COLLINS MWANGE

Dallas, TX, 75252 | +1 682-406-8635 | collinsmbwika10@gmail.com | https://www.linkedin.com/in/collins-mwange/

PROFESSIONAL SUMMARY

Application Security Engineer with a strong foundation in DevSecOps, AI/ML security, and secure software development practices. Experienced in securing cloud-native applications, integrating security into CI/CD pipelines, and implementing secure coding standards. Successfully led AI-driven projects with a focus on risk mitigation and accessibility, and collaborated cross-functionally to embed security into the SDLC. Passionate about safeguarding AI models and software supply chains in dynamic development environments.

SKILLS

Technical Skills: Application Security, Secure Coding (Python, Java, JS), OWASP Top 10, OWASP LLM Top 10, SBOMs, SAST/DAST, Burp Suite, OWASP ZAP, Threat Modeling, Risk Assessment, Incident Response, GitOps, Infrastructure-as-Code Security, Jenkins, GitHub Actions, Docker, Kubernetes, Terraform, AWS, Azure, Model Vulnerability Assessment, Federated Learning Concepts, Privacy-Preserving Machine Learning, Python, Java, R, C, Node.js, FastAPI, SQL, PL/SQL, TensorFlow, PyTorch, Edge TTS, SBOM Tools. **Certifications**: CompTIA Security+. **Soft Skills**: Analytical Thinking, Problem-Solving, Stakeholder Engagement, Cross-Functional Collaboration

PROFESSIONAL EXPERIENCE

The University of Texas at Dallas, Richardson, TX **May 2024 - Present**
DevSecOps Engineer

- Conducted static code analysis and threat modeling for Tafsiri AI application, remediating 20+ critical vulnerabilities across the backend FastAPI Python codebase.
- Designed and enforced secure coding guidelines for AI-based systems, reducing injection and exposure risk by 40%.
- Secured CI/CD pipelines with Jenkins and GitHub Actions by integrating SAST tools (SonarQube), decreasing deployment-related security incidents by 30%.
- Developed Software Bills of Materials (SBOMs) for AI services and validated open-source components against CVE databases, ensuring full software supply chain visibility.
- Embedded secure design principles into Edge TTS and seamlessM4T integrations, addressing key concerns from OWASP LLM Top 10 including prompt injection and data leakage.

SwahiliPot Hub Foundation, Mombasa, Kenya **Aug 2017 – Aug 2023**
Cybersecurity Researcher

- Integrated secure authentication workflows (JWT, OAuth 2.0) across 5 client-facing applications, preventing unauthorized access and improving access control compliance.
- Performed regular code audits and vulnerability scans using OWASP ZAP and Burp Suite, proactively fixing XSS and CSRF issues before deployment.
- Implemented robust DevOps pipelines with built-in security gates, accelerating secure feature delivery while maintaining compliance with internal policies.
- Championed secure API design standards and encryption-in-transit practices, aligning backend services with best practices for data protection and privacy.

EDUCATION

The University of Texas at Dallas **Richardson, TX**
Master of Science in Cybersecurity, Technology, and Policy *Aug 2023 - May 2025*
Scholarships: ISACA Digital Trust Scholarship; ISC2 Center for Cyber Safety Graduate Scholarship
Relevant Courses: Cybersecurity Analytics & Malware Analysis; Digital Forensics & Incident Mgt; Cybersecurity Policy; Legal Aspects of Cybersecurity & Ethics; Governance, Risk, & Compliance (AWS); Cognitive Psychology; Open-Source Intelligence; and Cyber Physical Systems & Critical Infrastructure.

Maseno University **Kisumu, Kenya**
Bachelor of Science in Computer Science *Aug 2012 - Apr 2016*
Relevant Courses: Data Structures & Algorithms, Software Project Management, Network Administration.