OT Security Sydney 2026 Tuesday10 February	
08:20	*Register; grab a coffee. Mix, mingle and say hello to peers old and new.*
09:00	**Welcome from Corinium and the Chairperson** Speaker: **Lauren Veenstra** CSO **Iberdrola Australia**
09:10	**Speed Networking – Making new connections!**
09:20	**Measuring Effectiveness: When Is Enough in OT Security?** Speaker: **Maryam Shoraka** Australian CISO Advisory Board Member **Corinium Global Intelligence**
09:45	**From Engineers to Cyber Champions: Embedding Security in Operations** Speaker: **Andrew Thyrd** Network & OT Security Manager **Sydney Airport**
10:10	**Critical Infrastructure Cyber Security-Strengthening Protection with Air Gapped Endpoint Security** Speaker: **Brett Williams** Senior Manager, Solutions Engineering **SentinelOne**
10:35	*Get refreshed! Mingle*
11:05	**Panel: Threat Management to Strengthen OT Defences in the Age of AI** As OT environments face increasingly complex threats, leaders are exploring how AI can support detection and response without disrupting operations. • How can AI enhance threat detection and monitoring in OT environments? • What are the limits and risks of relying on AI for critical operations? • How can organisations balance automation with human oversight in incident response? Moderator: **Maryam Shoraka** Australian CISO Advisory Board Member **Corinium Global Intelligence** Panellists:

	Eric Cheng Enterprise Architect **Komatsu Australia** **Umair Zia** Head of Cyber Security **Sydney Local Health District, NSW Health** **Mark Kovacik** Sales Director **HCLSoftware**	
11:40	**From Safety to Cyber Resilience: Securing Modern OT Environments** Speaker: **Mark Kovacik** Sales Director **HCLSoftware**	
12:05	**Panel: Rethinking OT Architecture for Cyber Resilience** From SCADA to PLCs, each industry has unique architectures that bring both opportunities and risks for cyber resilience. • How can organisations design OT networks that account for both operational needs and security? • What lessons can be learned from industries with highly customised OT environments? • How should IT–OT integration be approached without weakening resilience? Moderator: **Pippa Flanagan** Former Manager ICT & Cyber Security **ex-GWMWater** Panellists: **Neeraj Amlani** Senior Security Architect – IT & OT **Blackwoods** **Gijo Varghese** Information Security & Cyber Resilience **Endeavour Energy (NSW)** **Usman Sultan** Senior Cyber Security Architect & Tech Team Lead **CleanCo Queensland**	
12:35	**Who Owns the Alert? Clarifying Roles in OT Incident Response** Speaker: **Sarah Lugay** Cyber Security Manager **South Western Sydney Local Health District**	
13:00	*Lunch*	**OT Security Leaders Private Lunch** *(Invite Only)*
14:00	**Panel: Protecting Critical OT When Patching Isn't Enough** Unlike IT, OT systems can't always be patched or taken offline, leaving leaders to balance security, safety, and continuity in high-availability environments. • How can organisations prioritise vulnerabilities when patching is limited or impossible? • What strategies help ensure controls are adopted by OT teams, not just designed on paper? • How can compliance and standards be translated into practical steps for managing OT risk? Moderator: **Lauren Veenstra** CSO **Iberdrola Australia** Panellists: **Feli Gouw** Senior Central OT Engineer **EnergyAustralia** **Siddharth Rajanna** Head of IT Security **BINGO Industries** **Nabeel Chaudhary** Cyber Security Manager **Metro Trains Sydney** **Lee Barney** Former CISO **TPG Telecom**	
14:35	**Mind the Air Gap: How Living off the Land Attacks Are Crossing the Line**	

	Speaker: **James Murphy** Cyber Security Solution Engineer **OPSWAT**
15:00	**OT Security That Gets Funded: Crafting a Compelling Case** Speaker: **John Morcos** Head of Cyber Governance & Operations **Blackmores Group**
15:25	**Group Discussion: From Compliance to Real Adoption** Many organisations have frameworks and controls on paper, but the real challenge is getting them adopted and embedded into OT operations. This discussion invites participants to share successes, failures, and lessons learned in moving from design to practice. • What barriers have you faced in getting OT teams to adopt security controls? • How do you balance regulatory requirements with what's actually practical on the ground? • What examples of successful adoption can others learn from? **Pippa Flanagan** Former Manager ICT & Cyber Security **ex-GWMWater**
15:50	**Chair's Closing Remarks**
16:00	**Afternoon tea and close of OT Security Sydney 2026. Join us to reflect, connect and network over afternoon tea.**