same time, 71% are burned out to some extent in their work environment, and while workloads have increased for over half of them, their teams are still understaffed.

Even if they do love their jobs, burnout can lead to employee churn; as we'll see later, the majority are looking to switch jobs in the next year. In the next sections, we'll investigate some of the reasons why security analysts are experiencing mental and physical drain.

Top three skills needed to succeed as an analyst

What's going to be the most valuable skill a security analyst can have to help them succeed in the future?

30.1%

#1: Learning to code

The number one skill identified is learning to code, according to nearly one-third of respondents. While it may seem unrelated to the day-to-day tasks, analysts see that knowing how to code will help with task automation.

13.5%

#2: Learning computer forensics techniques

The second most valuable skill will be learning computer forensics techniques, as knowing the process of recovering data from crashed servers and drives after a failure or attack is a critical skill to helping analysts uncover what went wrong.

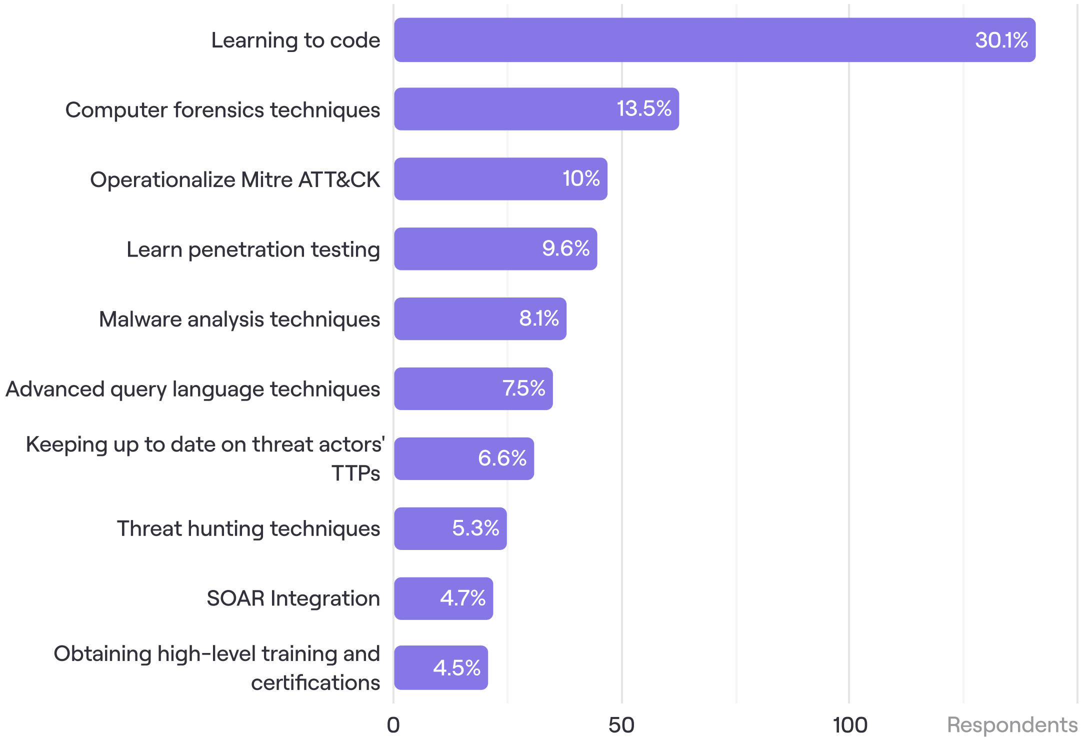
10%

#3: Knowing how to operationalize Mitre ATT&CK

The third most valuable skill will be knowing how to operationalize Mitre ATT&CK , or knowing how to do threat intelligence and modeling in order to be more proactive against attacks.

However, instead of being a coding wizard, there are options for no-code automation, meaning that analysts can spend more time on developing skills directly related to security analysis.

What is the #1 skill you feel will be the most important to succeed as an analyst in the future?



PART TWO

Where time goes

Many security analysts spend time on tedious, mundane tasks that are necessary yet of low-impact for the SOC team. This also keeps analysts from engaging in more high-impact work for their organizations. But what exactly are these tedious tasks, and how much time are they taking from analysts' workloads? This section gives us some insight into where the SOC team's time goes.

Top five tasks consuming the most time

What are the tasks that an analyst spends most of their day working on? (We asked them to select all that applied.)

50.4%

#1: Reporting

The number one most time-consuming task is reporting. Whether it's capturing notes and metrics related to cases, analyzing team performance, or demonstrating value to leadership, reporting matters — but it's not supposed to be the main part of the job.

46.6%

#2: Monitoring

The next most time-consuming task is monitoring for threats and alerts. While a critical part of the role of a security analyst, the concern here is that 71.6% of respondents are Level 2 and 3 analysts, who are spending most of their time doing front-line monitoring.

38.2%

#3: Intrusion detection

The task that analysts spend the most time on next is intrusion detection.

13.5%

#4: Detecting

Followed by general detecting.

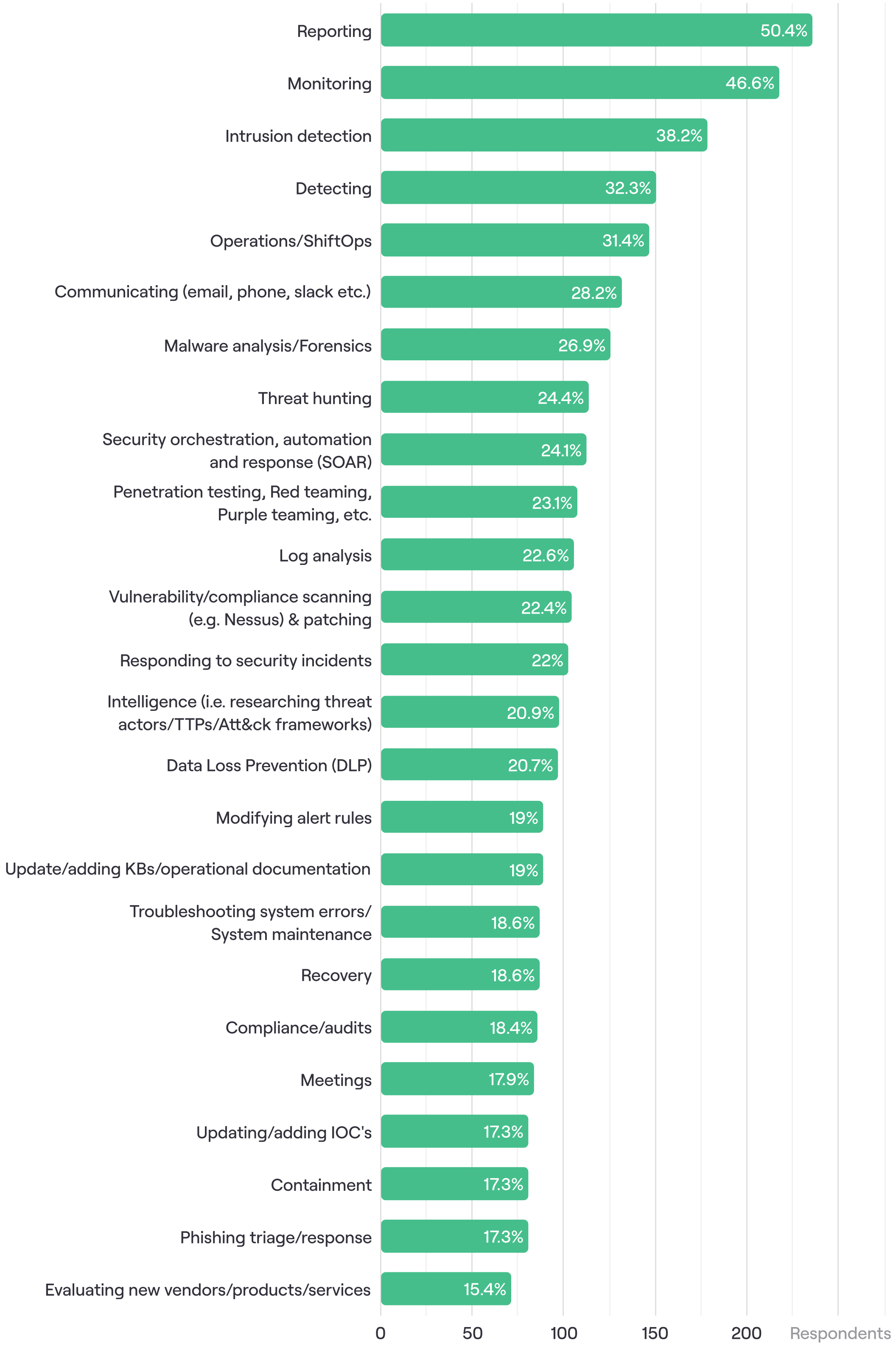
10%

#5: Operations or ShiftOps

Rounding out the top five tasks are operations or ShiftOps tasks.

And to highlight how things are the exact opposite of how they should be, lower on the list are more proactive, higher-value efforts, like updating or adding IOCs, modifying alert rules, updating operational documentation, and intelligence research.

What tasks do you spend the most of your time on?



Top three tasks analysts enjoy the least

Which tasks do analysts least enjoy, that are uninspiring, drain their energy, or are simply a slog to get through?

17.7%

#1: Triage

Number one task on the list was triage. While triaging is a core skill of a security analyst, and while many enjoy it because of its detective work, the far less enjoyable parts include manually deduplicating alerts, repeated similar cases, and too much noise.

16.2%

#2: Reporting

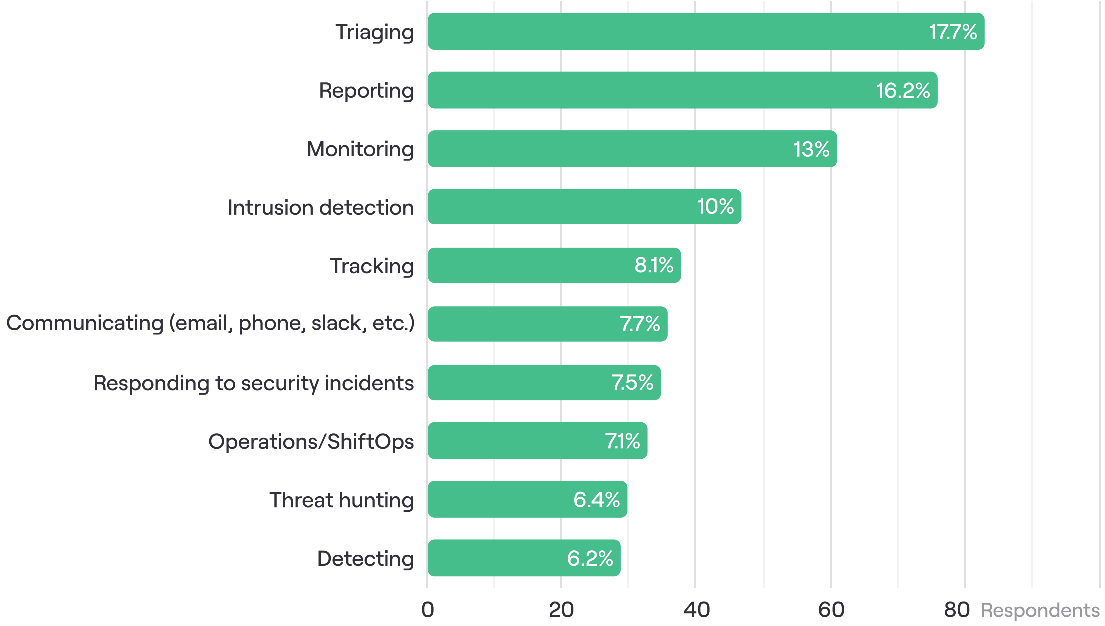
The next task that analysts enjoy the least is reporting, which, as we saw above, is the task they're spending the most time on during the day. Again, reporting matters, but streamlining reporting through automation can help reduce time spent and increase job satisfaction.

13%

#3: Monitoring

Finally, analysts also least enjoy monitoring, which is the second most time-consuming task in an analyst's day. Like reporting, much of this kind of front line manual monitoring can be automated to free up analysts to focus on tasks that have more impact and that they enjoy.

Which of these tasks do you enjoy the least?



Top five key metrics used to measure job performance

How are analysts' job performance being measured? In other words, what metrics should SOC teams be looking to improve first to optimize team performance?

54.1%

#1: Mean time to investigate

For the majority of analysts, the top measure of their job performance is mean time to investigate. So SOC teams should look for ways to reduce time between detection and investigation.

43.8%

#2: Number of alerts

The second metric they're most measured on is number of alerts. SOC teams should focus on ways to reduce false positives and reduce alert fatigue amongst their analysts.

40%

#3: Mean time to respond

The third most-used metric is mean time to respond, and tools such as automation can help reduce time spent investigating, remediating, and eliminating threats or incidents.

37.6%

#4: Time to detect

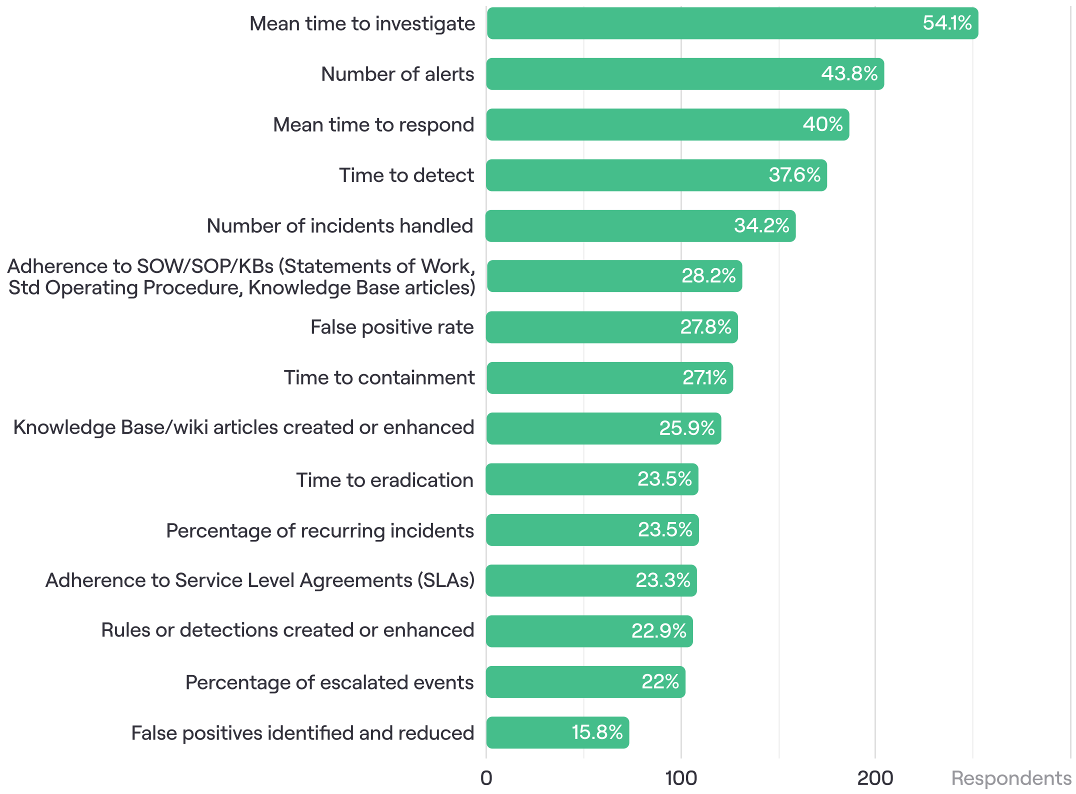
Next, they're measured on time to detect. SOC teams should focus on ways to identify issues faster and ensure that they have tools in place to catch something they may have not even seen before (the dreaded zero-day exploit).

34.2%

#5: Number of incidents handled

Finally, the fifth key metric used to measure performance is number of incidents handled, which teams can decrease by having better, faster, and more thorough alert and resolution tools in place.

What key metrics are used to measure your job performance?



Summary

Where does an analyst's time go? According to our respondents, their time is mostly spent on necessary but tedious manual tasks, like reporting, monitoring, detection, and other operational duties. It's also least spent on tasks that could more proactively position the organization's security, like updating documentation, modifying alert rules, and intelligence and threat research.

Unfortunately, the tasks that analysts enjoy the least about their job are the same tasks they're spending most of their day working on. When someone spends the majority of their day working on tasks they don't enjoy — tasks that, if automated, could free them up for more engaging work — it's no wonder 71% are feeling some level of burnout.

Automation can also help improve the metrics used to measure analyst job performance, like decreasing mean time to detect, investigate, and respond, decreasing the number of alerts received, and more efficiency responding to incidents.

PART THREE

What prevents good work

Everyone wants to do their best work, especially highly-engaged security analysts. But as we saw in the past section, processes that are both tedious and unenjoyable — processes that could be streamlined and automated — are taking up most or all of an analyst's time. What are some other challenges or barriers that SOC teams encounter?

Top five challenges analysts face

In order to understand analysts’ pain points so that team leaders can work towards better solutions, we asked respondents to choose their primary day-to-day challenges.

13.9%

#1: Being understaffed

The majority said their biggest challenge was being understaffed. We’ve seen this appear multiple times now in this report from our respondents: Too much work and not enough people to do it.

10.5%

#2: Time spent on manual tasks

Their second biggest day-to-day challenge is time spent on manual tasks. Which, as we saw above, include tasks like reporting, monitoring, and detection. Having this be a challenge specifically means that manual tasks are eating away at their day at the expense of more impactful activities.

8.6%

#3: Poor visibility into the environment

Another challenge is poor visibility into the environment or a lack of tools that allow them to see threats across networks and devices which could put them on more proactive footing.

8.1%

#4: Poor processes

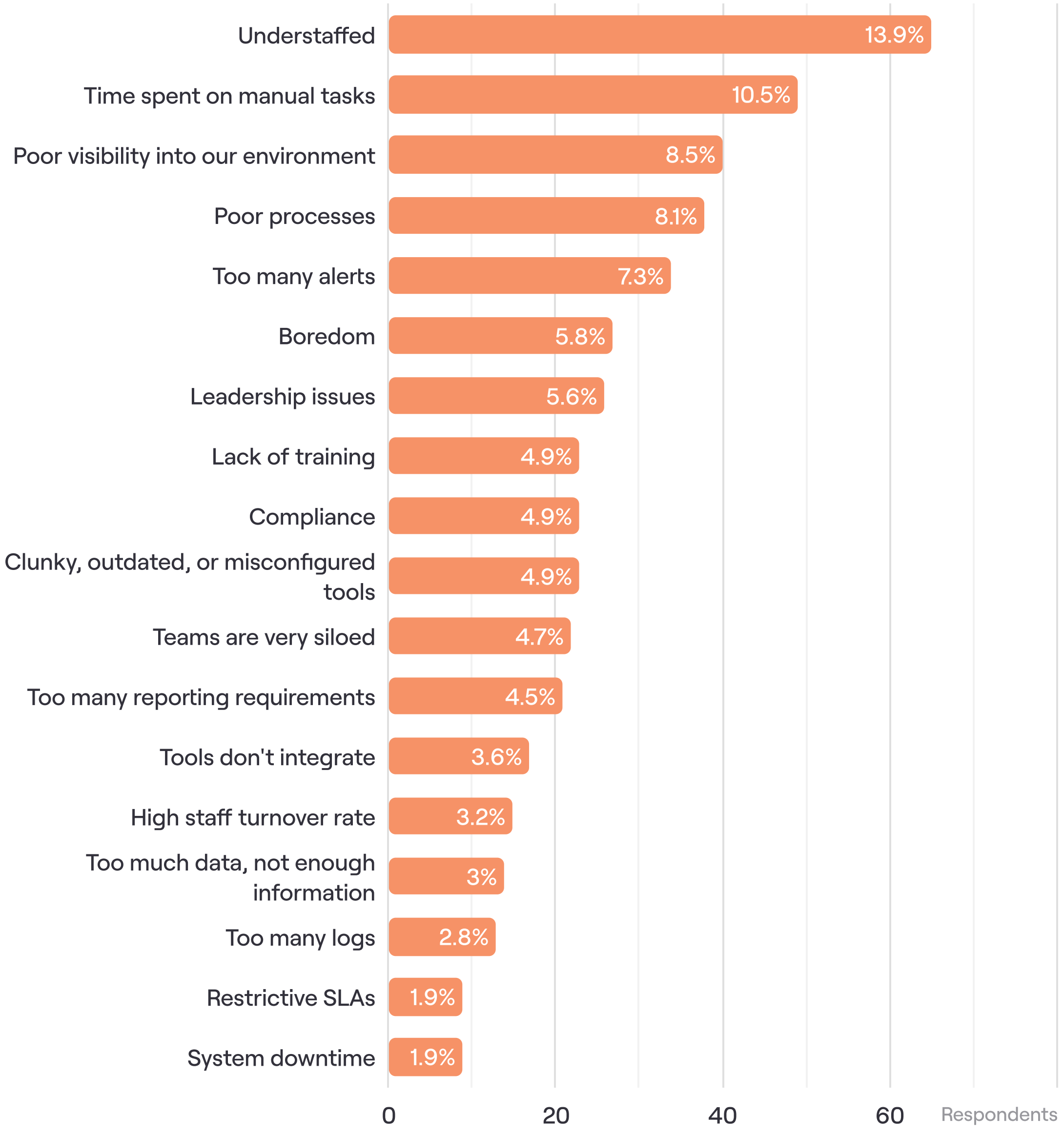
They also stated poor processes, which, as one of their day-to-day challenges, which can cause frustration, lack of engagement, and burnout as well.

7.3%

#5: Too many alerts

Finally, too many alerts is their fifth challenge — too many alerts in general, and too many false positives, which can cause alert fatigue and time taken from true threats and lead to everyone’s worst nightmare: false negatives.

What is your biggest challenge day to day?

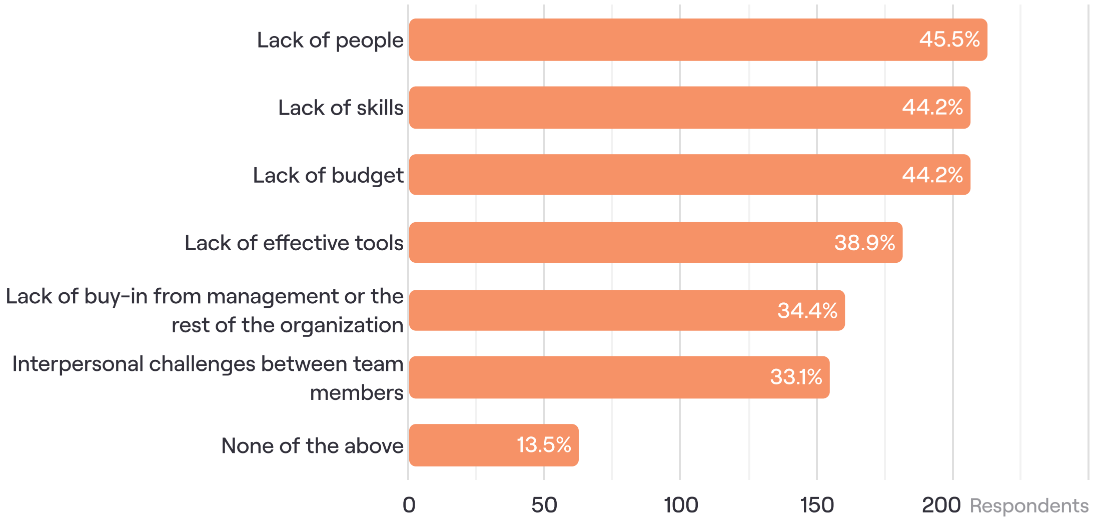


Lack of people, skills, and budget are inhibiting SOC teams

Overall, what prevents the SOC team from doing their best work? Our respondents (selecting all that applied) said a lack of people (45.5%), lack of skills (44.2%), and lack of budget (44.2%) are all factors holding them back from doing their best work.

They also cited a lack of effective tools (38.9%), a lack of buy-in from management (34.4%), and interpersonal challenges between team members (33.1%).

As a team, what prevents you from doing your best work?



Top five things that frustrate analysts the most

We're seeing that frustration from having to do the same actions over and over again leads to questions about why the process is not more streamlined and prevents analysts from doing the best work.

50.6%

#1: Spending time on manual work

For our respondents, the most frustrating aspect of their day is spending time on manual work, like reporting, monitoring, and detection, as we saw above.

36.8%

#2: High false positive rates

The second most frustrating aspect is high false positive rates, which take time to investigate, and can divert energy from true positives.

34.4%

#3: Too many different consoles and tools to investigate incidents

Another frustrating aspect of their job is having too many different consoles and tools to investigate incidents, which could lead to gaps in response or inefficient processes.

33.8%

#4: Inaccurate or incomplete attribution

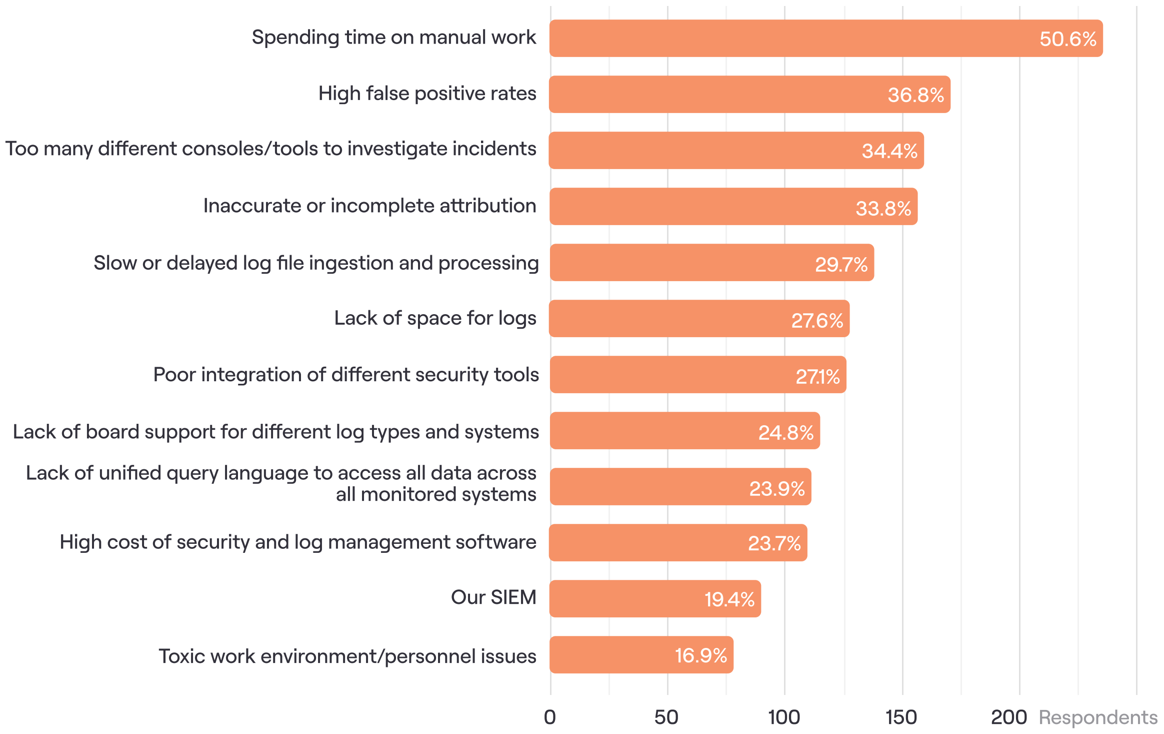
They also stated that inaccurate or incomplete attribution is another frustration they face, forcing them to take time and energy to seek out more context for alerts.

29.7%

#5: Slow or delayed log file ingestion and processing

Finally, they're frustrated with slow or delayed log file ingestion and processing creating lags on real time response.

What are the most frustrating aspects of your work?

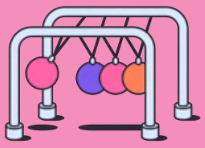


Summary

Security analysts want to do their best work, but they're stymied by a number of factors, including understaffed teams, too much time spent on manual tasks, a lack of tools that allow them full visibility into their environment, poor processes, and simply too many alerts.

It's a matter of needing better tools and better processes — not a work-harder approach checking off more manual tasks, but a work-smarter approach that automates and streamlines tasks, essentially restructuring security analysts' time commitments. This refocuses them on the proactive, higher-value efforts we mentioned before and is what ultimately keeps the organization safe.

As an added bonus, implementing better tools and processes will also address all of the areas of frustration that currently dog analysts and that can contribute to higher retention rates as well.



PART FOUR

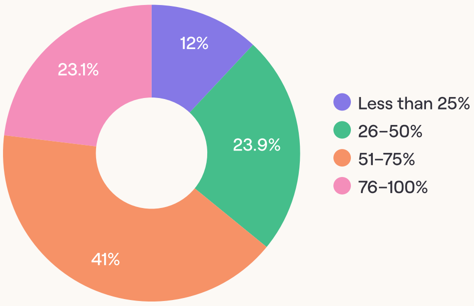
Manual work and automation

Lowering barriers to doing the best work, eliminating repetition, streamlining processes — it's what security leaders are looking to do for their teams. They can do so by building automation into their processes, like automating phishing attack responses, threat intelligence enrichment, or suspicious login alerts. But where do SOC teams fall on their utilization of automation? Are teams embracing it, or still not sure if it's right for them?

64% are spending over half their time on tedious manual work

How much time are analysts spending on tedious manual work? 12% say a quarter of their time is spent on tedious manual work while 23.9% say a quarter to half their time is spent that way. For 41% (the majority), half to three-quarters of their time is spent on tedious manual work, while 23.1% — one in four analysts — say three-quarters to all of their time is spent that way.

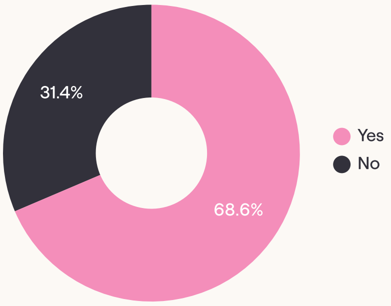
What percentage of your time at work would you describe as tedious manual work?



69% fear automation will eliminate their job

Despite the amount of time spent on tasks that could be automated, 68.6% worry that automation will eliminate their job — their co-workers' or their own — in the near future. However, 31.4% are not worried about automation replacing them.

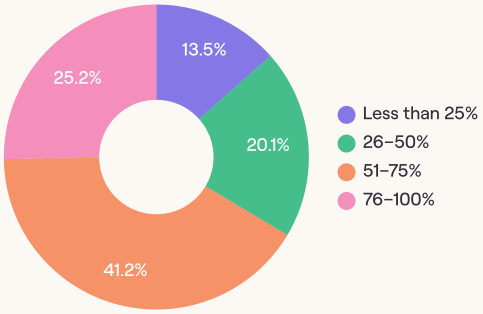
Do you worry that automation will eliminate your job/your co-workers jobs in the near future?



66% believe that half of their tasks to all of their tasks could be automated today

13.5% believe that only less than a quarter of their tasks could be automated, while 20.1% believe a quarter to half of their tasks could. 41.2% (the majority) believe that half to three-quarters of their tasks could be automated, while 25.2% — one in four analysts — believe three-quarters to all of their tasks could be automated.

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



Why analysts should not **fear automation**

Fear of losing your job is a common response to the suggestion of automation. But "automation" doesn't mean "replacement," and automating tasks as a security analyst can not only decrease tedious manual work to free up time for more high-impact projects, automation can become a learned skill to help SOC teams do their best work and increase the value of the analyst. Why shouldn't analysts fear automation?

1

Because we need more people than ever

Security leaders know that the current recruitment market is unprecedented, and that there isn't nearly enough talent in the pipeline. As we've seen in the answers in this report, teams are understaffed, can't find people with the needed skills, and are frustrated with spending their time on manual work. Even with the majority of L1 SOC analyst tasks automated, there's still "more work than ever," as seen from the above responses. Automation can help free up skilled workers for higher-level tasks, letting them play a more valuable role in the organization.

2

Because we can learn from history

Automation brings with it a negative connotation because it often gets conflated with the idea that "robots are taking our jobs," and the threat of not being able to put food on the table provokes an emotional human response. The truth is that automation has never acted to eliminate jobs in the long run. Instead, automation transforms and improves them. In security automation specifically, once analysts are given the superpower of automation, they start by replacing the mundane tasks they once had to do manually. Soon, however, they go on to build entirely new processes in a creative manner.

3

Because automation is a tool for you to use

Automation, and specifically no-code automation, will become a core competency of security analysts. It's nothing to fear, as automation can make the job more creative, giving analysts not just the ability to build, maintain, and evolve ingenious automated workflows, but also the ability to contribute more value to their organization, as well. Automated workflows aren't just a one-and-done build, either; analysts will need to modify, improve, and update those workflows on an ongoing basis.

Top five tasks analysts would automate to save time

If analysts could automate one task that would save them the most time, which task would it be?

24.8%

#1: Risk assessments

The majority said the number one task they would automate is risk assessments. As we've seen throughout this report, analysts are spending so much of their time and energy manually monitoring for and triaging risk, that if they could completely automate it, they would.

19.2%

#2: Intelligence analysis

Next, they would automate intelligence analysis so that alerts could arrive with richer, more actionable context, saving time on having to track down that information manually.

12%

#3: Threat hunting

The task they'd most like to automate next is threat hunting, allowing for the elimination of manual efforts to search out hacker threats or IOCs.

8.5%

#4: Email phishing response

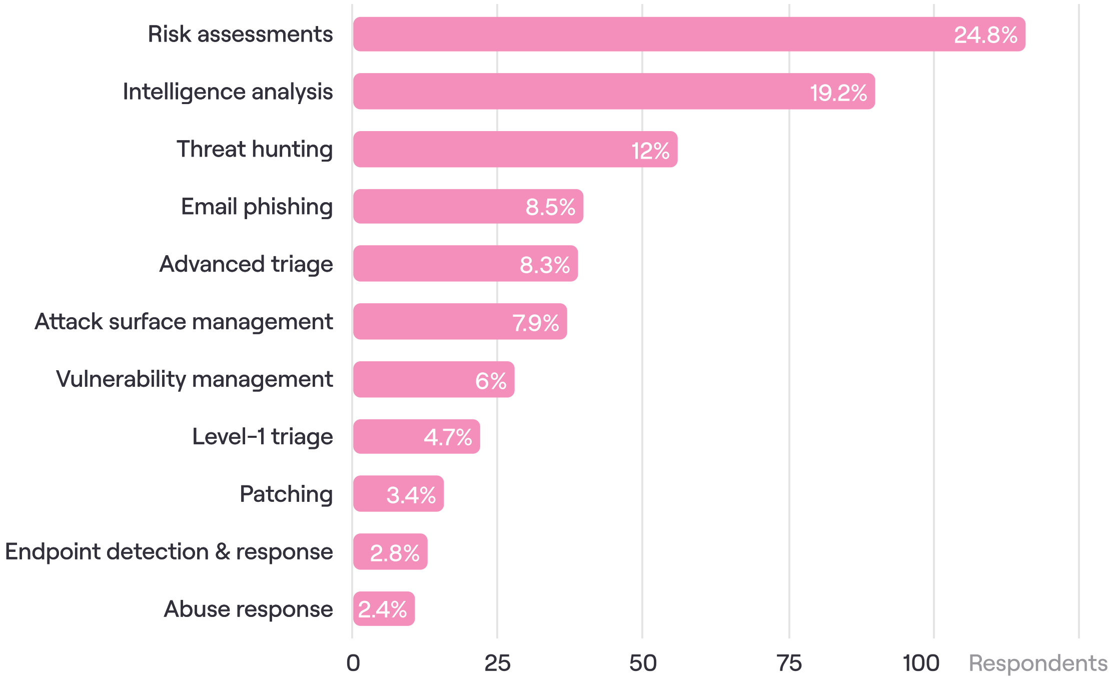
They'd also like to automate email phishing response, which can eliminate the manual task of threat evaluation, communication follow-up, and remediation.

8.3%

#5: Advanced triage

Finally, to save them time, they'd automate advanced triage, which is especially important considering that the majority of our respondents are Level 2 or 3 analysts.

What one task, if completely automated, would save you the most manual time?



What would analysts do if their work was automated?

If their tedious, low-impact tasks were automated today, what would security analysts be working on instead?

48.1%

#1: Updating operational documentation

The majority said that in the absence of manual work, they would focus on updating operational documentation. Having updated documentation is of course critical for the SOC team, but this indicates something else: That SOC teams are too busy to keep their documentation up-to-date, and have fallen behind. The first focus after automation would actually be catching up.

44.7%

#2: Developing advanced detection rules

The second highest ranked is developing advanced detection rules, which is a proactive way to improve their organization's security posture, as well as a way to improve the performance metrics listed above.

41.0%

#3: Integrating more systems and logs

If freed up, they would also focus on integrating more systems and logs, which is another proactive action that can help improve the previously mentioned poor processes that are causing frustration.

39.5%

#4: Research TTPs and focus more on intelligence

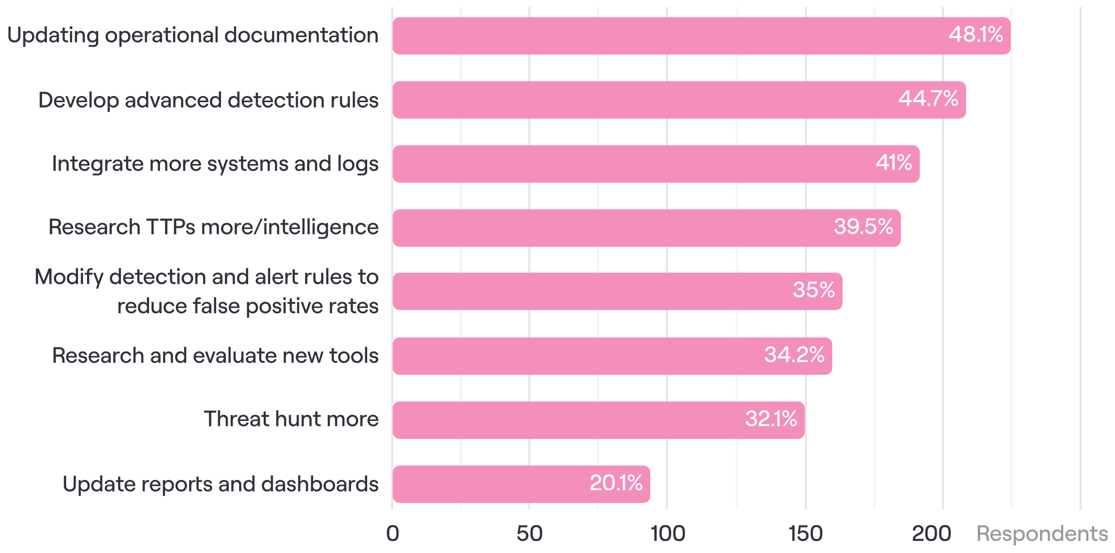
Automating manual tasks would also allow them time and energy to research TTPs and focus more on intelligence, increasing their offense on understanding and protecting against malicious actors.

35%

#5: Reduce false positive rates

Finally, automation would allow them to modify detection and alert rules to reduce false positive rates, reducing alert fatigue and burnout, and allowing them to focus on alerts that really matter.

If you no longer had to do tedious manual work, what would you prefer to be doing?



Summary

So far, we've learned more about areas where analysts are mired in time-consuming tasks, spending too much manual effort on reporting and detection, frustrated with the amount of alerts that come through or lack of context around those alerts, and worried about too much work and not enough hands on their team. Yet in this section, we get to see a security analyst's ideal day, if the tasks they're hindered with are moved off their schedule (and 66% believe that half to all of their tasks could be automated today).

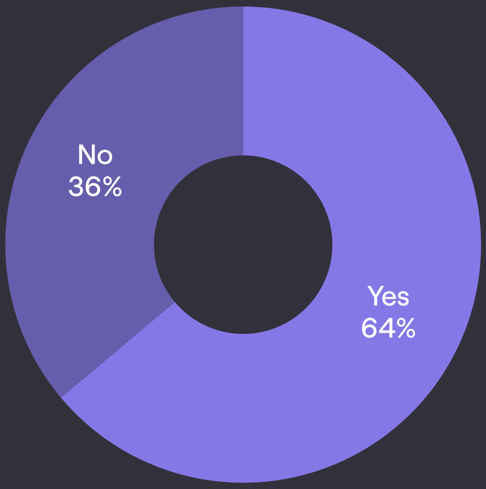
An analyst's ideal workday would include spending time improving processes and procedures, such as updating operational documentation and integrating more systems. It would also include proactive approaches to keeping their organization safe, like developing advanced detection and alert rules and becoming more knowledgeable about threat actor tactics, techniques, and procedures (TTPs). They would also build and maintain automated workflows in creative and intricate ways, as more sophisticated automation frees up the time to spend on the previously mentioned high-impact tasks.

Automate the present tasks, and security analysts can begin planning for the future.

PART FIVE

Improving retention

In considering the question of burnout from the previous section, the frustrations found in day-to-day manual operations, and the awareness that the pandemic has challenged many to rethink their career trajectory, we wanted to know if analysts were thinking of making job moves — and what their organizations could do to retain them.



64% are likely to switch jobs in the next year

Considering their frustrations with understaffed teams, spending time on manual work, and poor processes, it's no wonder that 63.9% of analysts say they're likely to switch jobs in the next year. 36.1% say they'll stay put.

Top three ways to improve retention

We asked our respondents about actions their organizations could take to improve their work, engagement, and likelihood of staying.

1

Provide tools that automate tedious manual tasks

The number one action analysts say organizations could take to improve retention is to provide tools that automate tedious manual tasks. By providing automation, especially no-code automation, analysts will be able to decrease their focus on manual tasks and increase their focus on more proactive tasks, reducing burnout and increasing engagement.

2

Provide more modern tools with advanced capabilities

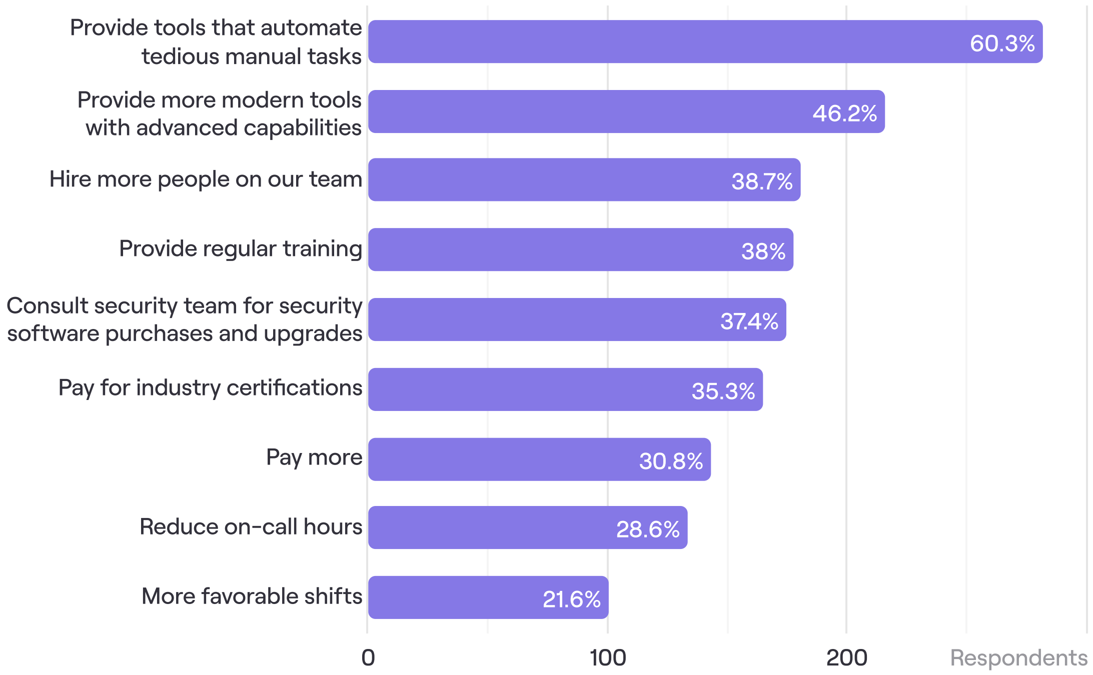
The second most favored action is for organizations to provide more modern tools with advanced capabilities. As we saw above, a frustration is having too many tools and consoles. By providing more best of breed tools with advanced capabilities like automation and better visibility, organizations are empowering their analysts to do their best work, unencumbered.

3

Hire more people

Finally, analysts would consider staying if their organization simply hired more people to the team. As we've seen above, understaffing is a challenge, and fewer people means higher workloads. Simply hiring more people would signal a commitment to the SOC and a recognition of its value, too, inherently increasing retention.

What could your current organization do to retain you?



Actionable takeaways for security team leaders

As we've seen in this report, SOC teams are passionate yet challenged. They're satisfied and engaged with their work, yet endless manual tasks, understaffed teams, inefficient processes, and too many alerts are stifling their ability to do more high-quality, creative work. They're stuck doing repetitive tasks today, unable to proactively work on preparing their organization's security posture for tomorrow.

What can SOC leaders do to improve their teams in 2022? Here are four ways forward.

1

Improving time spent on reporting

Since reporting is the task taking up most of an analyst's time, start there. Reporting is absolutely necessary in order to document case notes and inventory team performance, but it's responsive — collecting what happened after the fact — rather than proactive. Alongside the fact that teams feel understaffed (the greatest challenge experienced) and slowed down by a lack of people (the number one thing preventing teams from doing good work), streamlining the reporting processes through automation will allow your analysts to do their real job: analysis.

2

Make triage enjoyable

Triaging is the top task analysts enjoy the least, which is no surprise if they're being bogged down by deduplicating repeated alerts ("too many alerts" being in the top five challenges analysts face), dealing with similar cases again and again, and facing too much sheer noise overall. By having automated workflows address the bulk of low-value and duplicate alerts, triage can become enjoyable again: fun, high-quality, and high-impact detective work. Remember, too, that advanced triage was one of the tasks analysts would automate if given the chance.

3

Increase retention by measuring and minimizing burnout

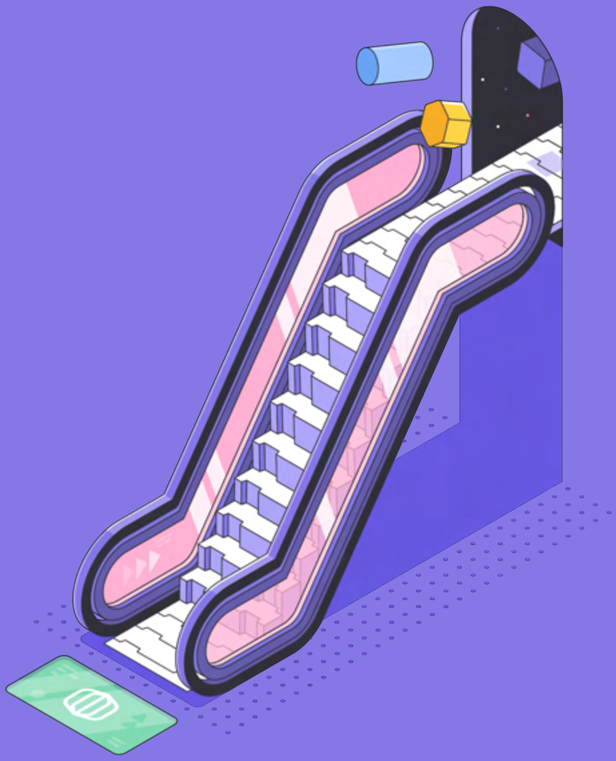
Security team leaders want to see their team happy, passionate, and doing their best work — and don't like to hear that their teams are burned out and looking to leave the jobs they're currently in. In addition to the metrics mentioned above to measure performance, security leaders need to count burnout as a key metric, too. What could increase their engagement and keep them around? Having the ability to automate tedious manual tasks, providing them with more flexible, best-in-breed tools with advanced capabilities, and hiring more people to mitigate the workload.

4

It's time for no-code automation

Automation has been hyped and sold in security for decades, yet teams continue to suffer under the pull of manual work. As we saw above, the most frustrating aspect of being a SOC analyst is "spending time on manual work," with one in four analysts spending over 75% of their time on "tedious manual work." This is the reason why "learning to code" is cited as the skill analysts will most need to be successful, as they believe that learning development skills may help to overcome the never-ending toil.

Fortunately, there's a better, faster, and easier solution: no-code automation, which removes the barrier of coding so that analysts can start building automated workflows today, without waiting on a development team. SOC teams that adopt this flexible, powerful form of workflow automation can reap the benefits of automation immediately, giving security analysts the ability and freedom to do their best work.



tines

No-code automation for security teams

The world's best companies – from startups to the Fortune 10 – trust Tines with their mission-critical security workflows.

tines.com/signup