Karim Ahmed

Cairo, Egypt • karim.ahmed4815@gmail.com • +201118808688

Cybersecurity Researcher & Engineer | (ISC)² Member | Specializing in AI-Driven Defense, Secure AI Systems, AI Integration and Cloud Security

Education

German University in Cairo (GUC)   **Cairo, Egypt**
Master of Science in Computer Science and Engineering   Awarded July 2025
Thesis Title: A Self-Adaptive Agentic Moving Target Defense Architecture for Real-Time Cyber Threat Response

German University in Cairo (GUC)   **Cairo, Egypt**
Bachelor of Science in Computer Science and Engineering   Awarded July 2024
Thesis Title: 3D Reconstruction of Human Characters

Experience

GUC
Teaching Assistant   **Cairo Egypt**
                                                                                                                         September 2024 – Present

- Taught more than 250 students the fundamentals of Full-Stack development using the MERN stack, and Cloud Computing fundamentals using VMware.
- Introduced a new course, Agentic AI development lab, to be taught in the Spring 2026 semester.
- Co-founded the Artificial Intelligence Research Lab GUC (AIRLab GUC), which focuses on researching and developing new technologies for cybersecurity, cloud computing and NLP using Artificial Intelligence, launches Spring 2026.

Clynto   **Remote**
Software Engineer   July 2024 – October 2024

- Developed and maintained the frontend for the webApp, consistently being one of the top contributors
- Initiated new security controls to further secure the online transactions using different threat models.

Certifications

ISC2 Certified in Cybersecurity (CC) - Credly   **AWS Cloud Practitioner CLF-C02 - Credly**
OWASP Top 10 - TryHackMe   **Google Cybersecurity Professional Certificate - Coursera**

Research and Projects

- **Automating Moving Target Defense Using LLMs**: Focus areas include dynamic network reconfiguration, Threat Intelligence enrichment through CVEs and TTPs, and autonomous policy generation.
- **Self-hosted cyber-rang**: Built a private cloud, automating VM lifecycles with Python/Bash and securing remote access through Tailscale VPN, SSH keys, RBAC, IP-whitelisting & audit logs; cutting CSP costs to zero while granting full control over deployment, access, and security for tailored cybersecurity and cloud-computing training.

Skills & Interests

Technical: Python, Bash, Java, Javascript, Typescript, C; MySQL, NoSQL; git
Cloud: AWS, GCP, VMware
Security: Metasploit, MSFVenom, Caldera, CyberBattleSim, BurpSuite, Nmap, Wireshark, Suricata, Splunk and Snort
Frameworks & Standards: ISO 27001, MITRE ATT&CK & D3FEND, NIST CSF/RMF, STRIDE, PASTA, TRIKE
AI: Agentic Design, RAG, TensorFlow, PyTorch, LangChain, Ollama
Soft Skills: Agile Methodologies, problem-solving, effective communication, team collaboration, time management