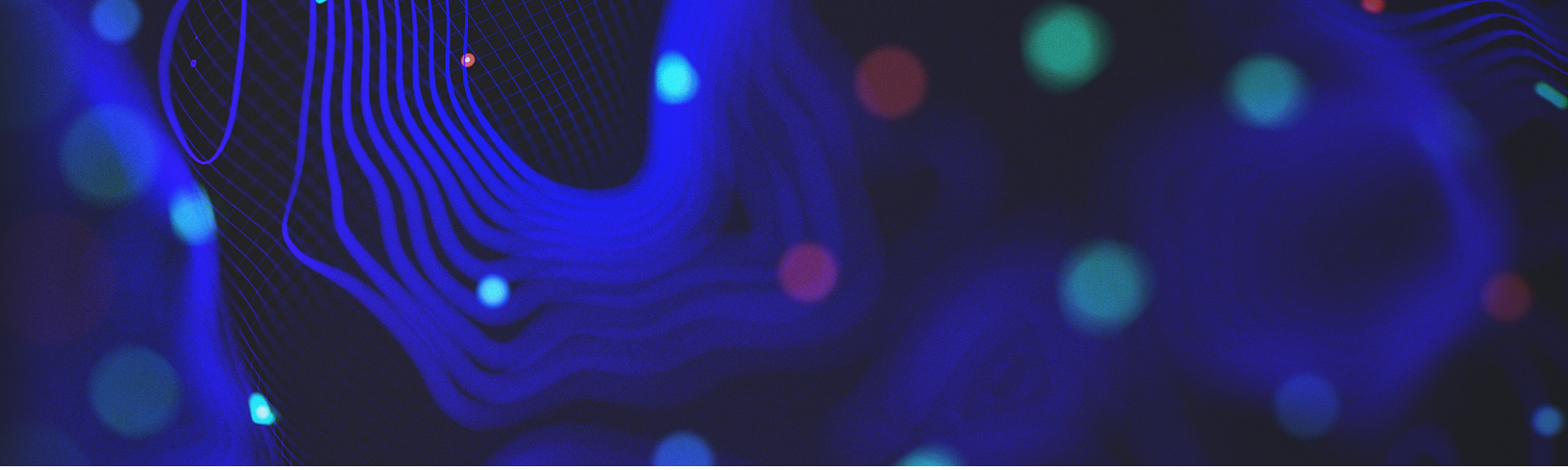
SentinelOne™

STOP THE CHURN, AVOID BURNOUT | HOW TO KEEP YOUR CYBERSECURITY PERSONNEL

WHITEPAPER

Contents



Introduction

According to recent research, the global cybersecurity workforce, currently estimated to be close to 3 million people, needs to grow by around 4 million or 62% in order to meet current demand. The shortage of cyber manpower has significant impact not only on organizations, which struggle to fill the ranks, but also security professionals, who have to cope with the pressures brought by understaffing. There are many indications that these professionals, who are in such high demand, suffer from stress, intensive workload and are likely to replace their current employer for a better paying job tomorrow.

Eight out of ten analysts say their SOC had experienced between 10% and 50% analyst churn in the past year. What are the reasons for these high churn rates, and what could a security manager do in order to combat this phenomenon? Let's take a look.

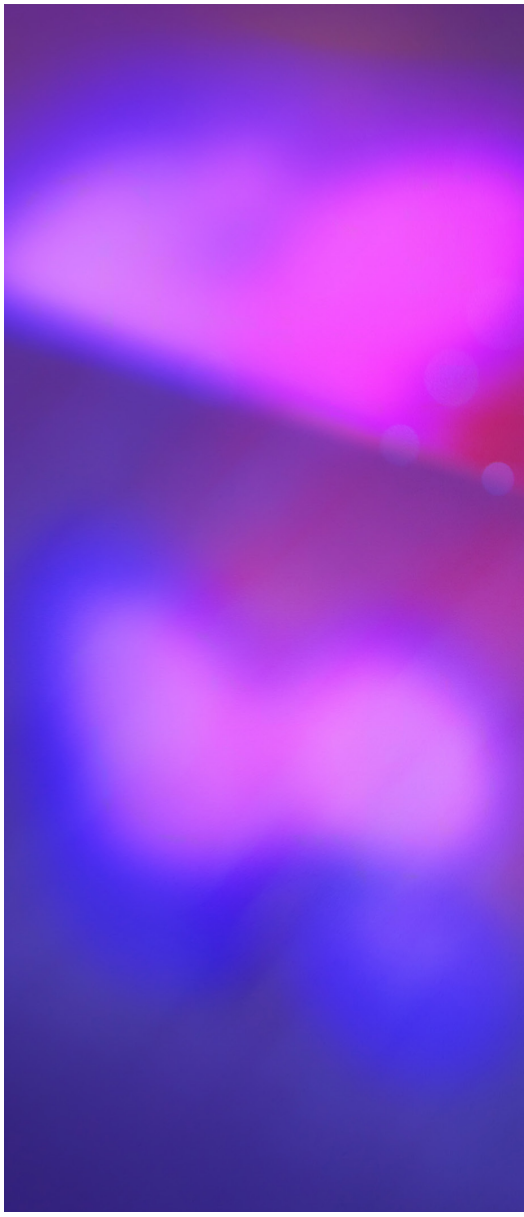
Security is a **Stressful Profession**

In a survey covering the first 6 months of 2019, some 1500 of 6000 (25%) cybersecurity professionals said their organization had been the victim of a data breach, and 2160 (36%) of those who had not been breached believed their organization could currently be facing a breach without their knowledge.

In the light of such pressures, it's perhaps not a great surprise that almost half (49%) of those surveyed reported that they are kept awake at night worrying about their organization's cybersecurity.

On top of worries about imminent threats, staff also report that a lack of security awareness among their organization's staff in general and a lack of buy-in regarding security best practices at the executive level contribute to increasing stress. Of major concern to cybersecurity professionals is that it is more often than not C-Suite executives that are most likely to disregard security safeguards, the very people most likely to be targeted in spearphishing and advanced threat actor attacks.

Increased Workload Due to **Lack of Manpower**



66% of respondents claim that the cybersecurity skills shortage has resulted in an increased workload on existing staff. Since organizations don't have enough people, they simply pile more work onto those that they have. This leads to human error, misalignment of tasks to skills, and employee burnout.

69% of organisations say their cybersecurity teams are understaffed, and 17% of professionals said that they had considered leaving their current position due to a lack of resources.

The average enterprise SOC encounters anything between 10,000 and a million alerts per day. Many of these alerts are false positives. One survey found that more than half of respondents reported a rate of 50% or higher. Most now say they spend the majority of their time trying to manage the high volume of alerts.

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 effect an employee's will to remain in their position.

What Can You Do To Retain **Your Cybersecurity Staff?**

The cybersecurity profession is fairly new, and it lacks a common, industry-wide, professional framework for career progression. However, there are still a wide-variety of respected certification programs, training courses and skills development platforms, not to mention an increasing number of hacker/security cons where training courses are often run alongside the presentation of papers and products. Despite the wealth of available resources, nearly half of surveyed SOC analysts say they get 20 or fewer hours of training per year.

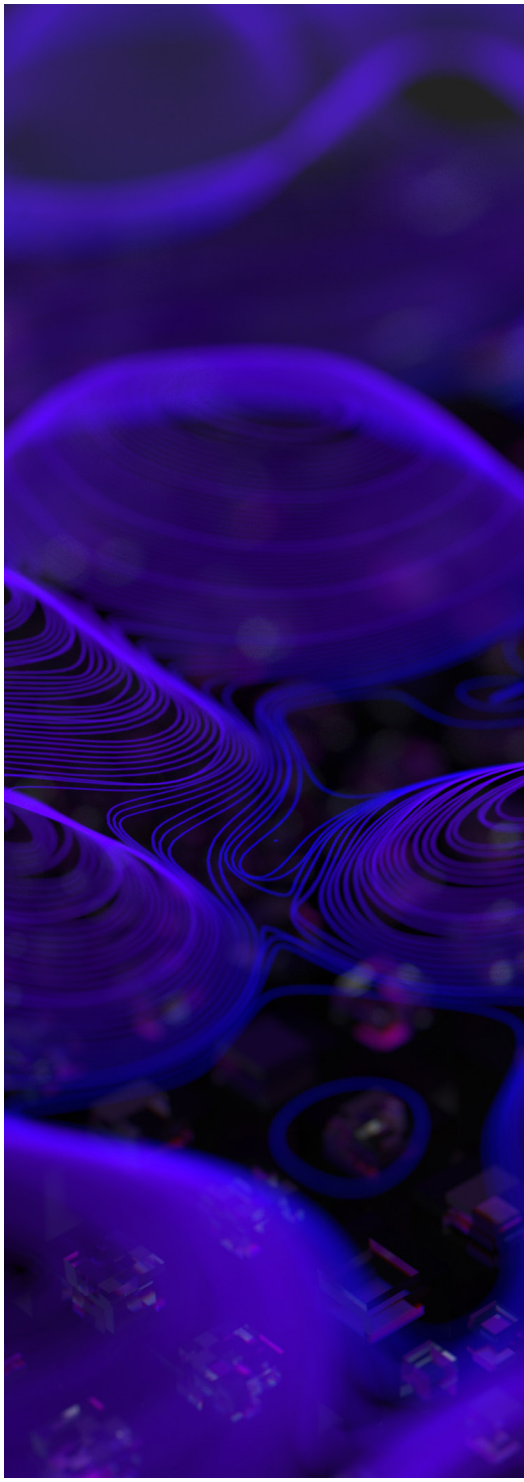
Invest In Skills To Keep **Your People, & Improve Enterprise Security**

Organizations would be wise to invest in building their teams' professional knowledge. This could be achieved by periodic training at Cyber-ranges, tabletop exercises or on-prem simulations. Allowing staff to attend professional lectures and encouraging the consumption of professional materials like reverse engineering training and threat intelligence is also a great way to invest in skills.

In some quarters, managers fear that investing in employee training only equips the employee to move on to a more lucrative job elsewhere. Viewed in that light, training can be seen as a cost rather than an investment. The facts, however, suggest otherwise. The main factors employees state for being happy with their current employer is that they are valued by management, constantly challenged to improve their skills, and prefer to advance in position rather than start out somewhere new.

Investing in skills doesn't just have the pay-off of stemming churn in your SOC either. It means you're actively improving the knowledgebase and in-house talent you already possess, which naturally makes a huge contribution to improved organizational security.

Educate Your Business – **“Security Aren’t The Bad Guys”**



Security analysts are people, and they work with, and provide services to other employees. For a long time, IT security people were perceived as the “bad guys” - technocrats whose interest in securing the organization outweighs their affection for their peers. How else can you explain their demand that you change your password every two weeks, and that they make you come to them to release a file your client has sent you?

Educating the broader workforce on the importance of cybersecurity, and the fact that these cyber-practitioners are actually securing the entire organization, will go a long way to boost their morale and sense of value to the organization.

Smarter Tech Works **For Everybody**

Security managers should invest in implementing the necessary procedures and tools to increase automation, reduce menial work and lower the frequency of alerts. Also, replacing older tech with modern security tools will give analysts professional satisfaction – they now work with the best tools in the business, and a modern UI is so much easier to work with, improving productivity and reducing frustration.

Conclusion

Reducing attrition should be an organizational task. It is tempting to think that technology alone will solve the issue, but it won't. People are the backbone of the security organization, and will remain such for many years. But given the scarcity of human resources, organizations must ensure that their people are utilized in the best way possible – meaning they are not wasting time chasing false positives or implementing difficult to use products. The people who are already employed must be well trained and equipped with the best tools to allow them to focus on the severe threats the organization is facing. They should also be appreciated throughout the organization. These actions will go a long way to reducing cybersecurity staff churn and improving efficiency and well-being within the business.