

Oluwatobi Mustapha

Cloud Security Engineer | Detection Engineering | Incident Response | IAM | Kubernetes Security

Nigeria | oluwatobymustapha@gmail.com | [LinkedIn](#) | [GitHub](#) | [Portfolio](#)

PROFESSIONAL SUMMARY

Cloud Security Engineer with 4+ years of production security experience across AWS, Kubernetes, Linux, identity, detection engineering, incident response, vulnerability management and DevSecOps. I turn telemetry and suspicious activity into scoped findings, containment, remediation, recovery checks and durable controls. Founded Identrail, build AI-assisted defense workflows at CloudSec Network, established security operations at Probuilt Tech, and bring 29 merged upstream security fixes.

SECURITY ENGINEERING EXPERTISE

Detection & Response: security monitoring, SIEM, alert triage, threat hunting, incident investigation, containment, remediation, MITRE ATT&CK, runbooks and recovery validation

Cloud, Identity & Platform: AWS IAM, CloudTrail, GuardDuty, Security Hub, OIDC, OAuth2, Keycloak, Okta, Authentik, Kubernetes, Docker, Linux, Terraform, RBAC, JIT access and secrets

Application & Vulnerability Security: Burp Suite, Nmap, Metasploit, OWASP Top 10, vulnerability management, root-cause analysis, access-control review and remediation reporting

Automation & Delivery: Python, Go, Bash, PostgreSQL, APIs, gRPC, GitHub Actions, CI/CD, SBOMs, Cosign, CodeQL, dependency review, telemetry and technical writing

PROFESSIONAL EXPERIENCE

Founder & Lead Security Engineer - Identrail

• Feb 2026 - Present

Production machine-identity security company and cloud platform

- **Founded and built a machine-identity security platform** that maps AWS IAM, GitHub Actions OIDC and Kubernetes relationships to expose overprivileged workloads, risky trust paths and clear remediation ownership; shipped a CLI, Docker image, API and hosted web application.
- **Build and operate production security workflows** across AWS, Kubernetes, Docker, Terraform, Go, Python and PostgreSQL, maintaining telemetry, detection rules, alerting, service recovery, runbooks and recovery validation.

Security Engineer - CloudSec Network

• Apr 2026 - Present

AI-assisted defense workflows, detection design and analyst triage

- **Build AI-assisted detection and triage workflows** across application, cloud, IAM, CI/CD and endpoint signals, improving alert quality and investigation context for analysts.
- **Translate security findings into validated remediation guidance** and operator-ready workflows that connect detection design to response, root-cause analysis and durable engineering fixes.

Cloud & Identity Security Engineer - Independent

• Feb 2024 - Feb 2026

Identity engineering, cloud security and upstream open-source work

- **Hardened identity and cloud control paths** across Keycloak OIDC, Okta federation, AWS web-identity credentials, Authentik OAuth2, Better Auth cryptographic validation and Cloud Custodian IAM telemetry.
- **Built IAM Logic Fuzzer and Boundary:** reduced manual IAM audit time by approximately 90% while enforcing CIS AWS Benchmarks; reduced JIT access provisioning from days to seconds with audit artifacts. Delivered 29 merged upstream security fixes across seven security repositories.

Cyber Security Analyst - Prodigy InfoTech

• Mar 2023 - Feb 2024

Vulnerability assessment, penetration testing and Linux security

- **Performed vulnerability assessments and penetration tests** on Linux-based targets using Burp Suite, Nmap and Metasploit; identified OWASP Top 10 risks and produced severity-ranked remediation reports.
- **Supported incident-response investigations and root-cause analysis** while hardening Linux through firewall and access-control reviews.

Information Security Analyst - Probuilt Tech

• Jan 2021 - Feb 2023

Company-based security operations, incident response and vulnerability management

- **Helped establish security operations processes** as an early security-team member, replacing ad-hoc response with repeatable workflows for investigations, escalation, vulnerability management and remediation.
- **Co-authored incident-response playbooks and runbooks** for triage, escalation, containment, recovery and post-incident review; partnered with engineering on actionable remediation.

SELECTED PROJECTS & OPEN-SOURCE CONTRIBUTIONS

Projects built · Identity, cloud and SecOps tooling: [Identrail](#): machine-identity security for AWS, GitHub OIDC and Kubernetes; [Boundary](#): JIT access broker with approval, expiry and audit evidence; [IAM Logic Fuzzer](#): IAM privilege-escalation fuzzer with CIS validation. Reduced manual IAM audit time by approximately 90% and moved JIT provisioning from days to seconds with audit artifacts.

Security investigations and technical write-ups · Incident response, endpoint and network analysis: [AWS incident response](#), [EDR](#) and [Wireshark traffic analysis](#) covering identity abuse, endpoint telemetry, C2 traffic, evidence and recovery actions.

[Fintech SOC Assessment](#) · 47 Datadog SIEM signals triaged; IAM, CloudTrail and S3 key containment; Log4Shell and KRI control validation.

Open-source contributions · 29 merged PRs: [Keycloak](#) · 37k; [Home Assistant Core](#) · 91k; [Better Auth](#) · 30k; [authentik](#) · 26k; [Cloud Custodian](#) · 6k; [Terraform AWS Provider](#) · 11k; [ZITADEL](#) · 15k.

CERTIFICATIONS & EDUCATION

AWS Certified Security - Specialty | AWS Solutions Architect - Associate | HashiCorp Terraform Associate | CompTIA Security+ | Non-Human Identity Certified Professionals (OASIS)

Ambrose Alli University | B.Eng., Electrical Engineering | Magna Cum Laude