SANS | GIAC CERTIFICATIONS

EY's Secret to Success:

Building High-Performing Cybersecurity Teams with Unconventional Talent

Anthony Switzer
Cybersecurity Leader at EY

The cybersecurity talent landscape presents a unique paradox: while demand for skilled professionals continues to surge, traditional hiring approaches often overlook promising candidates with the aptitude to thrive. For Anthony Switzer, a cybersecurity leader bridging offensive and defensive operations with enterprise risk, success lies in looking beyond conventional qualifications and prioritizing curiosity, adaptability, and diverse perspectives.

Switzer shares, "I find some of our best people in cybersecurity come from other career fields, particularly engineering or psychology," He narrates the story of one of his team's most skilled attackers, who comes from a chemical engineering background. "His experience with detailed technical writing and his ability to understand and apply complex scientific papers have proven valuable in cybersecurity engagements." This success story serves as a beacon of hope for professionals considering a career transition into cybersecurity.

Continuous Learning Culture

At the heart of Switzer's talent strategy lies a deep understanding of what drives cybersecurity professionals. "When hiring cybersecurity professionals, you need to look for people with a deep sense of curiosity," he explains. "Just as physical health requires nourishment, cognitive engagement beyond daily tasks is essential for peak performance."

This understanding shapes everything from hiring practices to professional development opportunities. For Switzer, cybersecurity success requires more than technical skills—it demands a commitment to continuous learning and growth. He encapsulates this philosophy in his "three by six squared" rule: "It means studying three to six hours a night, three to six nights a week. The intensity is higher when you start and decreases as your career advances, but it's essential to stay up with the latest trends." This principle has become fundamental to Switzer's approach to talent development, helping candidates understand from the outset that cybersecurity is a dynamic field that requires continuous adaptation and learning to stay effective.

The Power of Perspectives

Switzer's team has achieved notable outcomes by embracing different thinking and working methods. Through a neurodiversity-focused initiative within the team, they brought in a team member who demonstrated exceptional web application penetration testing skills. In one striking case, this team member identified ten security findings during a single engagement. "He has excelled in this role, combining natural curiosity with attention to detail and the ability to dig deep," Switzer notes. This demonstrates how different approaches to problem-solving can uncover vulnerabilities that might otherwise go undetected.

This principle extends to how Switzer structures his team's work. Rather than always relying on experienced team members, he deliberately puts junior staff in leading roles during security assessments. "When I look at the execution of identifying a potential exploit or an alternate path, I try to let the most junior person lead because they bring a fresh perspective, unencumbered by prior assumptions," he explains. This approach serves multiple purposes: it helps identify security gaps experienced professionals might overlook due to ingrained habits while simultaneously developing junior talent and building their confidence.

"I think a lot of it comes down to how individuals approach problem-solving and connect complex ideas," Switzer explains. "Bringing in someone who sees the world a little differently helps. We've seen that diversity of thought contributes to success, especially when trying to attack or break into a network."

He describes his penetration testers as "assumption validators"—professionals who challenge established thinking and find ways around presumed security measures. By combining different perspectives and experience levels, the team becomes more effective at identifying and addressing security vulnerabilities.

Navigating Recruitment Challenges

Finding the right cybersecurity talent requires looking beyond traditional recruitment methods. “Much of it comes down to networking,” Switzer explains. “Getting to know people in the community—those who may know someone with curiosity and potential.” This network-based approach helps identify candidates who might not appear ideal on paper but possess the right aptitude and drive to succeed in cybersecurity.

> **“I have a ‘three by six squared’ rule for people entering cyber-security. It means studying three to six hours a night, three to six nights a week. This is essential to stay up with the latest trends.”**

Effective collaboration between cybersecurity leaders and HR presents an opportunity to strengthen the talent pipeline. “In some cases, recruiters may naturally lean on predefined criteria when reviewing resumes, but it’s challenging to assess someone’s aptitude and drive to succeed from a resume alone,” Switzer notes. While feedback is regularly shared after candidate interviews, Switzer emphasizes that ongoing, structured collaboration through regular meetings helps better articulate the attributes and capabilities being sought—especially for cybersecurity roles that demand curiosity and adaptability.

The challenge is particularly acute when hiring for consulting roles requiring technical expertise and client-facing skills. This rare combination of technical and soft skills is difficult to find, prompting Switzer to emphasize the importance of being upfront with candidates about what success requires. Rather than focusing solely on technical qualifications, the team evaluates candidates’ willingness to learn and adapt. This approach has led to successful hires from various backgrounds, though Switzer acknowledges that hiring remains competitive in today’s market. The key, he suggests, lies in looking beyond immediate technical skills to identify candidates with the right combination of aptitude, communication skills, and commitment to continuous learning.

Certifications Drive Success

Professional development takes multiple forms within the team Switzer leads, with certifications playing a particularly vital role. “Certifications give the confidence or set the expectation of an individual’s knowledge,” Switzer explains. However, the value of certifications extends beyond individual knowledge validation. Switzer sees certifications as strategically valuable—not only for personal development but also for broader team effectiveness. For his team members, certifications provide structured paths for expanding their knowledge and expertise. In some cases, certifications also help reinforce client confidence in team capability. The investment supports both individual career growth and broader engagement outcomes. Switzer shares that certifications have, at times, influenced clients to advocate for his team during selection processes.

Beyond certifications, the team Switzer supports applies various retention strategies. These include structured break periods in summer and winter to promote meaningful time away from work and health and welfare bonuses that can be used to support mental and physical well-being. In some cases, supporting high-performing talent requires adapting quickly. Switzer shares: “Keeping up with high performers is all about growth—ours and theirs. It requires us to continually evolve how we support and challenge them.” His team emphasizes flexibility in its development programs, ensuring that high-performing individuals have opportunities to grow and take on new challenges.

Seeing Potential in People

Looking ahead, Switzer sees cybersecurity evolving toward greater business integration. “When I look at cybersecurity, I still consider it a young sector—still maturing compared to more established IT disciplines in business integration,” he observes. This evolution requires building both technical depth and business acumen within the team.

For Switzer, success in addressing the cybersecurity talent challenge ultimately comes down to seeing the potential in people rather than focusing on predefined requirements. “When hiring, I focus on the person—their mindset, adaptability, and potential—rather than trying to make them fit a rigid job description,” he explains. “Skills can be taught, but curiosity, discipline, and adaptability are harder to find. When I meet someone with those traits—even in a different domain—I ask whether their strengths could thrive in this one.”

This Case Study is Just the Beginning – Download the 2025 Cybersecurity Workforce Research Report for More Insights!

This case study is part of the *2025 Cybersecurity Workforce Research Report* published by SANS | GIAC. Informed by international survey results, the report delivers key insights on how HR and Cybersecurity Managers can collaborate to successfully build high-performing cybersecurity teams.

Download for More Insights

SANS | GIAC CERTIFICATIONS

EY