TOHEEB A. HUSAIN

Cloud Security Engineer | DevSecOps | Detection Engineering

toheeborelope@gmail.com | +44 7508 859056 | Northampton, UK toheebahusain.com | LinkedIn | GitHub

PROFESSIONAL PROFILE

Cloud Security Engineer with hands-on experience securing cloud-native applications, infrastructure, and enterprise environments across AWS, Azure, GCP, and Kubernetes. Skilled in DevSecOps, SIEM/SOAR, detection engineering, IAM, threat intelligence, and infrastructure-as-code. Proven ability to embed security throughout the software delivery lifecycle, automate cloud governance, and translate technical findings into actionable risk reduction. Recognised for practical problem-solving, open-source contributions, and award-winning AI innovation.

CORE SKILLS

Cloud Security	AWS, Azure, GCP, Microsoft Entra ID, Kubernetes, IAM, RBAC, Least Privilege, CSPM, Cloud Risk Assessments, Audit Logging, Compliance Alignment
DevSecOps & AppSec	OWASP Top 10, Secure SDLC, STRIDE Threat Modelling, SAST (SonarQube), DAST, Trivy, Checkov, Cosign, SBOM, Secrets Management (Vault), Supply Chain Security, OPA Gatekeeper
Detection & SOC	Microsoft Sentinel, KQL, Chronicle SIEM/SOAR, Azure Logic Apps, Detection Engineering, MITRE ATT&CK, D3FEND, Cyber Kill Chain, IOC Analysis, OSINT, Sigma Rules, Malware/Phishing Analysis
Automation & IaC	Terraform, GitHub Actions, Docker, Falco, Grafana, Python, Java, JavaScript, PowerShell, Spring Boot, FastAPI, REST APIs, Git

WORK EXPERIENCE

Cloud Security Analyst Consultant — Amdari Nov 2025 – Present | Manchester, UK

- Delivered cloud security engineering across AWS and Azure: IAM design, SIEM/SOAR, IaC governance, and security automation.
- Designed Microsoft Entra ID / Azure RBAC models enforcing least privilege, cutting admin onboarding to under 5 minutes and reducing permission creep.
- Built a Microsoft Sentinel PoC centralising Azure Activity, Defender for Cloud, and Entra ID telemetry; developed KQL detections for privilege escalation and suspicious sign-ins.
- Deployed Terraform-managed AWS/Azure infrastructure with OIDC-based CI/CD, S3 remote state, DynamoDB locking, KMS encryption, and production approval gates.
- Secured Kubernetes environments via workload hardening, OPA Gatekeeper policies, Falco runtime detection, HashiCorp Vault secrets injection, and Cosign image signing.

Cyber Threat Intelligence Analyst Intern — CSFI May 2025 – Feb 2026

- Delivered actionable intelligence reports using MITRE ATT&CK, D3FEND, and Cyber Kill Chain to strengthen organisational defence strategies.
- Analysed 50+ phishing domains, mapped adversary TTPs, and enriched threat feeds through malware sandbox analysis.
- Conducted OSINT-based threat hunting to identify IOCs and emerging threat trends; collaborated on RFIs and presented findings to stakeholders.
- Awarded Daria-Romana Pop Award — Best Intern, recognising standout cohort impact.

KEY PROJECTS

SecureFlow: End-to-End DevSecOps Security Platform 2026

- Identified and remediated 40+ vulnerabilities across a cloud-native banking platform; mapped to OWASP Top 10 and STRIDE threat model.
- Integrated SAST (SonarQube), secrets detection (Gitleaks), container scanning (Trivy), IaC scanning (Checkov), and a risk-based Security Gate blocking critical findings in CI/CD.
- Implemented HashiCorp Vault with Kubernetes auth and Vault Agent Injector, eliminating hardcoded secrets across manifests and source code.
- Deployed Falco + Grafana for runtime threat detection; implemented Cosign/SBOM for software supply chain integrity.

Cloud Threat Detection & Automated Response — Microsoft Sentinel 2026

- Centralised Azure Activity, Defender for Cloud, and Entra ID telemetry into a Log Analytics Workspace; built KQL analytics rules for suspicious sign-ins and out-of-hours privilege changes.
- Automated incident response with Azure Logic Apps playbooks; deployed entire solution via reusable Terraform templates, improving consistency and audit readiness.

AWS IaC & CI/CD Governance | SigmaHQ Open-Source Contributor 2025

- Migrated manual AWS console ops to Terraform + GitHub Actions with OIDC authentication, approval gates, and a full change-trail (commits → plan artifacts → deployment logs).
- Authored and merged a Sigma detection rule (PR #5801) improving DNS exfiltration coverage for Invoke-DNSExfiltrator — adopted by the global SigmaHQ repository.

EDUCATION

BSc Computer Science — First Class (Expected 2026)
University of Northampton | 2022 – 2026

CERTIFICATIONS

AWS Solutions Architect Associate | Google Cloud Cybersecurity Certificate
CompTIA A+ | Microsoft Azure AI Fundamentals
arcX Foundation Threat Intelligence Analyst

AWARDS & LEADERSHIP

▪ **Daria-Romana Pop Award — Best Intern, CSFI** | 2nd Place, Elevate Great AI Competition (£2,500) — Team Lead, SensoryNeural AI + IoT project
▪ Assistant Team Lead, CSFI (volunteer) | AI Society Volunteer, University of Northampton | SigmaHQ open-source contributor (PR #5801)