AYODEJI ALABI

Kitchener, Ontario • (437) 566-0419 • ayotwice@gmail.com

PROFILE STATEMENT

Strategic and hands-on Security Professional with years of progressive hands-on experience in Security Operations, Incident Response, Threat Detection Engineering, and GRC. Proven expertise in shaping detection and response capabilities, leading critical incident investigations, and automating operational efficiencies in security processes. Known for blending technical mastery with sound judgment to reduce risks, improve detection quality, and accelerate response maturity. Passionate about building secure, scalable systems and cultivating security-first cultures that align with business agility.

COMPETENCIES & SKILLS

Core Competencies

Security Incident Response & Management • Threat Detection Engineering & Tuning • SIEM, EDR & Automation Tooling • Security Operations & Playbook Development • Threat Intelligence & Threat Hunting • Compliance (SOC 2, ISO 27001, NIST, HIPAA) • Security Tooling (CASB, SWG, DLP, SSE) • Internal Security Controls & GRC Frameworks • Risk-Based Decision Making & Stakeholder Engagement • Enterprise Security Architecture • Security Risk & Threat Modelling • Secure Cloud Architecture (Azure, AWS, GCP) • DevSecOps Integration (CI/CD, SAST, DAST, SCA) • Forensics Coordination • Vendor Security & Contractual Risk Oversight • Security Policies, Procedures & Controls • Vulnerability & Penetration Testing • Identity & Access Management (IAM) • Infrastructure as Code (IaC) Security • Key Risk Indicators (KRI) Development • Security Metrics & Reporting Automation • Information Security & Privacy Principle • Security Awareness & Training.

Technical

Cloud Platforms: AWS, GCP, Azure, OCI
Authentication/Authorization: OAuth2.0, SAML, PKI, TLS/SSL
Security Tools: HashiCorp Vault, SIEM (Splunk, Wazuh, Elastic, Cribl, Logstash, Fluentd, Devo), SOAR (Shuffle, Tracecat, Tines), EDR (Crowdstrike, SentinelOne, Sophos), IDS/IPS, Vulnerability Scanners (Qualys, Nessus), Prometheus, Grafana, Datadog, Entra ID, DSPM, SSPM, Palo Alto Prisma Access, SAST, DAST, SonarQube, Trivy, Burp Suite, OWASP ZAP, CASB, SWG, DLP, Zero Trust Architecture.
DevSecOps & CI/CD: Kubernetes, Docker, GitLab CI/CD, Jenkins
Frameworks: SOC2, ISO27001, GDPR, NIST Series, MITRE ATT&CK, HIPAA, PCI DSS, FedRAMP, IT SOX, CIS Controls, PIPEDA.
Other Tools: Jira, Confluence, MS Power BI, Tableau, Metabase, Compliance as Code
Automation & Scripting: Python, Bash, Terraform, Ansible, PowerShell
Compliance Platforms: Drata, Vanta, CISO Assistant

Soft

Persistent Problem Solver – “No stone unturned” approach
Fast Learner & Adaptive in High-Velocity Settings
Communicates Complex Ideas Simply & Effectively
Strong Documentation & Knowledge Transfer Ethos
Collaborative with Engineers, Product, and Security
Driven by Curiosity, Precision, and Outcomes

PROJECT HIGHLIGHTS

- **Threat Risk Assessment Program:** Delivered over 25+ security assessments for internal systems and third-party integrations, providing control recommendations that reduced potential risk exposure by 30%.
- **Cloud Security Control Baselines**: Designed and implemented cloud governance frameworks in AWS and Azure for risk-based access management and compliance monitoring.
- **Risk Register + IR Playbook:** Built a scalable, business-wide risk management workflow and incident response playbook, enabling faster executive decision-making and clearer stakeholder communication
- **Automation of GRC Activities**: Leveraged Vanta to streamline evidence collection and reporting, reducing audit preparation time by 40%.
- **Security Risk Metrics Automation:** Designed a security risk tracking system that automated the collection, visualization, and reporting of security metrics, reducing manual effort by 30%.
- **Security Hardening Automation**: Developed a Terraform-based IaC framework embedding AWS security controls

(encryption, logging, IAM least privilege) used across 7 business units.

- **Cloud Security Posture Management (CSPM)**: Implemented tools like Prowler and AWS Config to provide continuous compliance insights.
- **Vendor Risk Management Program**: Led the implementation of a vendor risk management lifecycle, including contract security clauses, SOC 2 reviews, and third-party risk scoring using SIG Lite templates.
- **Zero Trust Enablement**: Integrated user and device trust signals with SSO and conditional access controls using Azure AD and Okta.

EXPERIENCE

IT Operations, Risk, Security & Strategy ***September 2019 – Present***
Honoris United Universities

- Developed automated security baselines using Terraform modules aligned with CIS AWS Foundations Benchmark.
- Led multiple incident response investigations across cloud and hybrid environments, reducing response time by 45% via tailored playbooks and enriched automation.
- Developed internal tooling in Python to streamline alert triage, IOC enrichment, and automated ticket creation.
- Tuned SIEM alerts in Sentinel and Splunk to reduce false positives and align with MITRE ATT&CK techniques.
- Integrated vulnerability scanning tools into CI/CD pipelines, reducing deployment-time risks by 65%.
- Built incident response runbooks and monitored telemetry data using CloudWatch and GuardDuty.
- Conducted security architecture reviews for microservices deployed in Kubernetes clusters.
- Implemented unified endpoint detection and response (EDR) and logging systems across on-prem and hybrid infrastructure.
- Integrated key rotation and secrets management workflows using AWS KMS and Vault.
- Facilitated adoption of secure-by-default engineering practices through playbooks and training.
- Partnered with DevOps to embed security guardrails in CI/CD pipelines using GitHub Actions and automated SAST tools.
- Coordinated ISO 27001 readiness and implemented risk treatment plans that aligned with identified gaps.
- Conducted threat modeling for logging infrastructure & developed risk mitigation plans to address telemetry data gaps.
- Facilitated quarterly tabletop exercises simulating telemetry outages and SIEM failures, enhancing team readiness & SLAs.

IT Systems and Security ***June 2017 – August 2019*** Honoris United Universities

- Assisted in the continuous improvement of incident response playbooks, enhancing response accuracy and timeliness by integrating learnings from incident retrospectives.
- Conducted proactive threat assessments and logged findings into Tenable.io, effectively identifying and remediating risks to decrease the organization's threat surface.
- Led SIEM implementation, enhancing threat detection and response capabilities.
- Managed security incident response efforts, coordinating with technical teams to resolve vulnerabilities and improve system security.

System Admin & IT Security Specialist ***April 2012 – May 2017***
Sidmach Technologies

- Analyzed security controls and conducted risk assessments to ensure alignment with internal and external compliance requirements.
- Supported PKI deployments and managed secure remote access via VPNs and federated identity.
- Led patch management and vulnerability remediation processes, reducing exploit risks.
- Executed end-to-end project management for complex IT security initiatives, including risk mitigation strategies.
- Facilitated disaster recovery and business continuity planning for the organization's IT infrastructure.

EDUCATION & PROFESSIONAL AFFILIATIONS

B.Eng. in Electrical Electronics Engineering FUTA

ISACA Member

TRAININGS & CERTIFICATIONS

Chainguard - Painless Vulnerability Management
AWS SimuLearn: Cloud Practitioner, Solutions Architect, Security
Securiti PrivacyOps, AI Security & Governance, Data Command Center Fundamentals.
Alison GDPR, Data Protection Officer, ISO 42001 AIMS, AI Risk Management and Incident Response
Onetrust Tech Risk & Compliance Professional,
ISO 27001 Lead Implementer,
PWC Risk Based Internal Audit,
Microsoft Certified Specialist Virtualization, Azure infrastructure Solution, Security, Compliance, and Identity Fundamentals,
Rackspace Cloud Technician,
Data Privacy Fundamentals.