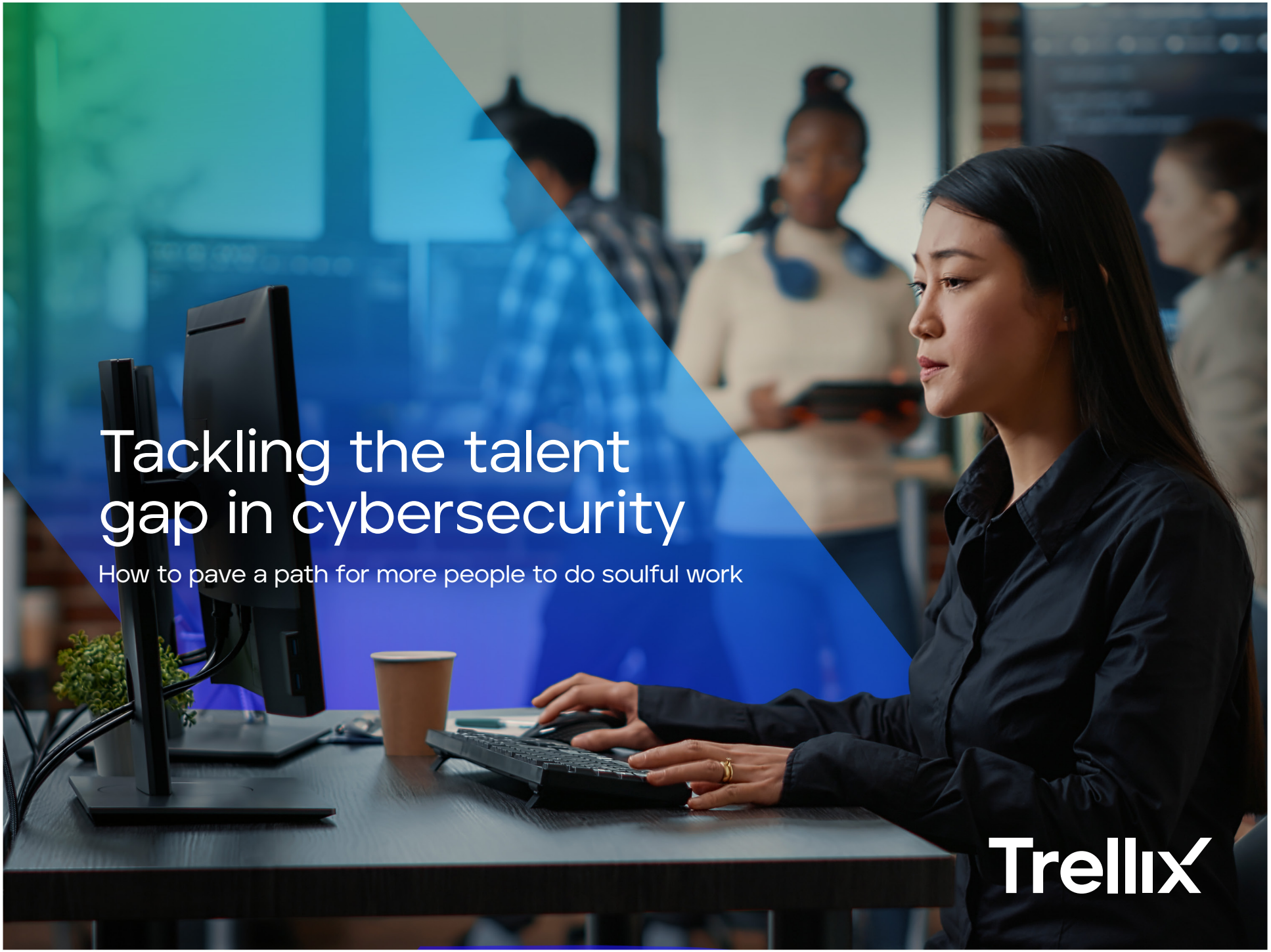

Tackling the talent gap in cybersecurity
How to pave a path for more people to do soulful work
Trellix

What do we mean by soulful work?

At Trellix, we talk a lot about how cybersecurity is soulful, meaningful work. Why?

Because cybersecurity is all about protecting people. Defending individuals from having their information stolen in a data breach. Warding off attacks to keep a country's power grid up and running. Guarding nonprofits and allowing them to safely process donations. Preventing hackers from shutting down vital medical services or accessing voting systems.

Cybersecurity professionals are the unseen heroes who keep the inner mechanisms of our society humming.

But our industry is at a crossroads: Our demand for talent far exceeds our supply. Our inability to attract and retain qualified employees, our lack of diversity, and the challenging nature of security operations only widens this gap further.

There's no simple answer to this problem. But in the pages that follow, we're going to discuss some solutions. We believe that by paving a path for more people to do soulful work—and giving security professionals the tools they need to make that work less stressful—we can close the talent gap once and for all.

—Bryan Palma, CEO, Trellix

The great cybersecurity skills gap

We've had a shortage of cybersecurity skills for years—so what's different now?

The demand for security analysts, engineers, researchers, and consultants has always been greater than the supply. But the costs of the skills gap are becoming too much to bear. The frequency and volume of cyberattacks are on the rise, and the impact of those attacks has increased.

In 2021, companies experienced 270 attacks on average—a 31% increase from the previous year.[1] The average cost of a single data breach? $4.24 million.[2]

Despite the high demand for cybersecurity skills, the gap only continues to grow across all industries around the world. And it's not just the private sector. In the US federal government alone, there are an estimated 35,000 openings for cybersecurity professionals.[3]

1. The state of cybersecurity resilience 2021, Accenture, November 2021 2. Cost of a Data Breach Report, Ponemon Institute, 2021 3. Even the government's premier cybersecurity bureau has a talent acquisition challenge, Federal News Network, November 2021 4. Cybersecurity Skills Crisis Continues for Fifth Year, Perpetuated by Lack of Business Investment, Business Wire, July 2021

A lack of diversity

For years, the industry has failed to tap into more diverse groups to fill its job roles.

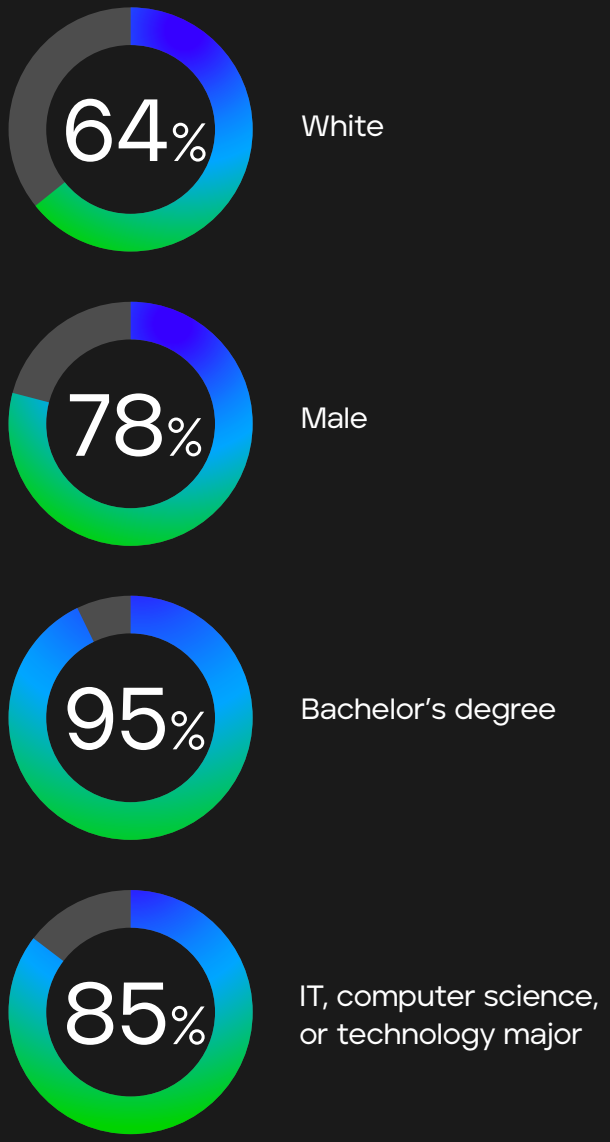
In Europe and North America, cybersecurity is dominated by straight white males. People of color, nonbinary people, and people from the LGBTQ+ community are massively underrepresented.

The workforce is also slanted towards four-year degrees, excluding qualified people who may lack the schooling but have earned certifications or completed other vocational training.

Today's threat actors have no such diversity problem.

They come from different backgrounds, cultures, and countries. And they approach problems in creative—yet malicious—ways. To defend more effectively against threats, the cybersecurity workforce should be as diverse and inclusive as threat actors.

Today's cybersecurity workforce[5]



5. Trellix Cybersecurity Skills Research, Vanson Bourne, May 2022

Stress and attrition in the SOC

Our industry is also suffering from overwhelming attrition. A career in cybersecurity can be meaningful and rewarding. But it can also be extremely challenging and demanding. Regardless of industry or company size, many cybersecurity employees face long hours and constant stress.

Day-to-day security operations are difficult enough. The global shortage of cybersecurity skills has only added to the pressure security professionals are feeling.

The top three impacts of the skills shortage[6] are:

1. Increased workload on existing staff
2. New security jobs remain open for weeks or months
3. High burnout and/or attrition among cybersecurity staff

Technology plays a key role in worker stress, for good and ill. Today's SecOps employees have to deal with a constant barrage of alerts, and they struggle to detect attacks across vectors because their tech stack is fragmented between different tools. They often lack the capabilities to proactively detect and respond to incidents.

Ultimately, work-related stress is driving people out of the profession. In fact, 62% of enterprises report difficulty retaining qualified security professionals.[7]

6. The Life and Times of Cybersecurity Professionals 2021, ESG, July 2021 7. State of Cybersecurity 2022: Global Update of Workforce Efforts, Resources and Cyberoperations, ISACA, 2021

What's on their minds?

SOC MANAGER

- Unifying siloed tools
- Hiring qualified staff
- Balancing tech needs with budget

SECURITY ANALYST

- Freeing up time
- Reducing alert fatigue
- Minimizing repetitive tasks

SECURITY ENGINEER

- Avoiding burnout
- Staying up to date
- Gaining more visibility

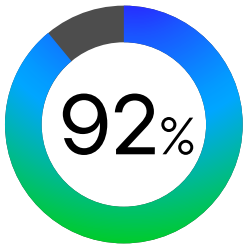
Putting people at the heart of cybersecurity

> Employees deserve more from their workplace, especially during the Great Resignation. We are investing in our people to build the premier home for diverse, cybersecurity talent."
>
> —Michael Alicea, Chief Human Resources Officer, Trellix

Filling the cybersecurity job gap requires a fundamental shift in mindset and willingness to rethink the future of meaningful work.

As part of the job market shift, employee expectations have changed in the last couple years. Huge numbers of tech professionals are leaving their jobs in search of more soulful work. People want work that offers them a higher purpose and the chance to do something positive with their skills.

There are workers from a variety of backgrounds who would thrive professionally in cybersecurity while also finding personal fulfilment. As employers begin to put people at the center of security practices, they can increase diversity and attract smart, passionate professionals into our industry.



of security professionals believe that more mentorships, internships, and apprenticeships would encourage **more people from diverse backgrounds** to enter cybersecurity[8]

8. Trellix Cybersecurity Skills Research, Vanson Bourne, May 2022

Investing in our cybersecurity future

Cybersecurity education and training isn't just a problem for government agencies and global enterprises. It's an issue that requires a range of solutions, including public-private partnerships.

According to a recent survey we conducted, there are three key areas that would inspire more people to work in our industry: raising awareness of cybersecurity careers (43%), encouraging students to pursue STEM-related careers throughout the education process (41%), and providing further funding support (39%).[9]

That's why we need to:

Transform our current K-12 educational system

Let's expose kids to cybersecurity at an earlier age. By creating age-appropriate cybersecurity curriculums beginning in kindergarten, we can encourage more children—of different backgrounds—to pursue STEM-related careers in the future. This would go a long way toward breaking down social, economic, and diversity barriers in our largely homogenized industry.

Increase college scholarship funding

Let's increase scholarship funding and internship programs, particularly at historically Black colleges and universities, liberal arts schools, and community colleges. This would enable more female and minority students to take advantage of academic opportunities and sharpen their cybersecurity skills. And for the industry itself, it would mean a larger, more diverse talent pool that better represents the population.

Create a national cybersecurity corps

Let's launch a federal cybersecurity corps in the United States. When it comes to training cybersecurity practitioners, the United States is at a major disadvantage. Other countries rely on compulsory service to develop their people's cybersecurity skills at scale. The United States needs its own program—in the mold of AmeriCorps—to provide entryways to cybersecurity for young adults who lack higher education.

9. Trellix Cybersecurity Skills Research, Vanson Bourne, May 2022

Building a diverse talent pipeline

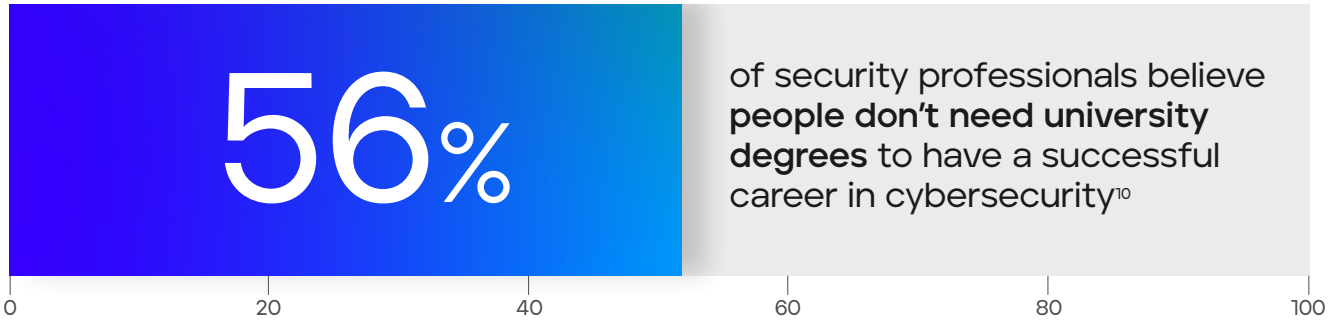
A direct line from college to cybersecurity shouldn't be the only path for professionals. We need to be open to hiring and mentoring new talent who may be well qualified but not hold a four-year degree. We also need to create avenues for early- and mid-career professionals looking to move into our industry.

With better access to cybersecurity programs at the community college level, more graduates would have the chance to join us in our industry. By extending internship opportunities to undergraduates, people entering the workforce with only their associate's degree would have the hands-on experience necessary to thrive in cybersecurity.

Early-career professionals with just a high-school diploma? They could flourish in our industry, too. Combining their passion for protecting people with the proper mix of vocational training is a surefire recipe for cybersecurity success.

Our industry would also benefit from more experienced professionals seeking to make a career change, whether from a different field like marketing or healthcare or an adjacent one like social media, computer science, or IT. By making certification programs more widely available, we could ease the transition for these individuals, providing them with the training they need to quickly reskill.

Are we too focused on hiring candidates with degrees?



10. Trellix Cybersecurity Skills Research, Vanson Bourne, May 2022

Committing to diversity in cybersecurity

To increase diversity and tackle our talent shortage, we all have to do our part. One way we can overcome our current challenges? Building programs specifically aimed at creating a steady stream of talent to flow into our industry.

By partnering with nonprofits, businesses can donate their time, money, and expertise to truly make an impact.

Here's how Trellix is lending a hand:

Disrupting gender imbalance with Gotara

Trellix is working with **Gotara**, a global career growth platform for women in STEM+. Through a series of development experiences—including hands-on and personalized opportunities guided by Gotara's STAR Program advisors—we're combating unconscious bias and empowering women to navigate and grow their careers.

Supporting Latinos' careers with HACE

More recently, Trellix partnered with **HACE**, the Hispanic Alliance for Career Enhancement. Aside from a financial commitment, we're providing expert trainers, developing content, and cosponsoring a cybersecurity accelerator program. The program is focused on equipping Latinos with a combination of soft skills—like communication and leadership—and hard skills related to cybersecurity.

With more organizations building internal programs committed to diversity, equity, and inclusion, our industry is primed for a huge resurgence—one where a variety of fresh perspectives propels us forward.

> Closing the cybersecurity talent gap is not only a business imperative, but important to national security and our daily lives. We need to remove barriers to entry, actively work to inspire people to do soulful work, and ensure those in the field are retained."
>
> —Bryan Palma, CEO, Trellix

Looking ahead

There's a clear path forward to solving our lack of diversity and overcoming our talent deficit. It involves attracting more bright individuals across genders, races, ages, ethnicities, and orientations. It includes enticing more skilled workers in search of more purposeful careers and more fulfilling lives.

By creating pathways for people from diverse backgrounds and equipping SOC employees with the tools they need to make their jobs and lives easier, we can meet the moment. But it's going to take all of us working together to reach our goal.

Retooling the future

As the volume of cyberthreats rises and SOC resources become more strained, smart organizations realize they can't simply hire more staff. No business can scale their cybersecurity operations or curtail stress with people alone. They need the right tools, too.

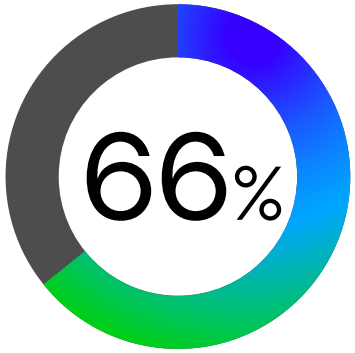
With a powerful XDR platform, organizations large and small can reduce staff workloads, helping their employees do their jobs more efficiently and effectively. How?

Consolidating security solutions

XDR brings together multiple security solutions in one place. Endpoint, email, network, cloud—they can all be seamlessly connected. This provides SOC teams with a complete picture of their security ecosystem, so they're better equipped to adapt and protect their entire attack surface.

Automating workflows

Powered by AI and machine learning, XDR helps enhance human expertise. Increased intelligence makes it easy to not just quickly detect threats but predict attacks. It even helps automate responses in real time and orchestrate remediation activities. In other words, XDR works around the clock so employees don't have to.



of surveyed organizations are consolidating their SecOps tools[11]

11. ESG Research Report, SOC Modernization and the Role of XDR, May 2022

Providing embedded expertise

The right XDR platform comes jam-packed with defensive playbooks with recommended tactics and countermeasures. Best-in-class intelligence and expertise are built right into the ecosystem, giving SOC teams all the insight they need to make the right cybersecurity decisions—before, during, and after an attack.

XDR makes soulful work simpler. For security managers, analysts, and engineers alike, XDR means unifying disjointed tools for greater visibility. It means automatically correlating and prioritizing threats across entire security environments. It means enabling guided investigations and SOAR workflows to take on end-to-end attacks.

And with their processes streamlined, employees are no longer bogged down by tedious manual tasks that increase stress and lead to attrition. The talent gap is being bridged—and more cybersecurity professionals are finding purpose in the work they do every day.

> SecOps teams are calling on the industry for a new approach to combat the challenges posed by increasingly hostile behavior across multiple attack vectors and the shortage of skilled talent."
>
> —Aparna Rayasam, Chief Product Officer, Trellix

Share your #SoulfulWork story

If there's one thing everybody in our industry can agree on, it's this:

We do soulful work.

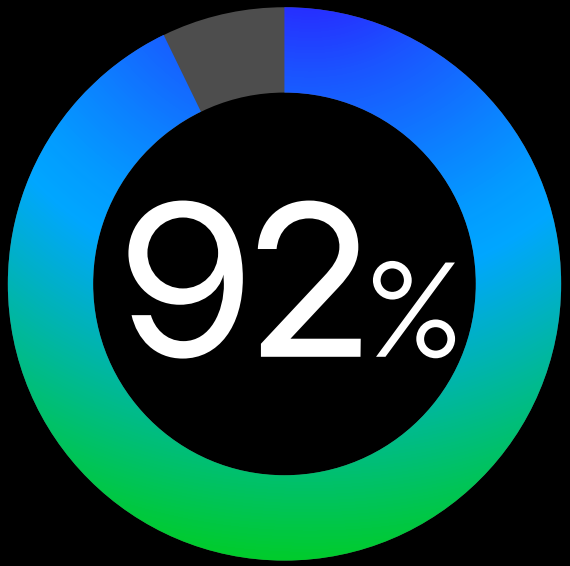
As SOC managers, analysts, and engineers, every one of our daily activities revolves around protecting people and keeping public and private organizations, essential infrastructure, and vital information safe.

Our role in contributing to the greater good of society is why many of us pursued cybersecurity in the first place. And it's one of the primary factors that keeps us working in this field. According to our research, 92% of security professionals agree that cybersecurity is purposeful, soulful work that motivates them.[12]

By amplifying the message that cybersecurity is the home of meaningful, soulful work, we could attract countless smart, capable people in search of a higher calling, helping us solve our lack of diversity and tackle our talent gap.

Visit our site to share your #SoulfulWork story—and inspire the next generation of cybersecurity talent.

12. Trellix Cybersecurity Skills Research, Vanson Bourne, May 2022



of security professionals agree that cybersecurity is **purposeful, soulful work** that motivates them[13]

Trellix

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.

13. Trellix Cybersecurity Skills Research, Vanson Bourne, May 2022

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com