

AGENDA**13:00 Registration and Networking with Refreshments****Session 1:** Chaired by **Kunle Anjorin**, Director Consulting Delivery, Cyber Security, UK & Australia, **CGI** and CW SIG Champion**13:30 Welcome from Cambridge Wireless**

- **Michaela Eschbach**, CEO, **Cambridge Wireless**

13:40 Welcome from CGI

- **Kunle Anjorin**, Director Consulting Delivery, Cyber Security, UK & Australia, **CGI**

13:50 Autonomy, Agency, Action!

- **Dr Madeline Cheah**, Associate Technology Director, **Cambridge Consultants**

What happens when your system starts to think and do things for itself? Autonomous systems don't just follow instructions; they act, adapt and deceive. As we hand over more agency to machines, we not only have to deal with the traditional attack landscape, but open the door to novel threats, from subtle manipulations to emergent misbehaviours to weaponisation by adversaries. This talk unpacks the risks of giving AI agency, explores how things can go sideways fast, and offers strategies to keep these systems assured.

14:20 Trust me, I'm an Agent

- **Simon Thompson**, Independent Consultant

To realise the benefit of Agent based systems users will have to trust them to act on their behalf, but some agents will be incompetent, and others will be malicious. How can users and Agents sort helpful collaborators from dangerous attackers? How are ideas of Trust different from ideas of Identity and Security? What kind of solutions exist for creating trust and running trust infrastructures?

14:50 Refreshments and Networking**Session 2:** Chaired by **Bob Oates**, Associate Director, **Cambridge Consultants** and CW SIG Champion**15:20 Title TBC**

- **Russell Goodenough**, Head of AI, CGI in the UK & Australia, **CGI**

15:50 Securing Agentic AI: Beyond Model Context Protocol (MCP) to Agent2Agent (A2A)

- **Jonathon Wright**, Chief AI Officer, **CAIO**

As autonomous AI systems become increasingly complex, traditional security models fail to provide adequate protection. This presentation reveals vulnerabilities in Model Context Protocol (MCP) and demonstrates how Agent2Agent (A2A) communication provides better security for enterprise agentic AI systems. The presentation will evaluate basic security weaknesses in MCP architecture through a comparison with A2A protocols' improved security features.

16:20 Concluding Remarks**16:30 Meet the Speakers in the Sky Garden****17:00 Event Close**