Job Description

Position / Job Title:	**Postdoctoral Research Fellow in AI-empowered Security Operations and Cyber Resilience (MosAIcSOC) (Fixed Term)**
Ref:	**887**
Location/Building:	**Poole House – Talbot Campus**
Faculty/Professional Service:	**Faculty of Media, Science & Technology**
Group/Section:	**School of Computing & Engineering**
Duration if Temporary:	**Fixed Term from January 2027 to August 2029**
Normal Hours per Week:	**37 hours / 1.0FTE**
(Some flexibility will be required in order to ensure that key time scales and deadlines are met).	
Grade:	**6**
Accountable to:	**Dr Ala Yankouskaya (Principal Investigator)**

Job Purpose

- To plan, design and conduct technical research within MosAIcSOC in AI-empowered security operations and cyber resilience, contributing to BU's technical work across the project.
- To contribute to the design, testing and validation of AI-enabled security capabilities, both in controlled experimentation environments and in real-world pilot settings.
- To provide technical input to BU's coordination and evaluation activities with consortium partners, linking research, development and pilot validation.
- To produce related published outputs and to disseminate the project results to academic, industry, policy and public audiences.

Main Responsibilities

Research

- Deliver the research objectives of BU's technical work within the timeframes of the project, ensuring the achievement of project deliverables, milestones and outcomes.
- Plan, design and conduct research using recognised approaches, methodologies and techniques in cybersecurity and artificial intelligence, including experimental design, prototyping, simulation, data analysis and evaluation.
- Undertake research on AI-enabled approaches to security operations, such as threat detection, incident analysis and response, situational awareness and decision support, with due attention to explainability, privacy and human oversight.

- Contribute to the design and use of simulation-based testing and experimentation environments (e.g., digital twins and cyber ranges) to study cyber threats, incidents and their wider operational impact under safe and controlled conditions.
- Contribute to the development of methods, metrics and evidence for assessing the performance, resilience and preparedness of security operations, including relevant regulatory perspectives.
- Collect, manage and analyse technical data and evidence to inform evaluation, refinement and reporting of project outcomes.

Technical collaboration and project contribution

- Attend and represent the BU team in work package, task and technical meetings.
- Contribute technical expertise to the deployment, integration, monitoring and evaluation of project technologies in pilot settings, working closely with technical and end-user partners.
- Work with consortium partners to translate operational and stakeholder requirements into technically sound and reproducible research and validation activities.
- Contribute technical input to project deliverables, periodic reports and review material, including clear documentation of methods, configurations and results.
- Support the Principal Investigator in planning and monitoring BU's technical contribution, identifying risks, dependencies and resource needs.
- Ensure the maintenance of data and records in accordance with the appropriate protocols, including research ethics approval, GDPR, the project Data Management Plan and the secure handling of security-sensitive information and results.

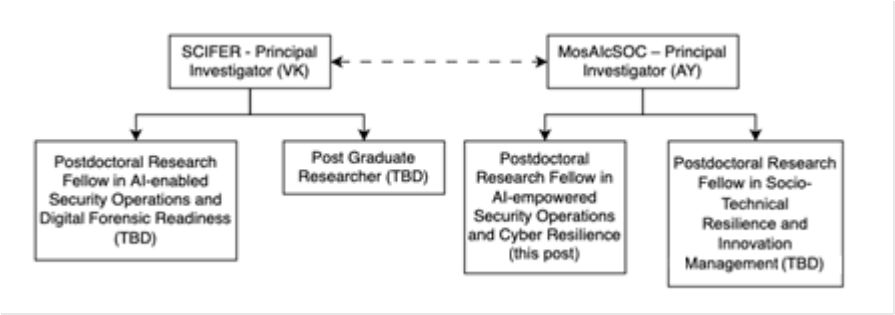
Innovation and sustainability

- Support the reuse, sharing and sustainability of technical outputs (e.g., software components, datasets and testing scenarios), in line with the project's intellectual property and security arrangements.
- Contribute technical input to innovation, exploitation and standardisation activities, including engagement with SMEs, technology providers and end-user organisations.

Dissemination and professional development

- Write up research work for publication, to include peer-reviewed journal and conference papers, project deliverables and reports.
- Present findings at national and international conferences, workshops and the project information day, and contribute to communication, knowledge exchange and public engagement activities.
- Contribute to technical workshops, demonstrations, training and exercise activities with end users, SMEs, public authorities and industry partners.
- Participate in team meetings and committees as appropriate and provide support and guidance to other staff and research students as appropriate.
- Continue to develop a body of published work relevant to own discipline both in terms of type and volume.
- Build relationships with internal and external contacts to exchange information, publish outputs and develop future collaborations and funding proposals.
- Undertake personal and professional development activities in line with the agreed appraisal and development programme to enhance personal knowledge and contribution to relevant activities.
- Contribute to the design and delivery of education activities in related subject areas.
- Supervise under/postgraduate students' projects, fieldwork, lab work, placements as appropriate.

Organisation Chart



MosAIcSOC is delivered at BU alongside SCIFER (SIEM Solutions for Critical Infrastructures sEcurity & Resilience), a sister Horizon Europe project in which BU is Technical and Innovation Manager and which is developing a federated, AI-native SIEM ecosystem and an AI-enabled Digital Forensic Readiness Framework for critical infrastructures. Both projects are delivered by a single BU research team, led by Prof. Vasilis Katos and based in the BU Cyber Competence Centre and its AI-powered Security Operations Centre of the Future. The team comprises three Postdoctoral Research Fellows, a PhD researcher (PGR) and two Research Assistants.

This post is one of two Postdoctoral Research Fellow posts that are shared and work across both projects. This post places its main emphasis on MosAIcSOC, with a complementary contribution to SCIFER, while the peer post places its main emphasis on SCIFER with a complementary contribution to MosAIcSOC. All members of the team are expected to collaborate and work with their peers across both projects, sharing methods, tools, testbeds and data where appropriate, so that the two projects reinforce each other.

Dimensions

Total project award: €5.9 million

MosAIcSOC (Modular Operational Security with AI-powered Intelligence and Collaboration for Security Operations Centers) is a 36-month, EU-funded collaborative project awarded under the HORIZON-CL3-2025-02-CS-ECCC-02 call and coordinated by Bournemouth University with 18 partners across Europe (Universities, SMEs, Industry, CERTs, Public Authorities and Healthcare Organisations). The project is developing a modular, AI-empowered Security Operations Centre (SOC) framework built around a Common Data Model, a trusted SOC App Store for validated security tools, Digital Twin environments for crisis simulation and resilience testing, federated learning and explainable, human-centred decision support. The framework will be validated in pilots across critical sectors, including healthcare and assisted living.

As Project Coordinator, BU leads project management, risk and quality management, and innovation and intellectual property management. BU also leads attack generation, crisis simulation and resilience validation, leads pilot execution, monitoring and data collection across all pilots, and is technical lead of Pilot 1 (healthcare and assisted living). The postholder will be a core member of the BU team and will focus on the technical research dimensions of BU's contribution, spanning AI-enabled security operations, simulation-based resilience testing and technical validation in pilot settings. Research delivery is the primary purpose of the post, supported by close technical collaboration with consortium partners to enable delivery of the project's research objectives.

Contacts:

Internal: Dr Ala Yankouskaya, Prof. Vasilis Katos, other Post Doc Researchers and PGR on MosAIcSOC and SCIFER projects.

External: all partners of MosAIcSOC consortium

Challenges: The main challenges are conducting rigorous technical research in a fast-moving field, designing experiments and validation activities that are realistic, safe and reproducible, and working effectively with technical and end-user partners across an international consortium. This requires

maintaining high standards of research ethics, data quality and security-sensitive information handling, while delivering research outputs within project timescales.

Information Governance Responsibilities

Data User

Comply with the associated data protection, information security, information management and information technology regulations, policies, processes and procedures.

Safeguarding and Regulated Activity

If the role involves engaging in regulated activity relevant to vulnerable groups including children and disabled adults, it is an offence to apply for and perform the role, if a person is barred from engaging in regulated activity. Further information is available in BU's Safeguarding Policy and Suitability Statement on the Recruitment and Employment of Ex-offenders.

Additional Information

NB:
The purpose of the job description is to indicate the general level of responsibility and location of the position. The duties may vary from time to time without changing their general character or level of responsibility.

BU is an equal opportunities employer which values a diverse workforce. The post holder must at all times carry out their responsibilities with due regard to the University's Dignity, Diversity and Equality Policy Statement.

Our highly skilled and creative workforce is comprised of individuals drawn from a broad cross section of the globe, and who reflect a variety of backgrounds, talents, perspectives and experiences to build our global learning community. Through fused activity, the post holder must have an understanding of and commitment to promoting a global outlook.

All employees have an obligation to be aware of the University's Sustainability Policy, Climate and Ecological Crisis Action Plan, Travel Plan and associated documents, and to ensure that they carry out their day-to-day activities in an environmentally responsible manner and inspire students to do the same.

November 2026

Person Specification

Post Title: **Postdoctoral Research Fellow in AI-empowered Security Operations and Cyber Resilience (MosAIcSOC)**

Post No:
Faculty / Service Faculty of Media, Science and Technology
Date: **November 2026**

SELECTION CRITERIA	Essential / Desirable
Knowledge (including experience & qualifications)	
PhD (or viva corrections completed by start date) in a relevant field (computer science, cybersecurity, artificial intelligence, engineering or a closely related discipline)	**E**
Research experience in one or more of the following areas: security operations, threat or intrusion detection, incident response, cyber resilience, or artificial intelligence and machine learning applied to cybersecurity	**E**
Practical experience of designing, running and evaluating technical experiments (e.g., in laboratory, testbed, virtualised or simulated environments)	**E**
Sound knowledge of networks, operating systems and security architectures, and of common security operations tools and data (e.g., SIEM, IDS/IPS, logs and telemetry)	**E**
Strong grasp of research ethics, data protection (GDPR) and the responsible handling of security-sensitive information	**E**
Evidence of research skills including production of peer-reviewed publications in a relevant field	**D**
Research experience in collaborative, multi-partner, externally funded research projects (e.g., Horizon 2020, Horizon Europe, UKRI)	**D**
Knowledge of simulation-based security testing, such as digital twins, cyber ranges, attack emulation or cyber exercises	**E**
Knowledge of explainable, privacy-preserving or federated approaches to artificial intelligence	**D**
Familiarity with threat intelligence frameworks and standards (e.g., MITRE ATT&CK, STIX/TAXII) and with cybersecurity regulation (e.g., NIS2, Cyber Resilience Act)	**E**
Knowledge of cybersecurity in healthcare, or of working with end users in pilot or operational settings.	**D**
Experience of contributing to competitive research funding proposals	**D**

SELECTION CRITERIA	Essential / Desirable
Experience of academic service, such as peer reviewing or conference/workshop organisation	**D**
Skills	
Strong programming and scripting skills (e.g., Python) and experience with data analysis or machine learning libraries	**E**
Research and writing skills to a publishable standard, including technical reports and project deliverables	**E**
Excellent analytical and problem-solving skills	**E**
Ability to work well both as team member and on own initiative, managing competing deadlines	**E**
Able to communicate technical work clearly at all levels, both internally and with external partners across an international, interdisciplinary consortium	**E**
Experience with virtualisation, containerisation or cloud environments (e.g., virtual machines, Docker, Kubernetes)	**D**
Experience of teaching, training or facilitating technical workshops or exercises for diverse audiences	**D**
Attributes	
Able to identify research and professional practice activities relevant to research community	**E**
Highly motivated to work in interdisciplinary research at the intersection of cybersecurity and artificial intelligence	**E**
Flexible, adaptable with strong team working skills	**D**
Willingness to travel within Europe for consortium meetings and pilot activities	**D**