TOM WELSH

07477 530308 | twelsh37@gmail.com | LinkedIn | Colchester CO1, UK

CYBERSECURITY, AI, AND OPERATIONAL RISK PROFESSIONAL

A dynamic and results-driven professional with a proven track record of success in cybersecurity, operational risk management, and IT infrastructure. Leverages extensive experience and technical expertise to deliver cutting-edge AI and automation solutions that drive down costs and increase productivity. Recognized for successfully streamlining the risk and control self-assessment process, reducing the timeline from 6-9 months to just 3 months, and developing a robust risk management framework aligned with regional regulations.

A proactive leader, spearheaded the implementation of advanced technologies such as Darktrace and developed innovative data classification solutions. Holds a master's degree in cybersecurity and has pursued professional development in Python and Data Science from prestigious institutions like Harvard and Stanford. Actively contributes to industry knowledge through insightful publications on incident management and data visualization.

Brings a unique blend of technical acumen, strategic thinking, and leadership skills to drive organizational success and mitigate risks in an increasingly complex digital world. Committed to staying at the forefront of cybersecurity trends and leveraging cutting-edge technologies to protect critical assets and maintain a competitive edge.

KEY SKILLS

Cybersecurity | AI and Automation
Operational Risk | Vendor Risk Management | Due Diligence
Information Technology | Infrastructure | Python | Linux | KRI
Risk Controls Self-Assessment (RCSA) | Risk and Controls Assessment (RACA)
Presentation Skills | Fintech | Darktrace | Security Tools | Disaster Recovery (DR)
Business Continuity Planning (BCP) | International Experience | Mentoring | Change Management

PROFESSIONAL EXPERIENCE

Cybersecurity and AI Consultant **January 2024 - Present**

The AIAA

- Delivered Cybersecurity Solutions to global clients.
- Advised on AI and Automation for clients.
- Produced Risk reports for the clients detailing weak points in their infrastructure/products and suggested mitigations.
- Created Ai insights new letters that were delivered to clients.
- Delivered in person and remote training on Cybersecurity matters.
- Ran Incident Management workshops.
- Executed multiple rollouts of hardware, phones, and display equipment
- Delivered clients onsite support.

OPERATIONAL RISK MANAGER **July 2019 - September 2023**

CMC Markets

- Delivered Operational Risk function for the European operation post Brexit.
- Produced Operational Risk reports for the European Board to enable them to make informed, risk-based decisions.

- Facilitated the annual Risk and Control Self Assessments across our 14 global locations. Reduced the time taken from 6-9 months to 3 months.
- Advised on vendor risk management (VRM) to the procurement team. Worked with Legal, Compliance and Financial crime teams to assess and score third-party suppliers prior to onboarding. Worked with Finance and IT teams to carry out retrospective VRM on already onboarded external partners.
- Implemented automated Risk and Control Self Assessment statistic generation, enabling the relevant committees and the Board access to risk information on a global scale.
- Created Risk Appetite Statement and Risk Management framework for the European offices, ensuring it was in line with MaRisk and other regional regulation and legislation.
- Attended various committees and Boards relevant to Operational Risk, including the Change Board, Release Board and Project Board.

CYBERSECURITY ANALYST **April 2016 - July 2019**

CMC Markets

- Executed daily tasks and dealt with security incidents when they occurred.
- Acted as the escalation point for any security matters and deputised for the Head of Security.
- Attended several committees on the Head of Security's' behalf, including the Security Forum, Change Board and Release Board.
- Implemented Darktrace across the global network, working with third-party suppliers to ensure that the project was delivered on time and within budget.
- Advised on cybersecurity risks posed by third-party suppliers. Had an active part in third-party vendor management and risk scoring.
- Researched and implemented a solution that allowed the company to identify and classify data, across the IT estate.
- Liaised with Risk Teams and throughout the business, providing security-based advice around new products and processes.
- Created several security policies that were rolled out globally to protect the IT Infrastructure.

INFRASTRUCTURE ANALYST **November 2013 - April 2016**

CMC Markets

- Provided support across the department working in multiple capacities.
- Improved infrastructure and connectivity between systems and networks to enable optimal performance, which in turn enabled the trading platform to deliver timely results to clients.
- Established playbooks to enable colleagues to efficiently handle incidents should they occur with infrastructure.
- Created policies communicating the company view on a specific subject area.
- Created standards to implement detailing what was acceptable surrounding policies.
- Created procedures to enable the implementation of the standard in a uniform manner.

EARLY CAREER SUMMARY

- Third Tier Support Analyst, CMC Markets
- Technical Operations Analyst, CMC Markets

EDUCATION

- MSc Degree, Cybersecurity (distinction), Northumbria University

PROFESSIONAL DEVELOPMENT

- Harvard University CS50x – Introduction to Computer Science

- Harvard University CS50P - Introduction to Programming with Python
- Stanford University Code in Place – Python
- IBM PY0101EN – Python Basics for Data Science
- IBM DV0101EN – Visualizing Data with Python
- IBM DA0101EN – Analysing data with Python

PUBLICATIONS

- Incident Management – Chapter in Cyber-Security Practitioners Guide
- Python Masking Data Before Plotting
- Preparing a Dataset for Analysis
- Code Portability – From Mitosheet to Your IDE
- Understanding Plotly Sankey Charting
- Further Adventures in Plotly Sankey Diagrams
- Practical Prompting: A comparison between ChatGPT and Perplexity
- Creating Stunning Visualisations with Plotly: A Beginners Guide to Plotlys' Basic Charts
- Creating Stunning Visualisations with Plotly: A Beginners Guide to Plotlys' Part-of-Whole Charts
- Creating Stunning Visualisations with Plotly: A Beginner's Guide to Plotlys' 1D Distribution charts.

Technical Skills

- **Systems**: Proficient in handling x86 hardware, HP, Dell, IBM, SUN, and Cisco switches.
- **Operating Systems**: Extensive experience with Linux (Red hat, CentOS, Debian, Ubuntu), Solaris, and Windows.
- Proficient in TCP/IP, SNMP. SMTP, DNS, NFS, SAMBA, SSH, SCP, FTP.
- **Programming**: Skilled in Shell Scripting (Bash) and Python.
- **System Administration**: Experienced in Linux/UNIX and Windows System Administration.
- **Hardware and Software**: Proficient in hardware build and deployment, VMWare build, deployment and management, and troubleshooting skills in both hardware diagnostic and software/config diagnostics.
- **Project Management**: Experience in leading engineering activities, technical design and implementation, and datacentre moves, planning and execution.
- **Monitoring**: Advanced knowledge of Nagios monitoring platform.
- **Methodologies**: Experience and use of the scrum agile delivery methodology.
- **Configuration Management**: Configuration and change management skills.
- **APIs**: Knowledge of the implementation and use of various APIs.
- **AI**: Prompt engineering, Ai Automation tools, knowledge sharing.

Non-Technical Skills

- **Leadership**: Agile trained taking on a Scrum master role leading elements of the team's work. Professional leadership skills with experience running several teams of up to 8 people.
- **Communication**: Excellent presentation skills to audiences at all levels both technical and non-technical. Excellent planning and communications skills.
- **Teamwork**: Excellent team working and interpersonal skills.
- **Compliance**: Working to stringent SLAs and defined policies and procedures ISO9001, ISO20000, ISO27000, ITIL framework