
# OT Security Melbourne

Tuesday, 14 July 2026

| | |
|---|---|
| 08:20 | *Register; grab a coffee. Mix, mingle and say hello to peers old and new.* |
| 09:00 | *Welcome remarks by Corinium & Chair's opening remarks*<br>Chair: **Justin Nga** Cybersecurity Manager **CitiPower and Powercor** |
| 09:10 | **Speed Networking – Making new connections at CISO Melbourne!** |
| 09:15 | **Opening headliner**<br>**The Decision Gap: When Visibility Meets Responsibility**<br>Security teams have more visibility into their environments than ever before, yet many organisations still struggle to translate data into clear security priorities. This opening presentation explores how security leaders move beyond dashboards and inventories to focus on the exposures that truly matter. By connecting visibility with risk, operations and investment decisions, organisations can turn insight into meaningful action.<br>**Maryam Shoraka** Corinium CISO Advisory Board Member |

| | |
|---|---|
| 09:40 | **Panel discussion**<br>**Who Actually Owns Risk When a Cyber Decision Can Cause Downtime or Endanger People?**<br>When cyber decisions have physical consequences, accountability can be unclear. This panel explores where responsibility truly lies between engineering, operations, and security teams during incidents or critical changes. Panellists will discuss how organisations can align authority with operational responsibility to reduce risk.<br>• Who is accountable when a decision affects both cyber and physical systems?<br>• Where do current governance models fail under operational pressure?<br>• How can organisations clarify decision-making authority in OT environments?<br>Moderator:<br>**Sascha Mueller-Jacobs** Senior Manager Enterprise Cyber & Resilience **ARTC**<br>Panellists:<br>**Aidan Hollier** Head of Asset Knowledge & Technology **Melbourne Water**<br>**Vijay Narayan** CISO **Mercy Health**<br>**Sajid Bavakunji** Cyber Security Manager **Australian Energy Company**<br>**James Murphy** Field CTO, Threat Intelligence, APJ **Trellix** |
| 10:15 | **Critical Infrastructure Cyber Security-Strengthening Protection with Air Gapped Endpoint Security**<br>Critical infrastructure faces growing blended cyber threats, with nation-states using cybercriminal groups to target OT and ICS environments, threatening safety, availability, and trust. This session looks at the threat landscape and will focus on practical defensive outcomes and deployable strategies. Discover how AI-driven endpoint security protects systems, even when fully disconnected or air-gapped.<br>• How static and behavioural AI detects and responds to threats in OT and ICS environments<br>• Maintaining protection, visibility, and service continuity in isolated or degraded systems<br>• Security architectures for connected, partially connected, and fully air-gapped deployments<br>**Brett Williams** Senior Manager, Solutions Engineering **SentinelOne** |
| 10:40 | *Morning Coffee and Connect* |
| 11:10 | **From Visibility to Velocity: Operationalising Exposure Management Across IT and OT**<br>As IT and OT networks converge, legacy vulnerability management is no longer enough to defend critical infrastructure against sophisticated threats. This session provides CISOs with a practical blueprint for implementing Exposure Management across both IT and industrial environments. You will learn how to precisely prioritise critical flaws without risking operational downtime, accelerate remediation, and secure your modern attack surface through a single, unified experience.<br>**Serkan Cetin** Security Engineering Manager **Tenable** |

| | | |
|---|---|---|
| 11:35 | **Panel discussion**<br>**Can OT Networks Be Secure and Reliable?**<br>OT networks—from SCADA systems to PLCs—are designed to meet operational needs, but they can also create security gaps. This session explores how organisations can design architectures that balance reliability, availability, and cyber resilience. Hear lessons from highly customised environments, discuss safe IT–OT integration, and identify practical strategies to strengthen resilience without disrupting operations.<br>• How can OT networks be designed to meet operational needs while limiting security risk?<br>• What lessons can we take from industries with highly customised OT environments?<br>• How can IT–OT integration be achieved without compromising resilience?<br>Moderator:<br>**Maryam Shoraka** Corinium Advisory Board Member<br>Panellists:<br>**Yi Wang** Executive Manager – Network Security Risk **nbn**<br>**Ameneh Jalali** Chief Cyber Security Officer **Yokogawa Australia & New Zealand**<br>**Bilal Baig** Senior OT Security Engineer **CitiPower and Powercor**<br>**John Paul Moore** Principal Architect – Network Services **Origin Energy** | |
| 12:10 | **Beyond the Perimeter: Securing OT in a Connected World**<br>With IT–OT convergence, IoT growth, and remote access, the traditional perimeter has evaporated. Relying solely on outer firewalls to protect industrial plants is no longer enough. This presentation explores what security means in a hyper-connected world and introduces what must replace the perimeter: true operational resilience. We will discuss how to design systems that absorb digital breaches, protect critical environments, and maintain physical control. Discover the practical strategies necessary to ensure your operations endure, even when outer defences fail.<br>**Joshua Alcock** Regional OT Cybersecurity & Threat Intelligence Manager - Australia & New Zealand **Fortinet** | |
| 12:35 | **How Do We Get Engineers to Care About Cyber?**<br>Engineers instinctively prioritise physical safety, but cyber security is often treated as someone else's responsibility. As operational systems become increasingly connected, that mindset creates risk. The challenge is embedding cyber security into engineering culture so it carries the same weight as HSE. This session will explore how organisations can advocate for cyber security within engineering teams without relying too heavily on a few security champions.<br>**Jenny Botton** Senior Manager Cyber Security **ABN Group** | |
| 13:00 | *Lunch Break!* | **Invitation-Only VIP Luncheon** |

| | |
|---|---|
| 14:00 | **Confidently Connected: Visibility, Remote Access Risk, and Securing IT/OT Integration**<br>Operational technology environments were built for reliability — not connectivity. Yet as OT integrates with IT, cloud platforms, and remote access tools, the threat landscape has fundamentally shifted, leaving a dangerous gap between how modern operations run and what security teams can actually see and control. This session examines what it means to be confidently connected: not avoiding integration but owning it. Drawing on real-world ICS/OT findings, we explore how remote access software has become one of the most prevalent and underappreciated risk vectors in industrial networks — and why the tools that make engineers productive can hand adversaries a persistent foothold in critical infrastructure.<br>**Nicholas Tangey** Senior Manager OT Hunting **Dragos** |
| 14:25 | **When the Supply Chain Becomes the Attack Surface**<br>OT attacks are increasingly targeting engineering processes, diagrams, and templates, not just software. This session explores how trusted workflows and vendor inputs can introduce risk, why these compromises are hard to detect, and how organisations can secure connected systems without relying solely on audits or compliance checks.<br>**Usman Sultan** Senior Cyber Security Architect **CleanCo Queensland** |
| 14:50 | **Beyond the Patch Queue: Continuous Exposure Management for OT Resilience**<br>OT environments can't run the scan-and-patch playbook. Uptime constraints, legacy systems, and device fragility make it unworkable. This session makes the case for Continuous Exposure Management: a model that maps real attack paths, prioritises exposures that matter, and applies compensating controls when patching isn't an option. Walk away with a practical blueprint for managing risk to an acceptable level of business resilience, without taking operations offline to do it.<br>**Dean Plant** Principal Sales Engineer **Armis From Service Now** |
| 15:15 | **Panel discussion**<br>**If We Designed OT Security from Scratch Today, Would We Recognise It?**<br>Legacy systems, inherited standards, and vendor constraints shape much of today's OT security. This panel asks panellists to imagine starting over, revealing which practices exist out of habit and which are truly effective. The discussion highlights opportunities to simplify, improve, and focus security on operational outcomes.<br>Discussion questions:<br>• Which current practices exist because of history rather than effectiveness?<br>• What design principles would matter most if starting from scratch?<br>• What practices would we eliminate immediately if rebuilding OT security today?<br>Moderator:<br>**Lauren Veenstra** Chief Security Officer **Iberdrola Australia**<br>Panellists:<br>**Trevor Goldman** Former AGL's OT Cybersecurity Manager<br>**Michael Haarsma** OT Security Lead **Power Utility**<br>**Ahmad Taufiq Abdullah Thani** Principal Control Systems & Cyber Security Engineer **Origin Energy** |
| 15:50 | *Closing Remarks by the Chair* |

| | |
|---|---|
| 16:00 | **Close of OT Security Melbourne 2026 & Afternoon Tea**<br>*Continue the conversation over tea and small bites* |