Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Bournemouth University	TAPCHA - a mobile first, non-instrusive and customisable CAPTCHA scheme	£31,072	£31,072

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It is a type of authentication test to protect online services from automated abuses leading to cyber attacks (e.g., password attacks) or resource wastages (e.g., spams). CAPTCHAs are often seen in association with user related online services (login, registration etc.) and other online communication and transaction related services (e.g., banking, flight ticket booking etc.). The core of a CAPTCHA service is its scheme which defines the challenge as well as the required and supported human interactions. Only when it is done right, it will protect the services while retaining users. TAPCHA is a new CAPTCHA scheme designed with 'mobile first' initiative and the utilisation of cognitive biases to address the following challenges for online businesses and service providers: 1. They need an effective CAPTCHA scheme to stop their services from automated abuses affecting their intended uses, leading to cyber attacks and brand/reputation damage. 2. They need a mobile-first CAPTCHA that fits nicely into their 'mobile-first' designed services (e.g., mobile apps, responsive web apps etc.). 3. They need a less-intrusive or immersive CAPTCHA scheme that users can easily complete to maximise online transactions.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
University of Gloucestershire	Generating strong cryptographic key from body physiological signal in securing medical implants communication	£24,000	£24,000
Imperial College London		£4,000	£4,000

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
An increasing number of people around the world are enjoying the health benefits of internal devices such as cardiac pacemakers and insulin pumps. An unfortunate reality is that there are also an increasing number of people who seek to do harm to others. The potential cyber security threat to these implants has become cause for concern. The solutions currently on the market to counter this threat have a number of known flaws which create vulnerabilities. Researchers at the University of Gloucestershire and Imperial College London have overcome these deficiencies by creating an encrypted communication protocol between the implanted device and the external gateway that controls it. With millions ofpeople relying on medical implants for their health and wellbeing, Innovate UK funding has helped researchers to complete the final stages of bringing a solution to market. A solution which will protect people from the threat of a cyber-security attack that could have life threatening consequences.

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
De Montfort University	INSURE: Intrusion detectioN System for pUblic hotspot cybeR sEcurity	£16,547	£16,547

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
Wi-Fi attracts great interest among Internet Service Providers and end users despite the growth in popularity of the 4G/5G technologies. Mobile operators want to see a closer integration between mobile broadband networks and Wi-Fi access points, also known as Hotspots, as these represent a key solution to improve the overall performance of the mobile communication. Unfortunately, public Wi-Fi hotspots pose many security risks to millions of laptop, tablet and smartphone owners, exposing banking credentials, account passwords and personal information to an increasing number of sophisticated, easy to launch and untraceable cyber-attacks. Hence, providing strong and reliable security mechanisms has become critically important. This proposal presents INSURE, an unsupervised anomaly-based Intrusion Detection System that will provide an extra level of assurance to end user devices in public Wi-Fi hotspot networks, by identifying different types of threats in real-time. INSURE advances the state-of-the-art as it exploits a novel detection methodology, which automatically adapts to the current characteristics of the network traffic without manual intervention from an administrator. It automatically constructs a reference from normal behaviour and flags as malicious information that deviates from this reference. The proposal aims to develop INSURE into a fully operational commercial Intrusion Detection System.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
University of Oxford	PhishAR: Using Augmented Reality to help users make better security decisions	£21,591	£21,591

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
Computer users must repeatedly decide whether to trust a received email or to consider it a phishing attempt. Knowledgeable users develop various phishing detection mechanisms: they detect unexpected spelling mistakes, spot suspiciously urgent sentiment, or check for mismatches between the sender's email domain and their claimed identity. These nuances, while complex for non-expert users to learn, lend themselves to being automated by machine learning models. We are working on an augmented reality based security assistant: a mobile device system that uses computer vision and machine learning techniques together with immersive AR capabilities of modern smartphones and headsets to supervise and provide seamless security guidance to non-expert users by _looking_ at the screens of other devices and instructing them on how to use them. More specifically, after an email is received, our solution allows the user to scan it with their mobile phone and receive an estimate of the likelihood of the email being a fraudulent phishing attempt, together with interactive explanations as to why such a conclusion was made.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Bournemouth University	Privacy in a Smart Circular Economy (PITCH)	£30,340	£30,340

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
The UK and the European Union (EU) are keen to reduce waste and promote reuse of resources throughout the European Economic Area (EEA). As part of this drive, a new initiative has been created to promote a Circular Economy in Europe (European Environment Agency, 2016). Circular Economy refers to achieving sustainability by reusing limited and finite resources and keeping them at their highest utilization. In order to achieve this, it has been recently acknowledged that data needs to be reused, re-circulated in or near-real time. This is referred to as data-driven Circular Economy where citizens become prosumers i.e. co-producers and co-creators of the data generated from their devices (European Environment Agency, Circular by Design, 2017). Data-driven Circular Economy is the pinnacle use case of privacy and security of personal data. This project seeks to create a tool that can be used to facilitate Privacy in a Smart Circular Economy (PITCH). PITCH is a comprehensive privacy risk assessment tool that will facilitate informed decision making of the suitability of data collected from organisations and prosumers for reuse as part of a Smart Circular Economy (SCE).

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
University of Plymouth	Cybersecurity Risk Assessment Box (CRAB)	£22,809	£22,809

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
Digitalisation is happening everywhere around us, however it increases cyber-attack risks. The proposed Cybersecurity Risk Assessment Box (CRAB) will identify types of cyber risks for shipping and provide data to everyone involved in maritime transportation. The UK is an Island nation with 95% of our international trade and 15% of domestic trade transported by sea, therefore secure maritime operations are of paramount importance. We believe that maritime cyber threats are, as for most systems, a combination of human factors and technology, therefore, we wanted to develop a system that would allow vessel owners to assess the level of cyber security risk resulting from behaviours of staff, their IT systems and potential attacks. Currently, there is no method to provide a real-time risk assessment of cyber threats on-board vessels. With the application of the CRAB, both shipping (through lower insurance premiums) and UK society (through improved security of maritime operations) will benefit as they will be better prepared for the digital era, driven by the 4.0 Industrial revolution.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Teesside University	Play2Secure: An AI enabled personalised cyberspace awareness game for young people	£31,482	£31,482

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
We will develop an intelligent game (Play2Secure) to empower the young people with knowledge relating to risks and threats in cyber space. This includes their needs on how to (i) identify secure sites to browse safe and secure form (ii) securely deal social media activities and (iii) prevent grooming, bullying and any abuse through online. The proposed game will give an opportunity to engage young people effectively, particularly to understand their ability in keeping them secure in the cyber space. So far, most of the similar games come with fixed objectives that does not help in engaging young people due to nature of dynamic needs of every game. It is worth mentioning that usually young people lose interest playing same scenario repeatedly. Secondly, there is no personalised training programme that can educate a user based on their need or level of understanding. Therefore, we consider that this is a new and innovate product, perfectly matching with the needs of young people in the market. The proposed game can be considered as a part of the training requirements of the young people in their everyday digital activities in their smart home, inside and outside school.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
University of Brighton	Escaping traditional training – developing an escape room for enhancing cybersecurity skills and awareness	£9,342	£9,342

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
This project aims to develop an innovative escape room concept, drawing on dual expertise in cybersecurity and gamification of learning, that can be used to provide introductory cybersecurity training with learning outcomes that greatly exceed traditional training approaches, addressing a significiant skills gap.

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Coventry University	Alternative Authentication Sequence for Mitigating Man-in-the-Middle Attacks	£31,350	£31,350

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
Everyone knows that the Web can be a dangerous place, and people are starting to be aware of the fundamentals of being safe on-line. The "lock icon" is one of these. It tells us when our communication is secure between our browser and the server it is talking to. What it can't tell us, is whether the server is the one we think it is. In fact, we could be securely handing our details to an attacker using something called a "man-in-the-middle" attack. This project is developing a new authentication system that allows web servers and web browsers to convince each other that they aren't just talking securely, but they're talking securely to the right people! Without requiring complex set-up or operation for the user, the new system can warn you of man-in-the-middle attacks before any compromising information is sent.

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
University of Winchester	Multi-Modal Continuous Transparent Biometric Authentication for Mobile Devices	£19,054	£19,054
ACCELERCOMM LTD		£1,552	£1,086

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
The modern mobile handheld device is capable of providing a plethora of multimedia services through a wide range of applications over multiple networks. These services are predominantly driven by data which is increasingly associated with personal and commercially sensitive information. There is an increasing dependence on mobile devices with more than 5 billion users globally and this raises the security requirement for reliable and robust verification techniques of end-users that extends beyond the traditional point-of-entry. This project will analyse the feasibility of developing a multi-modal continuous and transparent authentication architecture for mobile devices. The proposed solution will significantly enhance current state-of-the-art authentication approaches by using multiple biometric modalities (facial recognition, keystroke analysis, behavioural profiling) to continuously and transparently authenticate end-users. The proposed architecture will provide end-users with a convenient, non-intrusive, application specific authentication approach which is capable of understanding the different risk levels and requirements of individual applications. The proposed architecture utilises existing hardware technologies such as facial recognition, keystroke analysis, application usage and fingerprint recognition to continuously authenticate end-users based on their psychological and behavioural characteristics. This solution is scalable and provides further opportunities for additional authentication modalities such as smartwatch physical activity recognition.

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Goldsmiths College	TRANSACTIONAL ANALYSIS FOR INSIDER THREAT DETECTION	£31,896	£31,896

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
'Insider Threat' is a formidable risk to business because it threatens both customer and employee trust. Accidental or malicious misuse of a firm's most sensitive and valuable data can result in customer identity theft, financial fraud, intellectual property theft, or damage to infrastructure. Because insiders have privileged access to data in order to do their jobs, it's usually difficult for security professionals to detect suspicious activity. The 2016 Forrester Report "Hunting Insider Threats" identified eight key factors as common motivators of Insider Threat: Financial distress; Employee disgruntlement; Perceived employee entitlement to sensitive information and IP; Job insecurity; Revenge; Conflict at work; Ideology and Outside influence. Our goal in this project is to use advanced AI and transactional analytics to (i) identify communication patterns characteristic of both team and company breakdown (hence identifying potential lack of engagement within teams and employees at risk of losing their job); (ii) identify language use characteristic of deception (alongside proven metrics of message \`sentiment'), enabling automatic alerts on potential employee distress, disgruntlement, insecurity etc. and (iii) identifying a-typical communication patterns to foreground signals characteristic of potential outside influence within a company.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Royal Holloway Univ of London	BLEMAP: Security for Bluetooth Low Energy Enabled Applications	£17,994	£17,994

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
BLEmap helps companies develop secure personal and wearable IoT devices that communicate using Bluetooth Low Energy.

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
University of Glasgow	Privacy Engineering for Software Designers	£21,047	£21,047

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
Seemingly innocuous design decisions during software engineering can unintentionally affect user privacy. This is aggravated with everyday objects such as watches, cars and services that we depend on now becoming privacy threats because of their ability to seamlessly communicate with each other. Bad software design undermines information protection by distorting user expectations and obscuring privacy harm. Consequently, there has been policy-based and legal initiatives aimed to mitigate the privacy harm resulting from badly designed software. For instance, the General Data Protection Regulation (GDPR) and complementing UK Data Protection Act aims primarily to give control to individuals over their personal data. But while efforts to protect user privacy are being enacted through laws and best practice propositions, it is still the responsibility of software engineers to ensure that technologies are architected, designed and coded with privacy as an inherent property. Yet, designers lack tools and methods for evaluating their design with respect to stated privacy objectives. Hence, this project will investigate the commercial potentials of a tool that helps designers of software examine the privacy-preserving capabilities of their design and consider regulatory compliance. With this tool, designers can distinguish between good and bad software design, as well as alternative design choices.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Open University	CyberGaTE: A Gamified Intelligent Environment for Training and Assessing Cyber Security Behaviour	£28,000	£28,000

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
Recent studies indicate a severe global shortage of cybersecurity professionals. The reason for this could be attributed to; Lack of secure user behaviour that is contributing to increasing cyber-attacks. Fresh graduates and young professionals lack the skills that the industry demands. Cybersecurity as a discipline has an image of being 'geeky', 'technical', 'uninteresting' and 'unethical' leading to a small uptake of cybersecurity related degrees. Unlike other disciplines within the IT sector, cybersecurity is a combination of aptitude, skill and behavior. Traditional instructional-approach of providing information about risks and reactive measures is inadequate. 'CyberGaTE aims to address these challenges by using the concept of serious games for communicating secure behaviour, artificial intelligence to react to user's actions and thereby assessing user's secure behaviour against best practice principles and cloud environment will give user's, access to real devices. CyberGaTE will act as an intelligent, personalised training and assessment environment that organisations could use for effective cybersecurity behaviour training for end users and security professionals; To assess their current security behaviour to anticipate risk they pose and identify their specific training needs. Schools and Universities could use the environment for inspiring, engaging and identifying potential young talents with aptitude for secure behaviour.

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Birmingham City University	AngelPass	£15,142	£15,142

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
This project focus on an uncomfortable, yet unavoidable, perspective of life: death. It is a fact of life that we will all cease to physical exist and, yet, our digital existence may last forever if nothing is done. Upon death, there are digital assets one wants to transfer control to others such as family, friends or work colleagues; examples are passwords to access a laptop, social media, email, cryptocurrencies or digital documents. There are also digital assets a person may want to have destroyed so to be in control of memory. AngelPass will be a new product where anyone can securely manage passwords, documents, etc., for a long period; upon a life event, and depending on the person's wishes, they are either destroyed or sent to someone else. A key feature is that AngelPass will have no access to user passwords or documents at any time so all the secrets shared with us are completely secure.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
University of Southampton	System Security Modeller	£24,966	£24,966

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
With online banking and shopping being ever more critical to our daily lives and health data increasingly going online, protecting the security of our IT systems has never been more important. We have a cyber-security system modelling prototype which has reached a maturity level where it is already of interest to adopters in multiple sectors. The System Security Modeller (SSM) will improve the security of IT systems, reducing personal data breaches and system downtime. The tool analyses a complete IT system: networks, computers, processes, data, operators, users and physical and legal spaces. Using a novel threat and control identification technique we can identify threats from hackers, employees, software failure or misconfiguration and highlight non-compliance with data protection regulations. Our tool lets a user assess which threats have the highest risk (likelihood and impact) and propose appropriate security measures (data encryption, firewalls, etc.) which should be implemented. The SSM will automatically identify threats in an IT system, assess the risk level and choose the appropriate security controls (ISO 27005 process) significantly more robustly, reliably and efficiently than current practice. Security costs will be reduced and cyber-security increased supporting the UK's dependence on increasingly networked IT systems in business and society.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
University of Kent	Verifiable Credentials	£29,935	£29,935

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
Verifiable Credentials will help to provide users with the electronic equivalent of today's plastic cards and paper credentials, such as: passports, driving licenses, bus passes, EHIC cards etc. in an electronic form on their mobile devices. This innovative approach will enable the user to present them to any service at a time of their choosing, in order to gain access to the service. The project will: 1) provide an open source library of the Verifiable Credentials code so that organisations can freely download and use it. This will help to grow the market for Verifiable Credentials. 2) establish an SME that is able to provide consultancy support, bespoke tailoring, and application development and integration, using the open source code, for those organisations who do not have the expertise or staff to do it themselves.

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
University of Kent	Proof of Claim (PoC): A human-in-the-loop AI based solution for semantic information integrity	£26,600	£26,600

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
This project aims at providing an innovative solution to the grand challenge we are facing in many application areas of our modern society: how to detect false information that can have negative social impacts -- fake news and online frauds as two typical examples. Another side of the challenge is how to protect true information from honest people and organisations, who are often negatively impacted by false information provided by other people and organisations such as dishonest competitors, biased or incapable news reporters, fraudsters, and criminals. This problem is not new, but so far we are not winning the fight against false information, e.g., fake news and online frauds remain biggest challenges our society is suffering from. The project addresses the problem by introducing a new theoretical concept called "Proof of Claim" and apply the human-in-the-loop AI technologies to design a new technical framework that can protect true information and detect false information more effectively. It does not only depend on technologies, but also has an embedded mechanism to engage with and incentivise human users who are information consumers and beneficiaries of the proposed framework. It allows humans and machines to work seamlessly together to overcome problems existing solutions have.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
University of Wolverhampton	Safe Internet surfing with an intelligent child-centred shield against harmful content	£30,502	£30,502

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
The Internet provides high exposure to malicious content with direct impact on children's safety. Illicit, violent and pornographic material to name a few. The Internet is also an enabler for cyber victimisation such as cyberbullying evidently causing children (and adults) drastic and severe health implications including documented cases of self-harm and suicide. Recent studies show the problem continues with 1 in 4 children exposed to racist or hate messages and over 2,200 counselling sessions with young people took place in 2017/18 related to online sexual exploitation which is a 44% increase from the previous year. Hence, current solutions are clearly problematic. This project aims at superseding the obsolete techniques in use today with an innovative and intelligent child-safety shield. The value proposition is manifested by quicker intervention and better filtering capabilities with the ability to address emerging threats targeting children on social media. The project also aims at achieving incident response and safer Internet surfing without having to block popular services and websites.

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Bournemouth University	Cyber Threat Landscape Ruleset (CTLR)	£20,339	£20,339

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
Year by year the number of cybersecurity incidents and their diversity increases. Threat actors are becoming more skilled, determined and have at their disposal a great amount of resources and time. Security Information and Event Management (SIEM) tools are widely used against cybercrime. These tools are as good as the threat detection rules that they use. However, most companies -- especially SMEs -- do not have the resources and the expertise to create and update the SIEM rules. Cyber Threat Landscape Ruleset (CTLR) aims to provide a cost-effective, commercial service that generates the rules, improves security operations and allows the market to defend against the ever-increasing number cyber threats.

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
De Montfort University	Simulated Critical Infrastructure Protection Scenarios (SCIPS)	£14,548	£14,548

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
In order to build and maintain secure computer systems, it is vital that Cyber Security is understood and acknowledged as a critical issue by all levels of an organisation. To improve the awareness and understanding of cyber security in executives it is important that they recognise the potential impact that modern cyber threats may have on their business. SCIPS is a table-top exercise in which participants take on a predefined senior executive role. Teams are required to balance a limited investment budget against competing market, corporate and personal priorities. Each turn requires a team decision, this involves selecting from a range of potential security measures that may be implemented and also which budget will fund these measures. The game has been designed to encourage discussion within the teams, with all actions having potential benefits but a reduction in any budget leads to a negative financial situation for at least one player. As the game progresses, the actions taken by players can mitigate the impact of malicious actions upon their company, which in turn impacts upon the share price of the company. Success in the game is based upon the financial status of the company at the end of the game.

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
University of Essex	SensiTech - Secure Blockchain Alert System	£31,964	£31,964

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
The Blockchain market is showing a Compound Annual Growth Rate of 80.2% (ResearchAndMarkets.com). As more mission critical businesses continue to rely on the Blockchain technology, the major concern is the sensitive information stored on the Blockchain networks. Furthermore, the latest GDPR regulations require individuals to have full control of data while maintaining data confidentiality. Therefore, Blockchain enterprises require technology that provides individuals with full control over their data, while preventing data loss and information theft; which existing cloud solutions are unable to provide for Blockchain networks. Permissioned Blockchain provides integrity, provenance, immutability and transparency however lacks in providing confidentiality; that prevents mission critical enterprises from using Blockchains to store sensitive data and exploring its true potential. SensiTech is a pioneering enterprise solution that helps achieve military grade security by generating real-time alerts on encrypted Blockchain data. This provides enterprises and entities with complete control and trust on the permissioned Blockchain network while generating real-time alerts on the encrypted mission critical data. In comparison to it's competitors SensiTech offers greater levels of security and privacy, reduced network latency, enhanced efficiency and effectiveness. SensiTech could benefit different verticals including IoT, the military, banking, law enforcement agencies, healthcare domains, financial and e-commerce sectors.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Teesside University	Risk2IoT@home: An Intelligent and Predictive Assistant for Secure and Safe Smart Home	£31,892	£31,892

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
The exponential business growth of Internet of Things (IoTs) market is causing many manufacturers to follow an aggressive time to market policy, and this along with lower cost requirement are [producing insecure IoT devices][0], especially home devices. Many consumers, especially homeowners/users are buying and using these insecure IoT devices to make their home smart as they care more about price and features than security. These devices are causing or will cause security threats for their applications. The proposed Risk2IoT@home project will be using AI algorithms to significantly minimise threats and risks in home cyberspace by proactive measurements and security awareness training of the vulnerable home cyberspace users. This will cut down users' time required for security awareness training as it will be designed by the core concept of '_learning just what you need to know at the exact right moment_'. It will provide an optimal learning experience through an intelligent tutoring system which tailors the needs of each user based on their pre-existing knowledge and provide intriguing contents with gamification and game-based learning techniques. Moreover, the tool will provide support for home cyberspace policy implementation and enforcement that is not available in existing solutions. [0]: https://www.v3.co.uk/v3-uk/news/3028337/most-off-the-shelf-iot-devices-carry-frightening-security-risks-warn-researchers

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
London Metropolitan University	SYCAMORE: Vulnerability Analysis and Risk Assessment of Cyber Security Policies	£8,000	£8,000

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
Sycamore automates the process of analysing the logical vulnerability of business operations and assessing the risks associated with the security policies of organisations working in digital businesses. The tool can operate in monitoring mode, implementing full scenarios and in predictive mode, analysing the potential risks associated with particular security policies. It is based on semantic technologies and works with standard logical models of business operations and security policies which can be developed using standard semantic modeling tools such as Protégé and OntoEdit. The tool loads business models and security policies in OWL and SWRL format. The output of the analysis is presented in a graphical format as a flowchart, augmented with information about the vulnerability and risks. Sycamore serves the needs of large corporates, business and service providers and midrange companies which use third-party services. Sycamore has been tested in several application domains related to cyber security and safety management -- cross-channel fraud in digital banking, evacuation policy in public safety and business workflow management. It has been made commercially viable product with the support of DCMS on the basis of previous research and experimental development by an academic team of the Cyber Security Research Centre of London Metropolitan University.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Royal Holloway Univ of London	AISecure	£18,750	£18,750

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
The AI market size is expected to be USD 190.61 billion by 2025, with a CAGR of 36.62% between 2018 and 2025\. Furthermore, AI systems will be used in a wide range of applications, from cybersecurity threat prevention to autonomous vehicles and algorithmic trading strategies. As the reliance on AI systems in different existing and emerging technologies increases, so do the potential threats to such systems. Therefore, it is vital to make sure that AI systems: a) are well designed and resilient against cyberattacks through rigorous pentesting; and b) have digital forensics capabilities that can investigate cyberattacks and misbehaviour within the system. The provision of the listed capabilities through the AISecure suite will undoubtedly mitigate an AI algorithm's social, ethical, legal and technological risks. The first innovation is the ability to deal with the combination of traditional cyber-threats and specific AI attacks, like the poisoning of the learning mechanisms in a single AISecure suite, a crucial aspect that is missing in most current commercial pentesting solutions/services. The second innovation is to provide forensic investigation capabilities related to AI systems that help identify the culprits and influence the security design of future AI systems.

Innovate UK

Results of Competition: Cyber Security Academic Start-up Accelerator Programme Year 3 Phase 1

Competition Code: 1902_FS_DCMS_CYBERASAP_P1

Total available funding is £800,000

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Royal Holloway Univ of London	Transparent?Compliance (TC)?	£21,513	£21,513

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
The technology infrastructure of an organisation is a complex set of multitudes of services interconnected with each other. This complexity is?then?translated?into security and privacy-preserving policies/services?for the organisation. Most of these services are configured and operate in silos, with little interconnectivity. This creates an enormous challenge for managing security and privacy practices -- from organisational policies and services to monitored activities. The challenges are to: ?a.integrate all security- and privacy-related services into a single portal,? b.provide a real-time security and privacy visualisation and? c.provide a transparent auditing and compliance assessment service that analyses the activities in an organisation?as a whole and?not as a subset of individual services such as firewalls or IDS logs/events. Transparent Compliance will monitor security and privacy services in an organisation, integrating their monitoring logs and building a causality chain. The chain represents the sequences of inter-related events that might be temporally disjointed and allowed at the individual level but collectively might violate the security and privacy policies. The causality chain is analysed to verify an organisation's compliance with the required security and privacy preservation policies, thus providing a holistic, corporate-wide, real-time auditing and compliance assessment service.