expel

UNPLUG YOUR TEAM:

Combating cybersecurity burnout

Contents

Introduction

What's worse: The talent shortage or bad word of mouth?

There's no denying the talent shortage in cybersecurity. ISC2, the global association for cybersecurity professionals, tracked the shortfall at four **million people** in its 2023 workforce study. But if you've been blaming the talent shortage for low recruitment, high turnover, and middling productivity, it's time to take a closer look at another culprit: burnout.

Analysts working in security operations centers (SOCs) are suffering from high-stress work at all hours and on weekends, with often-inadequate support from cybersecurity management. Layoffs and restructurings, more commonplace in cybersecurity in the past couple of years, also ratchet up stress levels. And all this stress can cause cybersecurity professionals to bow out of their jobs early. The average tenure for a CISO is just 18 to 26 months—well under the average tenure of 4.9 years for executive leaders, according to the **CISO Workforce and Headcount 2023 Report.**

In the recent **State of Mental Health in Cybersecurity** report from Tines, two-thirds of cybersecurity professionals reported experiencing stress at work, and said that their work impacts their mental health. Only 47% ranked their mental health as "excellent" or "very good," and 27% said their mental health has declined over the past year—a massive red flag for security leaders concerned about caring for their team. It's safe to say that the past few years have not been good for burnout in cybersecurity.

And cybersecurity analysts no longer suffer in silence about the crash-and-burn pace of their jobs. They're telling their peers about companies that crush their SOCs with hours that go way beyond a reasonable workday and come with little or no support for analysts' mental health.

Bad news travels fast. Despite the shortage, there *is* talent out there. But the talent might not jump at your job openings if industry word of mouth says, "They'll chew you up and spit you out." Fighting the bad buzz will help you improve your image and retain good employees longer, but it means taking real and serious steps to beat burnout.

"100% of respondents surveyed **agreed that managed detection and response (MDR) services can help alleviate stress and burnout** of cybersecurity professionals."

Source: UserEvidence verified: 07/12/2024, Survey of 97 Expel users, conducted by UserEvidence.

Welcome to the burnout club

On Slack, in social communities like Reddit, and in online forums, cybersecurity professionals are airing their grievances about the lack of work-life balance in the industry.

"If you are in cybersecurity and are constantly feeling angry, exhausted, bitter and you jump up to the ceiling when your company mobile rings—welcome to the burnout club," reads a popular Medium post by Bozidar Spirovski, CISO at financial services platform Blue dot.

Crummy corporate cultures and unreasonable expectations are partly to blame for the high rate of burnout in cybersecurity. "I'm constantly reading contracts towards customers that literally demand my phone number and my ongoing availability 24x7 to every single random customer," Spirovski says. "That type of unreasonable expectation of magic being done still exists."

What causes SOC burnout?

CISOs are by no means immune to burnout. Even if they're not in the SOC trenches all day, the managerial role is demanding, and finding time to take a real break can feel almost impossible when you're always on the clock—including during holidays and special family events.

In one study of CISOs, respondents said that stress related to their roles (60%) and burnout (53%) were the **largest personal risks** they face. And 42% of CISOs say they have **missed out** on celebrating big holidays because of pressing security work.

However tough it is for CISOs, it's safe to assume that security analysts have it just as hard—if not harder when they're working in the crucible that is the SOC. Here's what typically contributes to their burnout:

The constant threat landscape. Your adversaries never take a day off. New vulnerabilities and attacks can occur at any time, and your analysts must be ready to jump in and respond immediately.

Threats that impact lives and safety. Bad actors are increasingly targeting critical systems like those in hospitals, involving security analysts in life-or-death scenarios and causing significant stress. When a security incident occurs, your team's expertise is crucial for managing and mitigating the impact, coordinating response efforts, and keeping everyone informed. It's a heavy responsibility, compounded by the need to deliver bad news regularly.

Repetitive, monotonous work. Responding to and investigating alerts is valuable work, but it's also a grind. "Overly complex, repetitive procedures can lead to security fatigue—a sense that security is an obstacle to be navigated around in order to get work done rather than an essential part of work itself," ***reported InformationWeek***. "Analysts may either attempt to shut down or circumvent alerts—known as discrepancy enhancing. Or they may attempt to keep on top of them despite their inability to do so—known as discrepancy reducing. Both are highly stressful."

> "An MDR that you trust and is communicative/ collaborates on a regular basis is a must! **It allows you to have peace of mind without checking your computer or phone on every alert** (such as vacations or off-hours)."
>
> **– Consumer Discretionary Company**

Source: UserEvidence verified: 07/10/2024, Survey of 97 Expel users, conducted by UserEvidence.

Resource constraints. Tight budgets make it hard to delegate responsibilities and your team's specialized knowledge and experience are hard to replace, even temporarily, so time off can feel like leaving a critical role unfilled. Downsizing can stretch cybersecurity professionals' workdays even further. In the **ISC2 2023 cybersecurity workforce study**, 71% of respondents said cutbacks in cybersecurity resulted in an increased workload. Too much work saps workers' confidence, with respondents citing an overload, overwork, and inadequate resources to protect their organizations.

Why burnout is bad for the industry

Job burnout is bad for people, certainly, but it's also hurting cybersecurity as a whole. In its recent report on fighting cybersecurity burnout, Forrester found that burnout is damaging the quality of cybersecurity work. "We spoke to folks who came to the realization that they haven't seen their kids for eight years, those who could no longer get up in the morning, and others whose bodies gave way to the physical symptoms of burnout," Forrester reported. "But, as well, burnout is causing critical talent to exit the industry and preventing others from entering—this ultimately impacts our ability to manage cybersecurity for organizations."

The pain is real

"I had a job where I was miserable and it was definitely the work environment and not depression. I would have physically made myself sick if I'd kept working there."

"Zero positive feedback or motivation, constantly using fear to try and 'motivate' people, and punishment for the smallest mistake. I felt an unnecessary pressure on myself to never make a mistake."

"Sometimes all it takes is getting out of a toxic environment and into a nurturing one to change everything."

—From r/cybersecurity, Reddit

There are no easy fixes for burnout, and change doesn't happen overnight. But just like security professionals spread the word about bad workplace cultures, they are also quick to notice when their employers do right by them.

Do enterprises care about the well-being of their security teams?

Organizations that offer mental health and wellness programs—and encourage employees to use those services—prove that they have a stake in workforce well-being. However, as the Tines survey noted, only a little more than half (57%) of respondents said their workplace provides mental health support and resources for staff, while 43% said their workplace does not.

A significant gap to tackle

Perceptions about support for mental health and well-being also matter. Only about half (54%) of Tines survey cybersecurity respondents said their workplaces care about and prioritize mental health in their operations, while 45% said their workplace doesn't prioritize mental health.

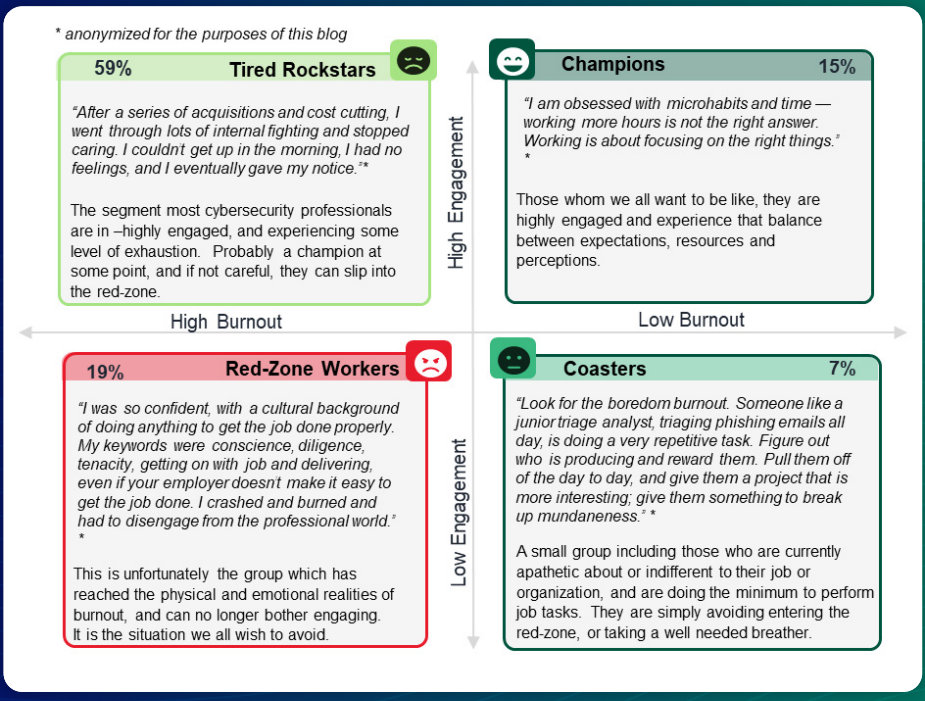
There's concern that burned-out teams are more likely to make errors that could result in more security incidents. "Happy workers are more motivated, more focused, and are less likely to make mistakes," reports ISC2.

To make matters worse, managers with burnout might not take evolving risks and threats seriously, which could also increase the likelihood of an attack.

"The cost [of burnout] is not just a human one," *says InformationWeek*. **"Organizations themselves are suffering because burnout ultimately results in lax security procedures and an increased likelihood of breaches.** Just as burnout may lead to fatal complications in medicine or friendly-fire incidents during sensitive military operations, it may lead to breaches in cybersecurity."

Close to the edge

In its recent report on controlling burnout in cybersecurity, Forrester mapped the relationship between engagement and burnout within its four "burnout segments." Forrester's most concerning finding was that the 59% of cybersecurity professionals who are "Tired Rockstars" are in danger of slipping into the "Red Zone." What's the Red Zone? It's where the best security professionals become so disengaged from their jobs that they leave—and perhaps quit the industry entirely.



Source: The Cybersecurity Firefighter's Guide To Controlling Burnout, Forrester Research, Inc., April 18, 2024

How to battle burnout

Get generous with PTO—really. Maybe your organization gives employees generous PTO and sets minimum holiday requirements, but doesn't offer the encouragement to take the time off. The SOC needs to be staffed and equipped in a way that actually allows analysts time off to help prevent burnout. So tell your team, "Go ahead—take your vacation."

Create career paths. Analysts should have a viable professional development path beyond the SOC, and managers should nurture that path. What's the growth trajectory for employees who are ready to leave the SOC? Is there training and conference-attendance support for the analysts who want to deepen their knowledge or shift into a different security role? A structure for career development helps an organization retain talented people.

Encourage creativity off-site. Cybersecurity conferences and hackathons push analysts to exercise their creative sides. It's refreshing and invigorating for analysts to learn something new, socialize with their peers, and put their skills to work for a tabletop exercise. Managers can also encourage analysts to take part in hacker summer camps—or any offsite that promises a head-clearing change from the daily grind of threat analysis.

Spruce up the SOC workspace. Cybersecurity team members like decent workspaces, too. In a field with a high likelihood of burnout, don't relegate the team to a dreary corner of the basement. Think about what SOC analysts need to get through the long, tough shifts: good lighting, ergonomic workspaces, easy-to-access break rooms, and even a way to go outdoors.

David Johnson, principal solutions architect at Expel, recalls the awfulness of one of his previous SOC workspaces from back in the day.

> "My SOC had no windows, which was the first thing for me because I like sunlight," he says with a shudder. "It smelled like peanuts all the time because we shared a wall with a peanut factory. It got too hot and it was way too dark. **The chairs were slowly crippling us and the desks were the wrong height, to the point where a workplace agency came in and forced them to correct all of it after somebody made a complaint."**

Take a look at your SOC—is it anything like the hellscape of David's memories? If so, it may be time to give your security analysts some light, fresh air, and better chairs.

Stop asking analysts to code. When they lack resources, analysts who see the need for better solutions may create their own software. That's nice, but it's also time-consuming, and the resulting tools may not be the highest quality. Allowing analysts to call on developers for help and advice paves the way for sophisticated software fixes that can benefit security more widely.

Stop trying to be perfect

"It's not *if* there will be an attack, but *when*," goes the common cybersecurity wisdom. Preventing breaches 100% of the time is impossible given the complexity of corporate networks, the disappearance of the network perimeter, and the ever-increasing sophistication of attackers. But that doesn't stop the goal of perfection from being a huge stressor for SOC teams.

"Switch your mindset," writes CISO Bozidar Spirovski in his much-shared Medium post. "The cybersecurity team doesn't guarantee nobody can attack you. A well supported cybersecurity team can guarantee resilience—high cost of attack, limited impact, good recovery, and proper understanding of an attack. In essence, having a good security team helps you be harder to bring down, and when you are down quicker to pick yourself up, dust yourself off, and continue doing business."

Automation can stop the churn and burn cycle

Automation has the power to reduce a major cause of cybersecurity burnout: the repetitive tasks that cause the most pain in the SOC. But automation can also make burnout worse when it's not applied intelligently, or if you forget to choose technology that complements human skills. **Here are some automation dos and don'ts:**

Do respect the mantra, "Technology first, but people foremost." That thought comes from David Johnson, principal solutions architect at Expel, who knows his way around the SOC. State-of-the-art technology is key, but it needs people to manage it effectively and shed light on the insights generated by automated alert tools. Choosing automation demands some trial and error to ensure you're not piling even more work onto the SOC.

> "Seek resources to help cover gaps within your teams. Look at historical events/incidents and take that evidence to your decision makers. **MDR is not cheap, but the ROI I've seen makes every penny worth it."**
>
> **- Nicholas Schopperth, CISO, Dayton Children's Hospital**

Source: UserEvidence verified: 07/10/2024, Survey of 97 Expel users, conducted by UserEvidence.

Don't view automation as a replacement for analysts. The answer to the talent shortage isn't to replace the cybersecurity team wholesale with technology. If an organization is already grappling with security team burnout, kicking people out will demoralize and deskill analysts even faster. Also, the quality of alert response will suffer.

Do choose automation and AI tools that complement analyst knowledge. Analysts can use automated solutions to present their findings from threat intelligence sources, as well as for testing and training. Automation also gives analysts more time to research threats for clients, since the tools reduce the time needed for repetitive tasks.

Conclusion

“Go ahead. Take PTO.”

This message—or something like it—should be part of daily conversations with security teams. While managers can’t eliminate every stressor in the security department, it’s critical to support their teams with policies and technology, and time away from the dashboards.

There’s an investment of time and energy when you’re working to mitigate team burnout. But it’s an investment with a healthy payoff once you see that team members can handle stressful hours-long investigations without the bad effects. Stress is part of cybersecurity, but burnout doesn’t have to be.

expel

About Expel

Expel is the leading managed detection and response (MDR) provider trusted by some of the world's most recognizable brands to expel their adversaries, minimize risk, and build security resilience. Expel's 24/7/365 coverage spans the widest breadth of attack surfaces, including cloud, with 100% transparency. We combine world-class security practitioners and our AI-driven platform, Expel Workbench™, to ingest billions of events monthly and still achieve a 23-minute critical alert MTTR. Expel augments existing programs to help customers maximize their security investments and focus on building trust—with their customers, partners, and employees. For more information, visit our **website**, check out our **blog**, or follow us on **LinkedIn**.

08/06/24