

17 de mayo de 2021

Estimados amigos:

A través de este nuevo boletín informativo, os hacemos llegar las últimas novedades del

**Clúster 3: Seguridad civil para la sociedad**

- Disponibles [las presentaciones y grabación](#) de la jornada informativa nacional para la convocatoria 2021 del Clúster 3 de Horizonte Europa "Seguridad Civil para la Sociedad", que tuvo lugar los días 5 y 6 de mayo.
- Recordatorio: jornada SMI2Gs 2021 (Security Mission Innovation and Information Groups), seminario y brokerage event Europeo organizado por la red de Puntos Nacionales de contacto de Seguridad - SEREN4, EARTO SECURITY RESEARCH, ECSO e IMG-S. La jornada tendrá lugar en formato on-line, los días 31 de mayo y 1 de junio.

Más información en el enlace siguiente: <https://smi2g-event.b2match.io/>

- ECSO lanza la Comunidad Europea de CISOs. [Webinar "Launch of CISOs European Community \(CEC\) & Discussion on CISOs priorities and challenges", on 7 June from 2-3pm CEST \(online\)](#).

Más información sobre un informe realizado recientemente por ECSO sobre el papel de los CISOs en el ámbito de la ciberseguridad a través del enlace siguiente: [ECSO website following this link](#).

- Comunicación del Consejo Europeo sobre Protección Civil: [Civil protection: Council adopts new rules to strengthen disaster response - Consilium \(europa.eu\)](#)
- Nueva página web de la REA (Research Executive Agency) – Sección Clúster 3: [Horizon Europe - Cluster 3: "Civil security for society" \(europa.eu\)](#)
- Búsquedas de socios convocatoria 2021 Clúster 3.
  - Entidad británica interesada en participar en el topic: HORIZON-CL3-2021-FCT-01-03: Disinformation and fake news are combated and trust in the digital world is raised. Ver **Anexo 1**.

- **Entidad británica interesada en participar en el topic:** HORIZON-CL3-2021-FCT-01-03: Disinformation and fake news are combated and trust in the digital world is raised. Ver **Anexo 2**.
- **Entidad británica interesada en participar en el topic:** HORIZON-C CL3-2021-CS-01-04: Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data. Ver **Anexo 3**.
- **Entidad británica interesada en participar en el topic:** HORIZON-CL3-2021-FCT-01-03: Disinformation and fake news are combated and trust in the digital world is raised. Ver **Anexo 4**.
- **Entidad británica que busca incorporar socios a una propuesta que están preparando para el topic:** HORIZON- CL3-2021-BM-01-01 - Enhanced security and management of borders, maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support. Ver **Anexo 5**.

Esperamos que esta información os resulte de interés.

Un cordial saludo,

*Maite Boyero Egido*

*Representante y Punto de Contacto Nacional Clúster 3*

*Departamento de Retos Sociales. Dirección de Programas Europeos y Cooperación Territorial*

*Centro para el Desarrollo Tecnológico Industrial, E.P.E.*

*C/Cid, 4. 28001 Madrid*

*maite.boyero@cdti.es, +34 91 581 55 62*

ANEXO 1



Looking to join a consortium

**HORIZON EUROPE**

**Civil Security for Society**

**HORIZON-CL3-2021-FCT-01-03**

**Disinformation and fake news are combated and trust in the digital world is raised**

## Jason Reifler, PhD

- Affiliations
  - Professor of Political Science (Exeter)
- Expertise and research area
  - **Misperceptions and fact-checking**
  - **Fake news**
  - **Public opinion** about foreign policy
  - **Surveys and experiments**
- Past and current projects
  - 20+ awards worth in excess of €4M
  - European Research Council (“DEBUNKER”)
  - Economic and Social Research Council (UK)
  - National Science Foundation (USA)
  - Volkswagen Stiftung
  - British Academy
- Impact
  - 54+ publications including *PNAS* (x2), *Nature Human Behavior* (x2), *American Journal of Political Science*
  - Google Scholar: 8863 citations (h-index 31)
  - Significant media coverage

## Mohsen Mosleh, PhD

- Affiliations
  - Lecturer of Business Analytics (Exeter)
  - Research Affiliate Institute for **AI** and Data Science (Exeter)
  - Research Affiliate (MIT)
- Expertise and research area
  - Computational Social Science
  - Combating online **misinformation**
  - Effective **fact-checking**
  - Digital **field experiments**
  - **Network** science
  - Natural Language Processing (**NLP**)
- Past and current projects
  - **Google** Scholar Award on effective fact-checking
  - US **DARPA** Next Generation of Social Sciences on Information Gerrymandering
- Impact
  - 21+ Publications including *Nature* (x2), *Nature Communications* (x2), and *PNAS*
  - Press release in **Washington Post**, **Financial Times**, **The Telegraph**, etc.

**Prof Reifler and Dr Mosleh (R-M) have proven track records studying misinformation and implementing successful interventions against it. As part of a consortium, they can make significant contributions to the calls *expected outcomes* as follows:**

***“Improved understanding of the cultural and societal aspects of disinformation and fake news, as well as on the key challenges related to combating it”***

**R-M have significant experience conducting multi-country studies and field experiments that examine drivers of sharing misinformation and conspiracy claims, as well as implementing successful interventions against their spread. They can use this expertise to:**

- Identify predictors of who spreads misinformation and via which pathways
- Help build models that detect coordinated actions by misinformation spreaders on social media
- Develop interventions against misinformation and fake news
- Assist in effectively targeting interventions within social networks
- Contribute to developing automated and visualization tools to provide insights for strategies against spread of misinformation

***“Enhanced perception of security thanks to an increased awareness of the citizens about the value of verified and trustworthy data sources and their content, obtained through education and training materials on trustable sources of information”***

**R-M can design and implement studies that examine how interventions affect consumption and sharing behaviour. Using similar methodologies, they can also design and implement studies that examine how exposure to these interventions affects:**

- Personal awareness and confidence in one’s ability to resist misinformation
- Awareness and confidence in institutional efforts to combat misinformation (thereby increasing confidence in the information environment)

***“Strengthen key personnel's knowledge regarding disinformation campaigns”***

- R-M have experience disseminating findings from their social science research to key stakeholder audiences



Interest parties please contact:

**Jason Reifler**

Department of Politics  
College of Social Sciences and  
International Studies

[www.jasonreifler.com](http://www.jasonreifler.com)

[j.Reifler@exeter.ac.uk](mailto:j.Reifler@exeter.ac.uk)

**Mohsen Mosleh**

Science, Innovation, Technology, and  
Entrepreneurship Department  
Business School

[www.mohsenmosleh.com](http://www.mohsenmosleh.com)

[m.mosleh@exeter.ac.uk](mailto:m.mosleh@exeter.ac.uk)

Proposal activity: *CL3-2021-FCT-01-03 : Disinformation and fake news are combatted and trust in the digital world is raised*

Professor Kevin McDonald  
Centre for Social and Criminological Research  
Middlesex University London

[k.mcdonald@mdx.ac.uk](mailto:k.mcdonald@mdx.ac.uk)

## Centre for Social and Criminological Research, Middlesex University London

### ➔ Expertise in:

- *Social media analysis*
- *Visual analysis*
- *Experimental methods and participatory research*
- *Working with hard-to-reach groups*
- *Affective research methods*
- *Ethnographic research of online worlds*
- *User experience and online agency*
- *Digital cultures and social worlds*
- *Working across different European languages: English, French, Spanish, Italian, German*

### ➔ H2020 Experience: TAKEDOWN (2018-20), PARTICIPATION (2020-23)



## Team Leader: Professor Kevin McDonald

- ➔ Experience:
  - ➔ Extensive research on extremism, social mobilizations, radicalization
    - ➔ Key outputs (books): *Radicalization* (Polity, 2018); *Our Violent World* (Palgrave 2013); *Global Movements* (Blackwell 2006)
  - ➔ EU experience: Expert Evaluator & Reviewer H2020, involvement in PARTICIPATION (2020-23)
  - ➔ Current research: communication practices and networks associated with far-right extremism in Europe

## Proposal: From Transmitters of communication to world-building communities

- ➔ *Disinformation is not just a 'thing' that circulates. It needs to be understood as a social relationship. Digital information flows are collective processes and need to be addressed as such.*
- ➔ *Malicious disinformation is not only mediated through news channels, but increasingly through conspiracies that take the form of alternate reality games – eg QAnon, Pizzagate*
- ➔ *We cannot address disinformation divorced from the 'world building' at stake in such increasingly pervasive 'alternate realities', where 'trust' is at stake in new ways*
- ➔ *Disinformation depends upon 'affect', hence the critical role of memes and humour as fundamental to information flows in digital culture*
- ➔ *Successful intervention strategies address network structures to stop propagation, but also empower users by addressing their agency: posting, forwarding, liking, commenting, researching, laughing, etc*
- ➔ *New generation of trust-tools need to empower users in ways that address contemporary communication practices such as memes and conspiracies, or the gamification of communication within digital space*

## Specific capabilities

- ➔ *Ethnographic analysis of communication flows, in particular through social media. Extensive experience of research of main meme generating sites (4chan, Reddit) and of the collective dynamics involved in meme generation and circulation*
- ➔ *Development of participatory methods, fundamental for user-generated actions*
- ➔ *Theoretical capability to map the flows of 'affect' that amplify communications – intensity, excitement, fascination, disgust, anxiety, awe*
- ➔ *Capability to work with visual and sensory data (fundamental to 'information') not simply text*
- ➔ *Capacity to work with data scientists and interdisciplinary teams to trace communications, build tools and generate experiments to explore ways to increase trust in digital worlds*
- ➔ *Social experiment capability, to understand user experience of tools developed – not simply their impact on individual users, but upon the circulation of disinformation at network level*

# Ionburst

Secure, Private Data stored across Public Clouds

Seeking technical partner(s) for HORIZON EUROPE

Increased Cybersecurity

CS05 - Human-centric security, privacy and ethics

CL3-2021-CS-01-04: Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data

## Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data

- Point of Contact      Dr David Lanc
- Email address        david\_lanc@ionburst.io
- Websites              ionburst.io; ionburst.cloud
- Information            Capability information is available on demand, please request by email

Ionburst's data defence technology brings a new paradigm in Cloud data security, privacy and resilience at the quantum level. For the first time EU member organisations and citizens can be assured of GDPR data privacy and security against theft, surveillance and ransomware from a EU-based scalable, resilient platform that reduces risk, carbon impact and costs. Ionburst is an API connect SaaS technology enabling ultra-secure data storage and transmission in lower cost Public Cloud than available in Private Cloud implementations, with superior resilience and on-demand recovery.

We are seeking complementary partners to help develop a futureproof solution for proposal CL3-2021-CS-01-04, "Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data."

# Project outcomes expected and challenges to be overcome

## Expected outcomes

- Improved scalable and reliable privacy-preserving technologies for federated processing of personal data and their integration in real-world systems
- More user-friendly solutions for privacy-preserving processing of federated personal data registries by researchers
- Improving privacy-preserving technologies for cyber threat intelligence and data sharing solution
- Contribution to promotion of GDPR compliant European data spaces for digital services and research (in synergy with topic DATA-01-2021 of Horizon Europe Cluster 4)
- Strengthened European ecosystem of open source developers and researchers of privacy-preserving solutions

Ionburst technology is uniquely positioned today to solve the immediate problems posed by the rapid adoption of 5G and EDGE computing and future-proofs PII and sensitive data against Quantum decryption and other advanced attack techniques.

With appropriate collaborative partners, Ionburst can be developed beyond TRL 4 to meet the challenges identified and the expected outcomes of proposal CL3-2021-CS-01-04. We are confident we can deliver a data privacy and recovery platform to meet the most stringent demands.

## Challenges identified

- Much of this data is personal data
- Leakage or abuse of personal data threaten individuals' privacy, society and the EU economy
- Adequate protection of this data according to the GDPR can also prevent its full utilization for society
- Advanced privacy-preserving methods need to be researched to address these challenges to ensure real-world applicability
- Developments such as homomorphic encryption and secure multi-party computation are often impractical or impose special infrastructural requirements.

# Project objectives & Ionburst status and development need

## Proposals should

- Address scalability and reliability of privacy-preserving technologies in realistic problem areas
- Integrate with existing infrastructures and traditional security measures (e.g. access control)
- Be geared towards citizens ' personal needs and profiles (incl. dynamic personalisation, gender)
- Address the legacy variation in personal data types and data models across different organisations and/or sectors
- A proposed solution should include validation or piloting of privacy-preserving computation in realistic federated data infrastructures and more specifically European data spaces involving personal data (e.g. the EU health data space)
- It should be guided by the EU's high standards concerning the right to privacy, protection of personal data, and the protection of fundamental rights in the digital age
- It should ensure, by-design, compliance with data regulations and specifically the GDPR. Wherever possible, solutions should be developed as open source software

## Ionburst capabilities

✓ Some development

✓ Some development

✓ Some development

Development area

✓ Some development

✓

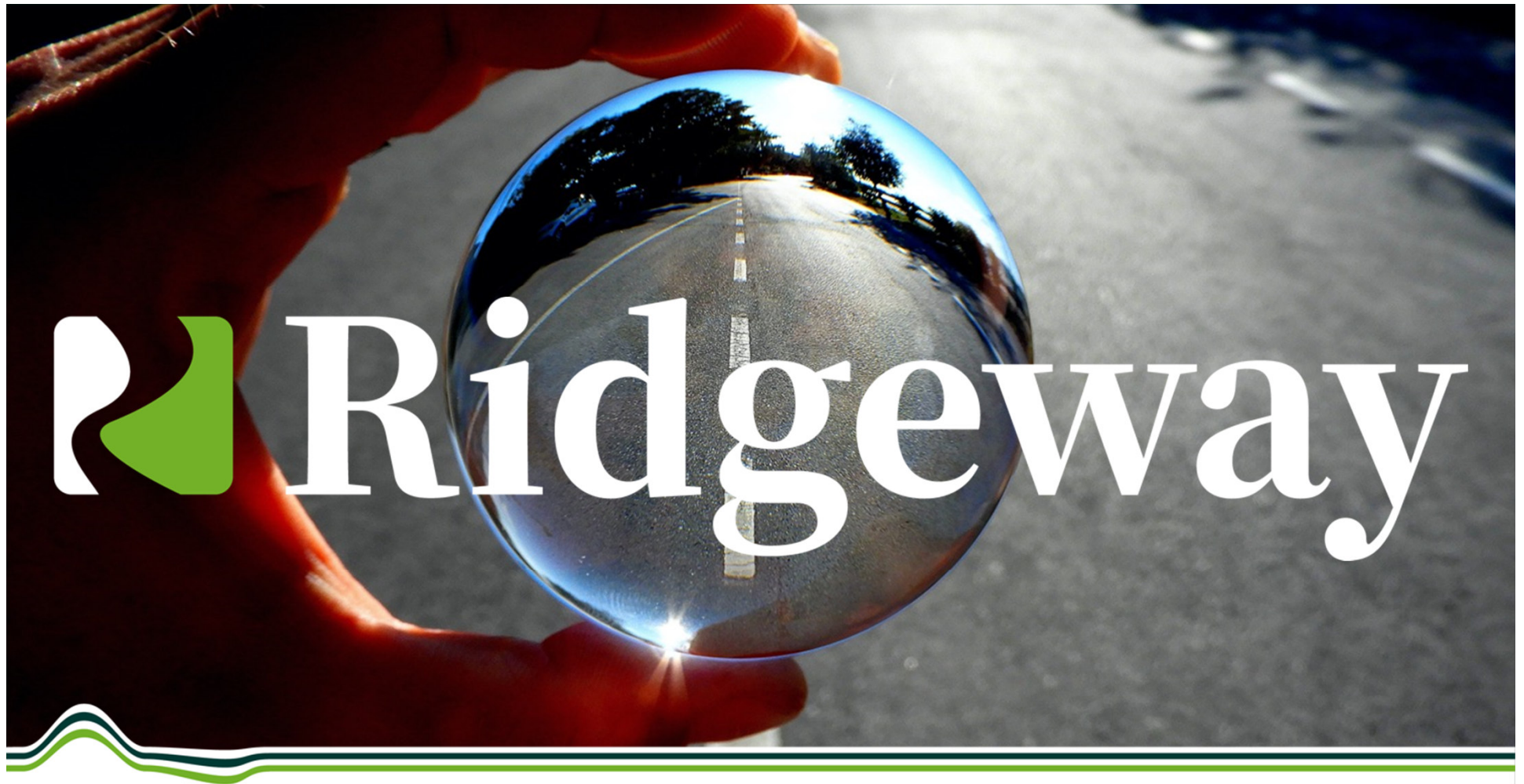
✓

# Ionburst background and collaboration partner information

- Ionburst's Cloud native data security, privacy and resilience SaaS technology is in market and available to evaluate and integrate via API
- Ionburst has been developed to date with supported of the UK Government and Scottish Enterprise
- It has attracted significant interest from sectors such as defence, financial services and the developer community
- Ionburst has been evaluated and validated by specialists in data privacy, GDPR and data sovereignty, and by cybersecurity specialists in global Cloud providers, the UK and US defence sectors and the FS sector, including regulators and banking associations
- We have collaborated with homomorphic encryption partners and understand key limitations in protecting such data under GDPR
- Ionburst can be developed to protect EU organisations and citizens at lowest financial and environmental cost of storage and data protection levels completely controlled by end users
- We are interested in collaborating with partners to work together to support initiatives that require the most advanced data security, privacy and multi-failover recovery available today



# ANEXO 4



 Ridgeway

# HORIZON-CL3-2021-FCT-01-03 Disinformation and Fake News

## Capabilities

- **Subject Matter Expertise** – in the practice and use of disinformation, and mechanism to call it out and counter its spread;
- **Operational capability building** – design and delivery of analytical ecosystems;
- **Verification** – expertise in the application of validation and verification approaches to sources and materials;
- **Language and cultural expertise** – operational capability in c.40 languages;
- **Testing and quality assuring** technical outputs focused on disinformation and fake news – including UAT and UX for analytical solutions;
- **Design and delivery** of tailored training, learning and development - on disinformation and fake news for senior leaders, managers and analysts;

## Recent Relevant Work and Experience

- **International Security Agency** – training and consultancy on identification and handling strategies for disinformation in a civil security context.
- **UN Agency** – developed a learning and development package on disinformation and fake news. With the objective of equipping communities to identify, call-out and counter disinformation and fake news, with particular emphasis on COVID-19.

## Approach

Ridgeway has expertise in the dynamics, systems and identification of disinformation as well as the practice of counter-disinformation. We are experienced in the analysis and assessment of information, news and other materials - including those designed to obfuscate, confuse and misrepresent. We adapt our approach for to each engagement but these are always underpinned by the rigorous identification, verification and analysis of sources.

## Company Background

Ridgeway Information provides research, analysis and risk advisory services. Much of our work focuses on international issues, including on cross-jurisdictional law enforcement matters, security and defence. We work with a range of public and private sector clients and have a track record of collaborative partnerships with technology providers.

Ridgeway benefits from close relationships with a range of world-leading universities and research organisations.

## Partnering

We are looking to partner with Police, law enforcement and public protection agencies, developers and technical suppliers focused on disinformation alerting, identification and case-management.



# Contacts

## Ridgeway Information

Chris Budd  
Chief Operating Officer

[chris.budd@ridgeway-information.com](mailto:chris.budd@ridgeway-information.com)

## Innovate UK UKRI

Zale Johnson  
National Contact Point & Global Innovation Lead – Security

[Zale.Johnson@innovateuk.ukri.org](mailto:Zale.Johnson@innovateuk.ukri.org)

# PROJECT PASSIM

Persistent AI derived multi-Sensor Surveillance and Intelligence in the  
Maritime

HORIZON-CL3-2021-BM-01-01

*Enhanced security and management of borders, maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support*

# The need for longer range, high fidelity, actionable data

SiriusInsight creates actionable intelligence for the maritime domain using data from its proprietary land/sea-based platforms and from aerial and satellite assets.

- Current terrestrial (land/sea-based) sensors are horizon limited
- Automated vessel detection and classification from manned helicopters (proven capability by SiriusInsight) is expensive and short-duration
- Satellite imagery (currently using ESA sentinel and others) data is high latency, and often limited by cloud-cover

***Opportunity to fill the gap with transformational data (and potentially bridge communication) with high-altitude, long range aerial support***





# Partners are sought:

Instruments	Aerial	Control	Users
<p>Land and Sea Sensor Data</p> <ul style="list-style-type: none"> <li>• Long Range Optical/Thermal Camera</li> <li>• EM Spectrum Analysis</li> <li>• Radar</li> <li>• Cloud-based Data infrastructure</li> </ul>	<p>Drone (and other Aerial asset) Data</p> <ul style="list-style-type: none"> <li>• Long Duration Drone</li> <li>• Autonomous Drones</li> <li>• Potentially... High Altitude Pseudo Satellite and Micro Satellite</li> </ul>	<p>Control, Intelligence &amp; Comms</p> <ul style="list-style-type: none"> <li>• Asset Coordination and Tasking</li> <li>• Machine Learning/ Computer vision</li> <li>• Real-time Behavioural analytics</li> <li>• Visualisation</li> </ul>	<p>End User Engagement: Agency</p> <ul style="list-style-type: none"> <li>• Minimum of 3</li> <li>• Border guard</li> <li>• Coastguard</li> </ul>



# SiriusInsight.AI

## Enabling Maritime Security and National Prosperity

- Save lives
- Protect waters and borders
- Disrupt illicit activity
  
- Clear persistent picture of activity from linked sensors
- Scalable, rapidly deployed, cost-effective
- Autonomous, remote operation with Artificial Intelligence driven analytics
- Secure, cloud-based, distributed to multiple users

Contact Details for further information and partnership discussions

Zale Johnson

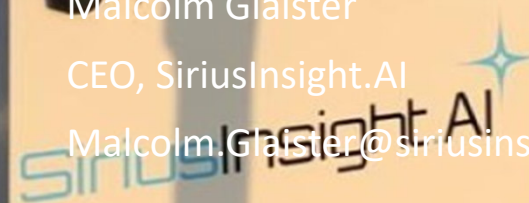
National Contact Point & Global Innovation Lead - Security

[Zale.Johnson@innovateuk.ukri.org](mailto:Zale.Johnson@innovateuk.ukri.org)

Malcolm Glaister

CEO, SiriusInsight.AI

[Malcolm.Glaister@siriusinsight.ai](mailto:Malcolm.Glaister@siriusinsight.ai)

The logo for SiriusInsight.AI, featuring the company name in a stylized font with a starburst graphic to the right.