EMMANUEL TIGOUE

Atlanta, GA | (404) 839-2214 | emmanueltigoue@gmail.com | LinkedIn | GitHub | Portfolio

SUMMARY

Security Engineer delivering AI-augmented cloud security platforms for **12 clients** on AWS. Integrates **LLM-driven automation** with SOAR orchestration for threat detection and incident response. Reduced attack surface by **85%** through Zero Trust architecture with **Splunk SIEM**, **Nessus**, and Wireshark.

CERTIFICATIONS

CASP+ (SecurityX), DoD 8140 IAT/IAM Level III | **AWS Certified Security – Specialty** | **SSCP** | **CCNA** | Security+ | Network+ | $(ISC)^2$ CC

Security Clearance: Eligible

PROFESSIONAL EXPERIENCE

CoreDirective — **Security Engineer**
Atlanta, GA | Sep 2025 – Present

- Delivered AI-augmented cloud security platforms for clients, integrating LLM orchestration, automated threat detection, and SOAR workflows processing live traffic **24/7** on AWS infrastructure
- Architected a Zero Trust access framework using Cloudflare Tunnels and identity-aware proxy across **6 production services**, eliminating all exposed ports and reducing lateral movement risk by **85%**
- Deployed production **LLM infrastructure** (Claude, Ollama) behind API gateway authentication with container isolation, enabling **AI-driven** security analysis and automated incident response for client environments
- Engineered AWS-native threat detection (GuardDuty, CloudTrail, Security Hub) processing **10,000+** daily events, reducing mean time to detect from **48 hours** to **4 hours**
- Automated **12** security operations workflows integrating Claude AI and SOAR orchestration, eliminating **20+ hours/month** of manual alert triage and enrichment
- Codified **30+** AWS resources via Terraform with enforced security baselines across VPC, IAM, EC2, and S3, eliminating configuration drift
- Hardened **8** Docker containers on Linux with network segmentation, unprivileged execution, and read-only filesystems, reducing container attack surface by **90%**

Texaco — **IT Operations Manager**
Atlanta, GA | Mar 2022 – Feb 2026

- Sustained **99.5%** network uptime over **2.5 years** across routers, switches, firewalls, and DNS infrastructure supporting continuous retail operations
- Segmented POS payment traffic into dedicated VLANs, reducing broadcast domains by **70%** and aligning network architecture with **PCI-DSS** requirements
- Administered Active Directory group policies enforcing password complexity, least-privilege access, and software restriction, preventing unauthorized application installs across all endpoints
- Automated user provisioning and credential rotation via PowerShell, reducing onboarding from **2 hours** to **20 minutes** per account
- Led incident response for **95%** of network security incidents within **2-hour SLA**, performing traffic analysis with Wireshark for root cause identification

TECHNICAL SKILLS

Security Architecture & Governance: Zero Trust (NIST 800-207), Defense in Depth, MITRE ATT&CK, Threat Modeling, Risk Assessment, Vulnerability Assessment, Penetration Testing, Incident Response, Vulnerability Management, NIST 800-53, CIS Controls, ISO 27001

Cloud & Application Security (AWS): IAM, GuardDuty, CloudTrail, Security Hub, Inspector, Config, VPC, Security Groups, KMS, Secrets Manager, WAF, S3 Encryption, Organizations, SCPs, Terraform IaC, GitHub Actions

Identity, Network & Endpoint Security: Active Directory, RBAC, MFA, SSO (SAML/OIDC), VLAN Segmentation, Firewall Rules, ACLs, VPN (IPSec/SSL), IDS/IPS, DNS Security, Cloudflare Zero Trust, Wireshark, Nmap

Security Operations & Automation: Splunk SIEM, Log Analysis, Nessus, Burp Suite, SOAR Orchestration, AI/LLM Security Integration, Python, PowerShell, Bash, Docker Container Hardening, Automated Remediation Workflows, Linux, Windows Server

EDUCATION

Georgia State University — Atlanta, GA
BBA, Computer Information Systems (Cybersecurity) | BBA, Business Economics | **GPA: 3.7** | May 2026
A.S., Business Administration | May 2025 | *Dean's List: Fall 2024, Spring 2025*