

07885650238
twu18@yahoo.com

Tina Wu

Cyber Security Researcher

LinkedIn: Tina Wu

As a Senior Security Advisor, I specialize in reviewing RIIO submissions from Operational Energy Suppliers (OES) and drafting consultation documents that shape security policies within the energy sector. In addition to my advisory role, I am an active security researcher, collaborating with the AI Taskforce to draft AI guidance and whitepapers focused on the integration of AI technologies within the OT energy sector. My work bridges regulatory compliance, cutting-edge research, and practical applications, ensuring the continued resilience and innovation of the sector.

SKILLS

Tools and Languages	Python, Git, TeX , Markdown, machine learning (Scikit-learn).
Other Skills	Excel, R, MySQL
Courses	GIAC Certified Forensic Analyst (GCFA) (2014-2018), 62443, NCSC CAF, NIST, SEC510: Cloud Security Controls and Mitigations
Frameworks	NCSC Cyber Assessment Framework (CAF), NIS Directive (Network and Information Systems Directive), NIST (National Institute of Standards and Technology) Cybersecurity Framework, , Energy Licence Conditions

EXPERIENCE

Senior Security Advisor (SC Cleared) <i>Ofgem</i>	May 2024— Present <i>Cardiff, UK</i>
<ul style="list-style-type: none">Reviewed and assessed security submissions from Operational Energy Suppliers (OES) under the RIIO framework, ensuring that submissions met regulatory requirements and aligned with industry best practices for security and resilience.Authored comprehensive consultation papers for RIIO-funded OT/IT projects, totaling over £200 million, outlining key security and regulatory considerations, and ensuring alignment with industry standards and Ofgem's strategic objectives.Led the development and implementation of licence condition updates, ensuring that changes were accurately communicated to stakeholders and effectively integrated into regulatory frameworks to enhance security measures in the energy sector.Collaborated with internal teams and external stakeholders to align security strategies with evolving industry standards, advising on risk management, compliance, and resilience to safeguard the energy infrastructure from emerging threats.Contributed to the AI Taskforce, helping draft guidance for the OT sector on the integration and implementation of AI technologies, and led the authoring of a whitepaper on AI use cases, showcasing innovative applications in the energy sector and contributing to academic research on AI's role in OT	
Senior Compliance Lead (Secondment) <i>Ofgem</i>	May 2023 — May 2024 <i>Cardiff, UK</i>
<ul style="list-style-type: none">Conducted detailed compliance inspections, ensuring adherence to regulatory standards and identifying potential risks in operations, systems, and processes.Drafted comprehensive inspection reports outlining findings, non-compliance issues, and actionable recommendations, contributing to the development of regulatory frameworks.Facilitated engagement meetings with internal and external stakeholders, effectively communicating inspection results and providing guidance on corrective actions to ensure compliance.Analysed complex evidence from inspections and audits, synthesizing data to provide accurate assessments of compliance levels and support decision-making within the organization.	
Lead Cyber Researcher <i>Ofgem</i>	April 2021 — May 2023 <i>Cardiff, UK</i>
<ul style="list-style-type: none">Work closely with academia and energy operators in researching cyber security issues gathering requirements and engaging regularly with energy operators.Using agile project methodology to work on real-world research problems.Lead projects on implementing and deploying cloud solutions for ICS and anomaly detection using machine learning on ICS networks.Write technical guidance, report and whitepapers for the energy operators.Supervise a PhD student at Royal Holloway University, guiding a PhD student on a research project focused on Attack Modeling for Digital Substations. This involved developing the research framework, providing mentorship, and overseeing the design and execution of the project to model and assess potential security threats in digital substations.	
Industrial Research Fellow in Penetration Testing <i>University of Plymouth</i>	October 2020 — May 2021 <i>Plymouth, UK</i>
<ul style="list-style-type: none">Working on the Cyber-SHIP project and penetration testing maritime technology, including radars, Voyage Data Recorders (VDR), Electronic Chart Display and Information Systems (ECDIS), Automatic Identification Systems (AIS), and communications devices.Write technical reports and presentations to external parties.	

Research Engineer Cyber Security/Forensics*Airbus Group***October 2012 — October 2014***Newport, UK*

- Build relationships with academia and Airbus Group business units.
- Manage various research projects related to SCADA/CNI cyber security, forensics, Penetration testing, and malware analysis.
- Design and setup of the Digital Forensic testbed and deployment of AlienVault SIEM, configured and setup for testing.
- Manage of interns and supervision of PhD student's workload and assigning research tasks.
- Manage of external clients research projects.

Digital Forensic Volunteer*Humberside Police Hi-Tech Crime Unit***May 2012 — August 2012***Hull, UK*

- This role involved using different forensic software to analyse various media devices.

EDUCATION**PhD in Cyber Security**, *University of Oxford*

2015 — 2020

MSc in Forensic Computing and Security, *University of Derby*

2010 — 2011

BSc Forensic Science, *Nottingham Trent University*

2007 — 2010