December 2025

MiC News

WISHING YOU ALL A HAPPY NEW YEAR!

MEMBER SPOTLIGHT

PATRICIA EMMANUEL

Tell us about yourself.

My name is Patricia Emmanuel, and I'm a cybersecurity professional with a background that spans software testing, security assurance, governance, risk, and compliance (GRC).

I didn't start my career in cybersecurity with a title. I started with curiosity, responsibility, and a strong sense of stewardship. Over the years, I've worked across healthcare, public & private sector, startup organizations, ensuring systems are not just functional, but secure, compliant, and resilient.

Alongside my professional role, I'm also a mentor, community builder, and co-founder. I believe cybersecurity is not just about controls and frameworks, it's about people, culture, and long-term trust.

Looking back on your career, what were some of the pivotal moments that helped you advance to your cybersecurity role?

One key moment was realizing that I was already doing the cyber security work even before I had the title for it. Coming from a testing background, I questioned assumptions, chased root causes, and paid attention to how decisions landed on real users. That mindset naturally pulled me closer to risk, assurance, and governance.

Another pivotal moment was I stopped explaining issues only in system terms and started explaining impact, doors opened. That shift moved me from being "involved" in security to being trusted in it.

For someone looking to move into the GRC analyst role, what is the most important mindset shift they need to make?

You have to stop seeing GRC as enforcement and start seeing it as stewardship. GRC isn't about catching people out. It's about understanding context, weighing risk honestly, and helping organisations make wise decisions especially when there's no perfect option for you to adopt that mindset, your role changes from "the person who says no" to the person people seek out when decisions matter.

You have graduated from our MiC LEAD Program. What is the single biggest piece of advice you would give to someone thinking of applying to the MiC LEAD Builders course?

Don't apply unless you're ready to be stretched internally, not just professionally. The MiC LEAD Builders course challenges how you think, how you show up, and how you see yourself as a leader. The growth doesn't come from the content alone it comes from what you're willing to confront and refine. If you're open to that level of growth, the experience is genuinely transformative.

In your opinion, how does the MiC community create a supportive environment where diverse professionals don't just enter, but remain in cybersecurity?

What stands out about Minorities in Cybersecurity is that people don't have to perform perfection to belong. There's room to ask questions, to admit uncertainty, and to grow without being reduced to a stereotype. That kind of psychological safety is rare and it's one that I appreciate greatly.

You co-founded Bluesky Citadel Consulting, a UK charity. How does its mission complement your work with MiC?

Bluesky Citadel Consulting was built on the belief that talent is evenly distributed, but opportunity is not. Our work focuses on practical access and training within the software development niche, mentoring, and real-world exposure for people who are capable but overlooked. That mission aligns naturally with MiC's work in visibility, leadership, and global community. Together, they create a fuller pathway: access, development, and longevity.

What is one small challenge you would give to our readers this month to help them grow professionally?

Choose one area where you usually stay silent and speak thoughtfully. Ask the question. Share the observation. Offer the perspective. Growth often begins the moment you stop shrinking your voice.

Any fun facts you'd like to share with our readers?

I write songs, lead worship, and think creatively often outside of structured frameworks. I've learned that creativity and cybersecurity are not opposites; both require discernment, pattern recognition, and restraint. And I still believe some of the most important leadership work happens quietly, long before anyone applauds it.

Operating Securely in the AI Era: A Practitioner's Guide

by Mukesh Makwana

AI services are transforming how cybersecurity teams operate by being a force multiplier that accelerates productivity and permits resource constrained security teams (i.e. staffing shortages, alert fatigue, speed of attacks) to broaden effectiveness and impact. But adopting such services securely requires navigating real risks to realize the benefits for smaller teams or individual practitioners.

This guide provides actionable advice for cybersecurity professionals to adopt AI tools effectively while managing the threats they may introduce. Any guidance provided in this article should be aligned with appropriate policies, standards, and risk appetites.

What is Large Language Models (LLMs), Agents, and AI?

Many articles discuss AI Agents and LLMs interchangeably. They are distinct concepts with very different uses and security concerns. It is beyond the scope of this article to go overly deep into the implementation of these services.

Broadly speaking, they can be defined as follows:

- **Large Language Models:** A Large Language Model (LLM) is a machine-learning model trained on large datasets to predict and generate content. It is a probabilistic model that predicts the next word (i.e. token) based on a given request. For all intents and purposes, LLMs are stateless by default, though context windows allow maintaining conversation history within a given session. Today, LLMs can:
    - o Answer questions (based on its trained data and/or external sources)
    - o Summarize information
    - o Assist with reasoning tasks
    - o Interpret and generate text, images, audio, video
- **AI Agents:** Leverage LLMs to observe and reason and then take any outputs to perform actions (via tools). AI Agents maintain state (via memory), can be chained, and be empowered to be autonomous. Understanding this distinction matters because the security controls you need differ significantly between LLM-assisted tasks and autonomous agent workflows.

How could Cyber Security Professional Leverage AI Services?

By no means exhaustive, the following are a few examples that are relatively easy to implement (using off the shelf tools) to provide immediate lift. Of course, mileage may vary.

AREA	DESCRIPTION	DIFFICULTY TO IMPLEMENT	RISK
Communication	Drafting incident reports that effectively translate technical findings into business language	Low	Low
Policy and Compliance	Mapping policies across frameworks, providing guidance on implementation, identifying gaps / inconsistencies, preparing for audits	Low	Medium
Security Architecture	Sounding board for vetting security design and engineering decisions	Low	Medium
Code Assist & Security Review	Creating detections in SIEM tools, reviewing code fragments, hunting for bugs, creating developer documentation, etc. Unlike "vibe coding" where the AI has full autonomy, code assist is effective support.	Medium	Medium
Vulnerability Analysis	Reviewing scan results, prioritizing remediation activity, summarizing CVE/CVSS information	Medium	Medium
Investigating and Responding to Alerts	Quickly parsing large data sets (i.e. trace logs) to quickly surface what occurred, build a timeline, create a plain English report, and automate response.	Medium	High

How Are Attackers Using AI Services?

Like Defenders, attackers are increasingly using commercial AI tools to expedite the discovery, reconnaissance and instrument automated attack. In effect reducing the time to compromise. Some known examples:

- **Phishing Campaigns (Targeted, Spear, etc):** AI tools permit the creation of "authentic" emails in a variety of languages. They are free from common issues present where a foreign advisory translates content into English (e.g. spelling mistakes, formatting issues, etc). Additionally, services can be used to more easily combine OSINT (Opensource Intelligence) into targeted campaigns and scale variation.

    - **Actionable Advice:** *Raise the bar for Staff Training by conducting "real-world" phishing simulations, ensure procedures are in place to detect / contain phishing attempts and potential service compromise, monitor effectiveness of training with gamified outcomes, and continually reinforce throughout the year with updated material.*

- **Impersonation (Video / Audio):** AI Video / Audio Generation tools have been leveraged to impersonate individuals in real-time. These services can parse recordings and videos that are freely available on the internet (e.g. Facebook, Instagram, YouTube, etc).

    - **Actionable Advice:** *Encourage users to lock down social media profiles, train staff to question unexpected audio / video engagements, evaluate critical business processes and increase due diligence before performing actions, and perform "red team" exercises that test key technical / support areas (e.g. password reset).*

- **Accelerated Attack:** Nation State agents have leveraged foundation model providers (i.e. Anthropic Claude) to orchestrate the attack chain and accelerate compromise.

    - **Actionable Advice:** *Ensure that processes and supporting services are in place to detect, contain, and recover compromised systems. Automate (as much as you are comfortable with) the incident response processes by leveraging tools provided by SIEM / EDR.*

AI Security Issues

It is important to ensure that there is clarity on the threat model and risks that apply when engineering and/or adopting AI services. Although this area is under active development, here are a few risks that should be considered:

- Supply Chain: LLM introduce additional risks beyond trusting a third party to a secure service. These risks span licensing, vulnerable pre-trained models, weak provenance, etc. Depending on purpose, each of these can lead to unexpected outcomes that could impact a multitude of security risks.
- Prompt Injection: Like other injection attacks, this can allow disclosure of sensitive information, providing unauthorized access, or even ability to execute arbitrary commands in connected systems.
- Hallucinations: LLMs can generate plausible sounding but factually incorrect responses collectively known as hallucinations. As such, solely relying on an output without validating its accuracy can be disastrous particular with the use of AI Agents.

Further details can be found here: https://genai.owasp.org/llm-top-10

How do you safely onboard, secure, and use AI Tools?
The following is a broad set of activities that a Security professional could leverage to support enabling and using AI within a corporate setting. It is intended to be a broad guide with actionable advice and not intended to be a how-to. Any use should be aligned with corporate policies, standards, and risk appetites.

- **Be Clear on Scope / Use-Case:** Establishing scope / utility of AI will ease investment, adoption, and allow partnering with key stakeholders on adoption. Many AI initiatives fail since there is no measurable ROI.
    - **Actionable Advice:** *Leverage AI tools for narrow and well-defined use-cases with clear stakeholders where measuring ROI is simpler. This allows building momentum and provides a case for ongoing investm***ent.**
- **Create a Paved Path for Secure Experimentation:** The rate of change of AI tools / services has rapidly increased over the last few years and likely will continue to increase as the ecosystem matures. Lowering barriers to entry will improve outcomes, reduce business frustration, and allow rapid iteration to find services that "work".
    - **Actionable Advice:** *Establish an AI governance framework that includes security/technical standards and processes that allow rapid risk review, assessment, sandboxing, and enablement whilst effectively managing risk. Partner with the business and technology to support secure enablement.*
- **Manage Costs By Controlling Access:** AI services are costly and will compound with each use-case (e.g. per seat licensing, token usage, etc). Enforce healthy access controls that align with ROI (Return On Investment) and address any concerns with data exposure.
    - **Actionable Advice:** *Adopt enterprise offerings and ensure alignment with corporate access standards (e.g. SSO with EntraID/Google Identity, etc), enforce corporate data protection of inputs and outputs (e.g. DLP, Windows Information Protection, etc). Periodically audit who should have access based on usage and ROI.*
- **Establish Data and Process Governance:** All AI services require some form of enterprise data to perform their function(s). One way of reducing risks is to effectively manage what data is permitted for use and setting expectations on staff.
    - **Actionable Advice:** *Establish an "AI Acceptable Use Policy" that clarifies what data is permitted to be placed with AI systems, what tools have been approved for what purpose, what business processes are not appropriate for AI enhancement, obligations on data training and residency, and how outputs should be treated (incl. compliance and labeling requirements).*
- **Supply Risk Management:** AI services require access to enterprise data for them to be effective. Generally, it requires trusting third party platforms to apply appropriate data confidentiality and security monitoring practices.
    - **Actionable Advice: :** *Establish trust by suitably vetting the security program of providers starting with standardized attestations (e.g. SOC 2 Type II, ISO 27001k, etc). Ensure they have reasonable practices in place to mitigate key enterprise risks and have adopted a "Responsible AI" practice. Dive deep to understand service architecture and, importantly, security controls to protect customer data.*
- **Have the Right Legal Protections:** Contracts are the backstop that permits an enterprise to hold another accountable in the advent of a lapse in security and/or service. It is by no means a replacement for performing suitable technical, functional, and security due diligence.
    - **Actionable Advice: :** *Partner with Legal and Compliance to identify the appropriate language to protect enterprise interests. Push to incorporate and or validate that they are in place especially when leveraging Free Tiers and/or limited time experiments. Ensure these teams are part of any AI Governance forums to quickly identify and manage potential impacts associated with AI initiatives.*
- **Be Compliant for Your Industry:** The intersection between generative AI, business process, and automation can complicate adhering to regulatory and compliance mandates. The misalignment of which can result in reputational and financial impact.
    - **Actionable Advice: :** *Ensure that Legal and Compliance is at the table to clear the use of AI in sensitive business processes especially where there is regulatory oversight.*
- **Hold Staff Accountable to Using Tools and Owning Outputs:** It takes more effort to effectively use AI services to provide accurate and reasonable outputs. Lack of knowledge on how tools should be used will hamper adoption, generate unnecessary friction, and result in lower quality. Where applicable, refactor staff roles within the organization to more accurately portray the enhanced capabilities these tools provide.
    - **Actionable Advice:** *Read the manual, create standardized templates and education material, have an ability for users to effectively engage with any subject matter experts, and gamify to incentivize adoption. Additionally, empower senior staff over junior to leverage their expertise in judging outputs and broadening their overall impact.*
- **Adopt AI features in Incumbent Tools:** Many existing security service providers are enabling AI features. These features natively address shortcomings and provide instant lift.
    - **Actionable Advice:** *Ensure the ROI case is clear, pilot features narrowly, and ensure contracts are updated to protect customer data.*

- **Guardrail Autonomy:** The non-deterministic nature of AI tools can lead to unexpected outcomes that can expose an organization to risk (technical, operational, legal/compliance, and security).
    - **Actionable Advice:** *Do not permit vibe coding without clear controls on validating outputs (incl. security). Ensure humans are in the loop for any sensitive processes where AI agents are empowered to perform actions.*

How do I use AI Services to Support My Day to Day

Here is a sample set of how I, personally, use AI tools to accelerate productivity. Mileage will vary and in no way is the below intended to promote a given product. Just like the never-ending debate between PC and MacOS users, it is all a personal choice.

- General Productivity and Thought Partner (OpenAI ChatGPT): Starting point for any general requests with a an interface that lends itself to easier project management and has a more intuitive voice chat feature. Recent examples: summarize a CVE/CVSS, compare NIST CSF and CIS Safe Guards, aggregate and deduplicate data from two files, iterate on a technical architecture and security controls, assist in planning a code feature, and image parsing/generation.
- Writing Critic and Code Assist (Anthropic Claude): Narrowly, this service has been great at helping to critic narratives, assist with well-defined coding tasks, and support analysis of code for security issues.
- Task Automation and Internet Summarization (Perplexity): I hold Perplexity as the "Google for the AI Age". It provides the ability to create tasks that can analyze internet sourced data on a periodic basis and send an email summary. For example, tasks that provide a snapshot of any trending security alerts or recent AI research papers.

Author's Bio:

Mukesh Makwana is the founder of Farsight Advisory, a boutique cybersecurity and technology advisory firm that brings enterprise-grade security to startups and mid-size companies pursuing regulatory compliance.

Across 25 years in the financial services industry, he has built and scaled security programs that protect business services while enabling innovation. Mukesh cut his teeth in strategic security roles at Credit Suisse before spending over a decade at Bridgewater Associates, where he led enterprise security functions and worked at the intersection of technology, risk, and business strategy, driving multi-million-dollar initiatives.

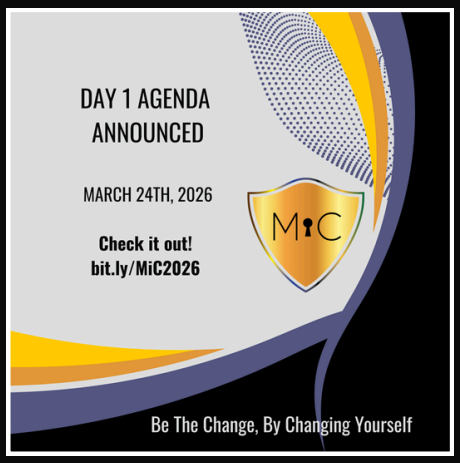
Originally from London, Mukesh spent twelve years in New York before relocating to Miami, where he lives with his wife and young child. He holds a Physics MSc from Imperial College London.

MiC Announcements

Register for the 2026 MiC Annual Conference!

Day 1 Agenda

Day 1 is announced! Get ready to dive in.

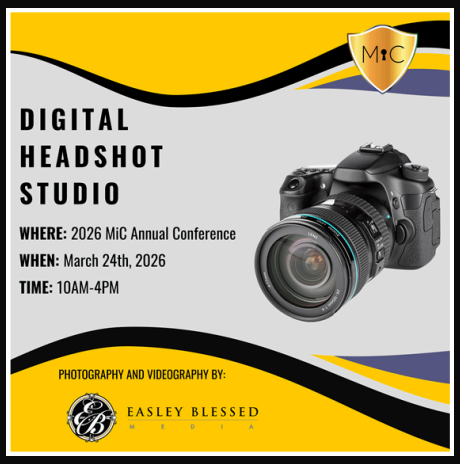


Day 2 Agenda

Don't skip the sequel. Day 2 agenda announced.

Digital Headshot

Level up your look! Step into our studio.



Room Block

Official rooms. Zero commute. Book the block

Register here: bit.ly/MiC2026

MARK YOUR CALENDARS

COMING SOON:

A NEW WAY OF TRAINING CYBERSECURITY TALENT

MNC-CTC
Mary N. Chaney
Cybersecurity Training Center

Follow us on LinkedIn: @MNC-CTC