Burnout, Imposter Syndrome, Alert Fatigue

It's okay to not be okay.

Due to the ever-changing nature, repetitive procedures, and constant learning, it is possible to develop and experience Burnout and/or Imposter Syndrome. These are mental health issues that can lead to negative consequences on your professional and personal life. We're here to explain them, and suggest ways to help mitigate them.

PROFESSIONAL BURNOUT

What exactly is Burnout?

Also referred to as; SOC Burnout, Professional Burnout Syndrome, and Professional Burnout

In short, when humans do the same tasks over and over again, we get tired and bored, so we focus less. Obviously, this isn't good in any profession, but when the individual is a security professional, this slip in attention could be devastating for their organization if they miss something like an early sign of a compromise. Individuals suffering from burnout can become distracted, unfocused, and begin to dislike the work they're doing – even if they truly love their role. It's hard, and we're sure that every security professional has experienced this in some way during their career.

This can happen more often in organizations that have a mature security posture because there are fewer juicy security events and incidents to analyze as a result of good defenses and security controls. While incidents or suspicious events aren't good for the organization, they give analysts something to do instead of just responding to the same repetitive low-level events constantly, such as IPs scanning the organization, or users getting locked out of their accounts.

How can Burnout be addressed?

There are a number of ways to reduce burnout, but it's important to understand that it is extremely hard to prevent it completely, and it's crucial that management personnel understand and support their employees that suffer from burnout.

- **Job rotation:** This can vary depending on the size of the organization the individual is working for. If they have a large security function, it may be possible for the burned-out analyst to change their responsibilities within the SOC or their current team, and move to work on a different project – as this will refresh their brain and get them engaged again.
- **New projects:** Whilst similar to rotating the individual into a new position, simply adding new responsibilities or allowing them to take up work-related projects can help to break the habit of completing the same tasks, and boost their motivation and drive. Mini projects could include tool development, training and self-development, threat hunting, and enhancing automation where it is needed.
- **Strong relationship between management and employees:** Appraisal goes a long way. When a member of management shows gratitude to their subordinates, it boosts motivation and lets the individual know they're doing good, working to battle imposter syndrome and professional burnout. It sounds simple, but this will make the world of difference. If you're a manager, team leader, director, or anything in-between – thank your team members when they do something good, even if it's just a few words in-person or in an email.

IMPOSTER SYNDROME

What is Imposter Syndrome?

Imposter syndrome is when an individual feels like they aren't good enough at what they do, and that they don't belong. It has been described as the self-belief of intellectual fraud. Let's give two potential scenarios to ensure you understand what this is:

1. You're trying to break into the security industry, you're studying whenever you can to learn new concepts and tools. One day you're studying and you just feel overwhelmed by all the information you need to learn to be "good enough". You feel like you're getting nowhere, and that you'll never find your first job in information security.
2. You're already working in the cybersecurity (or any other!) industry, and one day at work you feel exhausted. You feel like you're not performing as well as you should, no matter how hard you try. You think that you got hired by accident and that someone better should have your position.

How can Imposter Syndrome be Addressed?

The first step to overcome this is to realize that you're not alone. A survey in 2018 showed that "62% of people at work in the UK" were affected by imposter syndrome, feeling that they're not intellectually good enough.

Whilst individuals could turn to medical professionals or private support, most workplaces will (or should) offer some kind of mental health support system for employees. If you're not currently employed, it's good practice to reflect on your weakness in a positive way to grow stronger and reduce the effect imposter syndrome is having. No one is perfect, and we can all grow.

SUPPORT

We spoke with Ryan Louie (MD, Ph.D.), who is a board-certified psychiatrist who spends time in the cybersecurity industry and produced a list of resources to support individuals that believe they're suffering from burnout or imposter syndrome.

Using RDP and SSH
How to Start Your Exam

- This resource is focused on the burnout of psychiatrists and other physicians, but it is directly translatable to the cybersecurity world – https://www.psychiatry.org/psychiatrists/practice/well-being-and-burnout/well-being-resources
- American Psychiatric Association's Workplace Mental Health site, which is a great starting point for mental health in all professions – http://workplacementalhealth.org
- CABA resources for overcoming imposter syndrome – https://www.caba.org.uk/help-and-guides/information/overcoming-impostor-syndrome

ALERT FATIGUE

While we're discussing mental health, we believe it's a good time to visit the topic of "alert fatigue", a psychological condition among security professionals that can have devastating consequences. Individuals working in the security industry, specifically SOC analysts, will experience this condition.

So what is alert fatigue? When you're investigating and responding to alerts every day you will eventually become desensitized to alerts that are high in volume and repetitive, such as external IP addresses scanning the organization, something that is happening all day every day. You're able to triage these events fast because you know exactly what to look for. Over time this can lead to assumptions being made, resulting in investigation steps being skipped, or no analysis being done and the alert just being closed or skipped. This is also prevalent with false positives, where the analyst will not pay as much attention to a "known false positive" however, one of these could be a genuine alert of malicious activity. Still, it doesn't get investigated properly because it has been labeled as a false positive, and therefore isn't important.

So how can we mitigate alert fatigue? Well, there's no easy answer. If you're working in the security industry and start to think you're getting into a bad habit of rushing through alert analysis or skipping steps. If the alert is assigned to you you're responsible for ensuring that the activity that generated the alert is not malicious. Remember your crucial role as a defender, and that one piece of missed information could have uncovered an intrusion or covert attack.

It's hard when we're in the cyber trenches, but take your time, and make sure everything looks good.

Previous Topic
Back to Lesson
Next Lesson