THOMAS HAGGATH

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

PROFESSIONAL SUMMARY

Cloud Security Engineer with senior-level experience delivering security engineering and operational outcomes in enterprise AWS environments. Led initiatives that cut manual triage time by 40% through Python automation and boosted AWS Config compliance from 68% to 94% via control tuning and remediation. Skilled in implementing AWS Security Hub, GuardDuty, Macie, and Splunk-based monitoring while building repeatable runbooks and governance frameworks. Seeking to leverage cloud security expertise to strengthen the security posture and compliance of forward-thinking organizations.

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, Network security, Cloud Security, Information Security
- **Incident Response and Operations:** incident triage, containment support, runbooks, escalations management, operational readiness, investigations support, alert tuning, false positive reduction, NIST 800-61, ISO 27001
- **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, Cloudwatch
- **Infrastructure and Delivery:** AWS, Terraform, Infrastructure as Code (IaC), Kubernetes, Control Tower, Landing Zone Accelerator, secure cloud foundations, Managed Service Provider, Managed Services
- **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* **Dec 2024 - Present**

- Led security uplift for Public Sector AWS environments by implementing Security Hub and Macie, mapping controls to NIST requirements and strengthening audit outcomes in regulated accounts.
- Automated GuardDuty triage and enrichment using Python, correlating findings with CloudTrail events, VPC flow context, and account metadata to speed investigation and containment while reducing manual review effort.
- Embedded security governance into delivery by partnering with engineering and operations teams to standardize org controls, change guardrails, and evidence-ready logging across CloudTrail and CloudWatch Logs, improving audit readiness and reducing delivery friction.
- Drove vulnerability remediation and infrastructure hardening across cloud workloads, improving baseline security posture through tighter IAM permissions, secure KMS usage patterns, and Config-backed drift detection to reduce repeat findings.
- Built AI-assisted operational automation with data protection guardrails, ensuring sensitive customer data remained controlled while reducing process time by 30%.
- Authored and maintained incident response runbooks and operational procedures covering IAM, CloudTrail, CloudWatch Logs, and GuardDuty workflows, enabling engineers to resolve most alerts independently and reducing escalations.

INFOSUM LTD | *Information Security Compliance Analyst* **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* **Dec 2021 - Mar 2024**

- Engineered automation for AMS customers around active GuardDuty findings, tuning detection and triage logic to reduce false positives, increase signal fidelity, and improve coverage for common cloud threat patterns across IAM and VPC activity.
- Served as a primary escalation point for detection-driven alerts and security incident response support, building resolution paths that used CloudTrail, CloudWatch Logs, and Config to validate activity and drive remediation to closure.

- Led customer migrations into AWS using Control Tower and Landing Zone Accelerator, deploying secure landing zones with standardized networking (VPC), identity guardrails (IAM), encryption defaults (KMS), centralized logging (CloudTrail/CloudWatch Logs), and Config policies, reducing misconfigurations and accelerating delivery by 30%.
- Supported endpoint and workload security assurance of our customers by integrating IPS/IDS and EDR telemetry (Trend Micro, CrowdStrike) into operational reporting and posture checks, improving customer confidence in control coverage.
- Improved execution cadence across multiple customer environments by standardizing operational processes, escalation paths, and handoffs between teams to drive consistent delivery.

Operations Engineer I **Jul 2020 - Dec 2021**

- Established a Security Incident Response SME program to enable secure, repeatable incident handling without elevated credentials, cutting containment time by 45% and reducing escalation volume.
- Served as a Patching SME for Windows and Linux, diagnosing complex patch failures and coordinating change windows, improving patch compliance outcomes for large enterprise customers.
- Improved incident investigation speed by enriching security automation with CloudTrail context, IAM activity, and workload signals from CloudWatch Logs to support faster decisions during triage and response.
- Earned Train-the-Trainer and delivered enablement for engineers pursuing Security Incident Response SME accreditation, improving team readiness and response consistency across on-call rotations.

Cloud Support Associate **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 (GPA: 3.0) *Bournemouth, UK*

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