NEWSLETTER

MIC NEWS

APRIL 2026

TALENT SOLUTIONS

MORE STATES, MORE OPPORTUNITIES

MiC Talent Solutions secured ETPL approval in 12 states and counting!

Arizona
California
Colorado
Pennsylvania
Missouri
Nevada
New York
North Carolina
Ohio
Kentucky
South Carolina
Washington

MEMBER SPOTLIGHT:

LEESEL FRASER

LEESEL FRASER

Tell us about yourself.

I was born and raised in New York City, and I've always been curious about understanding the world around me, especially in science. That curiosity eventually led me to computer science and a desire to pursue a career in technology and engineering. Along the way, I explored different areas of engineering before finding my interests in software engineering and cybersecurity.

What initially sparked your interest in cybersecurity? Was there a specific moment or influence that led you to this field?

I initially started out interested in software engineering, but over time I became more curious about how to make applications more secure. That curiosity led me to explore cybersecurity more deeply. I wanted to understand how to think like a cybersecurity professional while building software, and that interest naturally drew me further into the field.

As I continued learning, I also became increasingly interested in how to protect myself from digital threats on a personal level, which further motivated me to keep going. With both personal and professional interests aligned, I focused on learning by doing. One of my first cybersecurity-related projects was building a custom password manager and password generator, designed for the command line as well as a web interface with a deployed website and database. That project marked a significant step forward in my journey into cybersecurity and helped solidify my interest in the field.

As a graduate of the MiC LEAD Builders course, what was the most valuable lesson or leadership skill you gained that you still use today?

One of the most valuable lessons I learned is that your starting point doesn't define your end destination. You can always pivot and grow into new paths. I also gained strong communication skills, especially in bridging the gap between technical and business perspectives.

How did the Builders course prepare you for the 'soft skills' side of your job—such as collaborating with different teams or communicating technical risks to non-technical stakeholders?

The program helped me better understand the goals and priorities of non-technical stakeholders and how my work in technology aligns with those objectives. This has made it easier for me to collaborate across teams and communicate technical concepts in a clear and meaningful way.

What is one thing your current employer or manager has complimented you on that you feel was a direct result of your MiC training?

I've been complimented on my ability to quickly solve technical issues and troubleshoot problems efficiently. I believe this comes from the combination of both technical and business-focused training I received.

Is there a project or a specific 'win' you've had in your current job so far that you are particularly proud of?

One of my proudest moments has been successfully troubleshooting and resolving complex technical issues under pressure, helping my team maintain efficiency and minimize downtime.

I'm especially proud of this because it reflects how far I've come. There was a time when this kind of technical work felt completely new and unfamiliar to me. Being able to now handle these challenges with confidence, backed by the experience I've gained, is incredibly rewarding.

In a field as fast-paced as cybersecurity, how are you staying updated and continuing to grow

I stay up to date by subscribing to cybersecurity newsletters, following relevant content on social media, and regularly reviewing industry updates. I also continue to build my skills through courses, guides, and refreshers to keep my knowledge current.

Any advice for the readers?

From a professional and personal perspective, I'd like to say that no matter how long the journey takes or what it looks like, you'll reach your destination. It's also okay if your goals change along the way: growth often comes from exploring new directions.

From a cybersecurity perspective, I'd encourage people to build simple habits early. Small steps like using strong, unique passwords for different accounts and enabling multi-factor authentication whenever possible can go a long way in protecting yourself online.

Any fun facts, favorite tech hobbies, or a professional 'manifestation' you're currently working toward?

I love participating in hackathons and building projects in my free time. Right now, I'm working towards manifesting winning some more hackathons or at least just developing something really cool and continuing to grow both personally and professionally through fun and exciting hands-on experiences.

HOW AI IS RESHAPING CYBERSECURITY CAREERS — NOT REPLACING THEM

BY KEN UNDERHILL

Artificial intelligence (AI) is rapidly transforming cybersecurity roles, but not in the way many expected.

Rather than just eliminating jobs, AI is redefining how cybersecurity professionals work, shifting the focus from manual task execution to higher-level decision-making and analysis.

The work of security professionals "becomes less about processing and more about applying strong judgment, logic, and reasoning," said Maruf Ahmed, CEO of Dexian in an email to eSecurityPlanet.

KEN UNDERHILL

How AI Is Changing Day-to-Day Cybersecurity Work

This evolution is creating both new opportunities and new challenges for organizations and professionals alike.

Contrary to concerns about job displacement, AI is increasingly embedded in day-to-day cybersecurity workflows, particularly within security operations centers (SOCs).

AI-driven agents now handle tasks such as alert triage, ticket generation, and initial incident investigation — functions that were traditionally performed by L1 SOC analysts.

In many cases, these tools can process and respond to incidents significantly faster than humans, accelerating workflows and reducing manual effort. It also frees up L1 analysts to upskill for threat hunting and deeper threat intelligence tasks.

Where AI Falls Short: The Need for Human Judgment

However, this shift does not eliminate the need for human expertise. Instead, it changes where that expertise is applied. As AI takes over repetitive and time-consuming tasks, cybersecurity professionals are increasingly responsible for evaluating AI-generated outputs. This includes assessing the accuracy of alerts, determining business impact, and making informed risk decisions.

The work is becoming less about processing large volumes of data and more about applying judgment, reasoning, and contextual understanding. While AI reduces the burden of initial analysis, it simultaneously increases the number and complexity of decisions that must be made on the back end.

How AI Is Impacting Pen Testing and GRC

This transformation is evident in areas such as penetration testing and governance, risk, and compliance (GRC). In penetration testing, AI can rapidly identify potential vulnerabilities and map attack paths. However, it often lacks the contextual awareness needed to understand how those vulnerabilities behave and impact a specific environment.

As a result, security professionals may spend less time discovering issues and more time validating, prioritizing, and chaining them into meaningful attack scenarios. Similarly, in GRC, AI can assist with control mapping and identifying compliance gaps across frameworks, but it cannot effectively communicate risk to business stakeholders or translate technical findings into organizational impact.

Rethinking Cybersecurity Talent and Job Requirements

The growing reliance on AI is also exposing a critical gap in how organizations approach hiring. Many job descriptions still reflect outdated expectations, emphasizing task-based responsibilities that AI agents can perform. As a result, organizations often struggle to find candidates who match these legacy roles.

The issue is not necessarily a shortage of talent, but rather a mismatch between hiring criteria and the current demands of the role. Modern cybersecurity positions increasingly require professionals who can interpret AI outputs, apply domain-specific context, and make informed decisions — not just execute predefined tasks.

Addressing this gap requires organizations to rethink their talent strategies. Job descriptions and hiring requirements must evolve to reflect the changing nature of cybersecurity work.

This may involve prioritizing skills such as critical thinking, communication, and business acumen alongside technical expertise.

In some cases, domain-specific knowledge — such as understanding clinical environments in healthcare — can be essential for accurately assessing risk and impact.

Why Fundamentals Still Matter in an AI-Driven World

For individuals pursuing careers in cybersecurity, the rise of AI underscores the importance of foundational knowledge.

Core concepts such as networking, operating systems, data protection, and how data flows across systems remain critical, as they form the basis for understanding more advanced technologies.

While AI tools can enhance productivity and automate workflows, they are built on these underlying concepts.

Professionals who develop a strong foundation are better positioned to adapt as new technologies emerge and integrate AI effectively into their workflows.

How Cybersecurity Professionals Should Work With AI

At the same time, cybersecurity professionals must learn how to work alongside AI. This includes understanding where AI can add value, how to integrate it into existing processes, and how to validate its outputs.

Rather than focusing solely on using AI tools, professionals should consider how AI can enhance specific tasks within their role and workflow, from incident response to threat intelligence.

Ultimately, the impact of AI on cybersecurity careers is less about replacement and more about evolution.

Organizations that recognize this shift and align their hiring, training, and technology strategies accordingly will be better equipped to build effective security teams.

Those that continue to rely on outdated role definitions risk falling behind, both in talent acquisition and in their ability to respond to modern threats.

As AI continues to mature, cybersecurity roles will continue to evolve, placing greater emphasis on human judgment, adaptability, and strategic thinking in an increasingly automated landscape.

MIC ANNOUNCEMENTS

MIC LEAD BUILDERS AND COMMUNICATORS COURSE

MiC LEAD Builders and Communicators courses are now accepting applications. Apply now and let's get to work!"

Lear more here: bit.ly/MiCLEAD

CHECK THIS OUT ...

Relive the highlights!

Official photos from the 2026 MiC Annual Conference are now available on the MiC website. Head over to our gallery now to check out all the incredible memories we made together.

Check Here: mincybsec.org

COMING SOON: THE MNC-CTC SEMINAR SERIES

The MNC-CTC Seminar Series officially kicks off on June 13, 2026.

Join us for our opening session, **"Learn. Lead. Leverage: A Framework for Intentional Career Progression in Cybersecurity,"** featuring guest speaker Romeo Gardner.

bit.ly/mncctcseminars