Thomas Haggath

Wiltshire | thomashaggath@protonmail.com | LinkedIn

Security-focused professional with over five years of experience in cloud operations at AWS, specializing in Security Incident Response, vulnerability management, and infrastructure hardening across Linux and Windows environments. Now pivoting toward a focused career in reverse engineering and cloud-based threat detection and response. Skilled in analyzing malicious behavior, dissecting threats, and building secure, resilient systems in cloud-native environments. Passionate about uncovering the mechanics behind malware and leveraging that knowledge to enhance incident response strategies. Seeking a challenging role where I can merge my cloud expertise with advanced reverse engineering capabilities to identify, analyze, and mitigate evolving threats.

KEY SKILLS

- Security Incident Response SME (NIST)
- Windows and Linux Patching SME
- Security Monitoring SME
- Infrastructure Monitoring SME
- Information Security
- Linux System Administration
- Digital Forensics
- Preventative Controls
- Communication
- Adaptability
- Problem-Solving
- Team Collaboration
- Leadership
- Attention to Detail
- Flexibility
- Time Management

EMPLOYMENT HISTORY

Operations Engineer II - AWS Managed Services, Manchester (Remote)
(*December 2024 - Present)*

- Continuation of previous role at AWS

Information Security Compliance Analyst - InfoSum, Basingstoke
(*March 2024 - December 2024)*

- Created Splunk Dashboards to identify connection attempts by Country, allowing for 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 results and worked with Engineering to implement during upcoming sprints.
- Developed automation with Python to generate reports based on AWS Config conformance, allowing consistency with reporting and actionable items.

Operations Engineer II - AWS Managed Services, Manchester (Remote)
(Dec 2021—March 2024)

- Developed automation for active GuardDuty alerts, reducing false positives and enhancing 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 engagements for migrations into AWS, utilising solutions such as Control Tower and Landing Zone Accelerator.
- Worked with endpoint security tools (IPS, IDS through Trend Micro, CrowdStrike) to ensure full compliance reports.

Operations Engineer I - AWS Managed Services, Manchester (Remote)
(July 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 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 - AWS Managed Services, Dublin Ireland (Hybrid)
(June 2019—July 2020)

- Resolved customer queries related to incident management, CloudWatch alerts, change management, service requests, and security backlogs.
- Acted as an Operational Engineer working on multiple queues, including those involving security incidents.

EDUCATION

Digital Forensics and Cyber Security - Bournemouth University, Bournemouth
(2019)

- 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)

INTERNSHIPS

Software Tester Internship - Evidence Talks Ltd, Milton Keynes
(Aug 2017—Aug 2018)

- Conducted quality testing and regression testing for new software versions to ensure functionality.
- Automated testing using Selenium C# for web-based products, improving testing efficiency.
- Performed penetration testing to identify potential risks within products.
- Ensured forensics workflows were compatible with different products, enhancing end-user experience.