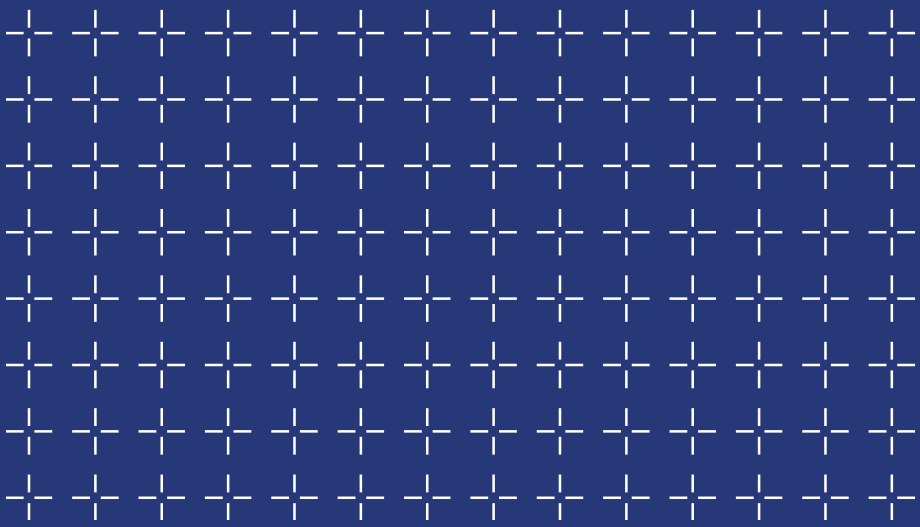
CYBER ASAP

Academic Startup Accelerator Programme

Year 8 Demo Day Programme 2025

Level 39
Canary Wharf
London



CyberASAP Programme Context

The Department for Science, Innovation and Technology (DSIT) is leading the government's work to accelerate innovation, investment and productivity through world-class science, to ensure new and existing technologies are safely developed and deployed across the UK, and to drive forward a modern digital government for the benefit of its citizens.

DSIT is working to improve the UK's cyber defences, protect our essential public services and grow a strong, innovative cyber ecosystem. This includes ensuring UK cyber businesses have the support and investment needed to grow, innovate and succeed.

CyberASAP is funded by DSIT and delivered by Innovate UK with support from Plexal for the thematic strand in Year 8.

Department for Science, Innovation & Technology

DELIVERED BY

UKRI Innovate UK

SUPPORTED BY

plexal

Expanding Skills

The only pre-seed accelerator programme in the UK's cyber ecosystem, CyberASAP helps to convert great academic research into great cyber innovations. The programme provides a dynamic interface between government, cyber security academics and the business and investment communities that drive the growth and development of this key sector.

This year's programme included a thematic strand alongside the open call, delivered in partnership with Plexal. This focused on AI model security, software supply chain security, and Industrial Internet of Things (IIOT) security or Operational Technology (OT).

Led by a highly experienced team from Innovate UK Business Connect, with input and assessment from expert industry connections, CyberASAP operates over two competitive phases:

PHASE 1

Developing a Value Proposition

Market Validation of the Value Proposition

PHASE 2

Creating a Proof of Concept

Kickstarting Commercialisation Training

2024 saw the successful launch of a short sister programme, CyberASAP Pathfinder. This introduces academics to the key principles, terminology, frameworks, and imperatives for successful commercialisation.

CyberASAP Pathfinder has run twice to date, in January 2024 and January 2025, with more than 60 participants selected to join the programme.

As well as providing an introduction to commercialisation, the programme acts as a useful step towards applying to the full CyberASAP programme.

Another Pathfinder is planned for the coming year.

Creating Business Impact

The CyberASAP programme is designed to give innovation-focused academics the confidence and know-how to translate their research into viable cyber products, technologies and services.

Key takeaways include:

- Commercial upskilling
- Entrepreneurial mindset
- Exposure to new business concepts and language
- Advanced market research and comms techniques
- Insights into how investors think and work
- Effective presentation techniques

There's no single pathway for the talented academics who participate in CyberASAP, but what unites them is the value they draw from being on the programme. The knowledge gained enriches their ongoing work either within academia or industry, creating more opportunities to extend the impact of their experience.

Our alumni have secured more than £40m to date in further funding to progress their projects. Success has come in many forms, including:

- Creating start-ups (more than 32 to date)
- Acquisition by technology firms
- Receiving seed funding
- Joining other accelerator programmes
- Securing government grants
- Partnering with commercial enterprises

You can read a selection of CyberASAP success stories in the Resources section of our website: cyberasap.co.uk

Event Running Order

01

12:30pm - Registration, Alumni Showcase and Networking Lunch

with CyberASAP Alumni

02

2:00pm - Welcome

Dr Emma Fadlon, Co-Director, CyberASAP, Innovate UK Business Connect

03

Keynote

Feryal Clark, Minister for AI and Digital Government

04

Pitches from CyberASAP Year 8 Teams

05

4:30pm - Year 8 Showcase, Demos, Networking and Drinks

Meet with the teams and discuss their proofs of concept

06

7:00pm - Event close

Team Pitches Running Order

01 **CyberMATI**
Sheffield Hallam University

02 **CyDRA**
London Metropolitan University

03 **AIMTI**
University of East Anglia

04 **LockEyeGaze**
University of St Andrews

05 **GridGuardian**
University of Sheffield

06 **VeriBee**
University of Manchester

BREAK

07 **CyberThemis**
Teesside University

08 **ARMOREX**
City, University of London

09 **SIROCCO**
Anglia Ruskin University

10 **AI360Degree**
Anglia Ruskin University

11 **RapidRANDefender**
Queen Mary University of London
Queen's University Belfast

12 **TeleHealth-CyberShield**
De Montfort University

13 **MetaGuard**
Aston University

14 **Pentestify**
University College London

CyberMATI

Cyber category: Threat intelligence, monitoring, detection, and analysis

AI-powered solution for detecting phishing and malicious websites.

Market Need

Large enterprises like financial institutions face significant cybersecurity risks, necessitating robust protection measures to safeguard sensitive information and ensure regulatory compliance. Phishing remains the leading cybercrime, despite billions spent annually on cybersecurity services, phishing training, and simulated red-team exercises. Sophisticated social engineering threats place relentless pressure on employees to remain vigilant. Unfortunately, current URL and content-based filtering techniques frequently fall short, particularly against new exploits and threats.

Solution

CyberMATI's AI-powered technology keeps users one step ahead of cyber threats by analysing visual elements, content inconsistencies, and website patterns to identify and block threats before they can cause harm.

The multi-modal AI system mirrors the decision-making process of security experts to assess whether a website is genuine or a phishing attempt. The system uses cutting-edge AI to identify vulnerability patterns among users and groups, and dynamically learns to recognise emerging threats and zero-day attacks, enabling tailored security measures and targeted training that keep threats at bay.

Target Market

Enterprises and cybersecurity providers

Likely route to commercialisation: Licence

Status & Needs

Status: Proof of concept deployed on vendor-neutral cloud services, testing completed, international patent application published (WO 2024/246543)

Need: Investment to expand testing and integrate the solution into cybersecurity ecosystems; expertise to create go-to-market strategies

Team from Sheffield Hallam University


Dr. Abdel-Karim Al-Tamimi
CEO and Founder


Dr. Chris Roast
Research and Innovation Lead


Dr. Neil Bowden
Innovation Funding Manager


Dr. James Walsh
IP and Innovation Manager

Contact details

Website: cybermati.co.uk
Email: a.altamimi@shu.ac.uk, info@cybermati.co.uk
LinkedIn: /meetcybermati
X: @meetcybermati

CyDRA

Cyber category: Information risk assessment and management

Software product for cyber security by design that is affordable, reliable, customised and user-friendly.

Market Need

Organisations in all sectors are experiencing financial losses as a result of inadequate security design, due to inability to assess security risks and implement safeguards.

Many businesses find current solutions unaffordable, inaccessible or difficult to customise to their specific needs, leading to cybersecurity not being treated as a priority and risks being left open to exploitation.

Solution

CyDRA is a desktop software that reduces losses from authorised online fraud and attacks by enforcing the security by design in system infrastructure and updates. The solution offers a budget-friendly, easy-to-use standalone software which upholds robust algorithms and intuitive graph-based modelling to support cybersecurity by design.

Target Market

Consultancy companies, service providers, audit and certification agencies, organisations that handle online transactions.

Likely route to commercialisation: Spinout

Status & Needs

Status: Architecture modeller and convertor implemented, tested and integrated with risk engine

Need: £150k-£250k funding to complete template development and software packaging

Team from London Metropolitan University

Dr Mohamed Chahine Ghanem
Project Manager

Reza Baghaeishiva
Back-End, Algorithm and Risk Calculation

Animesh Singh Basnet
Front-End, Modelling and Visualisation

Contact details

Website: www.cydra.tech

AIMTI (AI-enabled Multi-tier Trust Management in the Internet of Medical Things)

Cyber category: Internet of Things (IoT) Security

AIMTI provides robust, scalable end-to-end security solutions for personal healthcare devices.

Market Need

Internet of Medical Things (IoMT) manufacturers have not been held to any external mandates to deliver secure devices, resulting in vulnerabilities, with 40% of the IoMT having little to no security patches/upgrades at end-of-life stage. Over 88% of stakeholders in a survey conducted by the team suggested a need for more secure medical devices, as these are at critical risk of cyber threats.

Solution

AIMTI's approach addresses the critical need to secure IoMT ecosystems by offering a solution which ensures patient data integrity and operational safety. Easy-to-install software patches developed in this project make severely outdated legacy systems secure and trustworthy. Combining AI and fuzzy logic, the solution provides real-time and adaptive security measures for protecting against the rising cyber threats and enhancing the security of connected medical devices. This solution does not require any infrastructural alterations and will be device independent, which makes it scalable.

Target Market

UK healthcare providers, and IMT manufacturers and service providers who can integrate the solution into their devices. Other sectors such as industrial IoT, smart cities, and connected vehicles.

Likely route to commercialisation: Still deciding on best route

Status & Needs

Status: Testing and refining the solution

Need: Resources and infrastructure to field test the proof of concept; partnerships with healthcare organisations to validate the proof of concept; investment to expand the team and be able to offer free trials to users

Team from University of East Anglia


Muhammad Awais
Associate Professor


Mohsin Raza
Associate Professor


Beatriz De La Iglesia
Professor/ Head of School


Riaz Ahmed Shaikh
Associate Professor

Contact details

Website: https://research-portal.uea.ac.uk/en/projects/ai-enabled-multi-tier-trust-management-in-internet-of-medical-thi-2

Email: m.awais@uea.ac.uk
mohsin.raza@uea.ac.uk
riaz-ahmed.shaikh@uea.ac.uk

LockEyeGaze

Cyber category: Identification, authentication, and access controls

LockEyeGaze uses gaze stimuli and tracking to create eye movement biometrics for user verification.

Market Need

LockEyeGaze confronts the cybersecurity challenge of sophisticated computer vision and 3D modelling technologies, such as deepfakes and AI-generated tampering, which have begun to erode the reliability of facial recognition as a secure authentication method.

The LockEyeGaze system utilises the dynamic patterns of eye movements for security, which are significantly more difficult to replicate than static biometric features like static face, iris and fingerprints.

Solution

The system utilises sensors integrated into devices, like front camera and IMU sensors, to capture the user's eye movements. Three layers of authentication – eye movements recognition, deepfake attack detection, and face & pupil consistency authentication – protect the system.

LockEyeGaze's algorithms map and analyse the unique patterns of eye movements and behaviour patterns as biometric, similar to fingerprints, enabling personalised and secure authentication. These algorithms are designed to adapt over time, enhancing security through continuous learning of the user's eye movement and behaviour changes.

Target Market

Sectors with need for robust security and privacy protections, such as finance, healthcare and high-value consumer technology. System integrators and multi-factor authentication providers.

Likely route to commercialisation: Establish a company

Status & Needs

Status: Minimum viable product developed

Need: Funding to scale development and build a sales team; further testing across user scenarios; certifications like NCSC essentials and other ISO standards; industry partnerships and pilot projects to make iterative improvements

Team from University of St Andrews


Yaxiong Lei
Chief Executive Officer


Shijing He
Chief Operating Officer


Zihan Zhang
Chief Technology Officer


Yuheng Wang
Chief Scientific Officer

Contact details

Website: lockeyegaze.com

LinkedIn: /company/lockeyegaze

GridGuardian

Cyber category: SCADA and Information Control Systems

GridGuardian protects solar energy systems and EV charging stations from cyber threats.

Market Need

The energy sector is facing escalating cybersecurity threats, particularly due to vulnerabilities in solar inverters and electric vehicle charging stations. With 24% of cyberattacks in the UK targeting this sector, these devices pose significant risks to the grid, amplified by their growing adoption in the transition to renewable energy and electric mobility.

Additionally, stricter regulatory requirements now prompt manufacturers to adopt robust cybersecurity measures for compliance and product protection.

Solution

GridGuardian embeds advanced security directly into device firmware, providing continuous protection without costly hardware modifications. The solution assesses devices for specific weaknesses and implements customised security solutions aligned with current standards and regulatory frameworks, ensuring interoperability, robust cybersecurity, and demand-side response readiness.

The framework integrates into existing device firmware, avoiding costly hardware changes. It also provides continuous updates to counter emerging cyber threats, ensuring devices remain secure as risks evolve.

Target Market

Solar inverter manufacturers and EV charging station manufacturers.

Likely route to commercialisation: Licence

Status & Needs

Status: Currently testing finalised proof of concept

Need: Resources to scale testing to more devices and manufacturers; real-world validation of the framework's robustness and adaptability; collaboration with regulatory bodies to refine compliance and accelerate market adoption

Team from University of Sheffield

Jonathan Mayo-Maldonado
Lecturer in Electrical Machines and Drives

Mohammad Eissa
Lecturer in Digital Electronics

Contact details

Website: https://sites.google.com/view/gridguardianuk/

Email: j.mayo@sheffield.ac.uk, m.eissa@sheffield.ac.uk

VeriBee

Cyber category: Information risk assessment and management

Verification and AI for identifying and repairing security vulnerabilities in source code.

Market Need

Manual testing of software is impractical due to high costs, complexity, and a shortage of skilled testers. Existing automated tools often fail to identify or fix security issues and can generate many false alarms, creating additional challenges for developers. There is a pressing need for powerful and reliable testing tools to prevent cyber-attacks, especially in high-stakes industries.

Solution

VeriBee combines advanced verification and AI methods to detect and fix over 40 types of security vulnerabilities in C language source code (can be extended to other languages), while keeping false positives at a minimum. The containerised product can easily be integrated into a company's existing technology stack, can run on the cloud or locally, and generates detailed bug reports with locations, types, and suggested fixes, enhancing security and reliability, and enabling continuous learning of software developers. This has earned the solution 18 awards in international software testing competitions.

Target Market

C/C++ software testing segment, targeting security-conscious companies focused on low-level system development, including firmware, device drivers, compilers, and operating systems.

Likely route to commercialisation: Spinout

Status & Needs

Status: Proof of concept and testing complete, in discussions with possible early adopters

Need: investment to develop proof of concept into a minimum viable product, and to extend solution to multi-language support

Team from University of Manchester

Professor Lucas Cordeiro
CTO and Co-Founder

Dr Kaled Alshmrany
Head of Engineering and Co-Founder

Professor Richard Allmendinger
COO, Head of AI, and Co-Founder

Contact details

Website: veribee.co
Email: richard@veribee.co
Phone: +44 7527 191691
LinkedIn: /company/veribee/

CyberThemis

Cyber category: Information risk assessment and management

EU AI Act compliance assistants for software development organisations.

Market Need

CyberThemis provides continuous monitoring and compliance assurance for organisations developing LLM applications, with a particular focus on the EU AI Act. The Act presents compliance challenges to organisations developing LLM applications, particularly enforcements around AI literacy and prohibiting certain AI systems.

Cybersecurity is a crucial obligation under the Act, intersecting with multiple regulations such as the GDPR. Current solutions fail to prioritise LLM compliance during application development and address the diverse needs of stakeholders within an organisation.

Solution

CyberThemis employs advanced multi-agent architecture to continuously monitor LLM outputs and detect compliance violations. Through cutting-edge confidential computing technology, it ensures data security during processing while maintaining system performance.

CyberThemis empowers users across organisations to maintain continuous visibility of their projects' compliance status through customisable dashboards and automated reporting. This proactive approach significantly reduces the risk of financial losses due to non-compliance while streamlining the compliance monitoring process.

Target Market

Software development organisations in UK and Europe

Likely route to commercialisation: Spinout

Status & Needs

Status: Proof of concept ready

Need: Further development funding for minimum viable product; investors, partners and advisors

Team from Teesside University

Dr. Ioannis Sfyrakis
Project Lead and CEO

Dr. Zia Ush Shamszaman
Co-Investigator and CTO

Prof. The Anh Han
Co-Investigator and CSO

Contact details

Website: cyberthemis.co.uk
Email: i.sfyrakis@tees.ac.uk
LinkedIn: /company/cyberthemis

ARMOREX

Cyber category: Threat intelligence, monitoring, detection, and analysis

ARMOREX helps SMEs stay secure while streamlining the underwriting process for insurance providers.

Market Need

More than 50% of SMEs are not adequately protecting themselves against evolving cyber attacks, and 75% do not employ IT personnel. As a result, over 50% of organisations outsource their IT, yet struggle to meet cyber insurance requirements, leading to an increase in insurance costs.

Insurers need a novel cyber-security assessment solution to accurately understand the cyber risks facing SMEs. Without this, dynamic insurance pricing will remain elusive, hampering customer confidence, driving up premiums, and intensifying complexity in pricing models.

Solution

ARMOREX is developing an intelligent solution to help SMEs access cyber insurance cover.

The solution combines security checks and questionnaires to give insurance providers insights into an SME's cybersecurity status, to minimise their risks and payouts.SMEs can also install ARMOREX Smart Agent on their devices to gain insights into their cyber risk profile.

ARMOREX risk scores adapt as SME cyber practices evolve. This allows insurance carriers to align policies and prices with actual risk, reducing uncertainty and leading to more affordable insurance for SMEs who manage their cyber risks effectively.

Target Market

Small and medium-sized enterprises (SMEs) seeking to strengthen their cybersecurity posture and secure affordable insurance, and the insurance providers who underwrite their policies.

Likely route to commercialisation: Spinout

Status & Needs

Status: Proof of concept and testing complete

Need: Funding to transition from proof of concept to minimum viable product

Team from City, University of London

Veniamin Boiarkin
Co-founder, Doctoral Researcher in Cyber Sec.

Muttukrishnan Rajarajan
Co-founder, Professor of Security Engineering

Himali Wadhwa
Business Development Manager

Contact details

Website: armorex.co.uk

SIROCCO

Cyber category: SCADA and Information Control Systems

Cybersecurity solutions for wind farms using AI models to prevent disruption and damage.

Market Need

The distributed nature of windfarms makes them highly susceptible to cyber threats, yet current solutions fail to address these unique risks. A recent rise in cyberattacks on windfarms, such as those seen in Germany, Denmark, Portugal, and the Netherlands, has caused significant disruptions, production losses, and asset damage.

With cyber threats constantly evolving, and as wing energy expands, real-time adaptive AI models are crucial to stay ahead of emerging attacks and ensure continuous protection to critical infrastructure.

Solution

SIROCCO uses explainable AI algorithms to identify and mitigate cyber threats, ensuring continuous protection and transparency into decision-making processes.

The solution implements federated learning to create a cybersecurity system across turbines and control centres, reducing the risks associated with centralised systems, and applies online learning to adapt to emerging threats by training on new data as it becomes available. The tamper-proof models designed to address the unique challenges of wind farm infrastructure ensure robust protection against attacks targeting the AI models themselves.

Target Market

Operational technology security companies, energy companies, IoT companies.

Likely route to commercialisation: Licence

Status & Needs

Status: Proof of concept and a basic GUI are ready for use

Need: Collaborators to help develop the minimum viable product

Team from Anglia Ruskin University


Raj Mani Shukla
Senior Lecturer


Segun Popoola
Senior Lecturer


Sarinova Simanjuntak
Associate Professor

Contact details

Email: aru.sirocco@gmail.com

AI360Degree

Cyber category: Information risk assessment and management

Elevating fintech security with automated compliance and advanced AI protection.

Market Need

The rapid adoption of AI within the fintech sector introduces significant risks such as adversarial attacks, data poisoning, and non-compliance with regulations. Fintech companies encounter challenges in securing their AI models, automating compliance processes, and maintaining operational efficiency. In the absence of robust solutions, these businesses face financial losses, regulatory penalties, and reputational harm.

AI360Degree offers a robust AI bill of materials (AIBOM) framework, and an AI-enabled automated compliance suite tailored for the fintech sector, designed to secure the entire AI lifecycle.

Solution

The solution incorporates advanced security and automation features, including:

- Automation tools to ensure compliance with GDPR, ISO 42001:2023, and the EU AI Act
- Adversarial attack prevention mechanisms to detect and mitigate malicious threats
- Continuous real-time monitoring to uphold AI security
- AI model fingerprinting for tracking, documentation, and protection of AI components

AI360Degrees' solution ensures real-time compliance updates, reduces the burden on businesses and enables faster integration of evolving standards.

Target Market

Challenger banks, financial institutions, and AI service providers in the UK, Middle East and Europe.

Likely route to commercialisation: Spinout

Status & Needs

Status: Completed proof of concept

Need: Further investment to become a market leader; engagement and collaboration to create minimum viable product; sales and marketing partners

Team from Anglia Ruskin University

Dr. Mahmud Hasan
CEO and Team Lead

Prof. Silvia Cirstea
COO and Responsible AI Expert

Dr Roger Chittock
Technology Transfer Officer

Contact details

Website: ai360degree.co.uk
Email: md.hasan@aru.ac.uk
LinkedIn: /company/ai360degree/

RapidRANDefender

Cyber category: Network security

Adaptive, cost-saving solution for securing open and programmable next-generation wireless networks.

Market Need

The Open Radio Access Network (O-RAN) paradigm fosters innovative services and reduces overall costs by enabling new vendors to enter the market. However, mobile network operators and service providers must address the cybersecurity risks arising from the use of open-source software from multiple vendors. Within the O-RAN Radio Intelligent Controller (RIC), a breach could severely degrade network performance and result in substantial financial loss. There is a pressing need for low-cost, real-time threat detection solutions that do not require direct access to the live network or disrupt normal operations.

Solution

RapidRANDefender is a ready-to-install security software. It employs cutting-edge technologies to enable real-time threat detection without disrupting network services.

The solution creates a digital twin replica of the network which enables real-time offline evaluation, where an abusive adversary agent continuously simulates attacks on this replica, identifying potential vulnerabilities before they can be exploited.

RapidRANDefender's reliable, resilient and cost-effective Software as a Service (SaaS) platform enables mobile network operators and service providers to enhance their cybersecurity defences.

Target Market

O-RAN infrastructure vendors based in the UK and Europe. Network security vendors could be potential partners.

Likely route to commercialisation: Licence

Status & Needs

Status: Proof of concept ready

Need: Financial support to develop the proof of concept into a minimum viable product; test sites and potential early adopters; a broader network of industry contacts

Team from Queen Mary University of London


Dr. Antonino Masaracchia
CEO and Co-founder


Dr. Vishal Sharma
Scientific Advisor


Mr. Norbert Sagnard
Business Development Manager


Prof. Trung Q. Duong
Scientific Advisor

Contact details

Email:
a.masaracchia@qmul.ac.uk
antonino.masaracchia@gmail.com

LinkedIn:
/antonino-masaracchia-phd

TeleHealth-CyberShield

Cyber category: Network security

TeleHealth-CyberShield is a cybersecurity solution for medical data at rest and in transit.

Market Need

Modern healthcare systems face escalating data security threats from ransomware, supply chain breaches, and quantum based attacks. These challenges can erode patient trust, disrupt clinical operations, and drive costs upwards. Many existing solutions rely on outdated, resource intensive encryption methods that struggle to keep pace with current and emerging adversarial techniques, particularly the rise of quantum computing.

Solution

TeleHealth-CyberShield integrates post-quantum cryptography (PQC) with traditional encryption algorithms. It establishes safe tunnels for data transmission using ephemeral session keys derived from PQC key exchanges. This shields sensitive patient data from unauthorised interception. For data at rest, the solution provides full-disc or volume encryption, automatically managed via centralised key repositories to simplify rotation and auditing, and alert security teams to anomalies. The architecture allows for rapid adoption of new cryptographic standards as cyber threats and vulnerabilities evolve.

Target Market

Healthcare providers and medical device manufacturers

Likely route to commercialisation: Spinout

Status & Needs

Status: Implemented protection for data at rest, and completed a minimal proof of concept for data in transit

Need: Investment to transition from proof of concept to minimum viable product

Team from De Montfort University

Dr. Mujeeb Ur Rehman
Senior Lecturer in Cyber Security

Dr. Muhammad Kazim
Senior Lecturer in Cyber Security

Dr. Richard Smith
Associate Professor in Cyber Security

Contact details

Email: mujeeb.rehman@dmu.ac.uk
muhammad.kazim@dmu.ac.uk
rgs@dmu.ac.uk

MetaGuard

Cyber category: Threat intelligence, monitoring, detection, and analysis

An AI security platform that protects decentralised finance (DeFi) and crypto transactions.

Market Need

As DeFi ecosystems and the metaverse expand, they are increasingly targeted by fraud, phishing, and malicious smart contract activities. Users and businesses relying on these platforms face significant risks due to inadequate real-time security measures. Traditional methods are mainly reactive, often missing critical threats before funds are lost, compromising trust in Web3 and crypto ecosystems. Therefore, there is a strong need for proactive, AI-driven protection to analyse and secure real-time transactions, reduce fraud, safeguard digital assets, and ensure long-term user confidence.

Solution

MetaGuard monitors smart contracts and wallet activities to detect anomalies and malicious behaviours, issuing real-time alerts. The solution can integrate directly with users' crypto wallets and decentralised applications, or function as a standalone API, for protection without disrupting the user experience.

Key capabilities:

- Dynamic risk assessment identifies threats before transactions are finalised
- Semantic verification ensures smart contract interactions' authenticity
- Transaction simulation previews expected effects on user assets for greater transparency.

Target Market

Individual cryptocurrency users, DeFI platforms and DApps, metaverse platforms and institutional investors and enterprises.

Likely route to commercialisation: Spinout

Status & Needs

Status: Proof of concept ready

Need: Investment to evolve from proof of concept to minimum viable product; beta testing sites and early-adopter partners; partnerships with crypto wallet providers, DeFi platforms, and metaverse developers; sales and marketing expertise

Team from Aston University

Dr Bogdan Adamyk
Project Lead and Research Fellow

Dr Asma Patel
Tech Lead and Lecturer

Professor Vladlena Benson
Project Co-Lead and Professor of Cybersecurity

Contact details

Website: csiresearch.co.uk

Email: b.adamyk@aston.ac.uk
v.benson@aston.ac.uk

Linkedin: /bogdan-adamyk

Pentestify

Cyber category: Blockchain security monitoring and risk assessment

A continuous, post-deployment smart contract vulnerability detection SaaS.

Market Need

The growth of applications built on the blockchain and reliant on smart contracts is outpacing the creation of blockchain security talent. The innate complexity of securing a smart contract, along with the lack of available expertise and/or effective tools, contributed to over £1.5 billion being stolen from decentralised finance protocols in 2023 alone.

Although a number of smart contract auditing companies have attempted to address the issue, many lack the continuity, accuracy, automation and scalability required to be effective.

Solution

Pentestify is a SaaS platform that allows blockchain protocols to continuously secure their deployed smart contracts by delivering on-chain vulnerability detection, using AI threat intelligence and integrations with existing workflows.

The unique design pattern enables 24/7 AI learning from vulnerable patterns in bytecode, with global real-time threat intelligence and remediation. As well as addressing the root cause of smart contract hacks – the need for continuous, proactive security monitoring – Pentestify offers greater vulnerability detection accuracy.

Target Market

Decentralised finance protocols (DeFi)

Likely route to commercialisation: Spinout

Status & Needs

Status: Testing proof of concept in customer presence through keynotes, awards and competitions

Need: Further funding to turn the proof of authorities; more early adopters; highly specialised industry advisors

Team from University College London

Professor Java Xu
Project Lead

Lucas Martin Calderon
Technical Lead

Andrew Law
Commercial Lead

Contact details

Website: pentestify.io
Email: jiahua.xu@ucl.ac.uk
lucas.calderon.22@alumni.ucl.ac.uk
andrew.law@ucl.ac.uk
LinkedIn: /company/pentestify
X: /Imc_security

ALUMNI

FACT360

Cyber category: Network security

Insider threat, financial crime and compliance anomaly detection, monitoring and investigation.

FACT360 is an award-winning solution which uses cutting-edge technology to revolutionise how organisations detect and respond to threats within their communication networks. By identifying insider threats like cyber attacks, malicious users, or nefarious actors, FACT360 serves as a powerful post-incident investigation toolset as well as a proactive monitoring platform, offering early alerts for potential threats.

The solution is capable of analysing millions of emails, messages and documents in real time, and conducting AI and machine learning assessments to identify key individuals, communications and events.

Backed by pioneering academic research, the solution excels at uncovering 'unknown unknowns' and detecting suspicious activity without relying on user-defined rules or customised configurations. Trusted across industries for fraud detection, insider threat monitoring, and strategic decision-making, FACT360 provides a factual foundation for shaping businesses' strategic directions.

Paddy Lawton
Co-founder/CEO

Andy Slater
Commercial Director

Prof J. Mark Bishop
Chief Scientific Adviser

Abdelkrim Alfalah
Chief Product Officer

Fredrik Mattisson
Lead AI Engineer

Email: mark.bishop@fact360.co, paddy.lawton@fact360.co

Website: www.fact360.co

LinkedIn: /company/fact360

Phone: 07850 656438

ALUMNI

CyGamBIT

Cyber category: Awareness, training and education

Transforming cybersecurity training with game-based learning and practical resilience.

CyGamBIT is a game-based cybersecurity learning platform which revolutionises cybersecurity education, using interactive, scenario-driven gameplay to reinforce critical decision-making skills under pressure. Already adopted by businesses, educational institutions, and government agencies, it provides a high-retention alternative to ineffective compliance-based training.

Expanding on this foundation, Cyber First Aid (CFA) delivers a structured, research-backed approach to cyber resilience. CFA is the first training programme to integrate technical response skills with psychological resilience, ensuring organisations can handle cyber crises effectively. It reduces downtime, mitigates financial losses, and embeds a security-first culture.

CFA' subscription-based cybersecurity support system with interactive resources and response guides is a proven scalable model, enabling internal trainers to become certified for long-term organisational impact. It's designed to integrate into cyber insurance policies, reducing claims and strengthening risk management.

Emily Rosenorn-Lanng
CEO & Chief Impact and Operations Officer (CIOO)

Professor Vasilis Katos
Chief Technology Officer (CTO)

Dr. Jane Henriksen-Bulmer
Chief Business Development Officer (CBDO)

Email: info@cyberinnovations.co.uk

LinkedIn: /company/cyberinnovationsltd/

Website: www.cyberinnovations.co.uk, www.cygambit.com

ALUMNI

FORENSIC

Cyber category: SCADA and Information Control Systems

Cybersecurity hardware to protect physical systems like industrial robots and medical devices.

FORENSIC is in the process of spinning out from the University of Essex to commercialise a hardware-based cybersecurity solution that protects critical physical systems, such as industrial robots and medical devices, from cyberattacks. The solution is an anomaly detection system that integrates seamlessly with existing systems to provide timely autonomous protection. FORENSIC is designed to be difficult to compromise, non-intrusive, lightweight, and independent of internal software modeling. It also offers fast and low-power consumption and the capability to be scaled to more devices.

The project is targeting early adopters in the automotive and healthcare industries, with plans to expand to chipset manufacturers and platform integrators in the future. Market validation has demonstrated interest in the technology, and the team comprises experts in embedded systems, cybersecurity, and technology transfer.

Sangeet Saha
Project Lead, Lecturer in Embedded Systems

Professor Klaus McDonald-Maier
Professor of Embedded Systems, Technical Advisor, Co-lead

Michal Borowski
Technical Researcher

Email: sangeet.saha@essex.ac.uk

Website: https://tinyurl.com/Forensic-essex

ALUMNI

Vouchsec

Cyber category: Incident response and management

Virtual shadow security team: AI agents automating cyber investigations.

Vouchsec provides a virtual shadow security team powered by AI agents that automates cyber threat investigation and response for security operations centres (SOCs) and managed security service providers (MSSPs).

Vouchsec transforms how security teams operate by eliminating the manual analysis burden that analysts face when dealing with thousands of daily security alerts.This approach enables comprehensive threat analysis and investigation automation, from initial alert triage through to detailed incident response recommendations. Vouchsec's differentiator is its ability to reduce overwhelming alert volumes to manageable events, conduct automated investigations across multiple security tools, and provide clear, explainable results.

Vouchsec delivers faster, more accurate threat responses while maintaining full transparency of AI processes. The solution integrates with threat intelligence and other cybersecurity tools, enabling organisations to scale their security operations efficiently.

Dr Michael Piskozub
Founder & CEO

Jon Inns
Product Advisor

Prof. Ivan Martinovic
R&D Advisor

Email: michael@vouchsec.ai

LinkedIn: /michael-piskozub/

Website: www.vouchsec.ai

Get involved in CyberASAP

Academics

CyberASAP and CyberASAP Pathfinder welcome participation from academics based across the UK who have an interest in commercialising their cyber research. The programmes are particularly keen to invite applications from academics in under-represented groups.

Future opportunities will be posted online and our social media channels. If you are interested in applying, please register your interest via the Get Involved section on our website: cyberasap.co.uk

Supporters

Investors and industry colleagues with an interest in supporting the programme in any way are invited to provide their details via the Get Involved section at cyberasap.co.uk.

We're always looking to extend our network of independent experts who provide valuable input to the teams and enjoy insights into the cyber innovations being developed on the programme.

Thank You To All Our Mentors, Supporters & Collaborators

CyberASAP is a collaborative enterprise, drawing on the experience and knowledge of Innovate UK Business Connect Programme Directors, Emma Fadlon and Robin Kennedy, and their expert connections. This extended network of industry specialists who generously lend their expertise and insight to the academic teams is central to the success and impact of CyberASAP. A huge thank you to every one of you.

CyberASAP in Numbers (Years 1-7)

171 Projects have participated

85 Projects have graduated

34 New companies have formed

Funding raised by CyberASAP participants:

More than £40m

as of January 2025

Contact us

CYBER + ASAP | Academic Startup Accelerator Programme

Website: cyberasap.co.uk

Email: cyberasap@iukbc.org.uk

LinkedIn: /cyberasap

X: @CyberASAP

LinkedIn: /company/innovateukbusinessconnect

Website: iuk-business-connect.org.uk

X: @IUK_Connect