CyberASAP

The Cyber Security Academic Startup Accelerator Programme is the only pre-seed accelerator programme in the Cyber Security ecosystem. Created in response to the need to commercialise academic cyber security ideas and translation of research.

CyberASAP is funded by the Department for Digital, Culture, Media and Sport (DCMS) and is delivered through Innovate UK and the Knowledge Transfer Network (KTN). Now in its third year, it is a programme of sector-specific commercialisation support to develop academics' entrepreneurial skills and translate their research into products and services. The programme contributes to a core DCMS objective, to develop and sustain a security sector that meets the national security demands. CyberASAP supports this ecosystem by helping UK universities to commercialise their cyber security ideas.

There are 13 project who are currently being funded to develop their Minimum Viable Product:

Year 3 – MVP Phase Projects

TAPCHA
Bournemouth University
TAPCHA: Online Fraud Detection and Prevention, Reinvented for Everyone
We improve the detection and prevention of non-authentic web traffic for global online service providers, by offering a new, localisable, non-invasive CAPTCHA solution because business revenue and user trust are adversely affected by the increasing amount of malicious online transactions.

Year 3 – MVP Phase Projects

CTLR
Bournemouth University
Cyber Threat Landscape Ruleset: A cost-effective correlation ruleset for advanced threat detection
We offer advanced and cost-effective threat detection for security service providers, smaller or larger companies by offering a standalone subscription-based service for correlation rules because threat detection tools without proper rules is a waste of resources.

Privacy Throughout
Bournemouth University
Privacy Risk in Context
We provide a context-aware privacy risk assessment tool clients that provides them with an overview of their privacy risk exposure. This allows them to confidently identify and embed appropriate security measures to reduce that risk, because our clients are serious about safeguarding their customers' privacy .

GuardKeeper
Coventry University
GuardKeeper: Creating secure connectivity and authentication of a consumer to an end user
We provide secure connectivity and authentication on the internet for a consumer by extending the green padlock security in the web browser with enhanced additional security because the green padlock doesn't indicate to the end user the identity of who they are connected with.

Year 3 – MVP Phase Projects

INSURE
De Montfort University
Secure Wi-Fi access wherever you go
Did you pack your cyber security system last time you went on a business trip? Cyber security in public Wi-Fi networks is frequently non-existent. Yet, only 17% of business travellers report using VPN to access work related files and services, and existing Wireless Intrusion Prevention Systems (WIPS) only provide centralised security at a fixed location. INSURE has developed a portable WIPS that offers business travellers unsupervised, dynamic and adaptive real-time protection when connecting to public Wi-Fi networks. The unique statistical detection engine at the core of INSURE has been designed by academics at De Montfort University, one of the UK's leading university for cyber security research. We are looking for industry partners that would help us extending the evaluation of INSURE in a real environment

BLEMAP
Royal Holloway
BLEMAP: We analyse and mitigate security threats of Bluetooth devices.
We secure bluetooth devices for IoT manufacturers by automatically analysing the application and device firmware, and producing patches for them because the complexity of Bluetooth is resulting in an increasing number of threats that can affect IoT and other Bluetooth-enabled devices.

CYBER
+ASAP

Academic
Startup
Accelerator
Programme

Year 3 – MVP Phase Projects

Prinesec
Royal Holloway
Shifting security paradigm from siloed-events to holistic-impact assessments
We enhance the information security resilience of organisations by utilising our patented technology that shifts the focus from siloed analysis of events to collective impact assessments because the existing paradigm of security control centres is insufficient. We aim to reduce the time to identify and contain a breach, which translates into significant savings for an organisation.

PriSAT
University of Glasgow
Privacy Engineering for Software Designers: GDPR compliance requires strong consideration of privacy-by-design.
We enable software designers to design technology that complies with privacy regulations For companies that build technologies which depend on personal data By automatically co-evolving design artefacts to reveal privacy risks and recommend design alternatives Because lack of privacy-by-design in technology increases risks of regulatory fines, reputation damage to brand and can become a barrier to technology adoption.

Year 3 – MVP Phase Projects

BioGenerate
University of Gloucestershire
Generating true random numbers from the body's physiological signals.
We generate True Random Numbers for SSL/TLS companies by using the body's physiological signals because they provide device independent, high rate, low-cost entropy as a standalone or complementary solution in random number generation. A disruptive evolution from Psudeo Random Number Generation (PRNG) to Quantum Random Number Generation (QRNG), now we bring you Bio Random Number Generation (BRNG). For when quantum is just not random enough.

Verifiable Credentials
University of Kent
Verifiable Credentials: On the Internet, everybody knows it's a dog
We provide the virtual equivalent of physical credentials (plastic cards, passports, qualifications, driving licenses etc.) for everyone and everything by converting them into cryptographically secure and privacy protecting W3C Verifiable Credentials so that they can be easily stored, carried and presented electronically as needed.

PhishAR
University of Oxford
"PhishAR: your employees' augmented reality vaccine against cyber attacks."
WE increase resistance to phishing and other social cyber-attacks   FOR your non-expert employees   BY using immersive augmented reality capabilities of mobile devices   BECAUSE existing security awareness trainings lack engagement and interactivity.

Year 3 – MVP Phase Projects

CyRysk
University of Southampton
CyRysk: ISO-Standard Automated Risk Assessment for IT Systems
We make risk analysis of complex IT systems faster and more reliable for cyber security consultancies and large companies by providing a software solution that models socio-technical systems (including IT components, people and physical spaces) and automates an ISO 27005 risk assessment over them using a built-in knowledgebase of threats and countermeasures. This is vital because right now risk analysis is generally done on a whiteboard and is therefore time-consuming and error-prone.

VACCYNE
University of Wolverhampton
Intelligent child-centred shield against harmful content and communications
Did you know that 1 in 4 children are being exposed to racist or hate messages online? The Internet is an enabler for cyber victimisation including radicalisation, bullying, stalking and grooming. We provide parents and schools with a highly automated safeguarding solution to maintain good parenting against harmful communications. We deploy a "prevent" strategy incorporating machine learning-powered detection, automated real-time intervention and age-sensitive gamification techniques to train and raise awareness. Our solution has an intelligent virtual assistant to block the bad and promote virtue.

@CyberASAP