Candidate Information

Position:	Research Fellow
School/Department:	Momentum 1.0 Trading
Reference:	26/113390
Closing Date:	Monday 27 July 2026
Salary:	£41,519 - £49,536 per annum
Anticipated Interview Date:	Friday 14 August 2026
Duration:	Fixed Term - Full Time; available for approximately 36 months (or until 31/07/2029)

JOB PURPOSE:

This role addresses research into the cyber security of Cyber-Physical Systems (CPS) and the complex integration of IT-OT environments within critical infrastructure and advanced manufacturing systems. This project will be hosted by the Centre for Secure Information Technology (CSIT: https://www.qub.ac.uk/ecit/CSIT/) at Queen's University Belfast. The role will include working with CSIT engineers in the design and implementation of high fidelity testbeds and experiments, that replicate real- world utilities, coordinating with industry and external research partners. You will conduct research to investigate detailed threat models, and create use-cases and experiments, applying CPS domain knowledge to map attack paths and physical process deviations, and develop scenarios where vulnerabilities are exploited in testbed environments. Experience in developing AI architectures or agentic frameworks is desirable, as the role may also consider autonomous cyber security responses and the need to ensure and validate that novel AI interventions are secure and effective in securing physical assets, and comply with relevant safety and regulatory constraints. Please note that the successful candidate will be required to undergo Baseline Personnel Security Standard checks.

MAJOR DUTIES:

1. Undertake high-quality and novel research in the area of cyber security of Cyber-Physical Systems (CPS) within critical infrastructure and advanced manufacturing systems.
2. Design, develop, and refine experiments to evaluate cyber threat detection and response approaches, using testbeds that reflect real-world IT-OT networks and devices.
3. Carry out analyses, critical evaluations, and interpretations using AI-based methodologies and other techniques appropriate to IT-OT systems.
4. Coordinate research tasks, work packages, deliverables and publications with external academic research partners and industrial collaborators, including external visits where appropriate.
5. Present regular progress reports on research to members of the research group or to external collaborators and audiences to disseminate and publicise research findings.
6. Prepare material, in consultation with the line manager, for publication in national and international journals and presentations at international conferences such as IEEE Security and Privacy and ACM Computer and Communications Security.
7. Produce high-quality research outputs consistent with project aims and commensurate with the career stage.
8. Undertake supplementary duties relevant to the success of the project including administrative duties and additional training and development activities as required.

ESSENTIAL CRITERIA:

1. Normally have or be about to obtain* a PhD in computer science, engineering or physical sciences. *must be obtained within 3 months of closing date of post.
2. Significant, relevant high quality research experience in cyber security related to critical infrastructure, advanced manufacturing, IT-OT, cyber-physical systems (CPS), or AI-based autonomous systems for cyber response, as evidenced by a strong track record of publications in leading journals and conferences in relevant areas.
3. Domain knowledge of critical infrastructure related technologies (IT-OT, CPS, ICS, etc.).
4. Software programming skills.

5. Excellent oral and written communication skills.
6. Articulate, confident, and able to clearly communicate complex concepts.
7. Ability to collaborative effectively as part of a team.
8. Prepared to work closely with industrial collaborators.
9. Demonstrate a high degree of integrity, honesty and openness in professional conduct.
10. Able to visit collaborative partners and to attend meetings and conferences nationally and internationally as requested.
11. On-site presence required in accordance with QUB policy (currently for a minimum 3 days per week).

DESIRABLE CRITERIA:

1. Have or be about to obtain a PhD in an area related to cyber security, security of IT-OT or CPS, or related to AI and machine learning.
2. Hands-on experience using IT-OT devices and technologies (e.g. PLCs, IEDs, and related network protocols such as Modbus, IEC61850, etc.).
3. Hands-on experience building testbed environments related to IT-OT, for data collection, threat modelling, pen-testing, etc.
4. Hands-on experience developing threat models and carrying out security related experiments, e.g. for data collection, pen-testing, security evaluations, and related outcomes.
5. Hands-on experience related to AI, machine learning and/or agentic systems.
6. Experience in initiating and developing research plans.
7. Experience in collaborating with industry.
8. Proficient in Python or C.
9. Experience related to transformers, clustering and anomaly detection methods.
10. Ability to design, train and test machine learning/AI systems using appropriate methodologies and datasets.
11. Experience leading, coordinating or managing research across multiple institutes or industry partners.