Kieran Maher

Northwest England | 07398777137 | kieran@deeptrace.co.uk | www.linkedin.com/in/kieran-maher

Profile

I am an experienced Cyber Security Consultant and qualified Expert Witness (UK Register of Expert Witnesses) with a background in organisation-wide software deployments, digital forensics, incident response, and security engineering. I have acted as a named expert on software fitness-for-purpose and system analysis reports, and as assistant expert supporting instructed experts on complex software litigation, eDiscovery exercises and public inquiry work — including the Post Office and Grenfell Tower inquiries. With expertise in architecture, cloud computing & security, I provide clear, robust, and defensible technical opinions in legal and commercial contexts. I am also the founder of Traces, a managed digital evidence collection service, and have developed and deployed AI tooling in production within a large FCA-regulated enterprise — giving me current, practical experience of how AI-assisted software is built, deployed, monitored, and governed in commercial organisations.

AI & Software Development

- Founder and lead engineer of Traces, a managed digital evidence collection service — designed and built the platform end to end, from acquisition across mailboxes, code repositories and third-party APIs through to court-ready evidence bundles with documented chain of custody.
- Developed and deployed a production AI agent into Aviva's security tooling, automating analyst and engineering workflows across a 4TB-per-day SIEM estate.
- Advise on enterprise AI deployment, AI-specific threats, and the monitoring and logging of AI tooling as SIEM Lead within a regulated financial services organisation.
- Extensive hands-on experience building production software using AI development tooling, giving practical insight into how AI-assisted systems are designed, governed, and where they fail.

Skills & Abilities

- Explaining technical concepts in plain language
- Team management
- Digital forensics
- eDiscovery
- Software analysis
- Software deployment in organisations

Courses & Qualifications

- University of Central Lancashire – BSc Digital Forensics (2019)
- Open University – Software & The Law
- Reverse Engineering & Malware Analysis
- Cribl – Certified User
- AWS – Security Fundamentals
- AWS – Security Best Practices: Monitoring and Alerting

Experience

Founder & Lead Engineer | Traces (traceslab.com) | 2025 – Present

- Founded and built Traces, a fixed-fee managed digital evidence collection service for instructing parties, billed up front rather than on open-ended hourly expert rates.
- Designed and developed the collection pipeline and software architecture covering mailboxes, code repositories and arbitrary third-party APIs, producing court-ready evidence bundles with full chain of custody and collection documentation.

- Designed and developed the architecture and implementation of an analysis toolset, allowing for large-scale code comparison exercises to be conducted according to industry standards and replicable process.
- Structured outputs to load directly into mainstream eDiscovery platforms, allowing legal teams to obtain the core evidence for a matter with minimal technical overhead.
- Built the platform end to end using industry-current AI-assisted development tooling where appropriate, alongside cloud infrastructure, API integration and evidential-integrity controls.

Security Incident and Event Management (SIEM) Lead | Aviva | February 2025 – Present

- Platform owner and SME of Sentinel & Cribl log monitoring platforms within Aviva (4TB per day processed).
- Delivered SIEM onboarding, threat modelling, and cost-saving initiatives. Reduced Sentinel ingestion by 35% per day with no operational costs.
- Developed documentation and emergency processes for engineering teams, including outage procedures, disaster recovery, day-to-day operations including RBAC and governance compliance.
- Managed a team of 11 engineers, improving onboarding times and platform efficiency.
- Authored internal specifications that influence logging standards across Aviva.

Senior SME Security Engineer | Dentsu | August 2023 – February 2025

- Aligned to security architecture, I was the lead engineer on several large-scale software deployments, including Microsoft Defender deployment to 45,000 workstations and 6,000 servers.
- Migration of SIEM solution (1TB per day processed) to Azure Sentinel.
- Deployment of cloud-based solutions including CNAPP and CSPM tooling, heavily involved with project management.
- Ensured ISO 27001 compliance and led detection rule development with CSIRT, TI, and SOC.
- Utilised platforms including FireEye (now Trellix), Sentinel, Mimecast, Tenable, Defender, Proofpoint.

Cloud Security Engineer | Dentsu | September 2021 – August 2023

- Designed and deployed security solutions in Azure and AWS using Terraform / Ansible.
- Integrated SSO and audit platforms, and reviewed security architecture for best practice compliance.

Cyber Operations Analyst (Cloud) L3 | Dentsu | May 2020 – September 2021

- Managed vulnerability scanning and incident response across cloud platforms.
- Developed bespoke asset management tooling, used company-wide.
- Deputy SOC Lead, mentoring junior team members and organising training and shift patterns.

Senior Software & Systems Consultant (Expert Witness) | IT Group UK | May 2018 – May 2020

- Assistant and named expert on 30+ reports on software fitness-for-purpose, general IT consultancy, and system analysis for litigation.
- Conducted forensic acquisitions using Axiom and EnCase.
- Code review exercises covering a wide array of programming languages and technology, focused largely on JavaScript, Python, PHP, C++, C, C#.
- Undertook deep system analysis to understand the root causes of software failure and failure to deliver.
- Performed large-scale eDiscovery exercises using Intella and Relativity.
- Authored documents explaining complex technical concepts in plain language, to aid legal teams in understanding the technology involved.

Digital Forensic Examiner | IT Group UK | May 2017 – May 2018

- Assisted with digital forensic, eDiscovery, and mobile forensics investigations.
- Contributed to large-scale eDiscovery exercises and cyber incident responses.
- Developed open-source tools to advance forensic processes.
- Utilised Axiom, EnCase, Cellebrite, Relativity, Intella.