Emmanuel Tigoue

Atlanta, GA | 4048392214 | etigoue@tigouetheory.com | LinkedIn | GitHub | Portfolio

CERTIFICATIONS

CISSP (In Progress, March 2026) | SecurityX, DoD 8140 | SSCP | CCNA | Security+ | Eligible for Security Clearance

EXPERIENCE

AI Security Engineer | CoreDirective
Atlanta, GA | Sep 2025 - Present

- Secured OpenClaw production AI gateway running Claude Opus **4** inference against OWASP Top **10** for LLM Applications and **MITRE ATLAS** threat models, securing all AI-powered services across inference and NeMo-sandboxed local model pipelines.
- Red teamed all deployed skills for prompt injection, jailbreak, system prompt leakage, excessive agency, and data exfiltration, remediating findings before production launch.
- Reduced the external attack surface to zero exposed ports by routing all traffic through Cloudflare Zero Trust tunnels with mTLS certificate authentication.
- Cut security alert noise from **200+** daily events to **12** actionable findings by tuning Falco eBPF runtime rules and routing critical alerts to Datadog dashboards via Falcosidekick.
- Built a shift-left CI/CD pipeline with Trivy container scans, Semgrep SAST, Gitleaks secrets detection, and OPA policy gates on every pull request. Signed all images with Cosign and generated SBOMs with Syft for supply chain security.
- Executed authenticated DAST assessments using OWASP ZAP against the production SOAR platform, verified zero injection vulnerabilities across **8** attack categories, identified and remediated **4** header misconfigurations same-day through Cloudflare transform rules.
- Defined all infrastructure as code across **16** Terraform files managing **30+** resources on DigitalOcean and Cloudflare, with **8** OPA/Rego policies blocking non-compliant deployments.
- Eliminated standing admin privileges by deploying Teleport PAM with JIT access provisioning and session recording, and centralized IAM through Keycloak SSO with role-based access control.
- Automated security operations through n8n SOAR with NVIDIA NeMo-sandboxed AI workloads, local Ollama inference for sensitive triage data, and Claude API orchestration. Cut routine triage overhead by over 80% across credential rotation, compliance monitoring, and incident escalation.
- Authored **37** GRC documents from scratch: SSP with **800-53** controls mapped, POA&M tracking **37** findings across **4** assessment sources, **10** security policies, **5** IR playbooks, a risk assessment, and a tabletop exercise.

IT Security & Operations Manager | Texaco
Atlanta, GA | Mar 2022 - Feb 2026

- Led incident response across **3** retail locations, handling POS skimmer investigations with Wireshark packet analysis, credential compromises, and suspicious vendor access.
- Developed a **6**-step IR runbook that cut average containment time from **8** hours to **90** minutes.
- Segmented a flat network into **4** VLANs isolating POS payment traffic, back-office systems, guest Wi-Fi, and management. Validated with Nmap network scans. Reduced lateral movement to near zero.
- Deployed Splunk for SIEM log aggregation across all endpoints and network devices with correlation rules that cut mean time to detect from **48** hours to under **4** hours.
- Locked down Active Directory with Group Policy baselines, stale account removal, least-privilege admin rights, and automated credential rotation. Reduced critical audit findings from **14** to **2.**
- Maintained PCI DSS compliance with vulnerability management across **45+** devices, quarterly Nessus scans, network segmentation validation, SAQ documentation, and payment processor coordination.
- Built Python and PowerShell scripts automating patch deployment, user provisioning, compliance reporting, and service contract tracking. Recovered roughly **12** hours per week.
- Assessed and hardened Google Cloud IAM across **7** GCP APIs, implementing OAuth 2.0 lifecycle management, organization-level security policies, and cross-domain identity federation.
- Established AI governance policies aligned to NIST AI RMF and deployed LLM-powered analysis for automated phishing detection and incident prioritization across all locations.

TECHNICAL SKILLS

Technical Skills: Python, Bash, HCL, Docker, Linux, AWS, Google Cloud, Kubernetes, Terraform, Burp Suite, OWASP ZAP, OPA/Rego, LLM Security, DevSecOps, Adversarial ML, FISMA, RMF, ISO 42001

EDUCATION

Georgia State University, J. Mack Robinson College of Business
B.B.A. in Computer Information Systems (Cybersecurity) | BBA in Business Economics
May 2026 | GPA: 3.7 | Dean's List
A.S. in Business Administration – May 2025