CSaaS SIG
An IT ISAC Community

AI Will Solve the Cyber Skills Crisis

Product of the IT-ISAC Critical SaaS Special Interest Group (CSaaS SIG) with contributions from:

David Bradbury
David B. Cross
Jeffrey DiMuro
James Dolph
Kaitlyn Palatucci
Dhaval Parekh
Akshay Shetty

SEPTEMBER 2025

INTRODUCTION

Artificial Intelligence (AI) has evolved rapidly over the past few years, advancing into a ubiquitous and accessible tool used across industries. AI use has proliferated rapidly especially within the information technology and Critical Software as a Service (CSaaS) sectors, where it has become ingrained into all aspects of the job – from coding and development, to tech support and business operations. As AI models become more sophisticated, their integration becomes increasingly inevitable and invaluable, further powering automation, streamlining processes, and enabling new levels of scalability. Yet, contrary to popular fears, AI is not here to replace workers, although some jobs will be lost due to AI. Instead, it is a powerful tool that reshapes the nature of work itself, as it augments human abilities, creating new roles that require a mix of both technical and adaptive skills.

Concerns about AI-driven job displacement remain widespread, particularly in fields that are highly susceptible to being revolutionized by AI automation. However, the emergence of AI also presents unprecedented opportunities for organizations to innovate and for employees to upskill and pivot into new, emerging roles. Nowhere is this more apparent than in the cybersecurity industry. As of August 4, 2025, there were over 500,000 open cybersecurity-related positions in the United States alone. This talent gap represents a significant opportunity: by equipping workers with AI-driven tools and training and adapting to these ongoing changes, we can close the gap and build a more resilient cyber workforce.

CLARIFICATION ON AI'S ROLE: AUGMENTATION, NOT REPLACEMENT

It is crucial to address a potential misinterpretation of the statement "AI will solve the cyber skills crisis." This is not an argument for workforce reduction; rather, it's a framework for workforce multiplication. The challenge in cybersecurity is not a surplus of talent, but a staggering deficit, with potentially millions of needed roles worldwide. AI's primary role is to act as a powerful force multiplier, enabling the existing and incoming talent to operate at a higher level, more rapidly.

The goal is to foster human-AI cooperation. Think of it as elevating talent, not eliminating it. For instance, AI can automate the repetitive, high-volume tasks that currently consume a significant portion of a security analyst's day, such as basic log monitoring, running tedious data analysis or writing time-consuming summary reports based on cases or alert resolution. This frees up human professionals to dedicate their time to more valuable and complex work like strategic planning, threat hunting, SecOps automation, and innovation. Tasks that require uniquely human skills, such as critical thinking and creativity.

This dynamic will transform career trajectories. For example, by providing intelligent assistance, AI can help a junior SOC analyst perform tasks that were once the domain of a seasoned expert, effectively accelerating their journey from a level 1 to a level 3 SOC analyst. The objective is not to replace the analyst but to make them more effective and capable, faster. Ultimately, this approach is about building a more resilient and capable cyber workforce by enhancing human abilities, not making them obsolete.

IMPACT TO DIFFERENT CAREER STAGES

The insurgence of AI in the technology and software sector provides both opportunities and challenges to students and early-career employees alike. As these tools become more widely available, early-career professionals can position themselves for success by broadening their education to include skills in AI handling. These skills can also serve as a stepping stone and a major differentiator, making it possible for analysts to achieve more, faster. For instance, AI assistance can transform a SOC analyst by accelerating their threat detection capabilities, decision-making, and data analysis.

However, the increase of AI technology will also lead higher education institutions to rethink their strategies. Entry-level education models may no longer suffice, especially in sectors such as cybersecurity, where lower-skilled (manual) tasks may become automated by AI tools and agents. Curricula must still embrace the fundamentals, but those that go beyond the basics and incorporate hands-on experience with AI-driven tools will be prioritized. Otherwise, graduates risk being underprepared in a market that now values adaptability, AI fluency, and the ability to work collaboratively with these tools from day one.

AI is revolutionizing the IT industry by reshaping roles across every career stage, creating both challenges and opportunities for professionals. For early-career professionals, success lies in pursuing interdisciplinary education and focusing on flexible and evolving areas such as AI ethics, user experience, and cybersecurity. Individuals must gain hands-on experience with AI tools to remain competitive in a job market where traditional entry-level roles are becoming increasingly scarce. Educational institutions and skilling programs must adapt their strategies to better align with the AI-enhanced workplace. For mid-level professionals, AI can help enhance efficiency, broaden technical knowledge, and expand responsibilities. Mid-level roles are also evolving to include collaboration with AI systems for process automation and workflow optimization. Embracing AI at this stage better positions these professionals for future leadership roles.

Experienced professionals, who bridge technical execution and organizational strategy, can leverage AI to transition into more strategic roles, such as leveraging AI for advanced threat modeling, automating compliance, and mentoring junior staff more effectively. At the advanced level, AI accelerates the shift from tactical oversight to executive leadership, enabling senior professionals to focus on predictive risk management, AI governance, and other strategic initiatives. Across all levels, adaptability and continued learning are key to thriving in the AI-driven IT landscape.

ROLES (NEW AND OLD) UNDERGOING TRANSFORMATION

AI is rapidly transforming jobs, particularly those centered around repetitive or routine tasks. Roles such as data entry, help desk support, customer service, and cybersecurity monitoring are especially well-suited for automation. These positions often involve predictable, rules-based processes that AI excels at handling, allowing for increased efficiency and accuracy. However, this does not mean these jobs will disappear – rather, that they are evolving.

As AI handles the repetitive load, many traditional roles are being elevated in scope and value. For example, a cybersecurity analyst no longer needs to sift through logs all day manually; with AI assistance, they can focus on proactive threat hunting and strategic security planning. Similarly, customer-facing security roles can utilize AI chatbots to handle straightforward queries, thereby freeing them to address more complex issues that require a human. This shift empowers security professionals to engage more deeply in creative problem-solving and collaboration across teams and departments.

UPSKILLING FOR MID-CAREER EMPLOYEES

Upskilling for mid-career professionals is critical in ensuring they remain competitive in an AI-driven workplace. Unlike early-career employees, mid-career workers often possess industry or business expertise but may need to adapt by acquiring AI-related skills such as data analysis, machine learning basics, or AI tools relevant to their field. Additionally, AI-driven insights and training can support lateral movements, such as moving from operations to data-centric roles, which require a combination of technical understanding and business acumen. This adaptability will sustain career growth and also enables current experienced employees to thrive in leadership roles shaped by AI innovation. In addition, AI enables professionals at the mid-career level to rapidly provide insights, allowing them to research and develop plans and strategies based on their experience and knowledge. These insights are crucial for analyzing and submitting the right training data to achieve the desired outcomes.

TURNING AI INTO A CAREER ACCELERATOR

AI is no longer a distant concept as we all have witnessed - it is your new work partner, and it won't be going away anytime soon. Instead of shying away from it or viewing it as a potential threat, it should be viewed as a powerful and helpful tool. A tool that will support your current daily responsibilities but also accelerate your career growth and expand your knowledge. Organizations have already begun or will soon adopt AI-driven technologies and machine models to enhance productivity – this means learning how to utilize AI and understanding that it can go a long way. Professionals who take the time to learn, tune, and configure these tools have become indispensable. Not only do they understand the goals of the company, they also understand how to adjust the machines to these needs, bridging the gap between machine output and human thinking.

In addition to helping amplify work output and efficiency, AI is broadening the scope of job roles. For instance, AI-driven monitoring and analytics can help IT and security professionals identify patterns, detect anomalies, and anticipate risks earlier. They can now generate reports in minutes, based on collected data, rather than hours or days of content compilation, data summaries, and tedious reference validation. This shift identification can uplevel cyber defensive capabilities, for example, moving beyond tactical detection and playing a strategic role in shaping resilience planning and monitoring policies.

For workers whose organizations use an in-house AI or large language model (LLM) tool, becoming familiar with this model is essential. Ensuring understanding across not just general AI concepts, but the specific tool that you'll be working alongside most closely, will help you make decisions from a more informed standpoint and leverage the tools at your disposal more effectively in your day-to-day.

WHAT CAN ORGS DO TO SUPPORT WORKERS IN AI?

AI-powered tools will continue to transform the workforce landscape, directly impacting careers and roles. But this shift does not have to be negative. As AI continues to shape operations and output, organizations must support the workers who are behind or working alongside these technologies. From private-sector companies to industry associations, these organizations play a critical role in ensuring that AI is used as an accelerator and not a career endgame.

Companies that adopt AI and implement its capabilities can support their employees in numerous ways, including providing on-demand resources, offering hands-on training, and offering certifications. Ensure that workers, regardless of role, understand that even with AI there are clear career pathways. Promote and support collaboration among team members and other industry leaders on AI use cases and capabilities. Reward those who choose to learn and adapt to technological change. Provide flexibility to roles that encourage individuals to complement AI systems with their human "touch" as opposed to eradicating roles.

Maintaining clear entry-level pathways is also essential, rather than allowing automation to eliminate these roles. Entry-level positions are crucial for developing future skills and future employees – rather than eliminating these roles, AI can be leveraged to enhance them, automating tasks to allow employees to devote more time to learning and skill acquisition. In fostering a culture of experimentation and innovation in the workplace, organizations can encourage employees at all levels to partner with, rather than to resist, AI, ultimately building a more adaptable and resilient workforce.

CONCLUSION

If anything has been made clear by the integration of AI into so much of the technology sector, it's that AI is not a passing trend. In fact, its role is evolving rapidly and will continue to expand as new advances are made. However, just as the role of AI is adapting and changing, so too is the role of the human worker. For cybersecurity, humans will not become victims of AI's influx; on the contrary, AI aims to enhance the abilities of these workers, allowing them to reach beyond and achieve more – so long as they are willing to become adaptable in their own right. Leaders and organizations must be willing to ask "What can AI do for us?" and "How do we ensure it empowers our people?". Ultimately, AI opens doors for both employees and employers, providing pathways for workers to scale up their skills from their desks while also helping organizations operate more efficiently. Whether you are the employer or the employee, the time has come to welcome and harness the power of AI.

IT ISAC
CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

INFORMATION TECHNOLOGY - INFORMATION SHARING AND ANALYSIS CENTER (IT-ISAC)

Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform, and a trusted forum to engage with senior analysts from peer companies.

CSaaS SIG
An IT ISAC Community

CRITICAL SaaS SPECIAL INTEREST GROUP (CSaaS SIG)

The Critical SaaS Special Interest Group (CSaaS SIG) is part of the IT-ISAC and serves as a forum for CSaaS companies to collaborate on a collective defense strategy to improve the security and operational resiliency of their services and share intelligence information with the industry. It enables companies who are essential to the internet to share cyber threat intelligence and effective security practices. The SIG holds a weekly analysts meeting and is designed for security managers, analysts, and IT executives from Critical SaaS companies.