TOHEEB A. HUSAIN

NN4 8LG, UK

toheeborelope@gmail.com | LinkedIn | Portfolio |+447508859056

PERSONAL PROFILE

Cloud security-focused cloud engineer with hands-on experience in cloud risk assessment, identity and access management, threat intelligence, and security-focused automation, completing a BSc in Computer Science at the University of Northampton (First Class expected, 2026). Experience spans Microsoft Entra ID, GCP console, Azure CLI, Terraform, RBAC, phishing analysis, IOC development, and detection engineering, supported by projects in secure backend engineering, and privacy-by-design systems. Recognised for strong analytical writing, practical security problem-solving, and building secure, resilient systems across cloud, software, and cyber defence contexts.

CORE SKILLS

Cloud Security

Azure, Microsoft Entra ID, IAM, RBAC, least privilege, cloud security risk assessment, access control review, compliance alignment, audit logging, remediation support.

Security Operations & Detection

Threat intelligence, OSINT, IOC development, phishing analysis, malware sandbox analysis, MITRE ATT&CK, D3FEND, Cyber Kill Chain, Sigma rule improvement, threat reporting.

Infrastructure & Automation

Azure CLI, Terraform, PowerShell, security configuration, user provisioning automation, group management, role assignment, infrastructure auditing.

Engineering & Platforms

Python, Java, JavaScript, SQL, Spring Boot, REST APIs, Apache Kafka, H2/JPA, FastAPI, Docker, Git, MySQL, Oracle SQL, AWS.

Professional Strengths

Technical documentation, analytical problem-solving, stakeholder communication, cross-functional collaboration, project leadership, continuous learning.

EDUCATION

University of Northampton (UON) — BSc Computer Science

Northampton, UK | 2022–2026

First Class expected.

WORK EXPERIENCE

Cloud Security Analyst Consultant, AMDARI

Manchester | Mar 2026–Present

- Conduct cloud security risk assessments to identify vulnerabilities, review access controls, evaluate compliance alignment, and support remediation of security gaps across cloud environments.
- Contribute practical cloud security analysis aligned with secure configuration, governance, and risk reduction objectives.

Cyber Security Forum Initiative (CSFI), Cyber Threat Intelligence (CTI) Analyst Intern Jul – Aug 2025

- Delivered actionable intelligence reports using MITRE ATT&CK, D3FEND, and the Cyber Kill Chain to strengthen cyber defence strategies.
- Conducted OSINT-based threat hunting to identify indicators of compromise and emerging threat trends.
- Analysed 50+ phishing domains, mapped adversary TTPs to MITRE ATT&CK, and contributed to threat feed enrichment through malware sandbox analysis.
- Collaborated on RFIs and presented findings to stakeholders, strengthening written and verbal cyber intelligence communication.

PROJECTS

Cloud Threat Detection and Automated Response with Microsoft Sentinel

- Designed and deployed a Microsoft Sentinel proof of concept to tackle fragmented visibility, weak alert correlation, and slow manual incident response across Azure.
- Centralised Azure Activity, Defender for Cloud, and Entra ID telemetry into a dedicated Log Analytics Workspace to enable unified investigations and monitoring.
- Used KQL and analytics rules to build detections for suspicious sign-ins, privilege changes, and risky out-of-hours activity, and tuned incidents to reduce alert noise.
- Integrated Azure Logic Apps playbooks and Terraform templates to automate response workflows and deliver repeatable, infrastructure-as-code deployments.

Respond and Recover from a Cloud Data Breach (Google Cloud)

- Investigated and contained a cloud breach affecting a VM, firewall configuration, and public storage bucket that enabled data exfiltration through misconfigurations.
- Used Security Command Center to identify public exposure, excessive access, and logging gaps, then shut down the compromised VM and rebuilt it from a hardened snapshot.
- Locked down storage and firewall rules, enabled logging, and re-ran compliance checks to validate remediation and improved overall cloud security posture.

Cloud Infrastructure Security & IAM Automation (Azure)

- Designed and implemented a secure IAM architecture in Microsoft Entra ID, enforcing RBAC and least-privilege access across multiple administrative tiers.
- Automated user provisioning, group management, and role assignments using Azure CLI and PowerShell, reducing manual configuration and improving consistency.
- Conducted a security audit to identify excessive permissions and remediated misconfigurations by moving to group-based RBAC.
- Used Azure CLI, PowerShell, Microsoft Entra ID, and Terraform to demonstrate enterprise-aligned identity governance and access control practices.

SigmaHQ Detection Rule Contributor, 2025

- Authored and improved a Sigma detection rule for Invoke-DNSExfiltrator to strengthen behavioural detection of DNS-based data exfiltration.
- Collaborated with maintainers to refine signature accuracy and meet Sigma's global detection standards.
- Analysed tooling behaviour, refined detection logic, tested locally, and contributed a merged improvement to the official SigmaHQ repository.

CERTIFICATIONS

- Google Cloud Cybersecurity Certificate
- CompTIA A+
- Microsoft Certified: Azure AI Fundamentals
- arcX: Foundation Level Threat Intelligence Analyst
- Make Foundation

AWARDS & LEADERSHIP

- **Daria-Romana Pop Award**, Best Intern Award, CSFI, recognising standout impact during the internship cohort.
- **Assistant Team Lead, CSFI** — supports CTI task coordination, report review, and intern mentoring on a volunteer basis.
- **AI Society Volunteer, University of Northampton** — contributed to workshops and co-led a channel sharing AI opportunities and resources.
- **SensoryNeural – AI-Powered Sensory Support System, Team Lead** — 2nd Place, Elevate Great AI Competition (£2,500), leading a privacy-aware AI & IoT project for stress-responsive environments.
- Self-financed my degree while maintaining strong academic performance, demonstrating resilience and time management.