CYBER + ASAP

Academic Startup Accelerator Programme

14 March

Demo Day Programme 2024

Level 39, Canary Wharf, London

CyberASAP - Programme Context

The Department for Science, Innovation and Technology (DSIT) is leading the government's work to develop the world's best and most secure digital economy. DSIT wants the UK to be the best place to start and grow a business.

The National Cyber Strategy is the Government's plan to ensure that the UK remains confident, capable and resilient in this fast-moving digital world; and that the UK continues to adapt, innovate and invest in order to protect and promote our interests in cyberspace.

This strategy delivers on a commitment made in the government's Integrated Review of Security, Defence, Development and Foreign Policy.

CyberASAP is funded by DSIT and delivered by Innovate UK.

Department for Science, Innovation & Technology

DELIVERED BY

UKRI Innovate UK

The 5 Pillars

The National Cyber Strategy set out five 'priority actions' which form the pillars of the UK government's strategic framework, guiding and organising the specific actions we will take and the outcomes we intend to achieve by 2025:

Pillar 1

Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry

Pillar 2

Building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected

Pillar 3

Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies

Pillar 4

Advancing UK global leadership and influence for a more secure, prosperous and open international order, working with government and industry partners and sharing the expertise that underpins UK cyber power

Pillar 5

Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace, making more integrated, creative and routine use of the UK's full spectrum of levers

CyberASAP is funded by DSIT and delivered by Innovate UK. In 2021 CyberASAP introduced a new funding stream for PETRAS projects, part of the Security of Digital Technology at the Periphery programme (SDTaP) funded by UKRI.

Expanding Skills

The only pre-seed accelerator programme in the UK's cyber ecosystem, CyberASAP helps 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 helps drive the growth and development of this key sector.

For year 8, CyberASAP will include a thematic strand alongside the existing open call and is recruiting projects focussing on: AI model security, software supply chain security, and Industrial Internet of Things (IIOT) security or OT (Operation Technology) security in partnership with Plexal.

Led by a highly experienced team from Innovate UK Business Connect, with input and assessment from their 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

Driving Innovation

Commercial upskilling; an entrepreneurial mindset; exposure to new business concepts and language; advanced market research and comms techniques; insights into how investors think and work; honing effective presentation techniques - just some of the takeaways designed to give innovation-focused academics the confidence and know-how to translate their research into viable cyber products, technologies and services.

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 can enrich their ongoing work either within academia or industry, creating more opportunities to extend the impact of their experience.

Our Alumni have secured more than £23m in further funding to progress their projects. Successes come in many forms including: creating start ups (more than 30 to date); acquisition by technology firms; receiving seed funding; joining other accelerator programmes; securing government grants; partnering with commercial enterprises. Read our Impact Report and Case Studies at cyberasap.co.uk.

Event Running Order

01

12:30pm Registration and Networking with Lunch

Meet with selected CyberASAP Alumni over lunch

02

2:00pm Welcome

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

03

Keynote

Viscount Camrose, Minister for AI and Intellectual Property

04

Pitches from CyberASAP Year 7 Teams and break

See running order for Team pitches on next page

05

4:00pm Year 7 Showcase/ Demonstrations, Networking and Drinks

Meet with the teams and discuss their proof-of-concept demonstrators

06

7:00pm Event close

Team Pitches Running Order

01. **BlockHawk – University of Oxford**
    Monitoring Blockchains to detect attacks and misbehaviours
02. **FORENSIC – University of Essex**
    Secure Device operation to protect future Cyber-Physical-Systems
03. **TwinSecure – De Montfort University**
    Securing Critical National Infrastructure: A Digital Twin-Powered Decision Support System
04. **CyberHeels by LITERALLY NEED – University of Oxford**
    Improving digital-physical wellbeing with IoT enabled cyber smart shoes
05. **IoT-Armor – University of West London**
    Empower IoT's future with education on seamless secure-by-default integration
06. **TrueDeploy – Edinburgh Napier University**
    Mitigating Open-Source Software Risk for SMEs

Break

07. **CybPass – University of Sheffield**
    Autonomous Penetration Testing and Threat Modelling for securing AI
08. **CyberSecurityAId – University of Essex**
    A dynamic, AI-powered self-assessment cybersecurity tool for small businesses
09. **AI-bility 4Ds – University of Middlesex**
    Empowering Cyber Learning for diverse minds
10. **SirenPod – Kingston University**
    AI Enhanced Honeypot for Cybersecurity on IoT devices
11. **ECG.ai – University of Strathclyde**
    Powering the healthy heartbeat of AI – securing AI models, improving resilience, reducing risk and enabling compliance
12. **ACE: AI Privacy Orchestrator – University of Essex**
    Privacy-oriented AI training and permissions control for compliance-by-design
13. **Vouchsec – University of Oxford**
    Conversational Cyber Security Platform for the AI Era

BLOCKHAWK

Monitoring Blockchains to detect attacks and misbehaviours

Market Need

Attacks on Blockchains can harm users and providers, but businesses are now adopting Blockchain in broader applications – and compromise could result in significant damage.

Businesses need to be able to detect and respond to attacks, but Blockchains are often adopted with little or no tooling for attack detection, putting organisations at risk and creating compliance challenges.

Solution

BlockHawk is an attack-detection software for Blockchain. It watches the Blockchain for indicators of external attacks or internal misbehaviours, using Machine Learning and rule-based algorithms. Understanding Blockchain security is complex, which is where the BlockHawk team comes in, as Dr Louise Axon explains:

"We have a deep technical knowledge of how attack detection works, and we're able to explain what an attacker might be trying to do, helping the user to contextualise it and take action".

BlockHawk presents users with information about potential attacks and the consequences in a way that is comprehensible and actionable. For businesses using Blockchain, this technology offers risk-reduction and compliance benefits. For providers, it offers the potential benefit of increasing clients' trust in the security of the Blockchain offering.

BlockHawk are looking for advisors and partners that can help them to spin out after the programme.

Target Market

- Blockchain consortia based in the UK and Europe.

Status & Needs

- ***Status:*** Proof of concept and testing complete
- ***Need :*** Test sites and potential early adopters
- ***Need :*** Increased contacts and network
- ***Need :*** Financial support to develop the POC into an MVP
- ***Need :*** Business development advice
- ***Need :*** Sales and marketing partners

Team from University of Oxford

Dr Louise Axon - CEO and Co-Founder
Professor Sadie Creese - Co-Founder
Professor Michael Goldsmith - Co-Founder

Contact details

Email: louise.axon@cs.ox.ac.uk
Phone: +44 (0)7570 767210
Website: blockhawk.co.uk
Linkedin: /company/blockhawk

FORENSIC

Fast and Autonomous Platform Anomalies Detection in CPS

Market Need

Critical systems, such as the power grid, autonomous transportation and industrial robots are examples of cyber-physical systems (CPS), which have recently seen an 80% increase in cyberattacks. These cost the sector huge monetary losses, approximately £20,000 per minute.

Solution

Industries rely on traditional software-based intrusive security mechanisms to tackle attack scenarios. FORENSIC is a hardware-software co-design-based solution that rapidly and autonomously monitors the system health by collecting low-level hardware features from the target device that are hard to compromise for threat detection.

It is quicker, cheaper and less power consuming than its rivals, as Project Lead, Sangeet Saha explains:

"We are directly observing the hardware, getting low-level information so that whenever we see changes, we can further analyse it for any kind of anomalies – bypassing the internal software."

FORENSIC employs novel, innovative AI techniques to detect any operational changes in the system when an attacker might reach the critical component of the system. The software doesn't rely on modelling of the software applications running on the platforms, and can be calibrated and adapted to different execution platforms.

"Our research is not only academic, we are constantly in touch with long-term industry partners who provide support from leading industry professionals", says Sangeet.

Target Market

- UK-based smart manufacturers and critical infrastructure providers
- Automotive industry and healthcare
- Security solution providers within Industry 4.0

Status & Needs

- ***Status:*** Proof of concept ready
- ***Status:*** Looking to spin out
- ***Need :*** Give potential investors a chance to interact with the POC

Team from University of Essex

Sangeet Saha: Project Lead and Lecturer
Xiaojun Zhai: Project co-lead and Reader
Klaus D McDonald-Maier: Project co-lead and Professor

Contact details

Website: Forensic-essex.com
Email: sangeet.saha@essex.ac.uk
xzhai@essex.ac.uk
kdm@essex.ac.uk

TWINSECURE

Securing Critical National Infrastructure: A Digital Twin-Powered Decision Support System

Market Need

Recent cyber attacks against critical infrastructure have resulted in more than 10 companies halting operations, totalling 50 days of production loss. The main reason for premature shutdown is lack of situational awareness that enables operators to make more accurate decisions.

Dr. Ashraf Tantavy explains how their findings led to TwinSecure:

"We asked ourselves, when there is an attack on critical infrastructure, what should we do? We wanted to create a software that could help operators depending on the situation they were facing.

"Most existing solutions fail to combine cybersecurity and systems engineering to get the bigger picture – we are trying to look at the problem from a different angle."

Solution

TwinSecure is an autonomous decision support system software powered by a digital twin model for the protected system. Performing real-time threat situational awareness, it provides the best set of actions in any given situation. The proposed actions are explained in a way that allows the decision maker to understand the potential safety, financial and environmental impact of every action.

The solution covers cyber and physical failure threats, such as natural disasters. TwinSecure supports safe and resilient critical infrastructure operation, with reduced downtime, fewer financial and environmental losses, and minimal disruption to public services.

Target Market

- Critical National Infrastructure

Status & Needs

- ***Status:*** Aiming to develop a visualisation tool that can give stakeholders a picture of how the complete software can help them achieve safe operation
- ***Need :*** Funding to develop the MVP in 12-18 months
- ***Need :*** Feedback and evaluation from those in the industry
- ***Need :*** Marketing and sales support

Team from De Montfort University

Dr. Ashraf Tantavy: Principal Investigator, Senior Lecturer in Computer Science

Dr. Iryna Yevseyeva: Co-PI, Associate Professor in Computer Science

Contact details

Email: ashraf.tantavy@dmu.ac.uk

Linkedin: /ashraf-tantawy-ph-d-20678915

Cyberheels by LITERALLY NEED

Improving digital-physical wellbeing with IoT enabled cyber smart shoes

Market Need

Cyberheels by LITERALLY NEED is crafting footwear that offers more than comfort and style.

The potential of AI to improve health and wellbeing is huge, but current solutions aren't considering the safety of such devices. The team behind Cyberheels plan to focus not just on creating the right product, but on educating wearers too.

Solution

The project envisions a future where our footwear becomes our first line of digital protection. By developing smart shoes embedded with cutting-edge IoT technology, the product can monitor our digital presence, protect our data and enhance our overall well being.

The team raise awareness about the vital connection between cybersecurity and digital-physical wellbeing. Founder and Project Lead Dr Adaku Agwunobi explains:

"We're trying to bring a human aspect to cybersecurity and bring about a positive impact through education. [...] By wearing Cyberheels, you're taking control of your digital life and contributing to a safer, healthier digital ecosystem."

With experience in a range of occupational backgrounds, the team can reach multiple markets – bridging the gap between cybersecurity and the fashion world.

Target Market

- Students
- Women
- Lone workers
- Nurses
- Medium-Large Businesses

Status & Needs

- ***Status:*** Proof of concept ready
- ***Need :*** Further funding
- ***Need :*** Strategic partners

Team from University of Oxford:

Dr Adaku Agwunobi: Founder
Jessica Agwunobi: Product Manager
Abiye Amachree: Tech Lead
Beauty Odeyemi: Cybersecurity Intern
Pippa Christian: Marketeer + Psychologist
Tara Collingdale-Williams: XR Specialist
Ifeoluwa Ogunbufunmi: Strategist

Contact details

Email: info@literallyneed.com
Website: www.literallyneed.com
X/Twitter: @literallyneed
Linkedin: /literallyneed

IOT- ARMOR

Empowering IoT's future with education on seamless secure-by-default integration

Market Need

IoT devices are becoming more integrated into our daily lives, but studies reveal that inadequate implementation of secure design principles is a major contributor to device vulnerabilities. In March 2024, a Code of Practice for Consumer IoT devices will be mandated by the UK government, emphasising Security-by-Default principles for enhanced security.

Yet, a substantial gap remains in educating individuals about implementing Security-by-Default principles. IoT-Armor founder Dr. Waqar Asif is on a mission to improve accessibility to cybersecurity education within universities.

Solution

IoT-Armor provides a custom firmware toolkit utilising widely available components. The toolkit empowers users to test, learn, and implement crucial security measures such as secure boot, remote attestation, device tamper detection, secure communication, and device authentication.

"Our competitors rely on SAS solutions on the cloud, which don't really do the job well", says Dr Asif. "We have a hardware component and a flexible firmware, meaning we can educate our manufacturers without forcing them to build their IoT device around fixed hardware."

Dr Asif hopes to pilot test the project with higher education institutes, before launching an MVP in the next nine to 12 months. Long-term plans include an entirely cloud-based solution as well as a standalone device for IoT device protection.

Target Market

- Higher Education Institutes
- Security Education trainers
- IoT Device Manufacturers

Status & Needs

- ***Status:*** Proof of concept complete
- ***Status:*** Funding
- ***Need***: Higher education clients for testing

Team from University of West London

Dr. Waqar Asif: Project Lead, Senior Lecturer of Cyber Security and Course Leader for BSc Cyber Security

Contact details

Email: waqar.asif@uwl.ac.uk

TRUEDEPLOY

Mitigating Open-Source Software Risk for SMEs

Market Need

The team at TrueDeploy understands that securing software code is a daunting task, especially for SMEs without cybersecurity expertise or sufficient resources.

Current solutions provide minimal insights and generic recommendations about improving software security, rather than customised insights and recommendations. TrueDeploy bridges the gap between management, security, and development teams through an easy-to-use AI solution.

Solution

While completing his PhD, CEO and Project Lead, Pavlos Papadopoulos identified a real-world application for his research. Joining forces with a diverse and complementary team of experts, has enabled him to commercialise.

As opposed to other complex developer-oriented solutions, TrueDeploy offers a simplified, single view of a company's software security status, accessible to even non-security experts. It continuously monitors software libraries to identify vulnerabilities and licensing compliance breaches.

TrueDeploy's platform correlates this information with the development team's activities, providing insights and recommendations to improve a company's security posture. Pavlos explains:

"We are doing this based on a virtual software security expert which is integrated into the software development systems that our customers use. [...] Our platform provides tailored insights and recommendations based on our users' unique software architecture."

Target Market

- Y1 (2024): UK Tech SMEs
- Y2 (2025): EU FinTechs
- Y3 (2026): Enterprise customers and US Expansion

Status & Needs

- ***Status:*** PoC ready, first revenue-generating MVP imminent
- ***Status:*** Building the TrueDeploy Vulnerability Database
- ***Status***: AI/NLP models being trained to provide insights & recommendations
- ***Need***: Further investment
- ***Need***: Clients to test the product in a real world setting

Team from Edinburgh Napier University

Pavlos Papadopoulos: CEO and Project Lead
Owen Lo: Technical Lead
Nigel Chadwick: COO
Richard Plant: Head of Engineering
Andreas Chitos: Front-end Developer
Bill Buchanan: Advisor
Nick Pitropakis: Advisor

Contact details

Email: hello@truedeploy.com
Website: truedeploy.com
X/Twitter: @TrueDeploy
LinkedIn: /truedeploy

CybPass

Autonomous Penetration Testing and Threat Modelling for securing AI

Market Need

Penetration testing is used to find and exploit vulnerabilities in a computer system, using a simulation attack to identify weak spots in a system's defences.

Current AI/ML penetration testing solutions remain manual, taking min. 15 days and costing at least $7000 for one penetration test, without guaranteeing the security of the client's tested IP (e.g AI model, AI algorithm, AI training data).

The CybPass team spotted a market gap for an AI-led solution that allows better cost efficiency and privacy of the data set and AI asset algorithms.

The team have utilised the MITRE ATLAS frameworks and the OWASP LLM top 10, prioritising client data confidentiality through a privacy-preserving methodology.

Solution

CybPass offers a unique platform that provides autonomous penetration testing as a service for AI-enabled assets, whilst safeguarding AI assets against evolving threats in the AI cybersecurity landscape.

"Our solution is fast, it's automated, AI driven and it's going to ensure the privacy of our client IPs", explains Dr. Aryan Pasikhani.

Primarily serving the financial industry, CybPass specialises in securing AI assets in areas like Fraud Detection, PayTech, WealthTech, and Algo Trading. The solutions are adaptable, catering to other AI-driven sectors such as Healthcare and Automotive.

The team have benefited from the CyberASAP programme and look forward to meeting potential investors and early adopters to test their demo.

Target Market

- AI-Driven Business
- FinTech/Banking
- Healthcare

Status & Needs

- ***Status:*** Proof of concept ready
- ***Status:*** The team are committed to protecting against the dynamic challenges in AI technologies
- ***Need***: Investors
- ***Need***: Early adopters to test the demo
- ***Need***: MVP development

Team from the University of Sheffield

Dr. Aryan Pasikhani: Principal Investigator - CTO
Dr. Prosanta Gope: Co-Investigator - CEO
PingChen Lin: Research Assistant - COO

Contact details

Email: aryan.pasikhani@sheffield.ac.uk
Website: www.cybpass.com
LinkedIn: /cybpass

CyberSecurityAId

A dynamic, AI-powered self-assessment cybersecurity tool for small businesses

Market Need

CyberSecurityAId is tackling the cybersecurity vulnerabilities of small businesses that often lack the resources to implement effective cyber hygiene practices – leaving them exposed to digital threats.

"We wanted to do something different to understand what firms do in terms of cybersecurity and how to improve their practices, and then we thought okay – let's actually create a tool instead of being passive observers", says Project Lead, Dr. Arroyabe.

Solution

CyberSecurityAId is a self-assessment tool powered by Large Language Models (LLMs). It's designed to provide small businesses with affordable and accessible means to enhance their cybersecurity knowledge and practices. The tool offers tailored recommendations that aim to protect their key assets, systems, and processes.

Knowledge Exchange Manager, Ville Karhusaari is confident in the potential of their solution:

"If our development & commercialisation plan works, over the next 12 months we've got the potential to spin out which would be a first from the social sciences.

"Within our team there's a real interdisciplinary mix of expertise, something that sets us apart from others in the field."

The team's long term goal is to see a large proportion of UK companies utilising the tool and noticing a difference in the safety of their business.

Target Market

- Insurance companies
- Cybersecurity accreditation bodies
- Cyber Resilience Centres
- Public support and membership organisations
- Managed service providers

Status & Needs

- ***Status:*** Proof of concept ready
- ***Status:*** Undergone extensive market validation
- ***Need:*** Further development funding for MVP
- ***Need:*** Investors & partners

Team from University of Essex

Dr. Marta Arroyabe: Project Lead
Prof. Haris Mouratidis: Co-Lead
Ville Karhusaari: Knowledge Exchange Manager
Kaylee Shurety: Technology Transfer Officer

Contact details

Email: mf17255@essex.ac.uk (Marta F. Arroyabe)
Website: www.cybersecurityaid.co.uk
Linkedin: /marta-f-arroyabe

AI-BILITY 4DS

Empowering Cyber Learning for diverse minds

Market Need

The team behind AI-bility 4DS identified a gap in supporting neurodiversity in the cybersecurity community, despite many cybersecurity professionals identifying as neurodiverse. As an educator, Dr Aiash interacts with a range of practitioners and found that they often experienced neurodiversity challenges when trying to complete training or scale up:

"They needed a tailored examination that met their needs, which is where the idea for creating AI-based assisted learning for neurodivergent cybersecurity professionals came in", says Dr Aiash.

Solution

AI-bility 4D is an AI-learning assistant addressing the distinct cognitive needs associated with each of the four dimensions of neurodiversity: Dyslexia, Dyscalculia, Dyspraxia, and Dysgraphia.

The team's solution empowers cybersecurity professionals with unique cognitive styles, fostering skill development and career progression.

Their long term aim is to support those with ADHD in cybersecurity roles. Dr Nalli explains:

"In order for us to tackle the problem, we need to access more funds, refine our design and get more experts on the team including psychologists.

"We have high hopes for Demo Day and hope to meet investors and partners who believe in what we do."

Target Market

- Vocational training providers
- Examination and certification boards
- Colleges and HEI

Status & Needs

- ***Status:*** Proof of concept ready
- ***Need***: Further funding
- ***Need***: Looking to recruit team of experts
- ***Need***: Investors
- ***Need***: Partners

Team from University of Middlesex

Dr Mahdi Aiash: CEO-Project Lead
Dr Giacomo Nalli: PI and Data Scientist
Professor Mark Gray: Director of Knowledge Transfer

Contact details

Website: www.ai-bility.tech
LinkedIn: /dr-mahdi-aiash-b25a069

SIRENPOD

AI Enhanced Honeypot for Cybersecurity on IoT devices

Market Need

IoT device attacks are rapidly increasing in volume and variety. Recognising the heightened risk posed by these factors through their own research, the team from Kingston University created SirenPod.

Project Lead Vasileios Argyriou explains the current solutions and what sets SirenPod apart:

"Currently, honeypots are built for a specific purpose. This is time consuming and can require a lot of engineers to work on one project. Our solution is AI based, meaning there's one applicable solution per device, so we're able to simulate any device."

Solution

SirenPod offers the latest in AI-enhanced intrusion detection and large-scale data analytics for IoT devices through a honeypot service, preventing real devices being hacked.

The unique solution comes in the form of a digital replica, finely tuned to match the actual device. This digital counterpart deceives potential hackers, providing more substantial and valuable insights.

SirenPod can collaborate with manufacturers to establish an online presence for a digital twin device before the physical device is launched, allowing them to identify vulnerabilities and apply patches before the genuine device becomes susceptible.

The team have experience in AI and delivering products and services end-to-end. They're looking to work with large-scale manufacturers before establishing a pilot project with a trust or healthcare service.

Target Market

- Energy
- Healthcare

Status & Needs

- ***Status:*** Proof of concept complete
- ***Status:*** Looking to develop MVP in the next 12 months
- ***Need :*** Investment
- ***Need :*** Partners
- ***Need :*** Advisors

Team from Kingston University

Vasileios Argyriou: Project Lead
Ben Nagy: Research Assistant
Eugene Park: Research Assistant
Adrian Bandy: Research Assistant

Contact details

Email: Vasileios.Argyriou@kingston.ac.uk
Website: blogs.kingston.ac.uk/kuil/

ECG.AI

Securing AI models, improving resilience, reducing risk and enabling compliance

Market Need

ECG.ai understand that the governance of AI tools is essential, especially when they are integrated with applications that have substantial business impact. But ethical issues are becoming more pressing.

Solution

ECG.ai enables businesses to deploy AI by providing a structured framework with API integration – with best practice guidelines for ethics, cybersecurity and governance.

ECG.ai also provides a risk/threat management and mitigation framework based on innovative academic research and industry threat frameworks for AI/ML models.

"We want to know how the AI is going to be used in an organisation, not just build the technology we think they should be using", says Project Lead, Dr Devraj Basu.

The team see value in being part of the AI tool's development, providing solutions and adapting to the processes of the organisations that they work with.

They also bring a unique perspective to the programme, as Dr Basu explains:

"Not only do we come from an academic background, but we come from a business school. Jai is well embedded in the financial services industry, and I have worked with startups and fintechs. We also have a good understanding of how innovators work – so we have an integrated perspective."

Target Market

- Financial Services
- Government/Defense
- Health Care

Status & Needs

- ***Status:*** Proof of concept ready
- ***Need***: Further funding
- ***Need***: Partners
- ***Need***: Looking to grow the team, especially with development expertise
- ***Need***: Evolve from cybersecurity into AI management solution

Team from University of Strathclyde

Dr. Devraj Basu: Co-Investigator and Academic
Jai Geelal: Co-Investigator, PhD Student

Contact details

Email: hello@ecgai.co
Website: www.ecgai.co
LinkedIn: /jaigeelal
/devrajbasu

ACE: AI PRIVACY ORCHESTRATOR

Privacy-oriented AI training and permissions control for compliance-by-design

Market Need

The team behind ACE: AI Privacy Orchestrator found that existing cloud middleware technologies do not enable businesses to integrate privacy into their AI design – so they took the opportunity to develop a middleware solution that could address the privacy issue of feeding data into AI.

Solution

Through ACE, firms can tailor the knowledge and accessibility of their AI services by the privacy and confidentiality restrictions of their data.

The team have developed a user-friendly middleware platform, allowing developers to specify the privacy semantics of their data and create cloud-native machine learning pipelines, differentiated by privacy needs.

ACE enables private-by-design creation and deployment of AI cloud-native services, with knowledge not only protected but inherently restricted by privacy needs. It will enable privacy-preserving and secure (re)usability even of sensitive data, ensuring adequate supply of data to AI-assisted digital ecosystems.

The team believe their combined skills, experience and network sets them apart, as Dr Naday explains:

"We know the data science business, we know the privacy issues that feed into AI and we know how cloud infrastructure handles software [...] and our university network helps us connect with a community of corporates and enterprises across the UK and Europe."

Target Market

- UK and EU-based companies providing or using AI services

Status & Needs

- ***Status:*** Proof of concept ready
- ***Need***: Market support helping towards MVP development and delivery in 12-18 months
- ***Need***: Investors
- ***Need***: Partners

Team from University of Essex

Mays AL-Naday: Project Lead
Haris Mouratidis: Project Member
Flavia Popescu-Richardson: Technology Transfer Officer

Contact details

Email: mfhaln@essex.ac.uk
LinkedIn: /mays-al-naday

VOUCHSEC

Conversational Cyber Security Platform for the AI Era

Market Need

Almost 80% of cyber security decision makers anticipate offensive AI to increase, evading traditional solutions. Users are overwhelmed by the number of alerts – 500+ per day on average, meaning critical alerts can be missed.

Security operation centres are dissatisfied with security talent shortages and cyber defence tool quality due to: high number of false positive alerts, slow and outdated threat detection, long threat processing, lack of visibility and interoperability between siloed cyber security solutions.

Solution

Vouchsec is a conversational detection and response platform to manage cyber incidents. It detects new types of threats and provides integrations with other solutions as data and alert sources.

This approach correlates alerts and automatically resolves the majority, offering a centralised threat remediation environment via visualisations and natural language interaction. Vouchsec allows security analysts to focus on high-priority, high-risk events, reducing financial and reputational losses.

Dr. Michael Piskozub wants to represent data in a more approachable way:

"I'm fascinated by how you can arrange data points to take advantage of senses like vision. It allows security analysts to process threats quicker. I envisage the future where visualisations will be created on-the-fly by simply describing them in spoken language."

Target Market

- Security Operation Centres (SOCs)
- Managed Security Service Providers (MSSPs)
- Large enterprises

Status & Needs

- ***Status:*** Proof of Concept (PoC) ready
- ***Status:*** Spinning out of University of Oxford
- ***Status:*** MVP development with support from Crossword Cybersecurity
- ***Need***: Investor funding & *Advisors*
- ***Need***: Engagement & collaboration on MVP

Team from University of Oxford

Dr Michael Piskozub: Project Lead & Cyber Security Researcher

Prof. Ivan Martinovic: Head of Systems Security Lab

Dr Paul Gass: Technology Transfer Officer

Amelia Griffiths: Technology Transfer Officer

Contact details

Email: info@vouchsec.ai

Website: vouchsec.ai

LinkedIn: /vouchsec

CyberASAP Alumni Showcase

In an ever-changing yet essential sector, the need to convert research into products for the cybersecurity world is becoming increasingly important. Academics are instrumental in providing the solutions to some of the sector's most pressing challenges, but need the training and support to take their knowledge to cybersecurity commercialisation.

CyberASAP is the only accelerator of its kind in the UK, and has been instrumental in helping many academics to develop and spin out their innovations. Over the years, our academic teams have demonstrated that no two solutions are the same. Every journey, from prototype to polished product, is different.

Our Alumni continue their commercialisation journeys in myriad ways. On the following pages we profile four, featured in the Alumni Showcase at this year's Demo Day.

FACT360

Insider Threat, Financial Crime and Compliance Anomaly Detection, Monitoring and Investigation

FACT360 leverages cutting-edge AI and unsupervised machine learning to revolutionise how organisations detect and respond to threats within their communication networks. Our advanced technology uncovers invaluable insights vital to an organisation's security and investigative efforts, delivering results that were previously unattainable. Whether it's identifying insider threats like cyber-attacks, malicious users, or nefarious actors, FACT360 serves as a powerful post-incident investigation toolset and a proactive monitoring platform, offering early alerts for potential threats. Backed by pioneering academic research, our solutions excel at uncovering the 'unknown unknowns' and detecting exceptional activity without relying on user-defined rules or customized configurations. Trusted across industries for fraud detection, insider threat monitoring, and strategic decision-making, FACT360 provides a factual foundation for shaping businesses' strategic directions.

At FACT360, we empower businesses with actionable intelligence derived from deep insights into their communication networks. Our solutions not only mitigate risks but also inform strategic decisions, guiding organizations towards success in an ever-evolving landscape of cyber threats. By harnessing the power of AI and machine learning, we offer unparalleled capabilities in fraud prevention, threat detection, and strategic planning.

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

LinkedIn: /company/fact360

Website: www.fact360.co

MINDGARD

Cybersecurity platform that secures AI/ML models, across in-house and third-party solutions

Mindgard, the leading cybersecurity platform for AI, specialises in securing AI/ML models, encompassing LLMs and GenAI for both in-house and third-party solutions. Rooted in the academic prowess of Lancaster University and launched in 2022, it has rapidly become a key player in the field by tackling the complex vulnerabilities associated with AI technologies. Our flagship service, Mindgard AI Security Labs, reflects our dedication to innovation, automating AI security testing and threat assessments to identify and remedy adversarial threats that traditional methods might miss due to their complexity.

It is supported by an extensive AI threat library, enabling the identification and mitigation of over 170 unique attack scenarios. This ensures that organisations can proactively protect their AI assets across their entire lifecycle. Mindgard seamlessly blends into existing security frameworks, bolstering the capabilities of (SOCs) in managing AI-specific vulnerabilities.

Offering tailored solutions like red teaming and detection and response, Mindgard is equipped to empower organisations to defend their AI innovations against the cyber threats. Available in both free and enterprise packages, our platform is designed to serve organisations of all sizes. Whether deployed through cloud, on-premises, air-gapped environments, or via API integration, Mindgard provides unmatched protection.

Peter Garraghan
CEO & Co-Founder

Lewis Birch
Founding ML Engineer

Ayomide Apantaku
Software Product Engineer

Email: peter@mindgard.ai

Website: www.mindgard.ai

X: @mindgard

LinkedIn: /company/mindgard

ATDPS

Security through Adaptivity

At present, the majority of large IT vendors invest in developing private security systems for their projects which — due to a failure to detect and mitigate zero-day trojans — leaves them vulnerable to breaches.

Whilst existing solutions make use of the Trojan Detection System, capable of mitigating known trojan signatures, there is currently no solution to combat unseen attacks. These solutions use firewall, cryptography, Automotive Penetration Testing and Authenticated frame transmission. However, they lack adaptivity, and are both expensive and resource exhaustive.

ATDPS seek to be the first in the market to provide significant protection against zero-day trojans, with a long-term ambition of providing security throughout the entire phase of an IC (integrated circuit) supply chain.

Our unique system provides a lightweight, adaptive and inexpensive solution with resilience against unknown trojans and scalability. It focuses on two areas: a Machine Learning (ML)-based approach for Trojan Detection and Prevention System and a Physically Unclonable Function (PUF)-based hardware protection system.


Dr. Prosanta Gope
CEO


Dr. Aryan M.P.
CTO


Soumadeep Das
Research Engineer


Pingchen Lin
Marketing Advisor


Kumi Thiruchelvam
Business Advisor

Email: p.gope@sheffield.ac.uk

LinkedIn: /company/atdps

Website: www.atdps4noc.website2.me

BASEEL (licensee of CityDefend)

Security – Technology – Transformation

Baseel is a trusted technology and cybersecurity partner for digital-ready businesses, specialising in delivering cyber forensics, strategic digital transformation, and data management solutions.

Baseel empowers clients to safeguard their digital assets, optimise their operations, and harness the full potential of their data so that they can thrive in the ever-evolving digital landscape. We serve clients across 100 plus countries.

Baseel is the exclusive licensee for CityDefend (CyberASAP Alumnus), which provides unique searchable encryption that enables clients to manage their most confidential data while maintaining absolute privacy and security.

CityDefend USPs

Enhanced security & privacy: Homomorphic searchable encryption schemes enhance security and give the user full control over their data

Reduced storage overhead: Eliminate the need for maintaining a centralised data structure to reduce storage overhead.

Intra-cloud scalability: Scalable across cross-cloud and nested cloud infrastructures allowing dynamic databases.

Reduced network latency: Functions with the minimum network traffic and hence reduces the network overhead.

Lightweight: Based on trust atomic primitives that are lightweight and can be used in resource constrained environments

Paresh Deshmukh
CEO

Raj Rajarajan
CTO

Email: paresh.deshmukh@baseel.com
Phone: +44 7825362359
Website: www.baseel.com
LinkedIn: /company/baseel

CyberASAP in Numbers (Years 1-6)

144 projects have participated

72 projects have graduated

78 universities have participated

65 universities have graduated

CyberASAP helps establish new cyber security businesses

32 Startup companies have been formed by CyberASAP participants

Funding raised

Over **£23m***

CyberASAP Alumni succeed in raising further funding from a range of sources to develop their product/service idea.

Sources: * Figure correct as of March 2024

Get involved in CyberASAP

Academics

CyberASAP welcomes participation from academics based all around the UK who have an interest in commercialising their cyber research. The programme is particularly keen to invite applications from academics in under-represented groups.

Future opportunities will be posted at cyberasap.co.uk and via our social media channels. If you are interested in applying, please register your interest at cyberasap.co.uk (via the Get involved section).

Mentors

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 such valuable input to the teams and enjoy insights into the cyber innovations being developed on the programme.

Thank You To All Our Mentors & 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.

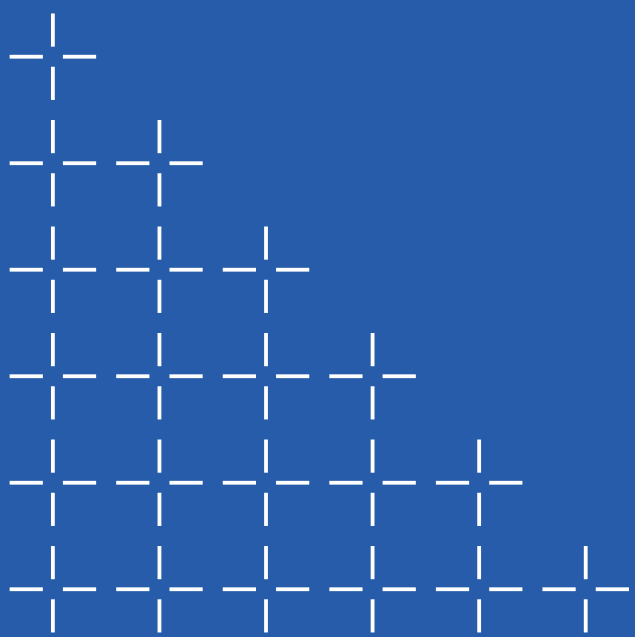
A huge thank you to each and every one of you.

Cyber Security Academic Startup Accelerator Programme
To find out more about the programme and how to engage with it, visit cyberasap.co.uk

Contact us

CYBER + ASAP | Academic Startup Accelerator Programme

Website: cyberasap.co.uk
Twitter: @CyberASAP
Email: cyberasap@iuk.ktn-uk.org
LinkedIn: /cyberasap



UKRI Innovate UK

Website: iuk.ktn-uk.org
Twitter: @innovateuk