Year 9

Demo Day Programme

25 February, 2026

Level 39, Canary Wharf, London

CYBER + ASAP | Academic Startup Accelerator Programme

Funded by

Department for Science, Innovation & Technology

Delivered by

UKRI Innovate UK

CyberASAP Programme Context

The Department for Science, Innovation and Technology (DSIT) is driving the government's efforts to accelerate innovation, investment and productivity through world-class science, while also championing digital transformation, strengthening cyber resilience, and fostering the safe development and deployment of new and existing technologies. DSIT's mission supports the development of a modern digital government and ensures that advances benefit citizens and businesses across the UK. Above all, DSIT's mission is to drive growth across the UK economy.

Cyber security plays a critical role in delivering this mission – both as a thriving sector in its own right and as a foundation that protects the wider economy, enabling growth and innovation. Strong cyber resilience ensures the services people rely on every day – from turning on lights, accessing safe water to knowing the NHS is there when needed – remain secure and dependable.

DSIT is committed to improving the UK's cyber defences, protecting essential public services and fostering a strong, innovative cyber ecosystem. This means supporting UK cyber businesses with the investment, expertise and networks they need to grow and succeed. Through initiatives like CyberASAP, **funded by DSIT and delivered by Innovate UK**, DSIT is helping academic teams turn cutting-edge research into commercial products and services.

This commitment to the cyber sector is delivering results. The UK cyber security sector continues to expand at pace, generating significant economic value and creating high-quality jobs across the country. Annual revenue within the sector is now estimated at £**13.2 billion**, representing a **12% increase** on last year's figure of £11.9 billion. Employment is rising too: around **67,300 full-time** equivalent roles are now based in cyber security firms, an increase of approximately **6,600 jobs** in the past 12 months – **growth of 11%**.

Additionally, investment in the sector is equally strong. In 2024 alone, dedicated cyber security firms raised £**206 million** across **59 deals**, providing the capital needed to scale innovative solutions and bring cutting-edge products to market. This momentum reinforces the government's ambition to make the UK the best place in the world to start and grow a business – and cyber security is a shining example of that vision in action.

Expanding Skills

Phase 1

- Developing a Value Proposition
- Market Validation of the Value Proposition

Phase 2

- Creating a Proof of Concept

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 drives the growth and development of this key sector.

Led by a highly experienced team from Innovate UK Business Connect, with input and assessment from expert industry connections, the CyberASAP programme this year featured an open call plus a thematic strand focused on National and Emergency Service Infrastructure Security; Operational and supply chain resilience; Harms; and Dual Use, National Security.

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 outcome 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 £47.4m to date in further funding to progress their projects. Success has come in many forms, including:

- Creating companies (more than 42 companies have been registered to date)
- Acquisition by technology firms
- Licensing their technology
- Receiving seed funding
- Joining other accelerator programmes
- Making their technology available Open Source
- Securing government grants
- Partnering with commercial enterprises.

Event Running Order

1

12:30pm — **Registration and Networking Lunch**

CyberASAP Alumni Showcase

2

02:00pm — **Welcome**

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

3

Keynote

Department for Science, Innovation and Technology

4

Pitches

CyberASAP Year 9 Teams

5

04:00pm — **Year 9 Showcase, Demos, Networking & Drinks**

Meet with the teams & discuss their proofs of concept

6

07:00pm — **Event close**

Team Pitches Running Order

1 — **GUARD**, Teesside University

2 — **Photarix**, Lancaster University

3 — **SynapTrack**, University of Birmingham

4 — **SOC4SMEs**, University of Wolverhampton

5 — **PrivacyEye**, De Montfort University

6 — **AutoTARA**, Coventry University

Break

1 — **Cairnlytics**, University of Edinburgh

2 — **CipherGrit**, Cardiff University

3 — **SecureCall**, University of Sheffield

4 — **VoxLith**, University of Portsmouth

5 — **MediVault**, Teesside University

6 — **AssetGuard+**, University of East London

7 — **DroneSentinel**, Ulster University

8 — **Presenza**, University of Greenwich

Open Cohort

GUARD

AI forensics tool for detecting and flagging undisclosed AI-created or manipulated advertisements.

GUARD addresses the rapid growth of AI-generated advertising content, which is undermining transparency and trust across the advertising ecosystem. Brands, agencies, and platforms face reputational risk and increasing regulatory pressure as rules emerge requiring disclosure of AI-generated or manipulated media. Moderating content at scale remains a significant operational challenge.

GUARD responds by detecting AI-created or altered advertisements before they are published, reducing the risk of misleading audiences or breaching regulations. The target customers include ad networks, creative agencies, and regulatory bodies responsible for enforcing advertising standards.

The project is currently at proof-of-concept stage, with a working AI forensics system capable of identifying synthetic or manipulated ad content and flagging missing disclosures.

To progress GUARD, investment is required to develop the proof of concept into a minimum viable product, supported by beta testing with early adopter partners. The project also seeks partnerships with ad verification platforms and pay-per-click platforms to support integration and scale.

The most likely route to commercialisation is licensing the technology to platforms and agencies seeking automated compliance and content moderation capabilities.

Team from Teesside University


Dr Chidimma Opara | Project Lead


Dr Mohammad Abdur Razzaque | Project Co-Lead

ad-guard.co.uk

info@ad-guard.co.uk

/company/ad-guard

Challenge Cohort

Photarix

Making quantum-secure photonic communications simple, cost-effective, and efficient.

Photarix addresses a growing global security risk: the vulnerability of today's encryption to future quantum computing. Sensitive data such as financial records, medical histories, and defence communications are already being harvested for later decryption. While software-based cryptographic upgrades help, high-assurance users require physics-based solutions to reduce long-term risk.

Our target customers are QKD system vendors, system integrators, and telecom/network equipment manufacturers who require a deployable, telecom-wavelength single-photon source to build compact, cost-effective QKD modules for metro and access fibre networks.

Photarix targets this gap by developing room-temperature, telecom-wavelength single-photon sources compatible with standard semiconductor manufacturing. The project has progressed from laboratory proof of concept to an active spin-out company, now focused on integration-ready prototypes for real-world quantum-secure networks.

Photarix now requires pre-seed investment to accelerate engineering development, improve device performance and reproducibility, and complete packaging and fibre-coupling work. Collaboration with integrator partners will support pilot demonstrations and validation within live fibre networks.

Commercialisation routes include scaling the spin-out company, licensing to system integrators, or a hybrid approach. The immediate focus is achieving integration-ready prototypes that enable practical, large-scale deployment of quantum-secure communications.

Team from Lancaster University


Gizem Acar Tekin | CEO


Dr Samuel Jones | CTO


Prof Manus Hayne | CSO


Jeremy Gidlow | Chair

photarix.com

gizem@photarix.com

/company/photarix

Challenge Cohort

SynapTrack

AI-powered cross-chain AML for crypto services, identifying fraudulent transactions with high accuracy.

SynapTrack addresses a growing compliance and operational challenge within the crypto and digital asset sector. Crypto service providers are required to meet stringent global Anti-Money Laundering (AML) regulations, including requirements set by bodies such as FATF, OFAC, and OFSI. However, many existing AML tools generate high false-positive rates and struggle to track illicit activity across the rapidly expanding blockchain ecosystem. Criminal activity increasingly spans hundreds of blockchains and cross-chain bridges, leaving traditional, single-chain monitoring tools unable to follow complex transaction paths.

This results in significant operational costs for compliance teams, poor user experience through unnecessary account blocks, and limited visibility into emerging money laundering techniques. SynapTrack responds to this market need with an AI-powered, cross-chain AML platform capable of tracing suspicious transactions across multiple networks in real time. By automating analysis and reducing reliance on static heuristics, the platform improves detection accuracy while significantly lowering false positives.

The target customers include centralised crypto exchanges, custodians, payment processors, decentralised finance platforms, and regulatory bodies. The project has implemented a proof of concept and demonstrated strong technical performance, including very low false-positive rates when tested against real-world laundering activity.

To advance, SynapTrack requires additional software developers to implement a full platform and dashboard.

The most likely route to commercialisation is a spin-out or licensing model, offering the technology as a SaaS API integrated into existing AML workflows.

Team from University of Birmingham


Endong Liu


Dr Pilar Carr


Dr Pascal Berrang

synaptrack.co.uk

contact@synaptrack.co.uk

Open Cohort

SOC4SMEs

Solidarity in protecting your SME from cyber threats.

SOC4SMEs addresses the growing cybersecurity challenges faced by small and medium-sized enterprises, which are increasingly targeted by threats such as phishing, ransomware, and data breaches. Traditional Security Operations Centre (SOC) solutions are typically expensive, complex, and designed for large enterprises, leaving SMEs without access to effective, continuous security monitoring.

The project responds to this gap by developing affordable, scalable, and customisable SOC solutions that allow SMEs to achieve enterprise-level protection without the cost or complexity of large-scale infrastructure. SOC4SMEs focuses on providing simple, budget-friendly tools that protect against common cyber threats, deliver real-time alerts, and support compliance with standards such as GDPR and ISO 27001.

The target users are digitally active SMEs, particularly those in regulated sectors such as retail and healthcare, that lack in-house cybersecurity expertise but handle sensitive data and require a practical way to monitor and improve cyber resilience. The project is currently at the proof-of-concept stage.

To progress SOC4SMEs, investment is required to develop the proof of concept into a minimum viable product and to establish effective sales and marketing strategies. Further work will focus on refining the open-source toolchain, improving usability for non-technical users, and validating the solution with SME pilot deployments.

At this stage, the project will commercialise through a spin-out/start-up company delivering SOC4SMEs as a scalable service for SMEs. Licensing and open-source elements may be used to support adoption. Engagement with early adopters will shape the final go-to-market approach and ensure alignment with SME needs.

Team from University of Wolverhampton


Emma Berry | Senior Computer Science Technician


MD Arafatur Rahman | Reader of Cyber Security


Nadia Refat | Research Assistant


Tan Sze Wei | Research Assistant

emma.berry@wlv.ac.uk

Open Cohort

PrivacyEye

PrivacyEye is an AI-powered real-time protection tool that detects and blurs sensitive content in videos created by children to prevent harmful sharing.

PrivacyEye addresses the rapid rise of self-generated harmful content created by children online. Existing safeguarding tools are largely reactive, relying on website blocking or moderation after content has already been shared, and are unable to intervene during real-time video creation. Parents and schools therefore lack effective tools to prevent inappropriate or exploitative content from being recorded and shared, particularly in cases of online coercion.

PrivacyEye fills this gap by providing proactive, real-time protection directly on a child's device. The target users are parents and schools seeking practical safeguarding tools, with secondary interest from child safety organisations and online platforms.

The project is currently at validation and proof-of-concept stage, with a working PoC under development to demonstrate real-time detection and blurring. Intellectual property is jointly owned and managed through the university's technology transfer office.

Next steps for PrivacyEye include completing and validating the proof of concept, securing access to relevant datasets, and further validating the market proposition. The project also requires engagement with schools, child safety organisations, and potential platform partners to support testing and trust-building.

Commercialisation is likely to follow a hybrid approach, combining direct subscription sales to parents and schools, partnerships with education and child protection bodies, and API licensing to online platforms. Early trials and freemium access are expected to support adoption and credibility.

Team from De Montfort University

 **Abdulghani Al-Yamani** | Senior Lecturer in Cybersecurity

 **Taha Rassem** | Senior Lecturer in Computing

 **Iryna Yevseyeva** | Associate Professor in Computer Science

 **Ali Al-Bayatti** | Associate Professor in Cybersecurity

privacyeye.co.uk

aa.ahmed@dmu.ac.uk

/abdulghani-ali-ahmed

Open Cohort

AutoTARA

AI-driven semi-automated Threat Analysis & Risk Assessment for automotive cybersecurity.

AutoTARA addresses a critical challenge in automotive cybersecurity: the increasing cost, inconsistency, and scalability limits of Threat Analysis and Risk Assessment (TARA) required under standards such as ISO/SAE 21434 and UNECE R155. As vehicles become software-defined and highly connected, manual TARA processes can take hundreds of hours per ECU and struggle to keep pace with growing system complexity.

At the same time, the automotive sector faces a shortage of experienced cybersecurity specialists, creating bottlenecks, delivery delays, and compliance risk. AutoTARA responds to this need by making TARA faster, more repeatable, and audit-friendly through AI-assisted automation.

The target customers are automotive OEMs, Tier-1 suppliers, and cybersecurity consultancies responsible for vehicle cybersecurity assurance. The project is currently at TRL 4, with a proof of concept implemented and validated against representative automotive use cases.

To progress AutoTARA, the project requires investment and design partners to expand prototype development and validation. This includes advancing to a higher-TRL prototype, enhancing security and compliance readiness, and conducting multiple pilot deployments with OEMs and Tier-1 suppliers.

The most likely commercial route is to prove value through funded projects and consultancy pilots, then scale AutoTARA as a B2B SaaS or on-premise solution. Early commercial agreements arising from pilot engagements will support transition toward a sustainable product offering.

Team from Coventry University

 **Dr Hesam Jadidbonab** | Principal Investigator / AI Lead

 **Kevin Vincent** | Strategic Partnerships & Market Exploitation

 **Albi Lamaj** | Business Development & IP Strategy

autotara.com

ad4953@coventry.ac.uk

/hesam-jadidbonab-ph-d/

Challenge Cohort

Cairnlytics

Compliance-ready, non-intrusive risk scoring for open-source dependencies and supply-chain collapse.

Cairnlytics addresses a growing systemic risk in modern software development: heavy reliance on open-source software that lacks formal governance or clear ownership. Open source underpins the majority of commercial and public-sector applications, yet organisations are increasingly expected by regulators to demonstrate resilience across their software supply chains. Traditional third-party due diligence approaches do not translate effectively to open-source dependencies, creating a governance blind spot.

Teams rely on CVE scanning and vulnerability alerts, which focus on known exploits but miss deeper risk signals such as maintainer concentration, project sustainability, responsiveness to security issues, and governance changes. These factors can determine whether a dependency becomes unmaintained, compromised, or vulnerable to supply-chain attack.

Cairnlytics provides a data-driven approach to quantifying the resilience of open-source dependencies. By analysing development activity and maintainership patterns, the platform produces dynamic risk scores and evidence-backed insights, enabling developers, security teams, and compliance functions to prioritise risk and understand exposure across complex dependency chains.

Target users include software developers, security teams, and procurement and compliance professionals. A clickable proof-of-concept prototype is live, demonstrating dependency scoring, trend analysis, and depth-of-dependency insights.

Cairnlytics now requires pilot partners willing to validate scoring against real SBOMs and incident histories. Support is also needed to harden the prototype into an MVP SaaS platform with integrations, monitoring, and reporting.

The most likely route to commercialisation is a spin-out company offering subscription-based access.

Team from University of Edinburgh


Dr Mojtaba Tefagh | Senior Researcher


Laura Antunes | Research Assistant

cairnlytics.com

mtefagh@ed.ac.uk

/company/cairnlytics

Challenge Cohort

CipherGrit

Real-time ransomware detection system that utilises hardware-level features in transfer-learning to identify zero-day threats with high accuracy.

CipherGrit is a cyber security research project addressing the growing threat of ransomware, particularly zero-day variants that evade traditional defences. Ransomware remains one of the most financially damaging cyber threats, with most existing solutions relying on signature-based detection that can only identify previously known attacks. This leaves organisations exposed during the earliest and most critical stages of an attack.

CipherGrit addresses this market need by moving detection to hardware-level behavioural analysis, enabling real-time identification of previously unseen ransomware before encryption or damage occurs. Its primary target customers are organisations in high-risk, high-value sectors such as banking and financial services, retail, manufacturing, and technology.

The project is currently at proof-of-concept stage, with a working system developed and early discussions underway with potential early adopters, demonstrating strong market relevance and interest.

To advance CipherGrit, further investment is required to develop the proof of concept into a deployable minimum viable product. This includes strengthening scalability, robustness, and integration into real-world enterprise environments, alongside validation through early user deployments.

At this stage, several commercialisation routes are under consideration. These include forming a university spin-out company, licensing the technology to established cyber security vendors, or pursuing a hybrid or open-source-influenced model depending on market feedback. Engagement with early adopters will play a key role in shaping the commercial strategy and identifying the most effective route to market while maximising impact and adoption.

Team from Cardiff University


Dr Shancang Li | Senior Lecturer


Dr Prosanta Gope | Associate Professor


Dr Aryan Pasikhani | Lecturer


Xueyi Wang | PhD Researcher

lis117@cardiff.ac.uk

Challenge Cohort

SecureCall

Proactive caller authentication and encrypted voice communication.

SecureCall addresses the growing problem of caller ID spoofing, impersonation, and voice fraud, which undermines trust in voice communication across telecoms, financial services, healthcare, and public services. As fraudulent calls increase, organisations and consumers struggle to distinguish legitimate communications, leading to financial loss, missed calls, and reduced confidence in voice channels. Existing solutions are often reactive, fragmented, or limited to specific network infrastructures.

SecureCall provides proactive caller authentication by verifying caller identity before a call is connected. The solution operates across both IP and non-IP networks, including legacy telephony, and supports trusted outbound calls, real-time risk assessment for inbound calls, and optional encryption for sensitive communications.

Target customers include telecom providers, contact centres, and organisations in regulated sectors. The project is at proof-of-concept and early validation stage, with a working prototype and initial market engagement underway.

Next steps include refining the proof of concept into a minimum viable product, improving scalability, reliability, and integration. This involves developing integration options such as APIs or telecom plug-ins and validating performance across diverse real-world network environments.

The project requires pilot partnerships with telecom providers, contact centres, or regulated organisations to test the solution in live settings and gather feedback. Further work will map regulatory and compliance requirements for deployment in sectors such as finance and healthcare.

The most likely route to commercialisation is a spin-out/start-up company. Licensing and OEM partnerships remain potential options as the technology matures and integration opportunities emerge.

Team from University of Sheffield


Mahshid Delavar | Lecturer


Dr Arayan Pasikhani | Lecturer


Muhammad Ajmal Azad | Senior Lecturer


Sam Trotter | Technology Transfer Officer

m.delavar@sheffield.ac.uk

/mahshid-delavar

Challenge Cohort

VoxLith LTD

AI-powered, real-time phishing protection that isolates risky clicks in lightweight micro-containers, running on any device with minimal resource use.

VoxLith ThreatAx Suite addresses phishing as a primary entry point for malware and ransomware, particularly in environments with mixed, low-spec, or unmanaged devices. Traditional endpoint tools are often too heavy or ineffective for browser-led threats, leaving coverage gaps across BYOD and legacy systems.

VoxLith ThreatAx Suite detects phishing in real time and isolates risky activity using lightweight, just-in-time micro-containers, limiting impact without degrading performance. The solution targets organisations of all sizes, with early focus on education and maritime sectors.

A proof of concept has been deployed, with patent protection filed and testing completed.

Next steps include securing an Investment Partner to expand testing with other cybersecurity products; Go-to-market expertise to accelerate market entry and reach the market before the end of 2026.

The project is expected to commercialise through a spin-out/start up company offering subscription-based deployment and enterprise licensing.

Team from University of Portsmouth


Prof Stavros Shiaeles | CEO & Founder


Dr Bander Al-Rimy | CTO & Founder


Matthew Pullinger | IP & Commercialisation Manager


Dr Louise Farrand | Head of IP

voxlith.com

info@voxlith.com

/company/voxlith

Open Cohort

MediVault

Collaborate on data. Without sharing data.

MediVault addresses a fundamental challenge in healthcare and life sciences: the need to collaborate on sensitive patient data to advance research and AI, while meeting strict privacy, security, and regulatory requirements. Current approaches to data sharing rely on centralising or transferring datasets, which creates significant breach risk, increases compliance burden, and often excludes smaller providers and innovators. As a result, valuable data remains siloed, slowing research and limiting the development of safe and effective AI-driven healthcare solutions.

MediVault responds to this market need by enabling privacy-first collaboration without moving or exposing raw data. Using federated learning and homomorphic encryption, the platform allows hospitals, researchers, pharmaceutical companies, and SMEs to jointly analyse data and train AI models while keeping all patient data encrypted and local. This approach directly reduces data leakage risk, supports GDPR and HIPAA compliance, and lowers the cost and complexity of secure collaboration.

The primary target customers include NHS trusts and hospital groups, clinical research organisations, pharmaceutical companies, health-tech SMEs, and academic research consortia. MediVault is currently at a post-market-validation development stage and is preparing for beta testing with real-world healthcare and research partners.

MediVault is now entering a critical build phase, requiring investment to develop a functional prototype and secure beta partners for real-world testing. Finalising pilot agreements with NHS trusts and CROs will be essential to validate performance and compliance claims.

The most likely commercial route is licensing, supporting adoption across healthcare and research organisations while aligning with institutional IP strategies.

Team from Teesside University

 **Usman Adeel** | Associate Professor

 **Jie Li** | Senior Lecturer

 **Safwan Akram** | Professor

u.adeel@tees.ac.uk

Open Cohort

AssetGuard+

AssetGuard+ is an AI-powered platform that fully discovers digital assets, classifies risk, and maps regulatory requirements in real time.

AssetGuard+ addresses a widespread visibility gap in modern organisations' digital estates. As businesses rely on cloud services, SaaS platforms, and third-party integrations, many lack an accurate view of what assets they operate and which fall under regulatory scope. This creates unmanaged risk, compliance failures, and audit challenges.

Existing tools are fragmented and poorly suited to cloud-native and proxy-restricted environments. AssetGuard+ provides unified discovery, risk scoring, and compliance mapping in a single platform.

The target customers are mid-sized organisations in regulated sectors such as finance, healthcare, retail, and professional services. The project is currently at an advanced MVP stage, with real-world testing underway using institutional data and early market validation completed.

To progress AssetGuard+ from an advanced MVP toward early commercial deployment, further technical hardening and expanded pilot testing are required. This includes strengthening hybrid asset discovery across cloud, SaaS, and managed environments, refining AI-driven asset correlation and risk scoring, and improving scalability and security for regulated and proxy-restricted settings.

Broader pilot deployments with regulated mid-sized organisations are needed to validate accuracy, usability, and operational fit in real-world environments, and to generate defensible evidence of improved asset visibility and compliance coverage.

Commercial support is required to formalise pilot partnerships, refine pricing and deployment models, and engage with investors to accelerate readiness for early adoption. At this stage, licensing of the University of East London–owned intellectual property to an independent commercial entity remains the most likely route to market.

Team from University of East London

 **Halima Ibrahim Kure** | Senior Lecturer & CEO

 **Ameer Al-Nemrat** | Reader & Co-Founder

 **Youssef Mahfoudhi** | Research Assistant

 **Ewald Schroder** | Research Development Manager

assetguardplus.com

assetguardplus@gmail.com

/assetguardplus-ltd-uk

Open Cohort

DroneSentinel

IoT-driven cybersecurity framework for intrusion detection in the Internet of Drones.

DroneSentinel addresses the growing cybersecurity risks associated with the rapid adoption of drones across public services, infrastructure, logistics, and emergency response. Many drone platforms lack robust protection against threats such as GPS spoofing, signal hijacking, and unauthorised data access, creating serious operational and regulatory risks.

Existing solutions are fragmented and often unsuitable for real-time deployment. DroneSentinel provides a lightweight, end-to-end cybersecurity framework covering the device, network, and cloud layers, without requiring hardware redesign.

The target customers include drone service providers, public sector operators, security companies, and drone manufacturers. The project has successfully deployed and validated a proof of concept, with live pilot deployments underway, and is progressing toward a market-ready MVP.

Next steps include IP protection, commercial structuring, and preparation for post-Phase 2 investment. The project will focus on maturing the MVP and expanding pilot deployments with early adopters.

The most likely route to commercialisation is a spin-out company focused on delivering deployable drone cybersecurity solutions at scale.

Team from Ulster University

 **Dr Usman Hadi** | CEO and Founder

 **Dr Sharatchandra Varma Bogaraju** | Research and Innovation Lead

 **Prof Alistair McIlhagger** | Professor of Advanced Engineering

 **Prof Dewar Finlay** | Professor of Electronic Systems

m.hadi@dronesentinel.com

/drone-sentinel-33a00439b

Challenge Cohort

Presenza

Continuous age assurance for virtual and extended reality: protect children, avoid Ofcom fines.

Presenza addresses a new compliance challenge created by online safety regulation in XR environments. Platforms hosting adult or gambling content must implement effective age assurance, yet existing methods are intrusive, disruptive, and pose privacy risks. They also fail to ensure the verified user remains the headset wearer.

Presenza provides XR-native, continuous age assurance using dorsal-hand imagery captured within the headset, avoiding facial data and reducing friction. The target customers include XR studios, platform providers, and device OEMs.

The project has deployed a proof of concept on Meta Quest devices, demonstrating feasibility in real XR environments.

Presenza now requires investment to complete an MVP, improve accuracy across age ranges, and secure pilot integrations with XR studios.

The most likely route to commercialisation is a spin-out/startup company targeting XR platforms and device manufacturers.

Team from University of Greenwich

 **Dr Riccardo Bovo** | Co-Founder

 **Prof Georgios Loukas** | Co-Founder

 **Dr Paul Williams** | IP Manager

gre.ac.uk/research/groups/sustainable-cyber-security-cs2

g.loukas@greenwich.ac.uk

/riccardobovo

Cavero Quantum

New global Post-Quantum Cryptography (PQC) standards, such as NIST's ML-KEM, are designed for high-resource servers and can require Megabytes of memory to operate. However, the 14 billion devices at the "Global Edge"—including defense sensors, drones, and critical SIM cards—operate on Kilobytes. These constrained environments physically cannot run standardized PQC, leaving national infrastructure defenseless against "Harvest Now, Decrypt Later" attacks.

Furthermore, existing security often relies on static "check-once" authentication. This makes them highly vulnerable to Man-in-the-Middle (MitM) attacks, session hijacking and phishing, where an identity is stolen immediately after login. Without a lightweight, continuous trust solution, manufacturers face multi-million pound hardware replacement cycles or catastrophic non-compliance risks.

Cavero Quantum provides a patented, software-only security layer uniquely built for the constrained edge. Our dual-product "Trust Fabric" solves the resource bottleneck without requiring hardware redesigns:

Symmetrikey™ ("The Lock"): An ultra-lightweight, quantum-safe key exchange protocol. It runs natively in Kilobytes, making it compatible with legacy SIM cards and IoT modules where standards crash. In verified lab tests, it performs up to 2x faster than NIST standards.

Authentikey™ ("The Guard"): The world's first Continuous Trust Verification Protocol. By replacing one-time checks with constant mutual re-authentication, it provides a persistent "heartbeat" that eliminates Man-in-the-Middle attacks and session hijacking in real-time.

Cavero enables organisations to achieve rapid regulatory compliance and protect mission-critical data with a drop-in software upgrade for the hardware already in use today.

Team from Cavero Quantum


James Trenholme | CEO


Prof Ben Varcoe | Founder and NXD


Dr Frey Wilson | Founder and CTO

caveroquantum.com

james.trenholme@caveroquantum.com

/company/caveroquantum

Cyber Innovations Ltd

Cyber Innovations Ltd is a research-led cybersecurity company focused on helping organisations build practical, human-centred cyber resilience. Founded as a spin-out from Bournemouth University, the company combines cybersecurity expertise, psychology, and applied learning design to support organisations before, during, and after cyber incidents.

The company's flagship programme, Cyber First Aid (CFA), is an incident-response training model designed for real operational environments. CFA moves beyond traditional awareness training by focusing on how people actually behave under pressure, including stress, cognitive overload, decision-making, and social engineering tactics. The programme is informed by original academic research and tested through live organisational pilots.

Cyber Innovations has been supported through the Innovate UK CyberASAP programme, which helped accelerate the development and validation of its game-based learning and training approaches. This includes CyGamBIT, a cybersecurity learning game designed to engage non-technical audiences and improve learning retention, and which continues to form part of the company's wider training ecosystem.

The company works primarily with SMEs, regulated organisations, and critical service providers that face increasing cyber risk but lack dedicated incident response teams. Common threats addressed include phishing, ransomware, and business email compromise. Clients span professional services, infrastructure providers, charities, public-sector bodies, and SME networks.

Delivery is flexible and scalable, including in-person and blended training, digital resources via the CFA Toolkit, and a Train-the-Trainer pathway for organisations and partners. Cyber Innovations' approach is practical, evidence-based, and accessible, helping organisations reduce harm, recover more effectively from cyber incidents, and build long-term resilience across their workforce.

Team from Cyber Innovations Ltd


Emily Rosenorn-Lanng | Chief Executive Officer


Vasilis Katos | Professor of Cybersecurity and Chief Technology Officer

cyberinnovations.co.uk

info@cyberinnovations.co.uk

/company/cyberinnovationsltd

CybPass

CybPass is an AI assurance company providing continuous security, safety, and compliance validation for autonomous and safety-critical AI systems.

As AI systems increasingly operate autonomously and evolve after deployment, assurance has remained static, manual, and fragmented—creating a critical trust gap in regulated industries.

CybPass replaces point-in-time audits and isolated testing tools with a continuous, system-level AI assurance infrastructure operating across the full AI lifecycle.

The platform enables automated threat and risk analysis, adversarial AI testing, and unified safety, security, and compliance evidence generation from design through post-deployment.

CybPass serves regulated industries including automotive, aviation, robotics, and aerospace, working with engineering, security, and safety leaders responsible for certifiable AI deployment.

Unlike traditional cybersecurity vendors or AI testing tools that focus on isolated components, CybPass delivers unified, agentic assurance tailored for evolving AI systems in safety-critical environments.

The company is spun out of the University of Sheffield and is working with global autonomy players through paid pilots and design-partner programmes.

Team from CybPass


PingChen Lin | Co-Founder/CEO


Vishesh Sachdev | Co-Founder/CTO


Dr Aryan Pasikhani | Co-Founder/CSO

cybpass.com
pingchen@cybpass.com
/ping-chen-lin

FACT360

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.

Team from FACT360


Paddy Lawton | Co-founder/CEO


Andy Slater | Commercial Director


Prof J. Mark Bishop | Chief Scientific Adviser


Abdelkrim Alfalah | Chief Product Officer

fact360.co
paddy.lawton@fact360.co
/company/fact360

Pentestify

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.

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.

Team from Pentestify


Professor Java Xu | Project Lead


Lucas Martin Calderon | Technical Lead Lecturer


Andrew Law | Commercial Lead

pentestify.io
andrew.law@pentestify.io
/company/pentestify

Testimonials

"The programme has been foundational for me. It created the conditions for everything that followed: the development of CyGamBIT, the emergence of Cyber First Aid, and ultimately the formation of Cyber Innovations as a viable spinout. Without this support, I simply would not have had the confidence, structure, or networks to move from an idea to a fully developed pathway of research, product design, and commercial readiness."

Cyber Innovations
Emily Rosenorn-Lanng | CEO
Year 6 cohort

"CyberASAP has been highly valuable for MetaGuard, helping us translate a research idea into a clearer product proposition and stronger route-to-market plan. The mentoring and structured support improved our customer discovery, value communication, and confidence when engaging with the industry."

MetaGuard
Bogdan Adamyk | Project Lead
Year 8 cohort

"Personally, the programme has been transformative, shifting my mindset from academic researcher to technology founder and providing the confidence to lead a commercial venture.

Professionally, CyberASAP provided the essential commercialisation framework to bridge the gap between our hardware-level security research and the market. The external validation from the programme was a key catalyst in securing University support for our patent filings. Furthermore, the national visibility provided by the programme, culminating in our competitive selection for CyberUK 2025, has been instrumental in building the strategic network."

Forensic
Sangeet Saha | Project Lead
Year 7 cohort

"I think CyberASAP has had huge value in providing me with skills for ongoing cybersecurity-related commercialisation, and a stronger understanding of how to commercialise our research."

BlockHawk
Louise Axon | Project Lead
Year 7 Cohort

Kickstarting Commercialisation Training

CyberASAP Pathfinder

2024 saw the successful launch of a short sister programme, CyberASAP Pathfinder. Demand was such that the programme ran again in 2025 and 2026 attracting **over 100 participants** in total to date from universities throughout the UK.

It is anticipated that CyberASAP Pathfinder will run again in 2027 and beyond.

As well as introducing academics to the key principles, terminology, frameworks, and imperatives for successful commercialisation, Pathfinder acts as a useful step towards applying to the full CyberASAP programme.

Supporting Ongoing Success

CyberASAP Alumni Network

Taking part in CyberASAP doesn't end with Demo Day. Participants in the programme have access to a growing and active network of Alumni, peers and industry contacts; as well as to a dynamic programme of activities, all designed to support whatever commercialisation pathways our participants have chosen.

For example,

- In March 2026, we have a delegation of Alumni going to RSA in San Francisco
- Throughout the year, we offer our Alumni the opportunity to
  - Be showcased at national events
  - Take part in regular peer-to-peer meet ups
  - Participate in briefings by potential investors
  - Update their skills and knowledge with post programme workshops and events.

As part of the UK Government's plan to supercharge the UK cyber sector announced in June 2025, up to £10 million in additional funding will be invested in CyberASAP over the next 4 years.

CyberASAP in Numbers (Years 1-9)

£47.4M post programme funding leveraged

200+ projects from 80+ universities have participated

113 projects have graduated

42 companies have formed

*As of Jan 2026

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 and 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.

cyberasap.co.uk
cyberasap@iukbc.org.uk
/company/innovateukbusinessconnect

CYBER + ASAP
Academic Startup Accelerator Programme