University of Oxford Department of Computer Science

Job description and selection criteria

Job title	Research Associate on AI Threat Detection
Division	Mathematical, Physical and Life Sciences (MPLS)
Department	Computer Science
Location	Robert Hooke Building, Parks Road, Oxford
Grade and salary	Grade 7: £38,674 - £46,913 p.a. with the potential to underfill at Grade 6 with salaries in the range of £34,982 - £40,855 p.a.
Hours	Full time (part-time can be considered)
Contract type	Fixed-term contract until 31 August 2026
Reporting to	Professor Sadie Creese
Vacancy Reference	176949
Additional information	Candidates will be considered with strong potential and commitment who are seeking an opportunity for early research experience, for which an initial appointment would be at Grade 6 £34,932 - £40,855 p.a. with the responsibilities adjusted accordingly. This would be discussed with applicants at interview/appointment where appropriate.

Research topic	Threat Detection for Cybersecurity of Organisations Using AI
Principal Investigator / supervisor	Prof Sadie Creese (Computer Science) / Prof Michael Goldsmith (Computer Science) / Prof Stephen Roberts (Engineering Science)
Funding partner	The funds supporting this research project are provided by the Oxford Martin School (https://www.oxfordmartin.ox.ac.uk/)
Project web site	www.gcscc.ox.ac.uk/

Overview of the role

The Department of Computer Science is looking to employ a Postdoctoral Researcher to work within an interdisciplinary team on AI Threat Detection. The successful candidate will work as part of a project team, consisting of researchers in the departments of Engineering and Computer Science, supporting the Oxford Martin Programme on AI Threat Detection, as well as engaging across the wide local network of experts in AI, cybersecurity, AI safety & governance.

The Oxford Martin Programme on AI Threat Detection aims to fill a critical gap in AI security by developing advanced methods to detect attacks on AI systems. While much research focuses on preventing AI vulnerabilities, there is currently no way to effectively detect when systems have been compromised. The programme will create a continuous monitoring tool to identify threatening activity across AI data inputs, learning models, and algorithms. By researching optimal detection methods and building a database of attack-response information, the programme seeks to improve the accuracy and resilience of AI threat detection in various organisational contexts.

The successful candidate will be required to work primarily under the direction of Professor Sadie Creese and the supervision of Professor Michael Goldsmith, with guidance from other senior academics.

The proposed research considers:

- What data-points might present useful features for indicating that an AI system or component has been compromised.
- Whether we can determine the likely normal range of outputs from the AI system, and how we might be able to characterise threatening outputs.
- To what extent is that context specific, and how much might be more generally applicable; specifically, in the case of the AI model, whether we can utilise the body of work in understanding model-drift, anomaly-detection and adversarial-responses as mechanisms for detecting model evolutions that are threatening.
- Whether it might be possible to construct a feature vector that combines communication output channels and model evolution assessments, to improve accuracy of threat detection.
- Other data-points, such as human-system interactions, that might feed into the detection strategy.

Flexible working

This position is on-site. Working hours can be flexible subject to the line manager's approval.

Main Responsibilities/duties

Specific Tasks

- Develop a threat detection architecture for detecting threats to AI systems
- Research methods for identifying and modelling AI system behaviour baselines
- Collaborate with EngSci team on researching the spectrum of threat and vulnerability models for the AI systems
- Collaborate with EngSci team to investigate, through experimentation, the most efficient feature sets for determining AI system behaviours for the models in the library

- Collaborate with EngSci team to design and run experiments exploring the utility of the prototype threat detection systems for protecting the various AI models in the library, investigating the resilience of AI models to relevant security threats and interpreting results.
- Write and publish academic papers detailing findings
- Present research findings at international conferences [and contribute to grant proposals]
- Mentor graduate students and organise seminars
- Develop software tools and relevant databases

Additional Tasks

- Manage own academic research and administrative activities to meet team milestones and deadlines. This involves small-scale project management to co-ordinate multiple aspects.
- Adapt existing and develop new research methodologies and materials as required, under the guidance of the academic supervisors.
- Prepare working theories and analyse qualitative and/or quantitative data from a variety of sources, reviewing and refining theories as appropriate.
- Contribute ideas for new research tasks, and presentation of concepts to other senior researchers.
- Develop ideas for generating research income, and present detailed research proposals to senior researchers.
- Collaborate in the preparation of research publications and book chapters.
- Present papers at conferences or public meetings.
- Act as a source of information and advice to other members of the group on methodologies or procedures.
- Represent the research group at external meetings and seminars, either with other members of the group or alone.
- Carry out collaborative projects with colleagues in partner institutions and research groups.
- The researcher may have the opportunity to undertake ad-hoc paid teaching (this includes lecturing, demonstrating, small-group teaching, tutoring of undergraduates and graduate students and supervision of Masters projects in collaboration with principal investigators). Permission must be sought in advance for each opportunity.
- Any other duties appropriate with the role.

Selection criteria

Essential

- Hold a relevant PhD/DPhil (or be close to completion*) in a cybersecurity-relevant field (e.g. computer science, international relations, economics, political science, social or physical sciences, philosophy, cognitive or social psychology, law, anthropology, development or sociology), together with relevant experience.
- Ability to work independently and as part of a team.
- Manage own academic research and associated activities.
- Previous experience of contributing to publications and presentations.
- Ability to contribute ideas for new research projects and research income generation.
- Excellent communication skills, including the ability to write for publication, present research proposals and results, and represent the research group at meetings.

Desirable

- Experience of cybersecurity capacity-building activities and of multidisciplinary working are highly desirable.
- Experience of independently managing a discrete area of a research project.

*Evidence required:

EITHER a copy of your PhD/ DPhil award certificate;

OR an academic reference confirming the qualification has been awarded;
OR an academic ref confirming that you've submitted your thesis, if you have not yet completed

Pre-employment screening

Standard checks

If you are offered the post, the offer will be subject to standard pre-employment checks. You will be asked to provide: proof of your right-to-work in the UK; proof of your identity; and (if we haven't done so already) we will contact the referees you have nominated. You will also be asked to complete a health declaration so that you can tell us about any health conditions or disabilities for which you may need us to make appropriate adjustments.

Please read the candidate notes on the University's pre-employment screening procedures at: https://www.jobs.ox.ac.uk/pre-employment-checks

About the University of Oxford

Welcome to the University of Oxford. We aim to lead the world in research and education for the benefit of society both in the UK and globally. Oxford's researchers engage with academic, commercial and cultural partners across the world to stimulate high-quality research and enable innovation through a broad range of social, policy and economic impacts.

We believe our strengths lie both in empowering individuals and teams to address fundamental questions of global significance, while providing all our staff with a welcoming and inclusive workplace that enables everyone to develop and do their best work. Recognising that diversity is our strength, vital for innovation and creativity, we aspire to build a truly diverse community which values and respects every individual's unique contribution.

While we have long traditions of scholarship, we are also forward-looking, creative and cutting-edge. Oxford is one of Europe's most entrepreneurial universities and we rank first in the UK for university spin-outs, and in recent years we have spun out 15-20 new companies every year. We are also recognised as leaders in support for social enterprise.

Join us and you will find a unique, democratic and international community, a great range of staff benefits and access to a vibrant array of cultural activities in the beautiful city of Oxford.
For more information, please visit www.ox.ac.uk/about/organisation.

Department of Computer Science

The Department of Computer Science is consistently recognised as the internationally leading centre of research and teaching across a broad spectrum of computer science, ranging from foundational discoveries to interdisciplinary work with significant real-world impact. We are proud of our history

as one of the longest-established computer science departments in the country, as we continue to provide first-rate undergraduate and postgraduate teaching to some of the world's brightest minds.

Our world-class research is conducted across our research themes, which span the broad spectrum of computer science, ranging from foundational discoveries to interdisciplinary work with significant real-world impact. A significant majority of our staff are active in externally sponsored research, with both government and industrial funding. Our 2021 Research Excellence Framework submission saw 81% of our research activity ranked as world-leading (4*), with the rest ranked as internationally excellent (3*). We have had 19 ERC Fellowships in the last decade (including 7 Advanced) and we have 6 Fellows of the Royal Society, 4 Turing/Turing AI Fellows, a Fellow of the Royal Academy of Engineering and a Fellow of the Institute of Electrical and Electronics Engineers.

We enjoy close links with other Oxford University departments (Mathematics, Engineering, Physics, Statistics and Life sciences) and work collaboratively with Oxford research groups and institutes (including the Oxford Internet Institute and the Oxford e-Research Centre). At present, the department has 71 faculty members and 98 researchers housed across multiple sites within the University's South Parks Road Science Area and the neighbouring area. Through a programme of continuous improvement, the department is committed to promoting and nurturing a diverse, inclusive and equal culture, with a particular focus on growth in gender equality (from our students to our staff).

The department holds over £75m of external funding of which £58m is research. Research in the department is currently managed in ten themes:

- **Algorithms and Complexity Theory**, led by Professor Leslie Ann Goldberg, focusses on determining the inherent difficulty of computational problems, classifying problems according to this inherent difficulty, and designing and analysing algorithms that use computational resources as efficiently as possible.
- **Artificial Intelligence and Machine Learning**, led by Professor Michael Wooldridge, focuses on theoretical foundations of AI, multiagent systems, deep learning, reinforcement learning, and computational linguistics.
- **Automated Verification**, led by Professor Marta Kwiatkowska, investigates theory and practice of formal verification and correct-by-construction synthesis for software and hardware systems.
- **Computational Biology and Health Informatics**, led by Professor Blanca Rodriquez, is concerned with computational approaches for biomedical research and healthcare innovation.
- **Data Knowledge and Action**, led by Professor Ian Horrocks, includes databases, knowledge representation and reasoning.
- **Human Centred Computing**, led by Professor Nigel Shadbolt, includes human computer interaction, social computing, and the worldwide web.
- **Programming Languages**, led by Professor Nobuko Yoshida, includes functional programming, program analysis, and programming language foundations.
- **Quantum**, led by Professor Jonathan Barrett, focusses on quantum computing including quantum software, causality in quantum theory, quantum cryptography and foundations of quantum computing.
- **Security**, led by Professor Ivan Martinovic, specialises in cybersecurity, protocol analysis, systems security, trusted computing, and networking.
- **Systems**, led by Professor Niki Trigoni, focusses especially on cyber physical systems. We plan to substantially broaden our research in systems to complement our existing research areas.

Our greatest asset is our people. We consistently attract the best staff and students and, thanks to them, we have been ranked as the world's leading university for computer sciences for six years in a

row by the *Times Higher Education*. We have held an Athena Swan Bronze Award since 2014, reflecting our longstanding commitment to promoting and supporting gender equality.

Find out more information on our website https://www.cs.ox.ac.uk/

The Department of Computer Science holds a bronze Athena Swan award to recognise advancement of gender equality: representation, progression and success for all.

The Mathematical, Physical, and Life Sciences Division (MPLS)

The Mathematical, Physical, and Life Sciences (MPLS) Division is one of the four academic divisions of the University. Oxford is widely recognised as one of the world's leading science universities and the MPLS Division is home to our non-medical sciences, with 9 academic departments that span the full spectrum of the mathematical, computational, physical, engineering and life sciences, and undertake both fundamental research and cutting-edge applied work.

For more information about the MPLS division, please visit: www.mpls.ox.ac.uk

How to apply

Applications are made through our online recruitment portal. Information about how to apply is available on our Jobs website https://www.jobs.ox.ac.uk/how-to-apply.

Your application will be judged solely on the basis of how you demonstrate that you meet the selection criteria stated in the job description.

As part of your application you will be asked to provide details of two referees and indicate whether we can contact them now.

You will be asked to upload a CV and a supporting statement. The supporting statement must explain how you meet each of the selection criteria for the post using examples of your skills and experience. This may include experience gained in employment, education, or during career breaks (such as time out to care for dependants)

Please upload all documents **as PDF files** with your name and the document type in the filename.

All applications must be received by **midday** UK time on the closing date stated in the online advertisement.

Information for priority candidates

A priority candidate is a University employee who is seeking redeployment because they have been advised that they are at risk of redundancy, or on grounds of ill-health/disability. Priority candidates are issued with a redeployment letter by their employing department(s).

If you are a priority candidate, please ensure that you attach your redeployment letter to your application (or email it to the contact address on the advert if the application form used for the vacancy does not allow attachments).

If you need help
Application FAQs, including technical troubleshooting advice is available at:
https://staff.web.ox.ac.uk/recruitment-support-faqs

Non-technical questions about this job should be addressed to the recruiting department directly *(hr@cs.ox.ac.uk)*

To return to the online application at any stage, please go to: www.recruit.ox.ac.uk.

Please note that you will receive an automated email from our online recruitment portal to confirm receipt of your application. **Please check your spam/junk mail** if you do not receive this email.

Important information for candidates

Data Privacy

Please note that any personal data submitted to the University as part of the job application process will be processed in accordance with the GDPR and related UK data protection legislation. For further information, please see the University's Privacy Notice for Job Applicants at: https://compliance.admin.ox.ac.uk/job-applicant-privacy-policy. The University's Policy on Data Protection is available at: https://compliance.admin.ox.ac.uk/data-protection-policy.

The University's policy on retirement

The University operates an Employer Justified Retirement Age (EJRA) for very senior research posts at **grade RSIV/D35 and clinical equivalents E62 and E82** of 30 September before the 70th birthday. The justification for this is explained at: https://hr.admin.ox.ac.uk/the-ejra.
For **existing** employees on these grades, any employment beyond the retirement age is subject to approval through the procedures: https://hr.admin.ox.ac.uk/the-ejra.

There is no normal or fixed age at which staff in posts at other grades have to retire. Staff at these grades may elect to retire in accordance with the rules of the applicable pension scheme, as may be amended from time to time.

Equality of opportunity

Entry into employment with the University and progression within employment will be determined only by personal merit and the application of criteria which are related to the duties of each particular post and the relevant salary structure. In all cases, ability to perform the job will be the primary consideration. No applicant or member of staff shall be discriminated against because of age, disability, gender reassignment, marriage or civil partnership, pregnancy or maternity, race, religion or belief, sex, or sexual orientation.

Benefits of working at the University

Employee benefits

University employees enjoy 38 days' paid holiday, generous pension schemes, travel discounts, and a variety of professional development opportunities. Our range of other employee benefits and discounts also includes free entry to the Botanic Gardens and University colleges, and discounts at University museums. See www.admin.ox.ac.uk/personnel/staffinfo/benefits.

University Club and sports facilities

Membership of the University Club is free for all University staff. The University Club offers social, sporting, and hospitality facilities. Staff can also use the University Sports Centre on Iffley Road at discounted rates, including a fitness centre, powerlifting room, and swimming pool. See www.club.ox.ac.uk and www.sport.ox.ac.uk/oxford-university-sports-facilities.

Information for staff new to Oxford

If you are relocating to Oxfordshire from overseas or elsewhere in the UK, the University's Welcome Service website includes practical information about settling in the area, including advice on relocation, accommodation, and local schools. See www.welcome.ox.ac.uk.
There is also a visa loan scheme to cover the costs of UK visa applications for staff and their dependents. See www.admin.ox.ac.uk/personnel/permits/reimburse&loanscheme/.

Family-friendly benefits

With one of the most generous family leave schemes in the Higher Education sector, and a range of flexible working options, Oxford aims to be a family-friendly employer. We also subscribe to My Family Care, a service that provides practical advice and support for employees who have caring responsibilities. The service offers a free telephone advice line, and the ability to book emergency back-up care for children, adult dependents and elderly relatives. See www.admin.ox.ac.uk/personnel/staffinfo/benefits/family/mfc/.

Childcare

The University has excellent childcare services, including five University nurseries as well as University-supported places at many other private nurseries.
For full details, including how to apply and the costs, see www.admin.ox.ac.uk/childcare/.

Disabled staff

We are committed to supporting members of staff with disabilities or long-term health conditions. For further details, including information about how to make contact, in confidence, with the University's Staff Disability Advisor, see www.admin.ox.ac.uk/eop/disab/staff.

Staff networks

The University has a number of staff networks including the Oxford Research Staff Society, BME staff network, LGBT+ staff network and a disabled staff network. You can find more information at www.admin.ox.ac.uk/eop/inpractice/networks/.

The University of Oxford Newcomers' Club

The University of Oxford Newcomers' Club is an organisation run by volunteers that aims to assist the partners of new staff settle into Oxford, and provides them with an opportunity to meet people and make connections in the local area. See www.newcomers.ox.ac.uk.

Staff networks

The University has a number of staff networks including the Oxford Research Staff Society, BME staff network, LGBT+ staff network and a disabled staff network. You can find more information at www.admin.ox.ac.uk/eop/inpractice/networks/.

The University of Oxford Newcomers' Club

The University of Oxford Newcomers' Club is an organisation run by volunteers that aims to assist the partners of new staff settle into Oxford, and provides them with an opportunity to meet people and make connections in the local area. See www.newcomers.ox.ac.uk.