Your Security Analysts are leaving? Here's Why!

Thomas Kinsella @thomasksec
Co-Founder, Tines
How are security analysts doing in 2022?

We started our company because we care deeply about security teams and the people on them.

We often felt tools weren’t good enough, and it made work hard for folks on the team – especially analysts.

But it’s been a few years since we led teams! We wanted fresh, objective data on the lives of real analysts today.
Let’s talk to as many analysts as possible

2022 – Voice of the SOC Analyst

We surveyed ~500 security analysts in the last few months.

The plan was to uncover insights that we could use to perfect our own product, and to produce an original – but unbiased – research report.
Your Security Analysts are Leaving – Here’s Why

Who did we speak to?
Analysts based in the US. A good distribution of folks from different sized companies and in different industry verticals, but with a core focus on technology.

468 full-time security analysts

- Gender: Male 56%, Female 44%
- Age: 18–24 12%, 25–34 20%, 35–44 58%, 45–54 6%, >54 4%
- Country: United States 100%
- Employment Status: Employed for wages 100%
- Number of employees in company: 501–9k 53%, 9k–50k 30%, >50k 17%

What best describes the industry you work in?

- Technology 45.1%
- Manufacturing 4.9%
- Healthcare 6.1%
- Finance 5.1%
- Education 7.3%
- Utilities/Energy 8.5%
- Insurance 10%
- Services 10%
- Other 10%
- State/Local Gov 10%
- Retail 10%
Today, let's focus on two things

1. Three choice cuts of the data
2. Actionable takeaways for security leaders

If you want to go even deeper, check out the entire report at tines.com/soc
Your Security Analysts are Leaving – Here’s Why

Analysts LOVE their jobs...

The vast majority are very satisfied with their jobs, very engaged with their work, and feel respected by their peers.
Your Security Analysts are Leaving – Here’s Why

…but they’re burning out

- About half feel “very burned out”
- Most report more work than ever
- Almost all feel like the team is understaffed

1. Do you feel burned out at work?
   - 47.6% I feel very burned out at work
   - 28.6% I feel somewhat burned out at work
   - 23.7% I don’t feel burned out at work

2. How is your workload, currently?
   - 60% More work than ever
   - 25.9% About the same amount of work
   - 14.1% Less work than ever

3. In your opinion, is the team understaffed?
   - 81.6% Yes
   - 18.4% No
What percentage of security analysts plan to change jobs in the next 12 months?
Almost **two thirds** of analysts expect to leave their job in the next 12 months.

Average rate for all jobs ≈ 25% (Prudential, 2022)
Your Security Analysts are Leaving – Here’s Why

Being an analyst is a daily challenge...

Before we think about solutions, let’s try and understand the pain points that analysts feel.

Q: “What is your biggest challenge day-to-day?”

1. **Being understaffed** (13.9%)
   - The majority said their biggest challenge was being understaffed. We’ve seen this appear multiple times in this report from our respondents: Too much work and not enough people to do it.

2. **Time spent on manual tasks** (10.5%)
   - 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.

3. **Poor visibility into the environment** (8.6%)
   - 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.

4. **Poor processes** (8.1%)
   - 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.

5. **Too many alerts** (7.3%)
   - Finally, too many alerts is their fifth challenge. Too many false positives causing alert fatigue and spending too much time investigating them. This is time taken from more impactful, risk reduction efforts.
Your Security Analysts are Leaving – Here’s Why

...and it can be frustrating

Q: “What are the most frustrating aspects of your work?” (multiple choice)

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.

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.

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.

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.

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.
Too few people
Too much repetitive manual work
Too many false positives
Zoom in on manual work...

It’s clear that repetitive, manual work is the biggest challenge/frustration. But just how much time are analysts spending on this tedious work?
Your Security Analysts are Leaving – Here’s Why

...and what about automation?

Analysts view of automation is mixed
They believe it could be a solution – but perhaps too much of one?

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

- Less than 25%: 25.2%
- 26–50%: 13.5%
- 51–75%: 20.1%
- 76–100%: 41.2%

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

- Yes: 31.4%
- No: 68.6%
In the next 12 months will your security team?

A) Shrink
B) Stay the same size
C) Grow by less than 10%
D) Grow by more than 10%
Instead of manual work

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

- Risk assessments: 24.8%
- Intelligence analysis: 19.2%
- Threat hunting: 12%
- Email phishing: 8.5%
- Advanced triage: 8.3%
- Attack surface management: 7.9%
- Vulnerability management: 6%
- Level-1 triage: 4.7%
- Patching: 3.4%
- Endpoint detection & response: 2.8%
- Abuse response: 2.4%
Instead of manual work

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

- Updating operational documentation: 48.1%
- Develop advanced detection rules: 44.7%
- Integrate more systems and logs: 41%
- Research TTPs more/intelligence: 39.5%
- Modify detection and alert rules to reduce false positive rates: 35%
- Research and evaluate new tools: 34.2%
- Threat hunt more: 32.1%
- Update reports and dashboards: 20.1%
What’s going to be the most valuable skill a security analyst can have to help them succeed in the future?

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.

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.

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.
These results should be humbling for security leaders

1. Most analysts are burned out
   So much so that 64% will leave their job this year.

2. Too much manual work
   Security teams are overwhelmed by manual work and lack of staff.

3. Automation’s a solution
   But security teams feel threatened by it.
What can we do about it?
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 three ways forward.
Make triage fun

- Bad triage = repetitive, duplicate alerts, following the same script over and over, noise, easy & mundane
- Great triage = being a detective, creative, high-impact, fun, hard & worthwhile
- You need to design your team, and its tools and processes, around minimizing the bad, and maximizing the great.
Make triage fun

- Bad triage = repetitive, duplicate alerts, following the same script over and over, noise, easy & mundane
- Great triage = being a detective, creative, high-impact, fun, hard & worthwhile
- You need to design your team, and its tools and processes, around minimizing the bad, and maximizing the great.

James @James_inthe_box · Jan 31
Incoming #hancitor #malspam DocuSign subjects, forcedabortions[.]org sender.

cc @wavellan @noottrak @jw_sec @malware_traffic @executemailware @wwp96 @felixw3000 @HerbieZimmerman @ffforward @node5 @JAMESWT_MHT @JRoozen @pr0xylife

Halligan @halligast · Jan 31
Seeing a bunch of docusign subjects from this domain.

James @James_inthe_box
Replying to @halligast @wavellan and 12 others
Aye this is today's #hancitor #malware run for today.

9:39 PM · Jan 31, 2022 · TweetDeck
To increase retention, measure burnout

- You already measure MTTR, MTTI, etc – burnout is as important a measure of team performance as any of these.
- Additionally, it’s a leading indicator – of team churn.
- The first problem to solve is how to measure. Consider recurring employee surveys, management 1/1 rituals, etc.
- Establish a baseline, then improve it
Automation for security teams is imperative

- Despite decades of automation hype, teams are still suffering with manual work.
  - #1 most frustrating aspect of being an analyst = “manual work”
  - 1 in 4 analysts spend >75% of their time on “tedious manual work”
- Analysts believe they need to become engineers to be productive
  - #1 skill analysts identify for future success = “learning to code”
  - And engineers are perceived to displace analysts by building automation
- There is another answer! One that elevates the analyst.
IN CONCLUSION

Analysts are burning out, leading to retention issues.

There are solutions! Treat burnout as a KPI, invest in no-code automation.

Read the entire interactive report at tines.com/soc