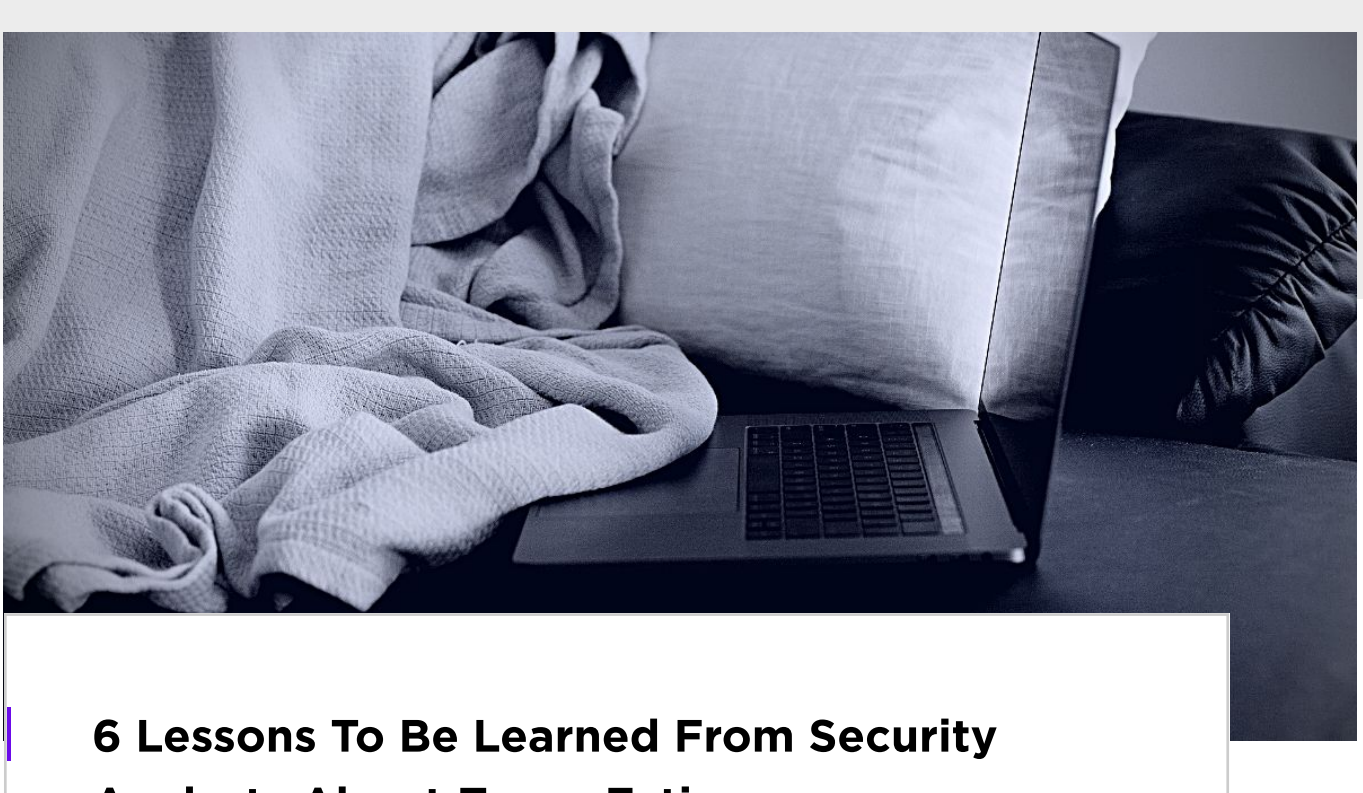

6 Lessons To Be Learned From Security Analysts About Zoom Fatigue

May 7, 2020
by Yotam Gutman

Have you been feeling tired and anxious lately? Sitting too long in a chair, glued to a computer screen? Welcome to the stressful world of working from home. Unlike what we may have imagined when tied to the office all day, working from home didn't turn out to be the utopian pleasure we'd dreamed of. Instead, many of us have found that having to juggle work and family and continue to be productive in a restricted workspace, cut off from our colleagues, is a real challenge. In addition, many have been feeling worn out due to the longer hours and more solitary nature of working from home and communicating with family, friends and peers via remote working software.

This is because the same technology enabling remote work and video-conferencing (Zoom, Teams and the like) is stress-inducing. There's even a name for this: Zoom fatigue, described as a feeling of exhaustion after a long day of video calls (By the way, this is not limited to Zoom and applies also to using Google Hangouts, Skype, FaceTime, or any other video-calling application or service).

There are several factors that contribute to this feeling: poor audio quality, the need to maintain eye contact with our counterparts and the ease with which we lose focus during video calls. In addition, we need to ensure our environment is clean, organized and quiet (which is no small feat for people working from small apartments with roommates or young kids).

All these stress-factors combine to drain our mental resources far quicker in video meetings than in real-life meetings.

There's More Than Zoom To Drain Your Brain

But the actual strain of working from home isn't limited to video conferencing. There's also the constant bombardment of notifications from email, WhatsApp, Slack, Zoom and similar remote working software, alongside "domestic disturbances" (such as kids knocking on the door or yelling in the adjacent room). In short, there's always noise, and never a dull moment. This erodes our ability to concentrate and respond quickly and accurately. And finally, many people find themselves working longer hours, on average, an additional two hours every day.

No wonder we feel overworked, on constant alert and just waiting for this period to pass.

Our New Normal Is An Analyst's Regular Day

The state described above is not unlike the day-to-day experience of security analysts. Working tirelessly in a stressful environment, security analysts are overloaded and understaffed. They know all about a similar kind of stress-induced fatigue: alert fatigue. Alert fatigue (a term coined by medical professionals) is now widely associated with passive detection and response security technologies. It causes stress, reduces productivity and, over time, leads to the psychological effects of depression and apathy. Obviously, these can greatly affect an analyst's ability to function properly and to remain in their position, which is one of the reasons that analysts suffer from significant burn and churn.

What Can Security Analysts Teach US About Dealing With Stress?

Analysts are not only required to function in this stressful environment, but their margin of error is far narrower than the average Work From Home employee. If an analyst misses an alert or responds in a sub-optimal manner, an organization could be breached. For most of us, the biggest risk in having an off-moment is likely to be no more serious than forgetting to join a scheduled call or someone seeing us in our pajamas.

Given the high-stakes involved in their work, analysts have come up with ways to deal with the pressure that enables them to cope and continue to operate at an optimum level, day in and day out. Perhaps we can borrow some of these methods and apply these to our WFH routine as well?

1. Divide and Conquer Your Tasks

On average, a modern SOC encounters hundreds of thousands of alerts everyday. It is impossible for humans to handle such massive amounts of incoming data, so analysts focus on the most severe alerts, and let machines handle the rest. For each case an analyst handles, they may have only a few minutes to deal with it. Focusing on the task at hand and setting aside competing demands on their time is a prerequisite skill.

The lesson to be learned here is that WFH is different from ordinary work. Your environment is likely filled with distractions, disturbances, and competing demands on your time. When we're in the office, we are typically 'quarantined' from our ordinary lives and other demands and worries until lunch time or after office hours. But our new WFH reality mixes and muddies our workspace with our home space, both physically and emotionally. In such a situation, you need to compartmentalize and prioritize just like a SOC analyst. Set aside *this* time for that, and *that* time for this, and so on. Within the times allocated, prioritize and focus on the tasks that are most essential.

2. Automate, Automate, Automate!

Whenever possible, alerts in a Security Operations Center are handled by an automated, predefined workflow. Given that the majority of security alerts are of low severity and mixed in with a number of false positives, this enables analysts to focus on the important stuff.

The lesson to be learned here is, when possible, automate or delegate menial tasks. There are many automation mechanisms available that can eliminate repetitive tasks. If you find yourself repeatedly typing the same response to certain emails, or endlessly copying structured data from one place to another, look into software that can set up scripts and hotkeys to reduce the toil of such tasks. Doing mindless, repetitive things is what computers were built for. Remember: your mental reserves are in short supply in times such as these, and mundane activities can drain them quickly.

3. Workflows – Define and Stick to a Plan

When an incident occurs, an analyst follows a predefined procedure or workflow. SentinelOne's Vigilance MDR team call this a playbook. Working from a playbook requires defining and categorising problems and then developing a procedure of steps to follow in advance depending on the circumstances. This reduces the need to think of an "attack plan" at the time of encounter, and it avoids endlessly "reinventing the wheel" for problems of a similar nature that you've dealt with before.

Try to have templates for everything that you can, from sales emails, to presentation and document templates. This is critical for having productive meetings, too. If the meeting has a well-defined agenda, many of the annoying aspects of video calls (like several people trying to speak at once) could be avoided.

4. Escalation – Pass It On, Move On

Analysts are divided into tiers. A lower-level analyst handles an alert up to a certain stage, and if he can't resolve it he escalates it quickly to a higher-level analyst or his manager. There's no shame or embarrassment involved in this; it is the normal protocol.

In a normal office environment, we are all used to holding on to problems and ensuring that we do everything possible to solve them. We all want to deliver and be seen as competent in our roles. But in the office we also have the support of people around us, of a familiar environment and trusted colleagues to bounce ideas off, tap for knowledge at the water cooler or point us to a case file buried in a locker somewhere. This invisible support is missing when we are working from home, and the temptation to hold on to a problem even though we may not have the resources to solve it is a hard habit to kick.

Employees working from home and who are cut-off from their peers and managers should communicate often with their colleagues and escalate issues to their superiors when the need arises. It will speed up the group's work and reduce stress.

5. Avoid the 'Always On Call' Mentality

It is essential to balance work and rest. Analysts work in shifts, often to provide "follow the sun" security coverage for their organization across the globe. But nobody can work at peak efficiency without proper rest and recuperation. When you're against the clock and desperate to solve a problem, things only get worse when you don't take a break.

Break your day into sessions and eat proper meals. This helps reduce the stress and increase focus. Work hard, but when your work is done, disconnect.

6. Don't Be a Slave to the Technology

Analysts have learned to make technology work for them. Gone are the days of ugly looking SIEM consoles where it was impossible to identify the acute alert. Modern management consoles are built to assist the analyst in responding quicker and more accurately. For instance, the SentinelOne console automatically groups hundreds of data points into correlated console alerts, showing unified alerts that provide a complete timeline of the incident. This reduces the amount of manual effort needed to investigate an alert.

Likewise, technology should assist those working from home. If the audio quality of your laptop is poor, buy a decent speaker or headphones. If the image quality is unclear, ensure your room is well lit and even invest in an external camera. And finally, use technology that's appropriate for the task. You don't have to use video conferencing for every communication, particularly when a phone call or email will do. For example, if a meeting only involves two or three people and does not include any visuals, why not leave the Zoom and simply make it a phone call? And if that's not practical, you can always turn off the webcam and go audio only. You are guaranteed a much better, less stressful experience.

Summary

We are all experiencing a stressful period, faced with new challenges that have demanded that we adapt quickly. But since this transition was so rapid, it has resulted in stress and ensuing fatigue for many of us, particularly if we do not possess the right tools and processes to be productive in this environment.

This is a great opportunity to learn from the people who operate under similar circumstances and learn from their experience. It's also a good opportunity to stop and appreciate the hard work these analysts perform every day in keeping us and our organizations safe.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Windows Security Essentials | Preventing 4 Common Methods of Credentials Exfiltration
- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022
- More Evil Markets | How It's Never Been Easier To Buy Initial Access To Compromised Networks
- 4 Steps Toward Successfully Measuring the Effectiveness of Your Security Controls
- Advancing Security | The Age of AI & Machine Learning in Cybersecurity