NEWSLETTER

MIC NEWS

MAY 2026

MEMBER SPOTLIGHT:

KENNETH UNDERHILL

KENNETH UNDERHILL

Tell us about yourself.

I started as a network engineer, got laid off, and then worked in medicine (as a medic/pediatric nurse) for several years while maintaining an IT side hustle (mostly installing SMB networks and providing IT support). I then performed penetration testing (network and web application) and subsequently moved into incident response in healthcare. Around 2018 I moved into the education space and over 2M people globally have gone through my various training courses.

You are a big advocate for continuous learning. What is a skill or tool outside of traditional cyber certifications that every security professional should learn today?

Many people trying to enter security lack fundamental knowledge of networking, operating systems, and Linux/Linux security. Outside of working on those, I'd suggest learning practical sales skills because everything (e.g., securing more cyber budget) is sales.

You have been featured everywhere from Forbes and Dark Reading to Reader's Digest, and you now contribute heavily to cybersecurity newsletters and media. What is the biggest challenge right now in communicating complex security risks to the general public?

I think for technical SMEs in general, the biggest challenge is speaking the language people care about. So, speak the language of business and address

topics that matter to the general public in their everyday lives. For example, if I want to talk to the average person about reducing their social media footprint, I don't use technical jargon. If they have kids, I ask what they would do if someone took the photos of their kids they are sharing to everyone no the web and turned them into inappropriate images and then posted those photos at the school. Security must relate to something the other person actually cares about.

You wrote the book, Hack the Cybersecurity Interview. If you could give our readers just one unconventional piece of advice to stand out in today's job market, what would it be?

This market is saturated with people colleting certs. You need to show projects and how they apply to the real world. So, if you are doing a lab for school, think through how this works in the real world and what else you might need to consider. genAI tools can help point you to this information. And screen record as you work through different security problems. A ket thing we lopok for in job interviews are people that can work through problems.

With so many milestones already checked off—from author to founder—what is the next big professional or personal goal you are targeting?

I'm supposed to be retired, but Mary Chaney won't let me (j/k). I'm studying for the TAISE cert from Cloud Security Alliance right now and they also want me to go through their train-the-trainer content, so those are the big projects right now.

What is one piece of advice you have for the aspirers in our community who are looking to make their own mark on the industry?

I never set out to be famous (people asked for my autograph this year at RSAC). I just focused on helping others. So, I suggest ignoring the attention-seeking people and posts on social media, and instead focusing on how you might help even a small number of people by posting content. You only need to be one chapter ahead of others in the book for them to learn from you. Baby steps snowball into big things. And keep learning because you will never know everything.

Any fun facts, favorite books, or new "manifestations" you'd like to share with our readers?

Life is full of ebbs and flows. Look at your career as a journey, not a destination, and, to be a bit cliché, "build a life you don't need to take a vacation from." The whole work/life balance thing is BS. It's more about putting yourself in a financial situation to choose the life you want, instead of experiencing lifestyle creep (like many people in cybersecurity) and then "having" to work a job you hate because of significant debt. I remember at Black Hat years ago there was a person dressed in Chanel and all sorts of labels who couldn't even pay for their dinner.

YOUR BEST IS NEVER SECOND BEST: THE HIGHS AND LOWS OF THE CYBERSECURITY GRIND

BY ADEMOLA OLANREWAJU

In the fast-paced, high-stakes trenches of cybersecurity, the mantra *"your best is never second best"* is more than just a motivational quote; it is a daily operational standard. Defending digital perimeters requires a relentless commitment to excellence. The threat landscape never sleeps, and those who choose to stand on the front lines must bring their absolute best to the terminal every single day. But this industry is a pendulum swinging between immense satisfaction and grueling challenges.

ADEMOLA OLANREWAJU

Here is a look at the real highs and lows of working in cybersecurity, and why bringing your best effort is the only way to survive and thrive.

The Highs: The Thrill of the Defense

The highs in cybersecurity are hard-earned and deeply rewarding. There is a distinct, adrenaline-fueled rush that comes from hunting down an anomaly. Whether it is sifting through a sea of Splunk logs to isolate a malicious IP, or analyzing network traffic packet-by-packet in Wireshark to stop an exploit in its tracks, the thrill of the catch is unmatched.

For those focusing on Governance, Risk, and Compliance (GRC) or Identity and Access Management (IAM), the highs look a bit different but are equally impactful. It is the deep professional satisfaction of designing a comprehensive risk management framework from scratch, aligning it with business objectives, and watching those policies successfully protect an organization's most critical assets.

Furthermore, the milestones of personal and professional growth offer incredible peaks. Seeing the word "Pass" on a grueling industry exam, like the CompTIA

Security+ after months of late-night studying is a profound validation of your effort. Mastering complex graduate-level modules and watching abstract concepts crystallize into practical, hands-on skills proves that the grind is worth it. When you operate at your highest potential, the security posture of your entire organization elevates with you.

The Lows: The Weight of the Shield

However, the reality of the field means the lows can be heavy. The sheer volume of alerts and the persistent nature of advanced threats can lead to intense burnout. Working as an analyst in a Security Operations Center (SOC) often means navigating a relentless tide of false positives, where missing a single true positive could result in a catastrophic breach.

There are days when the technology fails, when a meticulously configured firewall rule breaks a legacy application, or when a zero-day vulnerability drops late on a Friday night, rendering weeks of preventative work obsolete in an instant. The learning curve is also notoriously steep. Balancing the demands of a high-level corporate role with the rigorous pursuit of advanced degrees or new technical certifications requires sacrificing sleep, weekends, and personal time. The pressure to constantly evolve can sometimes trigger a heavy dose of imposter syndrome.

Win or Learn: The Ultimate Takeaway

This is exactly where the philosophy of "your best is never second best" proves its worth. In cybersecurity, you will face scenarios where the adversary adapts, or where a system fails despite your most rigorous defenses.

When you bring your absolute best to the table, a failure is no longer a defeat, it becomes a critical data point. The industry demands a strict "win or learn" mentality. A breached defense or a misconfigured network is not a reason to quit; it is an opportunity for collective iteration. You patch the vulnerability, update the incident response plan, refine the IAM controls, and emerge more resilient than before.

In the end, working in cybersecurity is not about achieving absolute perfection because a 100% secure system is a myth. It is about bringing an uncompromising, top-tier effort to the daily grind. When you continuously push the boundaries of your own knowledge and refuse to settle for mediocrity, your best will always be exactly what the front lines need.

MIC ANNOUNCEMENTS

MIC LEAD BUILDERS COURSE

MiC LEAD Builders course is still accepting applications.
Apply now and let's get to work!

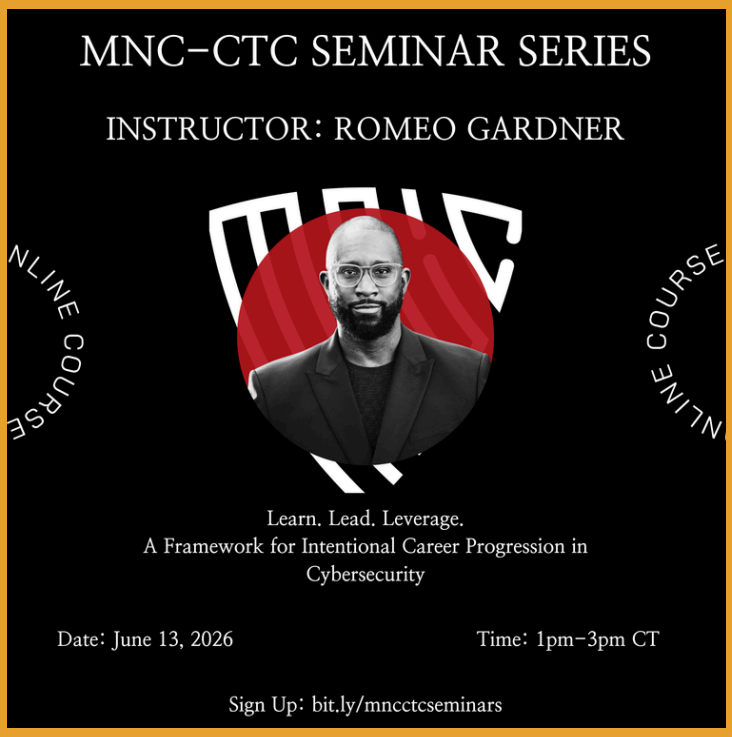
Lear more here: bit.ly/MiCBuilders

CONGRATULATIONS TO THE MARY N. CHANEY CYBERSECURITY TRAINING CENTER (MNC-CTC)

The inaugural cohort of the Mary N. Chaney Cybersecurity Training Center officially starts on Monday, June 1, 2026.

We want to extend a warm congratulations to the incoming residents for taking this intentional step toward career progression, and a huge thank you to everyone who helped make this launch a reality.

COMING SOON: THE MNC-CTC SEMINAR SERIES



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

Title: *"Learn. Lead. Leverage: A Framework for Intentional Career Progression in Cybersecurity,"*

Host: Romeo Gardner

Don;t miss it. Register now!

bit.ly/mncctcseminars