Google Cloud

The Art of Recognizing and Surviving SOC Burnout

A Complete Manual for Security Operations Professionals

The industry's deepest dive yet into the occupational hazards emanating from the SOC and what analysts, engineers and managers can do about them

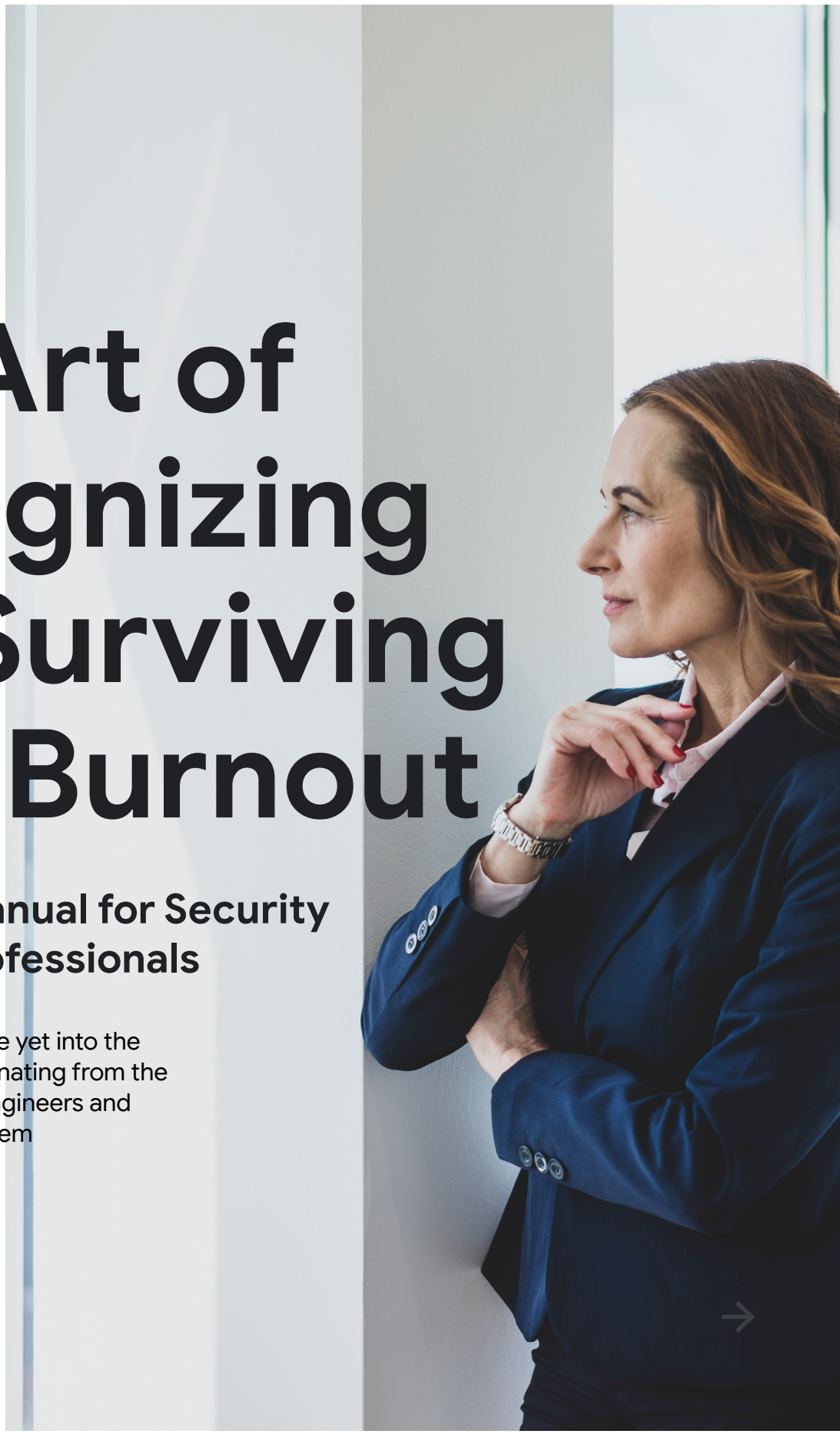


Table of Contents

Introduction

One Monday morning in the fall of 2017, in the pre-dawn hours of another alcohol-fueled business trip night out, Thom Langford hit rock bottom. The CISO had been passively spiraling for a while, but finding himself on the roof of a building in Rome, distraught and suicidal, he had reached his mental max. Langford was eventually talked down and spent the next month away from work and in the care of family and mental health professionals.

As he tells it now, alive and well, the build-up of his breakdown was barely noticeable to those around him. Catalyzed by the pressure of growing a security team at a global company that was "as politically charged as it was not interested in security," he essayed that the seeds had been long planted for his eventual "drowning."

"The cost … was an intense environment where my main role was PowerPoint and politics, and constant air support for the team," he wrote in a candid and heartfelt post. "Combine a tough travel schedule and the global, always-on element, I never truly switched off. That said, one of my mottos was 'Work Hard, Play Hard' so evenings with teams, internal clients and their customers in different countries were long, hilarious and helped us bond even closer to perform even better. Frankly it was exhausting and my sleep suffered. So I did what every self-respecting professional does, and started to self medicate with alcohol."

Langford's story was arguably one of the most important things to come out of cybersecurity in 2019, as it cast a real (and well-known throughout infosec circles) person's arc at the center of a boiling issue within the industry. The crisis of mental health is growing everywhere, and its tentacles are hardly limited to infosec. But this sector is notably unique in its susceptibility to the dangers of burnout - the most common manifestation of a prolonged period of workplace stress.

Consider that:

You're constantly on the defensive
As the saying goes, attackers need to be right only once, and you need to be right all the time. While that's probably overblown – adversaries require multiple things to break their way after establishing an initial foothold and before they can penetrate deeper into the network – the point stands that you are under constant threat bombardment and have far more ground to cover than your digital foes.

One transgression can impact huge numbers of people
Think about the most prolific data breaches of all time. They have affected tens, if not, hundreds of millions of people. In many cases, the incident began due to a simple oversight, such as a misconfigured system or unpatched vulnerability, or was enabled by a failure to promptly detect malicious activity underway. In many cases, junior employees are making these mistakes, the drivers for which will be discussed in depth in this e-book. But if you consider how costly a data security incident can be in terms of reputational harm, customer attrition, legal fees and more – the Ponemon Institute estimates the average cost of a breach is now pushing $4 million – the decisions being made in your SOC are arguably the most critical of all to your organization's bottom line.

Every day is a battle

With the attack surface only proliferating with the rise of cloud, mobile and Internet of Things, attackers have their pick at systems to compromise. Companies aren't experiencing devastating breaches every day, but they are under constant scanning and pinging. A University of Maryland study found that computers with web access are facing hacker attacks an average of every 39 seconds.

Malicious hackers seem to always be one step ahead

Intruders are regularly innovating and fine-tuning their methods to infiltrate targets and hide their tracks in the process. In fact, the very technologies organizations are adopting to fight back – like machine learning and artificial intelligence – are being used right back at you by the bad guys.

The "macho" culture pervades security teams

Sure, you're not donning a military or law enforcement uniform, but you're still working in defense and first response. Any psychological toll you feel is sometimes dismissed as having no place in an industry that prioritizes toughness, so there is a notion among some that raising issues of mental illness may be construed as weak.

The job can be monotonous, tedious, and repetitive

Not all security tasks are created equal. For as glamorous as the field of infosec can be described, much of your day may be spent mired in labor-intensive and very detail-oriented tasks involving general screen staring (commonly referred to as "eyes on glass") and paperwork. For example, boredom can reign supreme in the SOC if Tier 1 analysts are spending most of their hours manually clicking through thousands of daily alerts firing in from disparate detection mechanisms and then either ignoring or escalating. Ignoring or escalating. Ignoring or escalating. Aside from the monotony, self-doubt can creep in. What if you ignored an alert you should have escalated?

You can incite the ire of your adversaries

In early 2019, well-known cybersecurity industry veteran Jeremiah Grossman asked his Twitter followers a surprising poll question: "As an information security professional, how many death threats have you received?" Most respondents answered zero – thankfully – but more than 20 percent clicked that they have received at least one, with six percent of the nearly 800 voters responding their life has been threatened five or more times.

Skills are short

Probably the most talked-about shortfall in security is the talent gap, with some estimates suggesting there are more than a million unfilled positions in infosec. Good security is complex to get right without having adequate and adept personnel. And then there is potentially a bigger question to ask: Is the skills chasm self inflicted due to all of the above?

"We're an industry that's often measured on failure… on something going wrong," Langford said during a video interview with Information Security Media Group. "And when you combine that with the fact that we're an industry also charged with keeping secrets all the time. We don't talk about what we know. We're confidential for obvious reasons. I think it makes quite a toxic combination when combined with things like stress and burnout."

Fortunately, the tide is turning, and it feels like something of an epochal moment is upon us. The topic of mental health is coming out from the shadows with stories like Langford's and others. The greater industry is embracing this tough conversation as well. For example, the annual Black Hat USA conference in Las Vegas, considered one of the most popular infosec gatherings in the world, launched a session of tracks in 2018 specifically geared to mental wellness.

This e-book is dedicated to making sure you or your employees don't fall off the deep end. The last thing a depleted, but business-critical, discipline like security operations needs is more beleaguered professionals – or worse, ones who have reached their breaking point.

Part I

of this e-book, partly written by a veteran organizational psychologist and executive coach, delivers a compelling overview of the occupational burnout and chronic stress problem – where it originated, how and why it manifests itself and to what degree it connects to security professionals. The reason for presenting this "lay of the land" should be obvious: To defeat an enemy – in this case burnout – one must understand it and be comfortable talking about it.

Part II

is where we make the official jump from the theoretical to the practical and firmly tie the topic of burnout to security operations. It's also where you can get your hands dirty with actionable takeaways (although there are certainly some of those in Part 1 as well). The tips and tricks supplied are ones you can begin applying today – not next week, not next year, but right now – to ameliorate the possibility that either you're going to run out of fuel or your employees are going to abandon ship. Of all the subsets of infosec, SecOps practitioners may have the most at stake when it comes to burnout and overall mental health, and we are here to deliver timely support and guidance.

Security operations analysts of all tiers, engineers, architects and managers – really anyone with ties to the SOC, whether within the enterprise or a managed security services provider (MSSP) – will find value in the contents of this guide. Some may use it to help identify common burnout symptoms in hopes of staving off a meltdown. Others can leverage it to discover proven and practical solutions to remediate those warning signs – or for tips to help avoid a toxic, self-esteem-destroying workplace in the first place. Leaders and managers are also covered with best practice checklists for building a workplace where SOC pros can prosper.

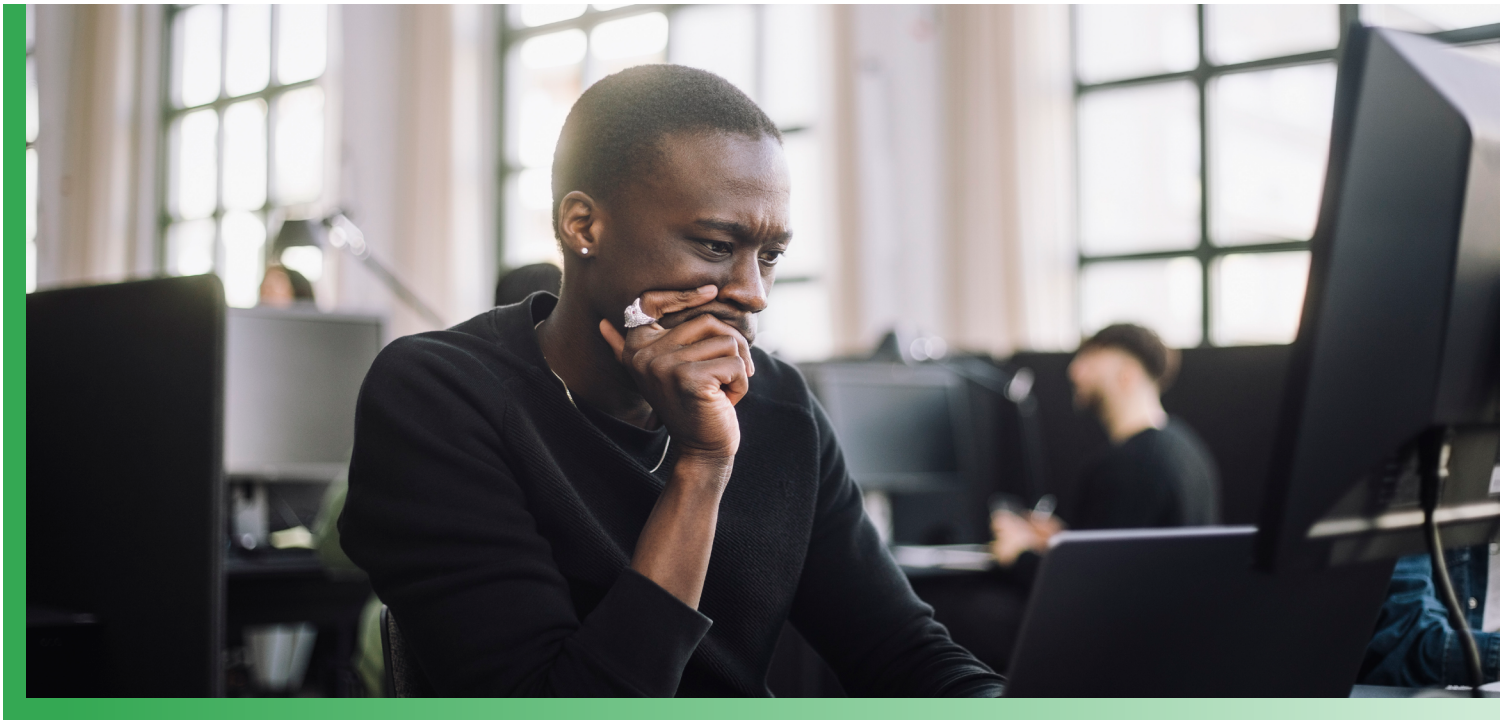
Remember, we're all in this together. Your adversaries spend their days collaborating to advance their craft. To counter them, we must not only be agile and clever, but also determined to dig in our heels together and fight on.

Part I:

The Basics of Burnout

1. How Have We Gotten Here?

If you feel stressed out at work more days than not, you're not alone. According to a study of nearly 2,000 professionals by the Korn Ferry Institute, nearly two-thirds of professionals report their stress levels at work are higher than five years ago. More than three-quarters of respondents say that stress has had an impact on their relationships, 66% say they have lost sleep from it and 16% say they've had to quit their job due to their levels of workplace tension. And data from the American Psychological Association backs the numbers up, asserting that 35% of adults in the United States report experiencing chronic stress on the job.



2. Understanding Stress and its Impact

When we talk about stress, what does that really mean? Stress can loosely be defined as anything a person perceives as a threat, be it physical or emotional. The key word in that sentence is perception: What one person detects as a stressful experience may be quite mild for another. Your body reacts to the impression of the stress, regardless of whether what you're responding to might be considered objectively stressful.

To illustrate how this works, consider this example: A husband and wife are sitting in a room together enjoying some relaxation time. Suddenly, the wife notices a spider crawling up the wall. She's had a fear of spiders her whole life. Her eyes widen, her body starts to tense up, and all of a sudden, she lets out a shriek that jolts her husband to attention. She is perceiving the spider as a threat and experiencing stress as a result of that perception.

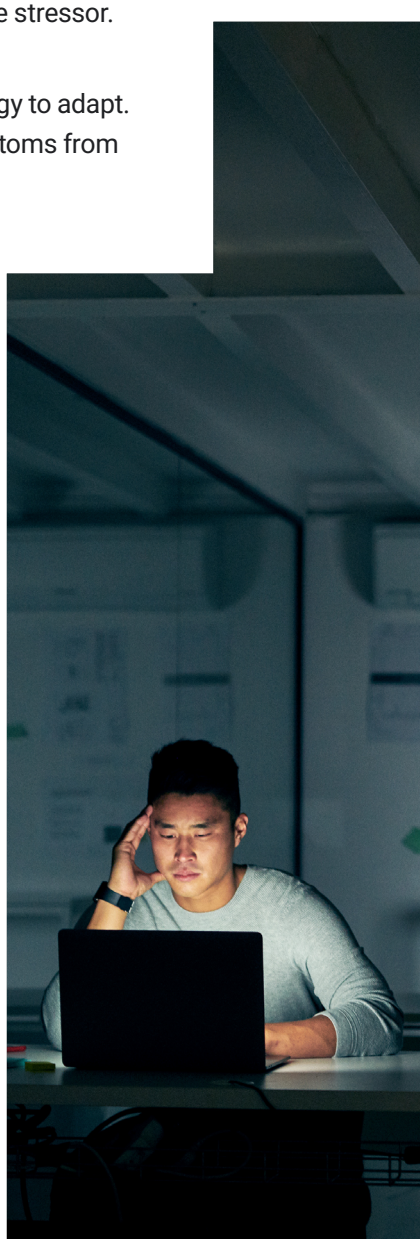
On the other hand, her husband has no problem with spiders and doesn't understand what the big deal is. He quickly picks up a tissue to dispense with the problem and goes back to binging Netflix on the couch with no significant effect. He doesn't perceive the spider as a threat, and so he does not experience the same level of stress as his wife, even though they are experiencing the same objective reality. The impact on each of them is a vastly different experience.

When that perception of a threat endures over the long term, it can have a far greater effect than the initial scare of a spider. Because stress has become so commonplace in our experiences, we toss around comments about being "stressed out," or even being "burned out," without really thinking about the impact of that reality. However, it's nothing to joke about. Although stress is the result of a perception that exists in our brain, prolonged stress is likely to lead to physical illness. To understand why this is, we need to cover a bit of history.

3. The Science of Stress

Back in the 1930s, Hans Selye (considered the father of stress research) began writing about the impact of stress from a medical perspective. He concluded that when the body is experiencing stress, it goes through three distinct stages:

1. First, the body recognizes the existence of the stressor. This is called the *alarm* stage.
2. Next, the body attempts to resist by adapting to the demands being placed on it by the stressor. This is aptly called the *resistance stage*.
3. Finally, when the stressor continues over time, the body will eventually run out of energy to adapt. This is called the *exhaustion stage*, and it's when we start experiencing outward symptoms from the experience.



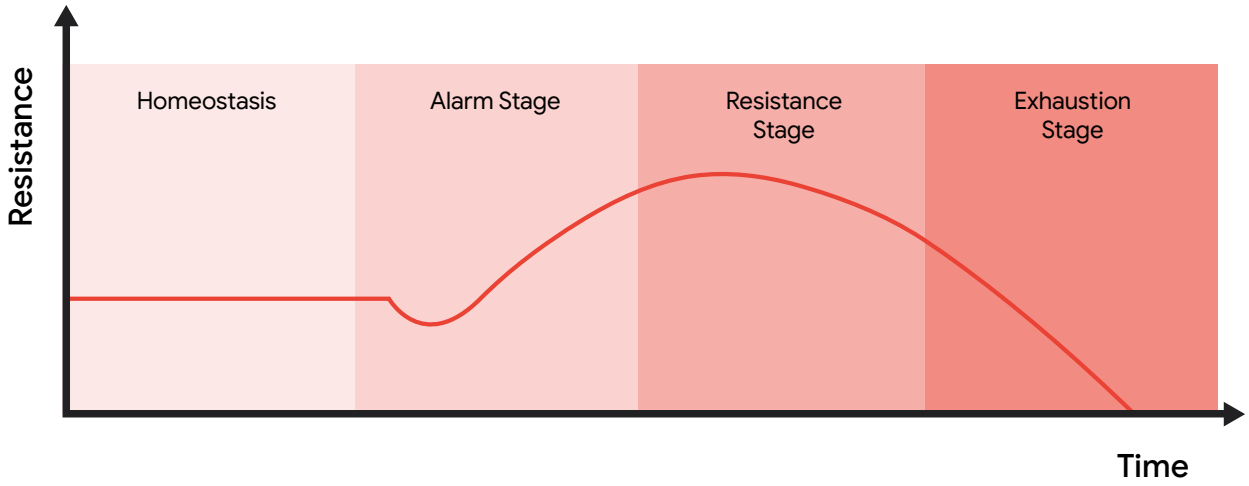
When we experience the perception of a threat, our brain does its best to prepare us to do one of two things: Fight the stressor off or run away from it as fast as we can. Commonly referred to as "fight or flight," this is part of our survival mechanism to escape things we perceive will cause us harm. However, when stress is consistent and ongoing, keeping the body in a state of high alert is what will eventually lead to Selye's exhaustion stage, and that's when we start to feel unwell.

The emotional implications of stress are the ones most commonly associated with the problem. For example, you may become easily agitated, frustrated or moody; feel constantly overwhelmed or out of control of your experience; have difficulty controlling your internal dialogue and perspective; and/or experience low self-esteem or even depression.

But here's the thing: Emotional stress, like the type of stress most commonly caused at work, likely will eventually lead to physical illness. That's because the body doesn't distinguish between stress that is experienced physically (think about working out too many days in a row without taking a rest day) and stress that is being experienced emotionally, which is what most of us experience in a work context. That emotional stress, over time, will manifest itself in the body and make you physically sick.

And here's the really scary part: There is little research to reference that will tell you what physical symptoms you might experience from stress. They could be minor, such as an upset stomach, teeth grinding, changes in your appetite or tense muscles. They could be more moderate, like insomnia or migraines. Or, if the stress is severe, the physical symptoms could be as serious as high blood pressure, Type 2 diabetes, stroke or heart attack.

This is why managing stress should be on the top of everyone's list of priorities: Your life may literally depend on it.



4. When Stress at Work Leads to Burnout

If your stress has been high on the job for a prolonged period, one of the signs that may eventually emerge is feelings of disengagement or burnout. According to Gallup, 23% of employees report feeling burnout at work very often or always, while an additional 44% report feeling it sometimes. In fact, burnout has become such a problem that the World Health Organization (WHO) has taken the notable step of adding it to its International Classifications of Diseases with the following definition:

"Burnout is a syndrome conceptualized as resulting from chronic workplace stress that has not been successfully managed. It is characterized by three dimensions:

1. Feelings of energy depletion or exhaustion;
2. Increased mental distance from one's job or feelings of negativism or cynicism related to one's job; and
3. Reduced professional efficacy.

Burnout refers specifically to phenomena in the occupational context and should not be applied to describe experiences in other areas of life."

This fact that the WHO has clearly distinguished between stress related to work and stress caused by other life factors is a significant acknowledgment of the severity of the problem experienced by many professionals. And although the WHO is the first major health organization to legitimize burnout with this inclusion, it may not be the last. The American Psychiatric Association, for example, has yet to add burnout to the DSM-5 (its official manual), but the group is starting to assess the topic seriously through a working group on well-being and burnout.

And while they sound similar, there is a distinction between prolonged stress and burnout. According to HelpGuide.org: "Stress, by and large, involves too much: too many pressures that demand too much of you physically and mentally. However, stressed people can still imagine that if they can just get everything under control, they'll feel better. Burnout, on the other hand, is about not enough. Being burned out means feeling empty and mentally exhausted, devoid of motivation, and beyond caring."

Physical Signs and Symptoms of Burnout

- Feeling tired and drained most of the time
- Lowered immunity, frequent illnesses
- Frequent headaches or muscle pain
- Change in appetite or sleep habits

Behavioral Signs and Symptoms of Burnout

- Withdrawing from responsibilities
- Isolating yourself from others
- Procrastinating, taking longer to get things done
- Using food, drugs or alcohol to cope
- Taking out your frustrations on others
- Skipping work or coming in late and leaving early

Source: HelpGuide.org

Emotional Signs and Symptoms of Burnout

- Sense of failure and self-doubt
- Feeling helpless, trapped and defeated
- Detachment, feeling alone in the world
- Loss of motivation
- Increasingly cynical and negative outlook
- Decreased satisfaction and sense of accomplishment

Know the Difference: 3 Main Varieties of Burnout

While the symptoms are generally thought to be same in every person experiencing burnout, researchers have classified unmanageable work-related stress into three categories. Understanding these profiles can help patients apply the appropriate coping strategies.

Frenetic burnout describes a typical "workaholic," someone who pushes themselves to the point of exhaustion in an attempt to achieve success without considering self-care.

Underchallenged, or boredom, burnout affects workers who toil in monotonous and unexciting environments, as a result exhibiting feelings of indifference.

Worn-out burnout involves employees who have lost all motivation and feel detached from their work due to overwhelming stress and lack of appreciation.

5. Why Security Pros Are Susceptible to Burnout

Every professional brings different preferences and tendencies to work with them each day that make up their work style. There is no such thing as a "best or worst" or "right or wrong" approach to work – each style has both strengths and challenges to consider in the work environment.

While the manner in which one works does not inherently dictate their career path, it is true that those with a more conscientious work style are more prone to be attracted to jobs in cybersecurity than other types of industries. This meticulous style places a high premium on accuracy, maintaining stability, and implementing policies, processes, and procedures that have been thoroughly thought through and vetted.

Security pros also tend to operate precisely and analytically and are able to dig into the weeds and the details that other work styles may find difficult and unappealing. This is what can make you successful in a critical field.

However, every work style has weaknesses as well. Those with an eye for details tend to be overly and unjustifiably critical of themselves and their work, seeking perfection at every turn. That means a minor error can be perceived as a stress-inducing threat.

Security practitioners also tend to be more skeptical due to the nature of the job. You must lie in a constant state of vigilance, never sure when an external or internal threat may arise or an attacker may strike.

Being in a perpetual watchful state allows for tough questions to be asked and issues to the business to be uncovered, but it also can lead to you expecting the worst possible outcome, all the time – which generates fear of potential failure.

For a work style that is filled with overachievers, focusing on all the things that could go wrong (rather than things that might work out in your favor) can keep you constantly on edge.

Here Are the 10 Most Stressful Aspects of the Cybersecurity Job:

1. Keeping up with the security needs of new IT initiatives (40%)
2. Finding out about IT initiatives/projects that were started by other teams within the organization with no security oversight (39%)
3. Trying to get end users to understand cybersecurity risks and change their behavior accordingly (38%)
4. Trying to get the business to better understand cyber risks (37%)
5. The overwhelming workload (36%)
6. Constant emergencies and disruptions that take me away from primary tasks (26%)
7. The fear of getting something wrong (25%)
8. Keeping up with internal and regulatory compliance audits (25%)
9. Monitoring the security status of third parties the organization does business with (24%)
10. Sorting through the myriad of security technologies used by the organization (17%)

Source: Information Systems Security Association (ISSA) and Enterprise Strategy Group (ESG), based on a survey of 267 security professionals

6. Proactive Coping Strategies

Selye once quipped "complete freedom from stress is death," meaning that it is an inevitable part of the human experience. The goal is to meet it efficiently and enjoy the process of adjusting and adapting to life as it happens. Another word for this is coping. Coping is the process of facing responsibilities, problems or difficulties and moving past them successfully.

But not all coping strategies are created equal. Fast forward a few decades after Selye's initial research on the medical impacts of stress, and you'll discover Richard Lazarus and Susan Folkman with their seminal work *Stress, Appraisal and Coping*. The pair discovered that there are essentially two methods of coping that individuals can use when handling stress:

> **Problem-focused coping** is when people concentrate their efforts on removing the stressor from their experience. At work that might mean trying a different tactic, attempting to work with colleagues differently, and thinking tactically about the problem to see what you are missing and what you can do to meet your goal. In other words, the goal is to solve the problem.
>
> **Emotion-focused coping** is when you make changes in your life to mitigate the impact of stress on it. This might mean going to the gym more frequently, spending more time with family or trying to maintain a better work-life balance.

Which tactic you choose to employ is a reflection of how solvable you perceive your stressor to be. If you perceive your trigger is something you can fix, you will generally try to tackle the problem head on with problem-focused strategies, while if you do not believe you can remove the stressor, you will generally focus on more emotion-focused strategies.

While neither form of coping is necessarily better or worse than the other, remember back to Selye's model outlined earlier in this e-book of the alarm, resistance and exhaustion stages. When emotion-focused coping strategies are utilized more aggressively than problem-focused coping strategies in the long term, you will remain in a state of resistance when it comes to the stress you are experiencing. Eventually, your body will run out of resources to repel stressors and it will enter the exhaustion stage. That is when you may start getting sick as a result of your stress.

Thus, to manage stress adequately, it is critical to use a combination of the two types of coping strategies by engaging in proactive measures to remove the threat from your experience, as well as measures to mitigate its impact.

7. A Dozen Personal Techniques to Manage Stress

The best way to start utilizing proactive strategies to manage the impact of stress at work is to start by making small changes to your work experience that you can commit to consistently for at least 30 days. This will help you to build new, positive habits and rewire your brain to maintain those habits over the long haul. Use these tips to get started, keeping in mind that not all of them will apply to you. Later on, we'll delve into more specific suggestions exclusive to security operations.

Know What's Stressing You Out

A key component of enacting proactive, problem-focused strategies to managing your stress is to know specifically what is causing it in the first place. You can use the earlier quiz to guide you in identifying the general problems that are impacting your stress levels at work. Then, peel back the layers of the problems you're experiencing to discover the root causes. For example, if your boss is the one stressing you out, ask yourself what they do to cause you stress. Is your workload too heavy? Do they ignore your ideas and input in important discussions? Do you feel micromanaged? Are you not getting the training you need?

The more focused you can become, the better. Once you've drilled down into your key concerns, brainstorm strategies to help alleviate or solve them. Look for the lowest-hanging fruit, aka the easiest things you can muster to make quick progress and build momentum. Some problems may take longer to fix, but the quick wins may free up your energy to help you focus on those bigger things.

Take Control of Your Workday by Blocking Your Calendar

What happens when you have open time on your calendar? Inevitably, someone is going to book a meeting at that time. That's why people are spending an estimated 35% to 50% of their time at work in meetings. And if they're not in the meetings, they're preparing for the meetings! Try this instead: Identify one to two hours per day that you can block on your calendar for productivity time. Consider this scheduling a meeting with yourself! This is time for you to shut your office door (or perhaps put on a set of headphones if you're at a cubicle) and focus on making measurable progress on your goals.

Your boundaries are only as healthy as you make them. Make this time sacred. Do not allow people to schedule you for meetings during this time unless it is a legitimate emergency. Just explain that you have it blocked to enable you to focus on a few specific tasks that you need to accomplish and that you'll be happy to meet with them another time. And remember, the time you spend focusing on your own tasks is no less meaningful or valuable to your organization than the time you spend in meetings. And when you're able to accomplish more in your time at work and move tasks off your plate, you won't spend so much time worrying that you're not doing enough when you're at the office.

Turn off Your Mail (or Mute Your Slack)

Now that you have some dedicated "you" time on the old calendar, you have to use it wisely. Don't let multitasking get in the way. Human beings are not creatures that are built to multitask. When you're jumping around from duty to duty, your brain must stop, shift its focus and start again. That doesn't allow for you to focus on something and produce your best work.

In the modern office landscape, there is no greater distraction than email or whatever communication platform you use. It is open on your desktop all day long, with notifications

popping up and sounds chiming every time you receive a new message. Instantly, your focus is drawn away from whatever you're working on to the new message that has landed in your inbox. Think of how many times you've told yourself: "I'm just going to ignore that notification." But let's be real, that is not easy to do. So, you stop what you're doing to read it, answer it if necessary, and then have to move back to your other task. This constant back and forth does nothing to help your productivity and ends up creating more stress because you can't get as much work accomplished as you'd like to.

Instead, try this: For the first 45 minutes of every hour, turn off your email, Slack, IM or whatever. Not just minimize it – turn it off entirely, so you're not getting notifications of new messages. Throw yourself into whatever you're working on with a new focus and allow yourself to solely concentrate on it without distraction. Then, after 45 minutes, open your email up and see what has come in. Respond as necessary and then shut it off again.

Rinse and repeat.

We've got to move from this place where every email is an emergency and needs to be responded to immediately. That just distracts you from working on the things that will move you toward your goals. In the case of an actual emergency, someone will come to find you or call you on the phone. And in all other cases, 45 minutes is not a long time to wait for a response. Give it a try, and you'll find that people really don't need immediate responses. We've just tricked ourselves into thinking they do.

Accept Your Boss as a Flawed, Imperfect Person

News flash: Your boss isn't perfect, and they don't know everything. And it's unreasonable to expect them to.

The head honcho tends to be the largest source of stress for the average person at work. What they say, what they do, what they're not saying or doing, how they write emails, how they manage, how much of a workload they push on you, etc. It is undoubtedly true that the majority of managers could make improvements in one or many of these areas. That is the responsibility they should accept when they take on a manager role.

However, it doesn't help your stress level to hold your boss to an impossible standard of excellence that simply is unrealistic in the modern workplace. It just sets you up for disappointment or to be in a constant state of angst when they don't measure up. Remember, your leader is probably just as stressed – or potentially burned out – as you are. And they are probably coming in every day just trying to do the best they can.

So, cut them a little break and try to direct your attention to things you appreciate rather than focus on things you don't like. Note: This is not about letting them off the hook. (We'll get to later what bosses can do to improve.) It's about minimizing their impact on your day-to-day stress levels.

Pick Your Battles

Speaking of his experience with politics at universities, Henry Kissinger once remarked: "The reason that university politics are so vicious is because the stakes are so small." Sadly, that's not just true of life in higher education. It can be so easy to get dragged into those vicious battles at work. You know the ones: They often leave people so perturbed that they forget what they were even fighting about in the first place.

Sometimes, all it takes to reduce stress at work is to keep your mouth shut and avoid being dragged into confrontations that ultimately don't matter. If difficult people are causing you stress, make a conscious effort to choose when to engage with them. Make sure it is worth it. Frankly, most battles at work are just not worth partaking in – when you "win," you don't really win much at all. So, if you're going to go to war, make sure you'll be happy if you come out victorious on the other side. If you won't, the very best thing you can do is to just walk away.

Stop Gossiping

Office chit-chat brings no value to the workplace. It hurts relationships, creates a climate of resentment and fear and feeds the stress – and paranoia – levels of all involved. And yet, when you hear those whispers in the kitchen, it can be almost impossible not to participate and find out the latest bit of dirt. Be honest with yourself: Does it ever do you any good? Does it help you meet your goals? Produce more? Do better quality work? Have a more fulfilling experience? The answer to all these questions is probably no.

Remember, you always have a choice: Office gossip is one of those things you can always choose to opt out of, and, like in the altercation scenario above, it's as easy as walking away. Just say no!

Get Your Workout In

Can you go to the gym and lift weights or hit the treadmill for 30 to 60 minutes and not feel strong and powerful when you're done? Of course not. And work is one of those places where you want to feel you're most powerful. You can get yourself there before you head into the office by scheduling a morning workout.

Working out has so many benefits when it comes to stress reduction, but perhaps one of the most potent is this: You've given yourself the gift of doing something just for yourself — showing yourself that love and appreciation will put you in the right frame of mind to take on those tough projects, humdrum tasks or those patience-testing colleagues. The type of workout you do – going for a walk, hitting a punching bag, doing yoga, surviving a challenging fitness class – is not as important as the simple act of making the consistent commitment to do something, even when you don't feel like it. (Your bed will always be there later. But make no mistake, sleep is also extremely important!)

Drink Your Water

This is one of the most straightforward solutions of the bunch. You have got to make sure you're staying hydrated. When you're not getting sufficient H20, your brain does not optimally function, and your cortisol levels (a stress hormone) will go up. And it's a Catch-22. Taking care of yourself by eating well and drinking water are often the first things that go out the window when you're under stress. Make a conscious effort to get this part right, and you'll set yourself up to deal with difficult situations from a much sounder place.

Get out of the Office

Breaks are something you should be liberal with at work. They give you the opportunity to recover from the psychological costs of working hard so that you can come back with new vigor. Whether you have built-in breaks or can take one whenever you need, you should. Start by pausing for lunch. Get up from your desk and force yourself to get out of the office for a change of pace. And don't just go from your desk to the break room. Get out of the building! Eat lunch on the grass outside, go to a nearby park, pick up lunch at a local eatery... even just get out and go for a walk or drive! Giving yourself that break mid-shift will allow you to destress and set you up to be even more productive, calmer and steadier when you come back to the office. You can find added benefits if you use this break time to breathe, meditate or practice mindfulness. According to the Mayo Clinic, mindfulness is the act of focusing on your breath flow and being intensely aware of what you're sensing and feeling at every moment, without interpretation or judgment. You can put this into practice in the workplace by facing situations with openness and patience.

Hand out Compliments

The gifts we give to other people we also give to ourselves. When was the last time you handed a genuine compliment to a co-worker? Not the one you felt like you had to offer because the boss was watching, but rather the one that was unexpected? Perhaps it was a sticky note left on someone's computer monitor letting them know you appreciate them or a genuine "great job" after they closed a difficult case or presented in a meeting. Not only will you make someone's day, but you'll experience reciprocal benefits such as better relationships, enhanced health and (yes!) even reduced stress.

And if you want a real challenge, try dishing out love to the colleagues with whom you are most disagreeable. The truth is, they are probably the ones that need those compliments the most, with the added caveat of creating a better companionship with them.

Define Your Boundaries and Create a Better Work/Life Balance

There is no such thing as a perfect harmony for everyone. We all have different priorities, are at different stages in our lives and are driven by varying things. However, to reduce stress at work, you need to set boundaries between your work life and your real life, and it is up to you to stick to them. Perhaps that means getting out of the office at close to on time as possible, avoiding email during nights or weekends or leaving your laptop at work. It may seem counter-intuitive, but the more you can disconnect from your job and enjoy other parts of your life, the more effective you'll be when you're back at work.

Express Gratitude

If you're reading this e-book, chances are you've got it pretty good. You have a computer and an internet connection. You're probably employed in a job and have money coming in, even if it may not be your dream role. You probably have a place to live and more food available to you than you could ever eat. And that's just the basics before you get into all the other enjoyable stuff you have going on in your life.

Whenever you're feeling angry or stressed out or frustrated, try to come back to the positives and be grateful for them. Most people have a lot more good than bad to worry about every single day, yet we are culturally conditioned to remain in negative thought patterns. Make sure you're not letting the unfavorable overshadow all the positive things happening to you both at work and at home. At the end of every day or to start every morning, try making a list of the things that went really well that day, or things you're proud of or thankful for. Reflect on it as you drive home or take a shower and give yourself a pat on the back for a job well done.

8. Why Employers Must Care About the Burnout Epidemic

Although unfavorable circumstances can show up in the working experience, the reality is that they are not just an employee problem. Organizations can spend millions, or even billions, every year when employee well-being is not placed high on a list of leadership priorities.

Consider the stats, courtesy of Stanford University, Gallup and Kronos Inc.

Burnout costs between $120 billion and $190 billion every year in health care-related costs. Researchers estimate that workplace stress accounts for 8% of national spending on health care.

Burnout often leads to disengaged employees, who show up every day doing just enough to get by instead of contributing to the full level of which they are capable. These disengaged employees cost employers 34% of their annual salary as a result of their underperformance due to stress.

Burnout is responsible for a significant amount of employee turnover, anywhere between 20% and 50% depending on the organization. Turnover costs employers between 30% and 150% of the annual salary of the lost employee based on how difficult they are to replace and the historical knowledge lost by that departure. (This can be especially hurtful in a discipline like security operations.)

All this means that employers who get ahead of the burnout curve will gain a distinct advantage over their competitors. Not only will employees be happier and healthier, but they will produce more, deliver better service to customers and clients, have significantly more loyalty to the organization, have reduced absenteeism, and contribute more to the bottom line than their burned-out colleagues.

9. Organizational Strategies to Reduce Burnout

To understand where your employees stand on the burnout scale, start by measuring it. The National Academy of Medicine offers access to different validated instruments to help construct an assessment of your organization's stress levels.

> Download Tools from the National Academy of Medicine to Measure Burnout

The results may warrant an honest discussion of what has caused the problem and what needs to change to rein it in. There is an opportunity to get your team involved in the process. Your workers likely will want to tell you exactly what the most important steps to take are as long as you ask them in a way they feel safe from any repercussions.

Managers and leaders should also take personal responsibility for mitigating, or even preventing, burnout among their employees through everyday acts that enhance employee wellness. Here are three of the most impactful investments organizations can make:

Increase Flexibility

Give employees the ability to spend time working outside of the office, be it from their home, a coffee shop, or a co-working space. Flexible working environments not only help employees to manage their stress levels, they also have a variety of business benefits. Research out of Stanford University found that remote work can lead to "astonishing" productivity, with one day at home being equivalent to a week's worth of effort in the office. Other advantages include increased employee retention, decreased sick days and overall reduced costs for employers. Note: For the SOC pro, remote work may not be an option, but that doesn't preclude companies from implementing flexibility around hours, days or shifts worked.

Require Real Vacations and Don't Reward Workaholics

Vacations are a chance to relax and rejuvenate, and come back to the office with a renewed perspective. However, according to research sponsored by The Huffington Post, one in four employees note being actively discouraged by their organization to use their earned time off, and that nearly half of all earned vacation days go unused every single year. Organizations striving to manage burnout well should not only encourage employees to use every single vacation day they have, but also should make sure they have the support to disconnect during their time off.

Incentivize Managers

What if part of the annual performance review for each manager included a wellness check for their team in which their stress and burnout levels were measured and each manager was reviewed on their ability to nurture a positive environment? What if their appraisals, promotions and raises depended on it? This would impact a plethora of decisions managers make, including when to bring in additional resources for their team when they are overworked, providing the team with tools and processes to support their productivity, and making sure they are giving positive recognition to keep their team in a good mental headspace. Measuring employee burnout and making it a part of an official review process will provide a tangible incentive to managers to do the right thing, by their team and by the organization.

Ultimately, there is no quick way to fix the problem of burnout on an organizational level. There's only hard work and commitment to making things a little bit better every day. However, the worst option is to choose inaction because if your organization isn't going to tackle the problem, you better bet your competitors are working on it. And once they find their solutions, they will reap the benefits of a more engaged and productive workforce, which will make them much more difficult to compete with for coveted security operations positions.

Part II:

A Journey into the SOC to Fix Burnout

"Over 60% of SOC Analysts Are Planning to Quit Next Year"

So read the daunting headline of a March 2022 story in Infosecurity Magazine. It's a startling stat, and one that should lead you to an important conclusion: For every CISO like Langford who is burning out, exponentially more rank-and-file infosec pros are spending their days and sometimes nights toiling in the proverbial trenches, bearing similar effects of physical and mental exhaustion. Their stories are less commonly seen and told, but are no less important.

The security operations center is no stranger to burnout; in fact, it may be the epicenter of work-related stress within the security program. But before we dig into the "why," it is important to remind you that all doom and gloom this is not. SOC work has many benefits: For many, it's a stepping stone to greater responsibilities within the security group and an optimal place to cut one's teeth, as you will be exposed to everything from threat intelligence to vulnerabilities to big data. And even as a low-tier analyst, you are on the frontlines of unfolding action, the handling of which is vital to the organization.

1. What is Working Against the SOC?

Between networks, endpoints, cloud technologies and critical infrastructure, digital footprints are growing for every business. Inside many of these companies, SOC analysts spend their days monitoring data streams and network logs for anomalous activity, and most enterprise SOCs receive thousands of alerts per day.

And therein lies the problem. Whether you're weeding through these notifications, searching for an indicator of compromise, rooting through logs or running queries to compile asset information relevant to the case you're working, time becomes your most precious commodity. Spending so many minutes and hours of your day on data gathering, enrichment and escalation decision-making can take time away from deeper investigations, analysis and remediation.

Plenty of false positives are rearing their ugly heads. Recent numbers from the Ponemon Institute found that organizations typically get about 17,000 alerts per week, with 80% of them being bogus. The consequences are two fold: 1) The important stuff that should be investigated further is sometimes missed amid all of the noise and 2) Overtaxed SOCs adopt a "see no evil" attitude to certain alerts by tuning down thresholds or outright ignoring certain categories.

Security operations teams have never had more data points available to them – according to Enterprise Strategy Group, organizations are averaging up to 50 security tools from 10 different vendors – to identify, investigate and analyze threats. That's a good thing, considering relying largely on prevention technologies and methodologies doesn't cut it in today's threat landscape. But it also means a lot of unorganized, out-of-context and unactionable data for you and the team to ingest.

Another side effect of this "alert fatigue" is that triage can involve performing similar manual tasks over and over again. This how the the SOC got the dubious distinction as being short for for "sitting on chair." (Sorry.) More importantly, this redundant work can result in consequences for the business in terms of mistakes being made and take an emotional toll on analysts in terms of boredom, which studies have found can be directly linked with burnout.

You also may not be getting the proper support. Within the SOC, communication among analysts and managers is essential. Both need to have a way with words: analysts to cogently and authoritatively discuss data security incidents, and managers to share technical guidance and build appropriate processes. Yet, lack of management support was cited as the fourth-biggest obstacle to a full SOC model, according to the 2019 SANS Security Operations Center Survey. To overcome this, leaders must work to improve workflow processes, introduce technology solutions and endorse training and career development.

Support can also simply mean showing appreciation. According to Paul White, a workplace relationship psychologist who recently polled 130,000 workers, nearly two-thirds hadn't received positive feedback in the past 12 months. Employees tend to thrive on affirmation, and underappreciation is a common reason for vacating their positions.

And then there's your schedule being off. If you follow professional football in the United States, you'll know the public narrative generally gives East Coast teams playing at home the advantage versus a squad traveling from the West Coast. The idea is that the changing time zones disrupts players' normal biological cycles, known as the circadian rhythm, giving the home team an edge.

The theory is not off base, and it has long been posited that shift workers who work irregular hours can experience sleep loss, among other physical and mental health problems. Organizations running 24x7x365 security operations centers stand to suffer the most.

2. A Q&A on Burnout

We asked Amanda Berlin, CEO of Mental Health Hackers, a nonprofit whose mission is to educate tech professionals about the unique mental health risks faced by those in our field, how and why the SOC both in enterprises and MSSPs can be a source of burnout and what negative consequences (to the person and the business) can result? She mentioned three cultural factors that are at play. Below is a transcript of her comments.

Business Value

Security operations, regardless of industry, do not produce revenue. (They) negatively impact profitability, and until very recently, has been treated as a necessary burden by executives. Ironically, however, headline-grabbing breaches have begun to change perceptions regarding the importance of SOCs, but prioritizing the wellness of SOC analysts has generally not improved.

Even in outsourced or managed SOC operations, costs are kept to a minimum by the purchasing organization. Contracted SOC analysts are often tasked with monitoring multiple enterprises in separate virtual machines to keep management costs low. Due to cost concerns, many SOC analysts are young professionals, or people who have changed occupations, and are in the early years of their information security careers. Culturally, this affords analysts little voice in the direction of security operations, and the day-to-day working life of the analysts. Since SOC analysts are in high demand, these professionals often move from company to company for compensation increases, better working conditions or scheduling considerations.

Attention to Detail

A SOC analyst's tasks require strict attention to detail. Even small changes in the data indicators presented can affect how the analyst will triage the alert, begin an investigation, generate a ticket or raise an alert. SOC analysts are pressured to sift through hundreds of alerts, looking for the right indicator of compromise. Playbooks are often ambiguous, or non-existent in some enterprises, leaving the analyst to fend for themselves. As previously mentioned, SOC analysts are often young professionals working at the bottom end of the information security wage scale. However, modest pay or limited experience does not mean reduced accountability. SOC analysts are expected to be

perfect, or nearly perfect in their ability to find the next malicious campaign. Poorly tuned alerts or substandard architecture can also add to the SOC analyst's challenges, as an analyst may need to sift through hundreds of false positive alerts. False positive alerts breed complacency. Complacency leads to missed indicators of compromise.

The Environment

Many SOCs occupy the least desirable office space an organization may spare. It is not unusual to find a SOC located in a basement, or tucked into a cramped corner, or lacking in newer office furniture and amenities enjoyed by profit-generating parts of the business. Although some companies are bucking this trend, many SOCs are treated as governmental SCIFs (sensitive compartmentalized information facility) and are contained in rooms devoid of natural light. SOC analysts are denied the ability to look outside at a tree, or interact with the world around them. The ability to disconnect, even for a few moments at a time, can do wonders for the mental health and grounding of SOC analysts. LED (blue range) screens, and sterile artificial light also have their own psychological effects on SOC analysts.

3. Words of Wisdom from a Real-Life SOC Analyst

This Reddit thread, titled "Coping with SOC Burnout," features a highly upvoted comment from user 'Hazerr'. We have published it in its entirety, with amendmets only made for grammar style.

First **cut off alcohol as much as you can**. It f*cks with your sleep (and general health), so it only puts you down more. Use caffeine with moderation and don't take it several hours before your scheduled rest time. Your rest time has to be of quality.

Working with rotating shifts, you need some kind of routine. Like, plan your meals so that you eat at the same time every day, even in different shifts. I know this is very difficult but it helps.

Adjust immediately your sleep/living patterns for the next shift. Even if you have to make an effort to not go to sleep after work.

I found that studying while working in shifts is super demoralizing. My brain couldn't hold anything in and keeping the focus was super hard. Do go easy with it. And do it after getting rest.

Socializing was put a bit on hold, especially if late nights and drinking were involved. You are going to pay for it, with interest.

This kind of work is really tricky because it can hold you back, so think about what you want, If you like the job, commit yourself to it and try to move up the ladder fast. If not just go for something else.

I used to work in a SOC with a NOC (network operations center) side by side, and people there were in the same low-level positions for many many years and seem stuck there. So get your sh*t together and decide what you want for yourself and act accordingly.

But know that there will be sacrifices. Sacrifices made early capitalize a lot in the long run.

4. Six Signs You May Entering the Wrong SOC:

Monitor LinkedIn: If employees are leaving the company in rapid succession, it probably means either the culture is toxic or roles aren't living up to expectations. Either way, beware.

Do they invest in you? When you're exploring or interviewing for a career opportunity, dig deeper into what the company offers other than the obvious stuff like salary and vacation time. Specifically, find out if the company invests in the health and well-being of their employees through things like stress management programs, work-life balance, flexible hours and overtime pay.

Let reputation guide you: Infosec is tighter knit that you might think, and people talk. Word gets around fast about unappealing workplace environments.

Network in the real world: Many cities host regular gatherings of infosec professionals, so take advantage. Sites like meetup.com and IT and industry groups like ISSA and (ISC)2 are good options. If formal get-togethers aren't for you, consider a "lobby con," the term given for informal hallway conversations common at shows like Black Hat or Defcon.

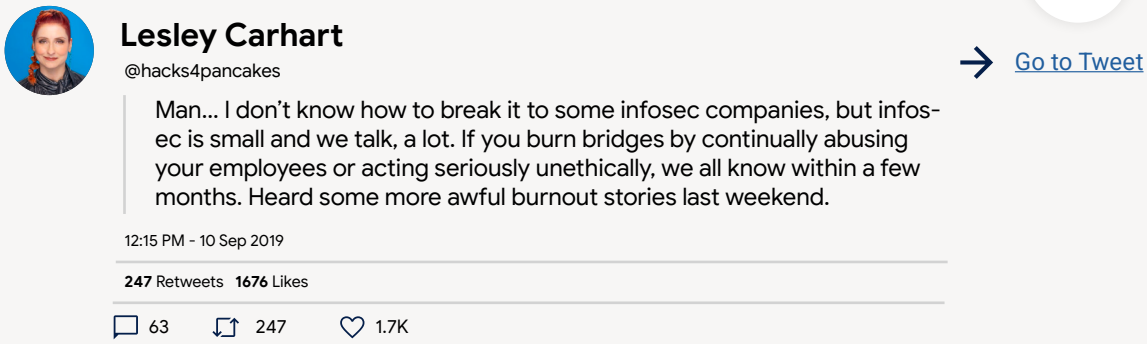
Beware of bloated Glassdoor reviews: Like the newly opened eatery down the street from you that has glowing Yelp reviews yet always seems to have empty tables, businesses can take the same approach to artificially boost their allure. If it a potential employer sounds too good to be true, it probably is.

If you see something, say something: If you're not the one seeking advice, be the one who provides it. The infosec community is exactly that – a community – and it is on you to both share your personal experiences (good and bad) and to be a role model for career health. Remember: While you may not be feeling the symptoms of burnout yourself and may, in fact, be thriving, choose your words wisely. The behavior you may be advocating for is not for everyone. Remember the husband-wife spider example from earlier?

5. Honing Your Soft Skills: A Mandate for Leaders

Visit any business, and you won't have to look far to find an employee who is emotionally checked out. They're frustrated. They're apathetic. They're just not giving their all. And in some cases, the worker may be dispassionate because of reasons other than burnout. Maybe the job just isn't for them. Maybe they have their next position lined up and are just coasting until they give their notice. And maybe – who knows – they're a trust fund kid, and earning a paycheck is optional.

But as this e-book has illuminated, chances are rising that if your employees are exhibiting indications of fatigue and dissatisfaction, there may be something underlying at play – and for leaders, it is on you to help discover and troubleshoot it. Granted, you can't solve everything, especially if the issues are fundamental to the organization or if you are feeling symptoms of burnout yourself, but you can implement mitigating factors.



At the very least, you need to be as good as you can be at difficult conversations: Great leaders exhibit high levels of empathy and emotional intelligence. Every one of your subordinates will have a unique personality and will respond differently to situations. Don't judge their feelings. Ask questions. Listen. Then speak.

Almost everyone will welcome gratitude. A person who feels appreciated will always do more than is expected. But be careful your words of admiration don't lead to employees feeling the need to overdo it, or else you may find yourself mired in a vicious cycle.

6. Leadership Lessons - by Amanda Berlin, CEO of Mental

Give Your Team Flexibility

If you want to invest in mental health in your workplace but aren't sure where to start, one option is to let employees choose.

- Monthly Stipend: It can be used for therapy appointments, massages, meditation apps, gym memberships, etc.
- Preferred working hours: I talked to an awesome person who recently allowed one of her employees to modify his work hours, which made him much happier and healthier.

Get Employee Buy-In

While several companies on Inc.'s 2019 Best Workplaces list offer monthly or annual stipends, employees don't always take advantage of benefits – even short-term services for people struggling with addiction and other personal problems. Only about half of the employees have any awareness that some of these resources even exist.

Make it Easier to Get Help

Opening a workplace dialogue and teaching coping strategies can go a long way in aiding employees' mental health, but sometimes people need professional treatment. While most health insurance plans cover at least some mental health care, therapy can be expensive – even with insurance – and it can be hard to find providers who both accept your insurance and are taking on new patients. To close this gap, some companies are turning to online services.

Bring in the Professionals

Another option is to bring professionals in house. For example, I know of an Illinois-based accounting firm where all of their employees have access to a psychologist on the company's dime. The company has also started bringing in a certified life coach to work with employees at least once a year.

Track Your Progess

Like any good new program you implement, it can be difficult to measure their success with any degree of certainty unless you specifically track your results. You should track productivity and quality of output as a whole, as well as turnover rate and absences.

Jesse Emerson,
VP of Managed Security Services
at Trustwave

How to sidestep burnout specific to the SOC:

1. Avoid scheduling your analysts for more than two to four hours “on console.”
2. Build task rotations into this shift to allow analysts’ minds to have some variety.
3. Provide tiers of support behind analysts so they are able and comfortable to ask for assistance.

7. How to Reclaim Surrendered Ground with SIEM and SOAR

For all its advancements, the modern-day security operations center will always need people and the decision-making prowess they provide. But technology can help SOC personnel, namely Tier 1 analysts, respond to key challenges – like data ingestion limitiations, alert inundation, visibility blind spots, overreliance on manual tasks, skills shortages and disparate detection tools – without removing the need for people. Instead, staff is freed up to have all the data it requires, free of blind spots, and able concentrate on more inspiring and higher-order duties, like threat hunting, malware analysis and incident response. A happier and more inspired analyst is one less likely to burn out.

Chronicle Security Operations brings together the capabilities that many security teams depend on to more quickly identify threats and rapidly respond to them. It unifies Chronicle's security information and event management (SIEM) tech, with the security orchestration, automation, and response (SOAR) solutions from the acquisition of Siemplify and threat intelligence from Google Cloud. The recently-completed Mandiant acquisition adds even more incident and exposure management and threat intelligence capabilities.

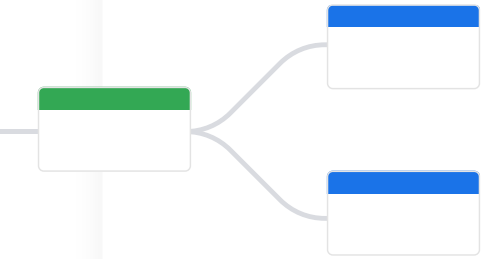
Cloud-scale data: By leveraging Google Cloud's hyper-scalable infrastructure, security teams can analyze security telemetry and retain that data much longer than the industry standard at a price point that's fixed and predictable.

At your fingertips: Sub-second search across petabytes of information can be as easy as running a Google search. Chronicle delivers threat-centered case management for simpler investigation and can surface the most relevant context to encourage consistently good decisions, which can enable teams to speed up investigation and response.

Fontline intelligence: We help democratize security operations with Google Cloud's expertise and best practices. Curated detections leverage Google Cloud's insights and threat intelligence gathered from protecting our billions of users so that organizations can focus their scarce expert resources on the unique security challenges that they face.

Automated response: Pre-packaged playbooks guide and automate responses to common security threats such as phishing and malware. Custom playbooks which can orchestrate hundreds of tools across security and IT can be built from a simple drag and drop interface.

Playbooks Offer:



Scalable and repeatable processes for incident response and triage, which are vital to analyst productivity.

Tribal knowledge capture. What's worse than trying to hire a new analyst? Having your most experienced analyst leave, along with the wealth of knowledge they have accumulated over the years, can deliver a big setback for the SOC. Playbooks put the wisdom of your most experienced analysts into the hands of everyone.

Faster analyst ramp-up. Step-by-step guidance on how to proceed with an investigation and clear escalation path enables new hires to essentially execute on day one.

8. Onward and Upward

Your marching orders have been set. If you're going to do one thing, speak up. Tell your supervisor how you feel. This should lead to adjusted expectations at the very least, and keep you better protected from your biggest stressors. If you're a leader and are sensing burnout is brimming among your troops, have a chat to gauge their mindset. And as we've told you, SIEM and SOAR are course-correcting technologies can result in faster, more thorough, and more informed investigations and responses for your SOC.

Shady syndicates have transformed cybercrime into a multi-billion-dollar enterprise. Yet the most nefarious threat of all that organizations face may be the well-being of their security team's psyche. Burnout is neither a badge of honor nor a bragging point. It only stands to further empower cybercriminals by making businesses weaker and more vulnerable to attack.

The good news is you can do something about it right now.

For more information about how Chronicle can help reduce you and your team's propensity to burnout, visit chronicle.security

Google Cloud

Additional Contributors:
Karlyn Borysenko, Zen Workplace
Amanda Berlin, Mental Health Hackers
John Toney, Agentive LLC