



**Innovate
UK**

Innovate UK

Global Business Innovation Programme - Australia

Cyber security | October 2023



CONTENTS

2. The UK and Cyber security
3. Innovate UK
4. Global Business Innovation Programme
5. Leading the visit
6. Map
7. CyberHive
8. Cyntegra
9. Digital Transit Ltd
10. FACT360
11. Gentium UK Cyber Training
12. Goldilock
13. Kaze Technologies Ltd
14. Lupovis Ltd
15. McCormickCo Ltd
16. Praeferre
17. Quantum Dice
18. Rickocity Ltd
19. SignalVision Ltd
20. Think Cyber Security Ltd
21. - 24. Notes



THE UK AND CYBER SECURITY

The UK and Australia share a common language and culture and maintain a long-standing partnership in the realm of defence and security including being members of the Five Eyes and the AUKUS trilateral partnership. Further deepening the UK's close partnership with Australia is deemed important to delivering the UK's Indo-Pacific tilt set out in the UK's Integrated Review.

The UK's National Cyber Strategy 2022 recognises the strategic importance of technologies that are vital to strengthening the country's cyber power. The UK Government takes a framework approach to generating strategic advantage that includes critical technologies across semiconductors, AI, future telecommunications, and quantum technologies. International cooperation with like-minded partners on research and innovation, standards, policy, and regulation will be necessary to encourage the creation and adoption of those enabling technologies that will underpin future cyber-secured products and services.

UK and Australia have complementary S&T strengths and capabilities with a spotlight case in secure and resilient computing systems. UKRI's [Digital Security by Design](https://www.dsb.dtech/)¹ (DSbD) programme is based on the research-led groundbreaking [CHERI](https://www.cl.cam.ac.uk/research/security/ctsr/d/cheri/)² approach to computing implemented on the Arm-based [Morello](https://www.arm.com/architecture/cpu/morello)³ prototype hardware platform that has the potential to block cyber-attacks from at least 70% of today's ongoing memory-related vulnerabilities. The DSbD technology is finding its way to global adoption, including across the RISC-V ecosystem, by working with international partners and sector-specific value chains.

Meanwhile, Australia has successfully transitioned its leading research to a high-performance verified operating system kernel, known as [seL4](https://sel4.systems/)⁴, that has been deployed across a range of safety-critical products and applications. Bringing these two transformative technologies together opens up synergies such as in using the formally verified hardware architecture to bring capability protections and benefits to seL4 system processes and applications in addition to the software kernel.

Australia is at the crossroads of developing its national cyber security strategy for 2023-2030 having set an ambition to become the world's most cyber-secure nation by 2030. This is an exciting and opportune time having already engaged with Australia's cyber ecosystem over a Global Expert Mission (October 2022), now taking our learnings forward through a market visit as part of Innovate UK's Global Business Innovation Programme.

The UK delegation's business cohort includes a breadth of specialisms and forward-thinking innovators looking to engage with the Australian cyber ecosystem, make contacts with key stakeholders, build new collaboration partnerships and advance their innovation ideas.

On behalf of the UK delegation, I very much look forward to meeting, discussing, and working with Australian stakeholders - across Government, industry, research, and local cyber communities - towards collaboration opportunities and bilateral initiatives.

Georgios Papadakis
Senior Innovation Lead - Digital Security by Design & Cyber Capabilities, Innovate UK – part of UK Research & Innovation

1 <https://www.dsb.dtech/>
2 <https://www.cl.cam.ac.uk/research/security/ctsr/d/cheri/>
3 <https://www.arm.com/architecture/cpu/morello>

4 <https://sel4.systems/>

INNOVATE UK

Innovate UK



Innovate
UK

Innovate UK is the UK's innovation agency. We drive productivity and economic growth by supporting businesses to develop and realise the potential of new ideas, including those from the UK's world-class research base.

We work to **inspire** innovative businesses to create value through innovation. We work to **involve** talented organisations and people to create a vibrant and successful innovation ecosystem. We work to **invest** in innovation in order to make a clearly tangible, positive impact on the UK's economy and society.

We help businesses to grow through their development and commercialisation of new products, processes and services, supported by an outstanding innovation ecosystem that is agile, inclusive, and easy to navigate.

GLOBAL BUSINESS INNOVATION PROGRAMME

Supporting businesses and innovators to collaborate and grow internationally is a central theme of the UK Government's plan for growth, setting out a goal to be the most innovative country in the world by 2030.

The Global Business Innovation Programme, organised by Innovate UK and delivered by Innovate UK EDGE, consists of a preparation phase, five-day innovation visit focused on cyber security, a post-visit exploitation workshop and follow up support of approximately 12 months from an Innovate UK EDGE Innovation & Growth Specialist, helping your business maximise the opportunities identified, including developing innovation projects with partners in the territory. This initiative will be delivered physically and include virtual activities.

It will support these businesses with a structured programme across three main phases: getting ready for the market, visiting the market, and exploiting the opportunity.

This brochure details the 14 companies taking part in this Global Business Innovation Programme visit to Australia, their business overviews, and their objectives for this visit.

LEADING THE VISIT



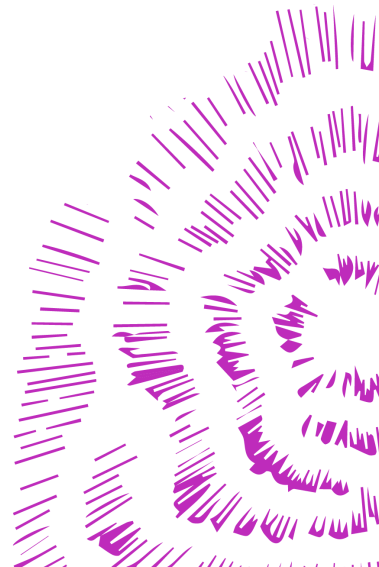
Georgios Papadakis
Senior Innovation Lead - Digital Security by Design & Cyber
Capabilities, Innovate UK
Email: georgios.papadakis@iuk.ukri.org
Mobile: +44(0)7824 626788



Asha Sudra
Innovation & Growth Specialist, Innovate UK EDGE
Email: asha.sudra@innovateukedge.ukri.org
Mobile: +44 (0)7970 110846



Stuart Coyle
Innovation & Growth Specialist, Innovate UK EDGE
Email: stuart.coyle@innovateukedge.ukri.org
Mobile: +44 (0)7717 200494



1. CyberHive
2. Cyntegra
3. Digital Transit Ltd
4. FACT360
5. Gentium UK Cyber Training
6. Goldilock
7. Kaze Technologies Ltd
8. Lupovis Ltd
9. McCormickCo Ltd
10. Praeferre
11. Quantum Dice
12. Rickocity Ltd
13. SignalVision Ltd
14. Think Cyber Security Ltd



CyberHive protects the most valued organisations, their people, data and assets, with patented technology that is simple, secure and performant.

Deployed in minutes, CyberHive enables customers to focus on their growth, profitability and innovation.

Key Products & Services

CyberHive Connect is a simple, secure and performant overlay mesh network that transforms how devices communicate. It delivers a Trusted Area Network, providing instant security that can be easily retrofitted into existing infrastructure including on legacy devices and systems. Connect delivers quantum-safe encryption as standard, future-proofing an organisation's communications.

Traditional approaches to cyber security try to detect the unknown and ever-changing threats and bad behaviours. CyberHive instead focuses on only allowing the known good to happen, making it possible to detect data breaches in seconds. **CyberHive Trusted Cloud** gives organisations precise control over which applications are running in their environments putting them back in control of their cloud workloads, critical connections, and most sensitive data.

Unique Selling Proposition

The number one comment organisations make when seeing CyberHive's products for the first time is "It can't be that simple - how can something that delivers so much value really be that easy to use and operate?"

Invention is in their DNA. Their products are based on a mix of tried and tested architecture and novel techniques and technologies for a variety of cyber security applications. Equally at home in enterprise environments or large-scale IoT implementations - CyberHive delivers award-winning security that's easy to use and highly performant.

Company Seeks:

We relish collaboration and partnerships. We seek ambitious partner companies who want to bring CyberHive products to new markets. We welcome like-minded investors who'd like to be part of our ambition to set the benchmark for cyber security, and our vision to make cyber-crime a thing of the past.



Sarah Blundell

Phone: +44 (0)7968 441692

Email: sarah.blundell@cyberhive.com

Website: www.cyberhive.com

Materially reduce disruption and costs from ransomware attacks.

Cyntegra's mission is to enable organisations to avoid potentially catastrophic disruption and financial costs resulting from ransomware or disruptive malware attacks and to ensure they never have to pay a ransom to do so.

Key Products & Services:

Ransomware and disruptive malware attacks leave computing systems completely disabled and unable to support critical processes. Cyntegra's patented technology (CyntOS®) enables customers to restore compromised systems to their familiar and fully functional pre-attack state in minutes, not days or weeks. There is no need to wait for costly IT resources or replacement hardware, and no need to pay a ransom, ever.

Their solution is platform independent and can be used with almost any computer system, including embedded systems found in production lines, medical devices, utilities and transport management systems and vehicles.

Unique Selling Point:

Traditional 'backup and recovery' solutions focus on restoring data and not the functionality of a computer system, and are of little use if the device itself cannot be used. Cyntegra's patented method and technology ensures a compromised system can always be restarted into their Recovery Operating System (CyntOS®) and the end user can then restore full functionality via a simple menu.

Company Seeks:

We are currently seeking:

- Potential OEM partners who would license our CyntOS® technology and embed it directly into their products to make them Ransomware-proof
- Potential distribution partners, such as Managed Security Services Providers, to resell our Cydecar® recovery solution direct-to-market
- Investors to participate in our current financing round



Giles Watkins

Phone: +44 (0)7500 072785

Email: gwatkins@cyntegra.com

Website: www.cyntegra.com

Digital Transit Ltd are an industrial research and development company specialising in railway safety critical software assessment and operational technology cyber security.

Their goal is to improve rail transportation by being part of the push to enhance 21st-century rail systems using digitisation and automation. Digital Transit Ltd are developing support tools and training media in the area of railway OT(Operational Technology) cyber security.

Key Products & Services:

Digital Transit Ltd:

- Provide safety critical software assessment to SIL2
- Provide training and support in railway operational technology cyber security
- NLP tools for developing and assessing cyber security artefacts
- Automated compliance evidence with the mandatory critical infrastructure regulations for OT cyber security standards for example, CENELEC TS50701 and IEC62443

Unique Selling Point:

Their current team has over 150 years of combined railway engineering experience, so they know the railway. They also have gifted computer and data scientists to enable them to capitalise on their experience of developing new ways of working, such as machine learning, that augment existing skills.

Company Seeks:

We already have contacts in Australia and would like to explore collaborations with relevant organisations, university research groups in Sydney and Melbourne, and regulation bodies in developing case studies, a body of knowledge and tools for OT cyber security in the railway and transit systems.



Howard Parkinson

Phone: +44 (0)7803 581849

Email: hjparkinson@digitaltransit.co.uk

Website: www.digitaltransit.co.uk

FACT360 have built the “Swiss Army Knife” for Insider Threat, Financial Crime, Compliance and Risk Investigations and Monitoring.

They focus on human communications: voice, email and instant messaging. This allows them to spot changes in behaviour over time using proprietary machine learning techniques. These anomalies are then presented to the user via a set of dashboards. FACT360 have a language engine that can extract entities in any language from communications and categorise the text into groups (abuse, fraud and insider trading) for ease of investigation or monitoring.

Key Products & Services:

FACT360 is the only product they offer. This is a software-as-a-service tool that can be deployed on-premise or in your private cloud or their cloud. This is the core investigation and monitoring tool. They ingest the communications data and then present back the anomalies for use in a retrospective investigation, or to be used as an ongoing monitoring tool to spot changes in people's behaviour inside your organisation.

Unique Selling Point:

FACT360 have a unique set of machine learning technique that allows them to initially build up a timeline of behavioural change without looking at the content of the messages (fully GDPR compliant). This is called a user's prestige - a proprietary metric from FACT360 - and from this you can then investigate this anomaly. The second part of the solution provides a method of extracting key data from the communications and placing them in categories (like a news website hierarchy) for ease of investigation. This again is a proprietary technique from FACT360.

Company Seeks:

We are looking to partner with cyber security software providers, cyber security investigators and financial crime investigation firms so that FACT360 can be offered and supported in the Australian market.



Patrick Lawton

Phone: +44 (0)7850 656438

Email: paddy.lawton@fact360.co

Website: www.fact360.co

Gentium UK Cyber Training are elite cyber security education specialists.

Their immersive learning experiences, including the Cyber Escape Room and Cyber Crisis Simulator, empower individuals and organisations to master cyber defence. Led by former UK cyber police officers, their expert team provides gamified, real-world training, equipping you to tackle threats with confidence.

Key Products & Services:

- The Cyber Escape Room - An immersive, linear game where the participants take on the role of a cyber detective, solving cyber-related clues in order to save a company from a global cyber terrorist organisation
- The Cyber Crisis Simulator Platform - Navigate your team through a simulated cyber attack scenario that mirrors real-world incidents, ensuring you gain practical skills and valuable insights
- CyberPro Higher Education course - A specially designed 25-module Criminology and Cybercrime course
- Cryptocurrency training and storage solutions
- Cyber awareness board games

Unique Selling Point:

Unmatched expertise and immersive approach to cyber security education. Led by experienced ex-UK cyber police officers, they combine real-world knowledge with gamified learning, offering hands-on training that's engaging and effective. Their international partnerships with GIZ, Interpol and the United Nations, underscores their credibility. Organisations choose Gentium UK Cyber Training for cutting-edge simulations, deep insights, and tailored solutions that empower individuals and teams to navigate the evolving cyber landscape confidently, making them the go-to choice for comprehensive cyber security training. Education meets entertainment making for a memorable training experience. Gentium UK Cyber Training offer a 24/7 cyber crisis management team that is deployed the moment a Ransomware attack is in process. The team of experienced NCA and GCHQ cyber security experts specialise in data recovery and threat actor negotiation.

Company Seeks:

We are eager to connect with cyber security firms, universities, law enforcement and organisations that require comprehensive cyber awareness and knowledge, whether this is to protect themselves from cyber attacks, educate a generation of young people or learn how to investigate the latest in criminal cyber activity. We seek partnerships for collaborative ventures, joint projects and potential investment opportunities to further expand our reach and innovative capabilities. Our goal is to strengthen global cyber security preparedness through strategic collaborations and knowledge exchange.



Daniel Garnham

Phone: +44 (0)7818 725408

Email: daniel.garnham@gentiumuk.com

Website: www.gentiumuk.com

Reinventing cyber security through true physical segmentation!

Goldilock Drawbridge is a revolutionary cyber security solution that enables users to physically segment their digital assets, devices, networks, operational control systems, and literally anything - remotely, instantly, and without using the internet to do it. Their patented technology ensures that your assets are unreachable, invisible and inaccessible to adversaries, and only physically connected to the internet when you need them.

Key Products & Services:

Any device with an IP address is visible and vulnerable to accidents and attackers, but Goldilock's unique and patented technology physically segregates data, networks, and people from harm. Goldilock is a 12-port network appliance that is controlled remotely and offers complete network isolation functionality via out-of-band and non-IP-based SMS commands.

- **Instant Accessibility:** Goldilock's secure non-internet communications allow for immediate access to your assets whenever needed, combining the security of cold storage with the speed and flexibility of hot storage
- **Enhanced Security:** By enabling physical disconnection of your digital assets from the internet when not in use, Goldilock significantly reduces the attack surface and provides a higher level of protection for sensitive data and systems
- **Customisable Control:** Goldilock's remote connectivity control and compatibility with any network outlet offer versatile options to protect a wide range of devices and networks, giving you the power to tailor your security solution to your specific needs

Unique Selling Point:

Goldilock has revolutionised the way data, devices and infrastructure are protected on networks by allowing you to physically connect and disconnect anything from anywhere, in seconds without using the internet to do so. Their unique, patented platform utilizes secure non-internet communications to keep your sensitive digital assets physically segregated from any network, while still having them accessible at a moment's notice from anywhere on Earth. CISCO's former SVP of Advanced Security Research says Drawbridge is an "essential technology to better protect and recover from Ransomware attacks, isolate mission-critical networks and digital assets from adversarial visibility, in addition to regaining full and physical control of the attack surface."

Company Seeks:

Meet with Cyber OT and IT buyers and MSSPs or other channel partners looking for an innovative solution to protect CNI. Also, system integrators looking for a unique solution that won UK's Hardware/End Point Device of the Year 2023. Thirdly, we are looking for investors who are interested in deep-tech hardware solutions in both the CNI and defence sectors. Lastly, we are seeking defence prime contractors and those looking for innovative solutions for securing field communications.



Stephen Kines

Phone: +44 (0)7553 587325

Email: stephenkines@goldilock.com

Website: www.goldilock.com

Make critical decisions with confidence.

Kaze Technologies empowers leaders to navigate pivotal moments securely and effectively, delivering strategy and technology solutions that make the difference when it matters most.

Key Products & Services:

Delivering strategy: They don't just develop impactful strategies – they deliver them. From boosting cyber resilience to anticipating market trends, they inspire bold ambition in their clients and work side-by-side to turn innovative thinking into real-world results.

Maximising technology: Their team of engineers, architects, developers, cyber security experts and technologists work seamlessly with their clients to put the latest digital technologies to work, creating frameworks that drive tech-enabled growth and strengthen security across enterprises and beyond.

Decision engineering: Using world-class AI, machine learning and data analytics, they develop solutions that build trust in data, use technology to augment decision-making and extract maximum value for their clients – from time - and cost-saving automation to robust digital security.

Unique Selling Point:

Kaze Technologies' experience is in the defence, security and intelligence sector, using world-class AI, machine learning and data analytics, to develop solutions that build trust in data and use technology to augment decision-making.

Company Seeks:

We want to grow and expand, we are looking to join forces with organisations that need to be secure and provide data-driven solutions to navigate pivotal moments with confidence.

**James Lang**

Phone: +44 (0)7810 524588

Email: james@kaze-consulting.com

Website: www.kaze-consulting.com



LUPOVIS

Lupovis Ltd

Lupovis provides precise, high-fidelity threat identification with a drastically reduced alert-to-noise ratio.

Gain targeted, contextual intelligence specific to your company. Stay steps ahead with insights that pinpoint insider threats, and pre-breach events such as leaked credentials. Dive into actionable intelligence without distractions.

Key Products & Services:

Their flagship products, Lupovis Snare and Lupovis Prowl offer innovative approaches to combat cyber threats. Lupovis Snare deploys, decoys, and traps to divert and detect attackers, providing real-time threat intelligence. Lupovis Prowl offers a global threat intelligence feed, continuously monitoring and analysing data for emerging threats. It constitutes one of the largest adversary interaction databases worldwide.

Unique Selling Point:

With its technology, Lupovis is able to detect pre-breach events and insider threats alike. Lupovis provides contextual threat intelligence in a "deploy and forget" fashion. Focusing on a zero to low false positive approach with fast and easy deployments, covering both IT and OT networks.

Company Seeks:

We're looking to meet with Managed Security Services Providers, CISOs, and SOC Managers across all sectors. MSSPs constitute our outbound go-to-market strategy, while CISOs and SOC Managers are the "job titles" we receive the most enquiries from, irrespective of the sectors.



Xavier Bellekens

Phone: +44 (0)7548 717949

Email: xavier@lupovis.io

Website: www.lupovis.io



McCormickCo is a cyber security consultancy committed to offering transparent tools for organisations to proactively manage their cyber security.

McCormickCo's vision is to enhance organisational resilience and demystify compliance, their core values emphasising transparency, empowerment, clarity, trustworthiness, and approachability. McCormickCo is passionate about empowering you to tackle cyber risks.

Key Products & Services:

TECTA – A SaaS cyber security threat insight tool that deepens organisational understanding of risk and compliance. Their offerings include cyber security as a service, vCISO, cyber security incident response, vulnerability management, remediation, training and support.

Unique Selling Point:

Their tool is the cyber security threat insight tool that enhances organisational understanding. By providing insight into an organisation's cyber risk, in alignment with multiple industry standard frameworks, and measured against metrics relatable to customers' specific industry we can support organisations in determining cyber security risk, and support their remediation, therefore reducing the susceptibility to attack. You no longer need a cyber security expert to manage your risk.

Company Seeks:

We are looking to establish partnerships, particularly in sectors like healthcare, insurance, and finance. Our goal is to embed TECTA across these industries, refining its capabilities to meet industry-specific demands. Additionally, we are on the lookout for investment and collaborative opportunities to further broaden the scope of our solutions.



Matthew McCormick

Phone: +44 (0)7579 003088

Email: matt.mccormick@mccormickco.co.uk

Website: www.mccormickcosecurity.co.uk

Positioned in the growing cyber security market, Praeferre is strengthening privacy management with its innovative cyber security solution, helping consumers and global corporations address data privacy challenges.

The UK Government's Department for Digital Culture Media and Sport has crowned Praeferre as one of the most innovative cyber security SMEs in the UK. The company is now moving towards national and international roll-out through rapid commercialisation.

Key Products & Services:

Praeferre's technology helps organisations with their data privacy management and engages with individuals to ensure they give informed consent to their data use. End users of the freemium consumer app can manage their digital security for all online activities, freely and easily change their data-sharing preferences and be rewarded for sharing their data for commercial use. Businesses benefit from being able to manage data privacy agreements in real time and automatically comply with country-specific data privacy laws.

Unique Selling Point:

1. Single window data privacy management for customers
2. Real-time data privacy acknowledgement
3. Data incentivisation for better customer engagement
4. Protect brand equity/compliance
5. Reduce marketing waste with informed user insight

Company Seeks:

Through the Australian market exploration, we will work on a list of activities and actions to be implemented to open new business collaborations and suggest new business opportunities in overseas locations. Our objectives are:

1. Industry introduction to Telco, Fintech and Retail sector operators for POC/Pilot Projects
2. Help in infrastructure and team scaling
3. Help in accessing Government and public sector funding to grow the team locally in Australia



Abhishek Ghosh

Phone: +44 (0)7706 345368

Email: abhishek@praeferre.com

Website: www.praeferre.com

Random numbers are an essential security, providing the keys to secure and encrypt data and communications. Having real-time trust, and proof of the quality and security of these numbers is essential to underpinning security systems.

Quantum Dice, stemming from the University of Oxford's Physics Department, delivers the world's swiftest, most secure, and user-friendly Quantum Random Number Generation (QRNG). Quantum Dice offers solutions to bolster data protection, enhance communication security, and drive forward scientific research initiatives.

Key Products & Services:

Trust in security keys is crucial for robust cyber security. Quantum Dice leads in quantum technology and cyber security, offering optical Quantum Random Number Generators (QRNG) patented by Oxford's Physics Department. This ensures keys are born from an unpredictable quantum process, providing unmatched trust in key quality and encryption. With diverse form factors like PCIe and compatibility for servers, their QRNG devices address all cyber security needs. They're not just limited to current tech, they're pioneering solutions for the expanding horizons of IoT and space-based security, emphasising their commitment to global and versatile cyber security advancements.

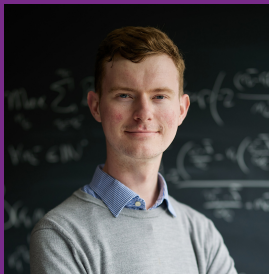
Unique Selling Point:

Utilising their unique and patented protocol, they harness distinctive properties from their quantum architecture. This enables them to consistently guarantee the inherent security and randomness of every number generated, even amidst environmental disturbances, or bad actor interference. Their breakthrough ensures a steadfast foundation for digital security, no matter the external challenges.

Company Seeks:

We are intent on connecting with innovators and partners in Australia's cyber security sector. We're interested in partnering to:

- Strengthen and enhance the resilience of pivotal security platforms and capabilities
- Integrate our provable quantum random numbers into cutting-edge security solutions
- Foster mutual growth and innovation in the cyber security domain



George Dunlop

Phone: +44 (0)7859 938894

Email: george.dunlop@quantum-dice.com

Website: www.quantum-dice.com

Riskocity® provides an easy-to-understand Cyber-Physical Risk Assessment with an initial focus on the shipping sector.

Cyber-attacks to maritime, and other areas of Critical National Infrastructure are increasing, and adequate approaches for appraisal of risk and the mitigations required, do not currently exist. There was a 68% increase in maritime cyber-attacks in 2021, costing many millions to mitigate. With a registered global fleet of 180,000 freight vessels, an even greater number of other vessel types and 95% of the world's freight moved by ship, the International Maritime Organisation has now mandated cyber-risk assessment.

Key Products & Services:

Riskocity® provides a cost-effective, Cyber-Physical Risk-Assessment to allow businesses, initially in the maritime sector, to properly understand their cyber vulnerabilities. This then enables tailored mitigation action with both cost and benefit properly understood. They apply Patented MaCRA® Dynamic Risk-Assessment tooling to assess risk to both Information Technology (IT) and Operational Technology (OT) aspects of a system. This gives owners and operators a higher fidelity risk-assessment bespoke to their operation, enabling the prioritisation of mitigation to spend in response to spiralling costs of business disruption and increasing insurance and regulatory drivers.

Unique Selling Point:

They apply Patented MaCRA® Dynamic Risk-Assessment tooling to determine cyber-physical risk presented by both Information Technology (IT) and Operational Technology (OT) aspects of a system, and uniquely draw on system-level vulnerability insight from the University of Plymouth's world-leading Cyber-SHIP Lab (this is a physical hardware twin of ship's critical systems for investigation of cyber vulnerability).

Company Seeks:

We would be very interested to engage with shipping and port operations to discuss and agree on how we could deliver bespoke Cyber-Physical Risk Assessments for their organisations - and we would also like to engage in partnering discussions around applying our Patented Risk-Assessment tooling to other areas of Critical National Infrastructure.



Kevin Forshaw

Phone: +44 (0)7814 288507

Email: kevin.forshaw@plymouth.ac.uk

Website: www.riskocity.com



SignalVision is a cyber security startup specialising in zero trust and identity protection.

With a core focus on zero trust security configurations, their proprietary technology is able to identify vulnerabilities that are otherwise missed and could lead to a compromised system.

Key Products & Services:

SignalVision's core offering is focused on enterprise customers that leverage Microsoft Conditional Access as part of their cloud security. Their system is able to rapidly assess existing configurations for vulnerabilities as well as guide future changes. While their primary market is in the UK, their global reach ensures that organisations everywhere can benefit from their unparalleled expertise in identity security.

Unique Selling Point:

Their core capability is unique to them, offering an unrivalled level of insight into the performance of your security configuration. Additionally, SignalVision's core team have an exceptional track record within this domain, recognised as experts in zero trust and identity-based security by both Government departments and enterprises.

Company Seeks:

We're on the lookout for pioneering early adopters who truly understand the value of our identity security solutions. We're keen to partner with local companies and tech providers that can complement our services. We also welcome collaborations with enterprises or government bodies interested in piloting our technology, echoing the successes we've had in the UK. Additionally, we're open to discussions with investors familiar with the cyber security landscape, aiming to expand and solidify our foothold in Australia.



Matthew Gribben

Phone: +44 (0)7807 551208

Email: matthew@signalvision.io

Website: www.signalvision.io

ThinkCyber delivers measurable secure behaviour change for their customers through a preventative and proactive approach to security awareness.

Founded in late 2016 by the ex-global Heads of IT and InfoSec from the Cyber arm of BAE Systems (previously Detica), ThinkCyber's Redflags[®] has won the techUK Cyber Innovator of the Year and SC Awards Best Professional Training Programme as well as being selected for the UK National Cyber Security Centre's NCSC for Startups Programme.

Key Products & Services:

ThinkCyber's Redflags[®] Real-time Security Awareness applies behavioural science theory to deliver context-sensitive, just-in-time security guidance. When people are about to click links, visit certain web pages, enter a password, handle attachments (for example), despite a >\$5.6bn security training market, 83% of cyber-attacks start with the human user. Technical controls can never promise to be 100% effective, so people will always be the last line of defence. But traditional awareness is infrequent, boring and quickly forgotten. Phishing tests leave staff feeling tricked/embarrassed. Redflags[®] delivers enduring security awareness and behavioural change, proactively preventing risky behaviours and empowering people to protect themselves against cyber threats.

Unique Selling Point:

Until now, the security awareness market has been pretty boring and lacking in innovation! Built working with academics with behavioural science approaches from the ground up, Redflags[®] is highly differentiated in the market, unique in:

- Proactively pushing awareness straight to the user on their device
- Adapting delivery according to continuous risk assessment of user actions
- Delivering awareness as real-time, in-context security 'nudges' with the potential to actually prevent risky behaviours
- Measuring engagement and risky behaviour trends over time

Company Seeks:

We would love to meet research scientists in human-centred cyber security e.g. at CSIRO's Data61; to explore opportunities/alignment with the Australian DoD, in particular, the Defence Science Technical (DST) group; to explore these challenges with the consortia who work together to deliver Government/Defence projects in the region and to engage with regional experts and consultancies to explore domain-specific applications of Redflags[®] behavioural nudges. We would like to build on our global/regional banking and financial services customers, meeting more regional organisations to explore their pains, challenges and how they are tackling the human factor.



Tim Ward

Phone: +44 (0)7789 278552

Email: tim.ward@thinkcyber.co.uk

Website: www.thinkcyber.co.uk



Innovate
UK

