THOMAS HAGGATH

Wiltshire, UK | thomashaggath@protonmail.com | LinkedIn | Github | Portfolio

PROFESSIONAL SUMMARY

Senior Cloud Security Engineer specializing in AWS security incident response and detection engineering across multi-account enterprise environments. Leads complex investigations into IAM abuse, anomalous API activity, and credential compromise, leveraging CloudTrail, GuardDuty, and VPC Flow Logs to drive incidents from signal to containment. Designed automation to enrich GuardDuty findings and improved compliance outcomes by deploying AWS Security Hub and Macie in regulated environments.

PROFESSIONAL EXPERIENCE

Amazon Web Services (AWS), Managed Services

Cloud Support Engineer II **Dec 2024 - Present**

- Executed end-to-end containment across 10+ compromised-credential and IAM-abuse incidents: credential/session revocation, policy tightening, KMS hardening, and drift remediation, consistently meeting a 15-minute response SLA.
- Authored 7 incident response runbooks covering IAM misuse, detection workflows, and logging investigations, driving a 35% reduction in escalations and enabling consistent response across the team without senior involvement.
- Built AI-assisted operational automation with embedded data-protection guardrails, reducing process time by 45% while maintaining sensitive data controls.
- Engineered 3 Observability SOPs integrated with an AI agent to guide engineers through structured alert triage across a 350-engineer organisation, reducing onboarding friction, enabling self-serve diagnosis without escalation, and progressing the team toward autonomous agentic response workflows.
- Delivered Call Leader training to 60 engineers across multiple sites adapting to a new customer-facing escalation responsibility, equipping the team with communication techniques, de-escalation strategies, and scenario-based practice to handle high-pressure customer calls with confidence.
- Established as the primary Major Incident Management contact for large-scale service disruptions, leading calls across AMS to communicate incident status, coordinate available workarounds, and maintain structured updates to key stakeholders throughout the event lifecycle.

INFOSUM LTD

Information Security Compliance Analyst **Mar 2024 - Dec 2024**

- Raised AWS Config compliance from 68% to 94% by tuning controls, prioritizing remediation with engineering, and aligning accepted risk decisions.
- Developed Splunk dashboards to analyze authentication and network access patterns by geography, enabling infrastructure changes to reduce high-risk exposure.
- Assessed security findings using AWS Security Hub, AWS Config and NIST 800-61 guidelines, and coordinated remediation with engineering teams, which improved monitoring maturity and cut repeat control failures.
- Automated AWS Config conformance reporting using Python, accelerating identification of non-compliance and reducing manual review overhead each week.

Amazon Web Services (AWS), Managed Services

Cloud Support Engineer II **Dec 2021 - Mar 2024**

- Deployed and operationalized AWS Security Hub and Macie in regulated environments, aligning controls to NIST 800-53/800-61 and measurably strengthening audit outcomes.
- Design and implement Python-based SOAR automation to enrich GuardDuty findings with contextual IAM and account metadata, automatically triaging, correlating, and routing alerts to reduce manual triage effort and accelerate investigation workflows.
- Served as the primary escalation point for detection-driven AWS security incidents, leading investigations of IAM activity, anomalous API behavior, and VPC-level indicators using CloudTrail, CloudWatch Logs, and AWS Config, which accelerated incident resolution and helped prevent potential breaches.
- Tuned and engineered GuardDuty-related automation to reduce false positives and improve signal fidelity across multi-account customer environments.
- Led customer migrations into AWS using Control Tower and Landing Zone Accelerator, deploying secure landing zones with centralized logging, IAM guardrails, encryption defaults (KMS), and Config enforcement, reducing misconfigurations and accelerating secure delivery by 60%.
- Integrated endpoint telemetry (CrowdStrike, Trend Micro IPS/IDS) into operational investigations, strengthening correlation between cloud and workload-level signals.
- Standardized escalation paths and cross-team handoffs to improve response consistency across customer environments.

Cloud Security Engineer I **Jul 2020 - Dec 2021**

- Established a Security Incident Response SME program enabling structured, repeatable incident handling without elevated credentials, reducing containment time by 45% and lowering escalation volume.
- Led patch management troubleshooting for Windows and Linux enterprise workloads, improving compliance outcomes and reducing security backlog.

- Enhanced investigation workflows by enriching automation with IAM activity and CloudTrail context to support faster evidence-based decisions.
- Delivered training and enablement for engineers pursuing Security Incident Response SME accreditation, improving on-call readiness and response consistency.

Cloud Support Associate (Security Focus) **Jun 2019 - Jul 2020**

- Resolved security-related customer incidents across alerting, change management, and backlog remediation, reducing resolution time by 30%.
- Coordinated across security response stakeholders to improve time-to-acknowledge and investigation quality across support queues.

Evidence Talks Ltd (CCL Group)

Software Tester Intern **Aug 2017 - Aug 2018**

- Executed functional and regression testing of digital forensics products using test-case management tools, confirming usability and stability and ensuring the release met quality standards.
- Built Selenium (C#)-based automated UI tests to increase test coverage and repeatability.
- Supported penetration testing activities to identify product security risks and report findings to the team.
- Verified and refined digital forensics workflows across products to improve compatibility and reliability for end users.

CORE SKILLS

- **Cloud Security (AWS)**: IAM, KMS, VPC, AWS Organizations guardrails, Control Tower, Landing Zone Accelerator, CloudTrail, CloudWatch Logs, AWS Config, Security Hub, GuardDuty, Macie, Encryption and Key Management, Centralized Logging
- **Detection and Incident Response**: Alert Triage and Investigation, Containment Support, Evidence Capture, Root Cause Analysis, Post-Incident Follow-up, Runbooks and Escalation Paths, NIST 800-61
- **Vulnerability and Risk**: Vulnerability Management, Patch Management, Risk Management, Continuous Improvement, Cloud Security, InfoSec, Security Vulnerabilities
- **Monitoring and Telemetry**: Splunk (SPL investigations, dashboards), metrics and reporting, EventBridge, CloudWatch alarms and logs pipelines, Log Analysis, Correlation
- **Infrastructure and Delivery**: Secure Cloud Foundations, Networking and Identity, Infrastructure as Code (Terraform), Managed Services Delivery, Managed Service Provider
- **Automation and Scripting**: Python, PowerShell, Bash, Alert Enrichment, Reporting Automation, Workflow Automation
- **Security Tooling (Exposure)**: CrowdStrike, Trend Micro (IPS/IDS), Nessus
- **Professional Strengths**: Stakeholder Collaboration, Clear Technical Writing, Prioritization, Project Delivery, Training and Enablement

CERTIFICATIONS

- AWS Certified Security - Specialty (target: 2025)
- AWS Certified AI Practitioner (target: 2025)
- IT Security Foundations: Network Security
- Azure Cloud Fundamentals: Explore Cloud Services
- Splunk Fundamentals
- AMS Builder Award
- AWS Partner: Generative AI Essentials
- Patch Management Subject Matter Expert
- Security Incident Response Subject Matter Expert
- Monitoring Bar Raiser
- Active Directory Administration

EDUCATION

Bournemouth University **Sep 2015 - 2019**

BSc, Digital Forensics and Cyber Security *Bournemouth, UK*

- **GPA:** 3.0
- **Coursework:** Systems Design, Networking, Digital Forensics, Ethical Hacking and Countermeasures, Business Strategy, Software Programming (Java, Python)