FISAYO SANGOLEYE

sangoleye.fm@gmail.com | 505 582 6318 | linkedin.com/in/fisayo-sangoleye

PROFILE SUMMARY

Application and Product Security Engineer focused on securing web, mobile, API, and cloud-native platforms at scale. Proven track record owning AppSec programs end-to-end - from threat modeling and security architecture through secure SDLC, CI/CD security, and production risk reduction - with deep expertise in GenAI, LLM, and agentic AI security. Developer-centric practitioner who embeds security into how products are designed, built, and shipped.

WORK EXPERIENCE

Senior Application / Product Security Engineer | Bumble Inc., Austin, TX *Aug 2026 - Present*

- Drive end-to-end AppSec program across Bumble's consumer mobile platform (iOS/Android) and cloud-native backend microservices - integrating threat modeling, secure design reviews, and vulnerability management into engineering workflows to reduce security risk reaching production.
- Lead threat modeling and security design reviews for new product features and platform changes - partnering with engineering and product teams to identify security risks early in the SDLC and directly influence architecture decisions before code is written.
- Own SAST/DAST/SCA tooling integration across CI/CD pipelines, shifting vulnerability detection left and reducing the volume of critical and high-severity findings reaching production environments.
- Conduct secure code reviews and AppSec assessments across mobile, API, and cloud-native services on GCP/GKE - identifying and driving remediation of security findings in partnership with engineering teams.
- Secure LLM-powered features and agentic AI systems against OWASP LLM Top 10 risks - threat modeling AI/ML pipelines and implementing controls against prompt injection, data leakage, insecure output handling, and model misuse across consumer-scale AI deployments.
- Partner with engineering teams to deliver developer-centric security guidance and remediation support - enabling secure coding practices and reducing security friction across the software delivery lifecycle.
- Apply AI-assisted tooling to scale security detection and triage capabilities - leveraging LLM-based approaches to improve AppSec program efficiency and expand security coverage across high-volume engineering output.

Lead Cybersecurity Engineer - Application and Product Security | GE Vernova, Niskayuna, NY *Jun 2023 - Aug 2026*

- Owned and drove end-to-end AppSec programs across web, API, cloud, and embedded products - establishing SAST/DAST/SCA tooling, secure code review processes, and threat modeling workflows within SDLC, shifting vulnerability detection left and significantly reducing critical risk reaching production.
- Led threat modeling and security design reviews for high-complexity distributed systems and GenAI platforms - identifying security design flaws and business-logic vulnerabilities early in development, directly influencing architecture decisions from design through production deployment.
- Secured production GenAI and AI/ML services against OWASP LLM Top 10 risks - implementing controls against prompt injection, data leakage, insecure output handling, and model misuse, enabling confidential and scalable AI service delivery.
- Partnered with engineering teams to deliver developer-centric security enablement - running security office hours, building secure coding guidelines, and establishing a findings feedback loop that reduced recurrence of critical vulnerability classes by 70% across active development teams.
- Designed and built a secure cloud-native AWS data pipeline (S3, Lambda, EC2, DynamoDB) for an AI-powered blade certification system - implementing OAuth2 authentication, KMS encryption, and presigned URL access controls to protect large-scale inspection data across cloud ML workflows.
- Designed and implemented secure software supply chain controls deployed at scale - developing automated security validation libraries using OpenSSL and Bouncy Castle to detect and prevent supply chain attacks across GE's software delivery pipeline.

Cybersecurity Engineer (Intern) - Application Security | GE Vernova, Niskayuna, NY *May 2022 - May 2023*

- Integrated SAST/DAST security tooling into CI/CD pipelines and led secure code reviews across active development teams - accelerating vulnerability detection by ~30% and reducing remediation turnaround across software delivery workflows.
- Conducted application vulnerability assessments and security testing across web-facing services - identifying and remediating critical security flaws before production deployment.
- Designed and implemented a Confidential Computing protection system using Intel SGX - enabling secure application execution in protected enclaves and mitigating IP exposure risk in untrusted cloud environments.

Cybersecurity Researcher - Secure Systems & Architecture | Sandia National Labs *Oct 2021 - Mar 2023*

- Designed and validated a defense-in-depth security architecture for large-scale industrial control systems - applying secure design principles, network segmentation, and layered access controls to eliminate attack paths across critical infrastructure environments.
- Developed and evaluated automated security detection capabilities for distributed industrial networks - building on ML-based approaches to improve threat visibility and reduce detection gaps across monitored systems.

- Conducted security assessments and gap analyses against NIST and ICS security frameworks - identifying architectural vulnerabilities and driving risk-based remediation recommendations across assessed systems.

Graduate Researcher - Cybersecurity | University of New Mexico, Albuquerque, NM *May 2020 - May 2022*

- Conducted cybersecurity research across IoT, smart grid, and wireless network environments - contributing findings to 5+ peer-reviewed publications focused on threat detection, resilience, and cyber defense strategies.
- Developed and evaluated cyber threat detection models for distributed network environments - improving detection accuracy over baseline approaches in simulated large-scale network conditions.

Application Security Engineer | TERAWORK, Lagos, Nigeria *Oct 2017 - Nov 2019*

- Conducted comprehensive SAST/DAST assessments and penetration testing across web applications and APIs - identifying and remediating 50+ critical and high vulnerabilities, including OWASP Top 10 risks, improving overall security posture by 40%.
- Designed, deployed, and managed WAF infrastructure - configuring rule sets, tuning policies, and enforcing traffic controls to protect web applications against injection attacks, XSS, and application-layer threats.
- Collaborated directly with developers to deliver actionable secure coding guidance - conducting secure code reviews, running OWASP-focused training sessions, and embedding security awareness into the engineering culture.
- Participated in application security incident response efforts - leading triage, containment, and post-incident remediation for web application security events and implementing controls to prevent recurrence.

Network Security Engineer (Intern) | Cyberspace Network Limited *Aug 2015 - Jan 2016*

- Configured and managed Cisco routers, switches, and firewall infrastructure - enforcing network security policies, access controls, and segmentation rules across organizational and client network environments.
- Monitored network traffic and security events across SOC infrastructure - supporting IDS deployment and tuning, identifying anomalies, and improving threat visibility across monitored network environments.

TECHNICAL PROFICIENCY

Web & App Security: OWASP Top 10 (Web, Mobile, API, LLM), Threat Modeling, Penetration Testing, Vulnerability Management, Secure Code Review, Business Logic Assessment, Secure Design Review, WAF

AppSec Tooling: SAST/DAST, SCA, Burp Suite, OWASP ZAP, Semgrep, DefectDojo, Bandit, Coverity, Prime Security

Secure SDLC & DevSecOps: Secure SDLC, CI/CD Pipeline Security, Software Supply Chain Security, Secrets Management, Security Automation, Trivy, Dependency-Track, Syft, Grype, Checkov, Snyk

Cloud & Infrastructure Security: AWS (Lambda, EC2, S3, SageMaker, DynamoDB, IAM), GCP, Terraform, CloudFormation, Container Security, Docker, Kubernetes Security, Wiz, Jenkins, ScoutSuite

Security Protocols & Standards: PKI, TLS, OIDC, OAuth2, Identity Federation, IAM (On-Prem/Cloud), NIST CSF, PCI DSS, ISO 27001

Programming & Secure Coding: Python, C, C++, C#, Secure Coding Best Practices

AI & LLM Security: GenAI Security, LLM Security, Agentic AI Security, OWASP LLM Top 10

EDUCATION

PhD, Computer Engineering (with Distinction) | University of New Mexico, Albuquerque, NM*2020 - 2023*

MS, Computer Engineering (with Distinction) | University of New Mexico, Albuquerque, NM*2020 - 2021*

BS, Electrical and Electronics Engineering | University of Lagos, Nigeria*2011 - 2016*

PROFESSIONAL DEVELOPMENT

- SANS SEC522 - Application Security: Securing Web Applications, APIs & Microservices | GIAC/SANS Institute (In Progress - 2026)
- Coursera - Application Security for Developers and DevOps Professionals (Aug 2025)
- PACT Network Security - Partnership for Proactive Cybersecurity Research and Training | Mar 2022