THOMAS HAGGATH

Wiltshire, UK | thomashaggath@protonmail.com | LinkedIn | Website

PROFESSIONAL SUMMARY

Cloud Security Engineer with 6+ years of experience delivering security engineering and operational outcomes across enterprise AWS environments. Strong background implementing cloud security controls (AWS Security Hub, GuardDuty, Macie), vulnerability remediation, incident response (NIST-aligned), and security monitoring with Splunk. Proven ability to reduce manual triage through Python automation, build repeatable runbooks and governance, and enable engineering teams to respond to security events independently. Open to relocation to Chicago, IL and surrounding areas.

CORE SKILLS AND KEYWORDS

- **Cloud Security Engineering**: AWS Security Hub, Amazon GuardDuty, Amazon Macie, AWS Config, security guardrails, data protection, security governance, cloud threat detection, security posture management
- **Incident Response and Operations**: incident triage, containment support, NIST incident response, runbooks, escalations management, operational readiness, investigations support, alert tuning, false positive reduction
- **Vulnerability Management**: vulnerability remediation, patch management (Windows and Linux), security findings review, risk acceptance coordination, continuous improvement
- **Monitoring and Detection**: Splunk dashboards, log analysis, security monitoring, detection-based alerting, metrics and reporting
- **Infrastructure and Delivery**: AWS, Terraform, Infrastructure as Code (IaC), Kubernetes, Control Tower, Landing Zone Accelerator, secure cloud foundations
- **Automation and Scripting**: Python, PowerShell, Bash, workflow automation, reporting automation
- **Security Tooling Exposure**: Trend Micro (IPS/IDS), CrowdStrike, Nessus
- **Professional Strengths**: stakeholder collaboration, communication, project delivery, prioritization, documentation, training and enablement

PROFESSIONAL EXPERIENCE

Amazon Web Services (AWS), Managed Services
Operations Engineer II — *Manchester, UK* · **Dec 2024 - Present**

- Led cloud security initiatives for Public Sector customers by implementing AWS Security Hub, Amazon Macie, and NIST-aligned controls, reducing compliance gaps and strengthening audit outcomes in regulated environments.
- Automated GuardDuty alert triage and enrichment to reduce manual review effort and accelerate investigation and mitigation workflows for cloud threats.
- Embedded security controls and governance into customer delivery by partnering with engineering, operations, and security stakeholders, reducing audit preparation time and improving delivery velocity.
- Drove vulnerability remediation and infrastructure hardening initiatives, reducing recurring security issues and improving platform resilience.
- Built AI-assisted automation for operational workflows with data protection guardrails, reducing manual effort and cutting process time by 30% while maintaining confidentiality requirements.
- Developed and maintained operational runbooks and security documentation that enabled engineers to resolve the majority of alerts independently, reducing escalations and improving operational consistency.

INFOSUM LTD
Information Security Compliance Analyst — *Basingstoke, UK* · **Mar 2024 - Dec 2024**

- Improved cloud compliance outcomes by partnering with SRE to raise AWS Config compliance from 68% to 94% through control tuning, remediation planning, and accepted risk alignment.
- Developed Splunk dashboards to identify connection attempts by country, enabling infrastructure changes to mitigate high-risk access patterns and improve security monitoring visibility.
- Reviewed cloud security improvement findings and coordinated with engineering to implement recommended controls, closing key security gaps and raising monitoring maturity.
- Automated compliance reporting using Python to generate standardized AWS Config conformance reports, accelerating identification of non-compliance and reducing manual analysis.

Amazon Web Services (AWS), Managed Services
Operations Engineer II — *Manchester, UK* · **Dec 2021 - Mar 2024**

- Engineered automation for active GuardDuty alerts, reducing false positives and unnecessary escalations while improving detection coverage against common cloud threats.
- Served as point of contact for detection-based alerting and security incident response support, expanding enablement so engineers could resolve most security alerts without direct security engineer involvement.
- Led customer migrations to AWS using Control Tower and Landing Zone Accelerator, enabling secure landing zone deployment and accelerating implementation by 30% with fewer configuration errors.
- Supported endpoint and workload security assurance by working with IPS/IDS tooling (Trend Micro) and CrowdStrike to provide compliance reporting and customer confidence in security posture.
- Collaborated with team leads to improve operational processes and execution cadence, supporting delivery consistency across multiple customer environments.

Amazon Web Services (AWS), Managed Services

Operations Engineer I — *Dublin, Ireland* · **Jul 2020 - Dec 2021**

- Launched the Security Incident Response SME program to enable engineers to resolve incidents independently without elevated credentials, reducing containment time by 30% and lowering escalation volume.
- Contributed to the Patching SME program, resolving complex Windows and Linux patching issues for large enterprise customers and improving patch compliance outcomes.
- Supported security automation planning and implementation by integrating additional investigative context from customer accounts, improving incident response speed and decision quality.
- Earned Train the Trainer qualification and delivered training for engineers pursuing Security Incident Response SME accreditation, improving team capability and response consistency.

Amazon Web Services (AWS), Managed Services

Cloud Support Associate — *Dublin, Ireland* · **Jun 2019 - Jul 2020**

- Resolved customer issues across incident management, CloudWatch alerts, change management, service requests, and security backlogs, reducing resolution time by 30% and improving customer satisfaction.
- Triaged security incidents across multiple support queues and coordinated with security incident response stakeholders to improve time-to-acknowledge and time-to-resolution.

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)