Thomas Haggath

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

Summary

Senior Cloud Engineer with over 6 years of operations and security operations experience, managing alerts and incident response across AWS environments in regulated settings. Skilled in threat hunting using GuardDuty and CloudTrail, vulnerability remediation, and NIST-based controls integration. Proven track record in automating response workflows and boosting compliance posture from 68% to 94%. Seeking to leverage broad security expertise to strengthen cyber defenses.

KEY SKILLS

- **Security Operations:** Security Monitoring SME, Infrastructure Monitoring SME, Information Security, Preventative Controls, SOC Experience, Security Operations
- **Threat Hunting and Incident Response:** Security Incident Response SME (NIST), Digital Forensics, Threat Hunting, Vulnerability Evaluation
- **Systems Administration and Patching:** Windows and Linux Patching SME, Linux System Administration
- **Professional Skills:** Communication, Adaptability, Problem-Solving, Team Collaboration, Leadership, Attention to Detail, Flexibility, Time Management

Work Experience

Amazon Web Services | *Operations Engineer II* **Dec 2024 - Present**

- Rejoined AWS Managed Services and led cloud security initiatives for Public Sector customers, implementing AWS Security Hub and NIST-based controls that reduced compliance gaps and improved overall security for managed services in regulated environments.
- Worked closely with engineering, operations, and security teams to embed security controls, compliance requirements, and best practices into customer AWS environments, leading to faster project delivery and improved audit outcomes.
- Enabled faster and more accurate security investigations by applying threat hunting methodologies and tools like GuardDuty and CloudTrail, which led to a measurable increase in threat detection rates and quicker incident resolution.
- Strengthened cloud security posture through infrastructure hardening, evaluating vulnerabilities, and patch management aligned with AWS security best practices.
- Designed AI-assisted automation tools for Operations Engineers that reduced manual work and cut process time by 30%, which sped up customer engagements, improved accuracy, and allowed the team to focus more on solving complex issues.
- Implemented security guardrails, data protection controls, and governance mechanisms to ensure customer data confidentiality while integrating automation into production workflows.
- Developed and maintained operational documentation and runbooks to support consistent security incident handling and knowledge sharing across teams.

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

- Created Splunk dashboards to support security operations by identifying connection attempts by country, enabling infrastructure changes.
- Worked with Site Reliability Engineer to implement changes to ensure compliance percentages were maintained or improved, reduced from 68% compliance to 94% compliance with accepted risk within AWS Config.
- Reviewed AWS Security Improvement Program findings and partnered with engineering to implement recommended controls, leading to the remediation of key security gaps and improved cloud security posture.
- Developed automation with Python to generate reports based on AWS Config conformance, allowing consistency with reporting and actionable items.

AWS Managed Services | *Operations Engineer II* **Dec 2021 - Mar 2024**

- Developed automation for active GuardDuty alerts within the SOC to reduce false positives and enhance security response time.
- Acted as the point of contact for Detection-based alerting and Security Incident Response, expanding training programs.
- Collaborated with Team Leads to optimise processes and addressed team grievances, resulting in improved efficiency.
- Led customer migrations to AWS using Control Tower and Landing Zone Accelerator, enabling clients to set up secure, scalable cloud environments 30% faster and with fewer errors.
- Worked with endpoint security tools (IPS, IDS through Trend Micro, CrowdStrike) to ensure full compliance reports.

Amazon Web Services | *Operations Engineer I* **Jul 2020 - Dec 2021**

- Released the Security Incident Response SME program, improving containment time for potential events.
- Contributed to the development and release of the Patching SME program, addressing complex patching issues.
- Played a key role in security operations automation planning and implementation, enhancing incident response times.
- Earned Train the Trainer qualification, elevating training initiatives and engaging others through training activities.

Cloud Support Associate **Jun 2019 - Jul 2020**

- Resolved customer queries on incident management, CloudWatch alerts, change management, service requests, and security backlogs, leading to a 30% reduction in resolution time and improved customer satisfaction ratings.
- Acted as an Operational Engineer managing multiple support queues, including security incidents, and improved response time by quickly triaging alerts and coordinating with the Security Incident Response team.

EDUCATION

Bournemouth University, Bournemouth **2019**

Digital Forensics and Cyber Security

- **Coursework:** Systems Design (2:1), Networking (2:1), Digital Forensics (1st), Ethical Hacking and Countermeasures (2:1), Business Strategy (2:1), Software Programming (Java and Python)