Day 1

Tuesday 10 February 2026

08:20	*Register; grab a coffee. Mix, mingle and say hello to peers old and new.*
09:00	**Welcome from Corinium and the Chairperson** **Aaron McKeown** CISO **NGM Group**
09:10	**Speed Networking – Making new connections!** In this 10-minute networking session, the goal is to connect with three new people. Enjoy the opportunity to expand your network!
09:20	**Reading the Signals – What Global Threat Intelligence Is Telling Us.** Cyber threat intelligence teams worldwide are observing a sharp rise in activity, from sophisticated state-linked campaigns to the growing overlap of criminal and geopolitical motives. The session will explore how global threat intelligence is evolving from state-linked activity to the growing overlap between criminal and geopolitical motives and what this means for national and regional cyber resilience. **Stephanie Crowe** Head of ACSC **ASD**
09:45	**The AI Agent: The Most Privileged Identity in Your Enterprise Isn't on Your Org Chart** AI agents are already provisioning infrastructure, writing code, and accessing sensitive systems, often with broad permissions and limited oversight. In effect, AI has become the most privileged identity in the enterprise. Many organisations are responding with policies and governance committees, but AI moves faster than documentation. Andrew will share how you can reframe AI security as a platform engineering problem, and not as a policy gap. CISOs can apply Zero Trust principles directly to AI, using strong identity, least privilege, and policy-as-code embedded into shared platforms to secure AI at scale without slowing innovation. **Andrew Brydon** Field CTO **HashiCorp**
10:10	**Fireside Chat: How to Land Cyber Deliverables – From Strategy to Impact** Bridging the gap between strategy and execution is one of the toughest challenges in cyber leadership. This candid conversation explores how to turn high-level plans into clear, achievable actions that deliver measurable outcomes. From stakeholder alignment to delivery roadmaps and the metrics that matter, the discussion focuses on making cyber real across the organisation. • What are the common pitfalls leaders face when trying to turn cyber strategy into actionable outcomes, and how can they be avoided?

	• How do you create buy-in across the organisation to ensure cyber initiatives move from plan to execution? • When cyber strategies are successfully implemented, what really makes the difference? Moderator: **Leron Zinatullin** CISO **Linkly** Speakers: **David Griffiths** CISO **Northern Beaches Council** **Roshan Fernandes** Information Security & Risk Manager **Sydney Children's Hospital Networks**
10:35	*Get refreshed! Mingle*
11:05	**C-Suite Panel: Driving Executive-Level Engagement in Security Strategy** While security professionals are across the threats, the same can't always be said for executive leadership and board members. Bringing together the C-suite in this panel, we explore how CISOs get meaningful cut-through with the executive suite when they're already swamped with compliance, governance, and operational pressures. • What was the defining moment or incident that fundamentally changed how you think about cyber resilience and your role in it? • How do you embed security into the way the business actually operates – not just slogans but as something enduring and strategic? • How do you, as CFO, set priorities, and where can the cyber leader add the most value? Has there been a moment or incident that shifted your view or priorities for cyber and resilience? • As a CIO, what qualities beyond technical expertise do you value most in a cyber leader? • What language, evidence, or framing truly resonates with non-security executives? • How can we influence the broader business to own and act on risk, creating accountability beyond the security team? Moderator: **Aaron McKeown** CISO **NGM Group** Panellists: **Andrew Karvinen** CISO **Macquarie University** **Rajini Carpenter** CTO **Beforepay Group** **Jon Blackburn** CFO, Executive Director Corporate Services **Sydney Opera House**
11:40	**The End of Manual Trust: Why Automation, Quantum Readiness, and AI Integrity Will Define Security in 2026** As digital ecosystems expand and machine identities outpace human ones, traditional, manual approaches to trust and security are reaching their limits. By 2026, organizations will face mounting pressure from shorter certificate lifecycles, growing outage risks, emerging quantum threats, and the urgent need to establish trust in AI-driven systems. In this session, we'll explore why automation is no longer optional for managing cryptographic assets at scale, how quantum-safe cryptography is moving from theory to reality, and why AI integrity has become a critical pillar of modern security strategies. Attendees will gain practical insights into how these shifts intersect, and what security leaders should prioritize today to build resilient, future-ready trust infrastructures. **Mike Nelson** Vice President, Digital Trust **DigiCert**
12:05	**Panel: Governing AI – Where Should We Draw the Line?**

	As AI adoption accelerates, leaders face the challenge of setting clear boundaries, not only around what AI should and shouldn't do, but also around who holds responsibility for its oversight. This panel explores governance from two critical perspectives: • Structure and Responsibility - Where does AI sit across the organisation? Which teams shared responsibility • Scope of AI – What tasks should AI be trusted with, and where must human oversight remain non-negotiable? How can organisations prevent over-reliance, ensure explainability, and avoid ethical or operational pitfalls? Panellists will debate practical approaches to establishing guardrails that support innovation without undermining trust, compliance, or human judgement. Moderator: **Matt Keast** Senior Solutions Engineer **Vanta** Panellists: **Mustafa Qasim** Former Global Head of Detection & Response **Leron Zinatullin** CISO **Linkly** **Daminda Kumara** CISO **Commonwealth Superannuation Corporation**		
12:35	**Secure the AI Future, Now** AI runs on data, and every leader knows it's no longer enough to simply lock information down. The real challenge is scaling AI securely and responsibly, without treating protection and progress as opposing forces. Yet today, only 14% of security leaders report success in doing both. In this keynote, the Cyera team will reveal the mindset shift forward-looking enterprises are making, to thrive in the AI era. **Antonio Rancan** Head of Solution Engineering, APAC **Cyera**		
13:00	*Lunch*	***Invitation-Only VIP Luncheon by Delinea***	
	TRACK A: **AI in Practice**	**TRACK B:** **Human-Tech Momentum**	**TRACK C:** **Partnerships & Ecosystem Security**
	Track Chair: **River Nygryn** CTO **CRVAA**	Track Chair: **Aaron McKeown** CISO **NGM Group**	Track Chair: **Prof. Dan Haagman** CEO **Chaleit** & Honorary Professor of Practice **Murdoch University**
14:00	**AI Agents Unleashed: Where Humans Fit In** This session explores the landscape of human–AI collaboration, focusing on how humans and AI agents co-create value, share trust, and define oversight in agentic workflows. Explore practical approaches to managing and governing agentic systems, including accountability, monitoring, and frameworks for	**Cyber Security Meets Human Behaviour: Rethinking Awareness in the Age of AI** Phishing and social engineering remain among the most effective attack vectors, and AI is making them more persuasive and scalable than ever. Yet traditional awareness programmes often rely on "gotcha" tests and compliance-driven training that fail to change behaviour. In this session, we explore how	**Seeing Around Corners: Threat Intelligence for Supply Chain Defence** Supply chains are now one of the most exploited entry points for attackers and too often, organisations only discover the risk once it's too late. When applied effectively, threat intelligence can give earlier warning of emerging exposures across these extended ecosystems. This session explores how consolidating and

	ethical, secure, and resilient systems. **Roger Millar** CIO & CISO **Angus Knight Group**	behavioural science and psychology can be applied to build more resilient human firewalls. **Dr. Alana Maurushat** Professor of Cybersecurity and Behaviour & Acting Associate Dean Engagement, School of Computer, Data and Mathematical Sciences **Western Sydney University**	operationalising intelligence feeds strengthens supplier oversight, reveals adversary patterns before they strike, and improves agility in response. **Saba Bagheri** Cyber Threat Intelligence Manager **Bupa**
14:25	**Making the Case for Asset Intelligence and Actionability** Security processes are hampered by the complexity of accessing data spread across many tools. This data problem limits individual tool contributions, yielding incremental instead of exponential improvement. Join us to review common suboptimal security scenarios and explore how Asset Intelligence and Actionability can resolve this. We'll also cover its impact on current operations and the future effectiveness of AI. **Paul Thomas** Solutions Architect **Axonius**	**AI Is Hungry: How to Stop Your Data Becoming Its Next Meal** AI is accelerating faster than ever and so are the risks. As organisations race to adopt generative AI, sensitive data is becoming the unintended fuel feeding these models. In this session, we'll break down how modern AI systems ingest and learn from corporate information, where the hidden exposure points are, and what leading APAC organisations are doing to stay in control. You'll leave with practical strategies to safeguard your data, enforce boundaries around AI usage, and unlock value without becoming the next cautionary tale. If your business is embracing AI, this is the playbook you need before the appetites grow. **Geoff Morrison** Director of Sales Engineering, APAC **Varonis**	**Pre-Emptive Cybersecurity: Blocking Threats at the First Question** Almost every connection on the Internet begins with a DNS request. This session demonstrates how Infoblox Protective DNS stops threats at the moment of intent, blocking access to malicious infrastructure before connections are established. Discover how a pre-emptive DNS-based security strategy dramatically shrinks attack surfaces while protecting users, devices, and networks everywhere they operate. **Brad Ford** Product Sales Security Specialist – Australia and New Zealand **Infoblox**
14:50	**When AI Goes Rogue: Responding to the Next Wave of Intelligent Cyber Attacks** AI driven attacks are escalating in speed, scale, and sophistication, overwhelming traditional defences and response playbooks. This session explores the practical	**Group Discussion: The Future Cyber Workforce – Humans, AI, and the Skills That Still Matter** AI is already automating parts of engineering and analyst roles. In this interactive group discussion, every participant will have the chance to share their	**Fireside Chat: Embedding Security Obligations into Partner Agreements – Contract Clauses That Matter** While legal teams own contracts, security teams play a crucial role in shaping the obligations that protect the organisation. This session

	techniques, tools, and decision points that matter when confronting intelligent, adaptive threats. **Umair Zia** Head of Cyber Security **Sydney Local Health District, NSW Health**	views on which skills will matter most in an AI-augmented workforce and how to reshape the talent pipeline to match. • Which current cyber roles are most likely to be transformed or replaced by AI? • What new roles or skills will emerge as AI adoption grows? • How can we work with education providers to prepare the next generation of talent? Facilitator: **Sharon Lee** Associate Director Cyber Security Operations **NSW Department of Creative Industries, Tourism, Hospitality and Sport**	explores how security leaders can collaborate with legal and business teams to ensure key risks are addressed in partner agreements. Learn which clauses matter most, from data protection and breach notification to audit rights and compliance obligations, and how to turn security requirements into enforceable commitments. Moderator: **Prof. Dan Haagman** CEO **Chaleit** & Honorary Professor of Practice **Murdoch University** Speakers: **Sarah Lattimer** Chief Legal and Corporate Affairs Officer **I-MED Radiology Network** **Jihad Zein** Global Head of Governance, Risk & Assurance **Toll Group**
15:15	**Managing Non-Human Identities (NHIs) in the Era of AI Agents** As companies continue to integrate AI agents to reduce costs and improve operating efficiencies, they also face new waves of security challenges from the new workforce of "non-human identities" (NHIs). With NHIs often outnumbering human identities, they introduce significant new attack vectors. Join security experts from Okta and Deloitte for an in-depth discussion of the new security challenges that arise with AI adoption, and the right approaches to safely integrate AI without compromising security. In this session we will cover emerging security	**Shadow AI and the OAuth Explosion: Shining a Light on the Invisible Perimeter** Shadow AI is moving from theory to a daily operational challenge as teams adopt tools faster than policy can respond. Corporate perimeters now stretch across OAuth grants, browser extensions, and third-party integrations that quietly connect sensitive data to unvetted AI models. This session focuses on practical observability: how to detect and score the risk of connected consent, analyse browser signals and OAuth activity, and build relative risk scores that help SecOps prioritise interventions without slowing innovation.	**Enabling Organisation Specific Threat Intelligence** Threat intelligence should reflect an organisation's unique risk profile. This session explores how security teams can move beyond consumed threat feeds to organization specific threat intelligence that informs strategic decisions. Understanding immediate and impactful risks enables a more confident response and better investment choices. **Craig Boyle** Principal Security Architect **XM Cyber**

<table>
<tr><td></td><td>challenges, including understanding new threats like prompt injection, data poisoning, and the challenges of managing "shadow access" created by autonomous agents, as well as addressing the risks of unintentional data leakage and the loss of traditional audit trails.
We will also cover the following:
• How to gain visibility to undermanaged NHIs
• Strategies to bring access control policies to these types of unfederated NHIs
• And considerations for using the same security framework for NHIs as human identities
<u>Moderator:</u>
River Nygryn CTO CRVAA
<u>Speakers:</u>
Mathew Graham APJ CSO Okta
Shweta Pandey APAC Cyber Risk Advisory Partner Deloitte</td><td>Phil Ross CISO UpGuard</td><td></td></tr>
<tr><td>15:40</td><td colspan="2">Get refreshed! Mingle</td><td rowspan="3">VIP Roundtable by Rapid7 – Invite only
As adversaries move at machine speed, the window between initial access and full-scale impact is shrinking to minutes. Organisations face a critical “Response Gap” — the time between spotting a threat and having the capability to contain it. Collecting telemetry alone is no longer enough; success depends on high-fidelity interpretation and decisive action.
This roundtable will explore:
• Operational bottlenecks in modern Detection & Response (D&R)</td></tr>
<tr><td></td><td>Track A: AI in Practice</td><td>Track B: Human-Tech Momentum</td></tr>
<tr><td></td><td>Track Chair: River Nygryn CTO CRVAA</td><td>Track Chair: Aaron McKeown CISO NGM Group</td></tr>
<tr><td>16:10</td><td>Group Discussion: Shadow AI in the Enterprise - Governing the Unseen
The rapid rise of generative AI has brought powerful new capabilities into the enterprise but also created “shadow AI,” where employees adopt unapproved tools without security review. For CISOs, the challenge is not only visibility but also accountability. Join us to share your thoughts on how</td><td>Fireside Chat: Building AI Capability Without Losing Momentum
How can organisations create the capacity for AI upskilling while ensuring regular work and operational tasks continue uninterrupted? Join us to explore practical tips on balancing training, workload, and business priorities, discussing approaches to integrate AI learning into day-to-day workflows effectively.</td><td></td></tr>
</table>

	to govern what is unseen, while enabling innovation. • Oversight: How should CISOs gain visibility into AI use without creating a culture of surveillance or distrust? • Accountability: Who should own the risks of shadow AI — security, business leaders, or individual teams? • Governance: What frameworks or guardrails can balance compliance, ethics, and innovation at scale? Facilitators: **Siddharth Rajanna** Head of IT Security **BINGO Industries** **Jim Marinos** Head of Security Advisory **REA Group**	• How can AI upskilling be integrated into existing workflows without disrupting productivity? • What methods ensure employees apply newly acquired AI skills effectively in real projects? • How can organisations measure the impact of AI upskilling on workforce capability, innovation, and business outcomes? • What's one lesson learned from failed AI upskilling attempts? Speakers: **Dr Tom Gao** Chief Technology & Digital Services Officer **City of Sydney** **David Norwood** CIO & Director **Sydney Local Health District, NSW Health**	• Moving from high-volume alerts to precision-based response • Closing "Detection Debt" and optimising collaboration between internal teams and external MDR partners **Robin Long** Regional CTO **Rapid7**
16:35	**Identity and the New AI Infrastructure Layer: Securing Every Interaction at Scale** As generative AI accelerates digital transformation across Australia and New Zealand, identity is emerging as the critical infrastructure layer that enables trust, security, and scale. In this session, Ping Identity unpacks how organisations can modernise identity to tap into the Agentic AI opportunity as well as protecting against AI-driven threats like deepfakes and account takeover—without slowing innovation. Learn how leading enterprises are unifying identity across edge, cloud, and third-party ecosystems to support massive-scale AI workloads while enabling	**Building Cyber Resilience through Threat-Informed Defence** Threat-Informed Defence has gained strong momentum over the past year, driven by regulations such as Australia's CPS 230 / CORIE and the EU's DORA, which require resilience testing based on real-world cyber threats. This session introduces practical, open-source tools and techniques to help organisations build a threat-informed defence strategy and strengthen their overall cyber resilience—whether operating in regulated environments or not. **Damien Skeeles** Head of Solution Architecture, Asia Pacific and Japan **Filigran**	

	seamless, secure access for every user, device, and agent. **Johan Fantenberg** Director, Product and Solutions Marketing **Ping Identity**		
	Track A: AI in Practice	**Track B: Human-Tech Momentum**	
17:00	**Group Discussion: Scaling Small Security Teams with AI – Tools and Tactics to Boost Productivity** This discussion explores how AI can help streamline workflows, automate repetitive tasks, and prioritise alerts, allowing teams to focus on high-value work. • Which AI tools provide the biggest productivity gains for small security teams? • How do you balance automation with human oversight to avoid missed threats? • What tasks should be prioritised for AI-assisted workflows versus manual handling? • How can small teams measure the impact of AI on efficiency and risk reduction? Facilitator: **River Nygryn** CTO **CRVAA**	**On the Stage Interview: Decisions That Shaped a CISO's Leadership Journey** This one-on-one conversation delves into stories behind the decisions, inflection points and leadership lessons that have shaped their journey. From earning trust and building influence to navigating complexity under pressure, the dialogue explores what they might approach differently today and what they still stand by. More than frameworks and controls, this session reveals how the CISO role is defined by the judgement calls that matter, focusing on the personal side of leadership in one of the most high-stakes positions in any organisation Interviewee: **Arun Singh** CISO **Tyro Payments** Interviewer: **Prof Dan Haagman** CEO **Chaleit** & Honorary Professor of Practice **Murdoch University**	
17:25	**Track A Chair's Closing Remarks**	**Track B Chair's Closing Remarks**	
17:30	**Networking Drinks Reception**		

Day 2

Wednesday 11 February 2026

08:20	*Register; grab a coffee. Mix, mingle and say hello to peers old and new.*
08:55	**Welcome from the Chairperson** **Dan Haagman** CEO **Chaleit** & Honorary Professor of Practice **Murdoch University**
09:00	**Opening Spotlight: How Do You Succeed When You Can't Win Every Battle?** In cyber security, no system is completely secure, and no plan survives every challenge. This opening keynote explores how leaders can achieve success despite uncertainty, setbacks, and evolving threats. • How do you choose what's worth protecting? • Can failure be an advantage?

	• What if your best defence still fails? • What separates teams that adapt from those that crumble? Speakers: **Sunil Rodhan** Head of Security & IT Risk **IPH** **Hank Opdam** Former CISO **Ausgrid** **Martin Doherty** CISO Australia **HSBC**
09:25	**Security as a Human Problem, Not a Technical One: Risk Management in ANZ's Evolving Cyber Landscape** Here's the reality: 68% of data breaches happen because of human error. Even with top-tier technical defences, phishing and social engineering attacks, particularly via email, are still the #1 threat facing organisations in ANZ today. In this session, we'll explore why email remains the weakest link and how phishing and social engineering continue to be the main gateways for breaches and ransomware, with AI making attacks more sophisticated than ever before. **Jake Mongston** Enterprise Account Executive **KnowBe4**
09:50	**Panel: CISOs in an Identity-Driven, As-a-Service World – What Really Matters Now?** As organisations shift more services, data and operations into an as-a-service model, identity risk becomes a critical business concern. This conversation explores what CISOs need to know beyond the technical detail to guide strategy, investment and trust. • What's the hardest part of managing identity sprawl across SaaS and multi-cloud? • What's the most effective ways to reduce complexity and maintain positive user experience while maintaining control? • How do identity failures affect operational resilience and regulatory standing? • How can CISO get a clear, continuous picture of trust, privilege and lifecycle in cloud-based environments? Moderator: **Prof. Dan Haagman** CEO **Chaleit** & Honorary Professor of Practice **Murdoch University** Panellists: **Chris Grisdale** Head of Information Security **hipages Group** **Sajeesh Patail** Global Cyber Operations Manager & Head of Cyber Operations **Orica** **Siddharth Rajanna** Head of IT Security **BINGO Industries** **Vishwanath Nair** GM Cyber & IT Risk **BaptistCare**
10:25	**From Human to Hybrid: How AI and the Analytics Gap Are Fueling Insider Risk** Insider threats have entered a new era — fueled by AI, shaped by behavioral blind spots, and overlooked by executive leadership. In this session, we will break down the findings from Exabeam 2025 global Insider Threat Report, and provide actionable insights for security analysts, SOC leaders, and CISOs alike. Whether you're building your first insider threat program or looking to level up detection and response, this session will ground you in the data and help you reimagine your strategy for the AI era. **Gareth Cox** Vice President, Asia Pacific & Japan **Exabeam**
10:50	**Panel: Doing More with Less - Budget Constraints and Tool Rationalisation** This interactive discussion explores how to optimise sourcing, consolidate tools, and make smarter budget decisions. Join us to share your experiences, discuss trade-offs, and uncover practical strategies to streamline operations, reduce costs, and maximise value from existing investments.

	• How can organisations decide which tools to keep, consolidate, or retire under budget constraints? • What strategies or framework help teams achieve more without increasing spend? • How do you avoid false economises that save money but increase risk? • How do you measure the impact of tool rationalisation on efficiency, performance, and cost savings? Moderator: **Madhuri Nandi** Head of Security **Nuvei** Panellists: **Arun Singh** CISO **Tyro Payments** **Leana El-Hourani** Head of Information Security & GRC **Mission Australia**	
11:10	**Tools Don't Defend Organisations, People Do** Most breaches don't occur because a tool failed. They occur because ownership, context, or response broke down. Despite unprecedented investment in cyber security technology, many organisations remain vulnerable. This presentation explores why, now more than ever, tools alone are not enough, and how human judgement, clear ownership, and decisive action ultimately determine security outcomes. **Tim Sank** Sales Director & Co-founder **Cythera**	
11:15	*Get refreshed! Mingle*	
	Track A: **Resilience & Leadership**	**Track B:** **Security Transformation & Operations**
	Track Chair: **Lauren Veenstra** CSO **Iberdrola Australia**	Track Chair: **Dan Haagman** CEO **Chaleit** & Honorary Professor of Practice **Murdoch University**
11:45	**Reputation, Risk and Recovery: Good Cyber Crisis Leadership** In a cyber crisis, technical controls matter, but leadership defines the outcome. Crises demand fast decisions and trade-offs, and incidents quickly become organisation-wide challenges. This session explores how security leaders align technical response with executive-level crisis management to ensure clarity, speed, and coordinated action, building resilience before, during, and after the storm. **Mustafa Qasim** Former Global Head of Detection & Response	**The Paradigm Shift from Castle Walls to Zero Trust** The shift from perimeter-based defence to Zero Trust marks a fundamental transformation in cyber security thinking. Rather than relying on static boundaries, Zero Trust requires a reimagining of how trust, identity, and access are governed. This talk examines how such shifts reshape the mental models of practitioners, emphasising the socio-technical dimensions that drive sustainable security change. • Explore how trust is redefined as contextual, provisional, and continuously evaluated. • Identify shifts in practitioner mental models and the cognitive load of adopting Zero Trust logic. • Examine the socio-technical integration required for cohesive, organisation-wide Zero Trust implementation. **Hani Arab** CIO **Seymour Whyte**

12:10	**Identity Is a System: Why Visibility and Intelligence Are Now a Board-Level Requirement** AI agents, automation, and non-human identities are reshaping how enterprises operate—but they are also breaking the assumptions that identity security has relied on for decades. Boards are rightly asking whether AI can be trusted to make decisions. Yet a more fundamental risk often goes unaddressed: *do we have visibility into which identities are actually acting inside the enterprise, at machine speed, and with what authority?* Identity is no longer a static access control function. It has become a **dynamic, distributed system**—executing continuously across cloud platforms, legacy infrastructure, APIs, SaaS, and autonomous AI agents. Managing identity as configuration rather than behavior creates blind spots that traditional IAM, PAM, and CIEM platforms cannot close. This session introduces **Identity Visibility and Intelligence Platforms (IVIP)** as a necessary evolution of identity security in the AI era. IVIP treats identity as an observable system, collecting authentication telemetry across environments, applying behaviorral intelligence, and enabling adaptive Zero Trust enforcement in real time. Using Silverfort's evolution as an illustrative case study, this talk demonstrates how identity visibility becomes a foundational capability for AI trust, cyber risk quantification, and digital resilience—without requiring application rewrites or operational disruption. **Abbas Kudrati** Chief Identity Security Advisor, APJ **Silverfort**	**From Lists to Graphs, from Detection to Dominance - An Enterprise's Journey in Transforming Cyber Defence** Today, the primary function of cybersecurity is to boost resilience. In this session, we'll look at how leading enterprises are evolving from detect and respond cyber 'whack-a-mole', to positions of confidence in sustaining operations under inevitable attack. Transforming reactive operations and proactive security architecture through cyber cartography and Zero Trust. **Andrew Kay** Senior Director, Sales Engineering APJ **Illumio**
12:35	**Group Discussion: Three Things Every SME Should Check in Their Security Posture** Small and medium enterprises often face tough security challenges without the resources of larger organisations. In this interactive discussion, we'll explore three critical areas to strengthen security posture—from access control and data protection to incident response and vendor risk. Participants will share experiences, practical tips, and examples to protect their	**What Actually Strengthens Security Operations** This session examines how security operations can move beyond volume and noise to focus on outcomes that actually reduce risk. This session reflects on prioritisation, decision-making, and what makes SecOps effective when resources are limited and everything appears urgent. **Doug Hammond** CISO **Uniting**

	businesses effectively without overburdening teams or budgets. **Andrew Hottes** Chief Digital Information Officer **Cranbrook School**	
13:00	Lunch	***Invitation-Only VIP Lunch by F5***
13:55	**Prize Draws**	
14:00	**Architecting Resilience: Strategies for Web Application Security in an AI and Multi-Cloud Landscape** Native cloud controls are no longer sufficient in an era of AI-driven attacks and multi-cloud fragmentation. This talk demands a fundamental shift: fusing security and resilience into a unified design principle. We explore how to move beyond disparate tools to a unified defence posture, ensuring consistent protection and resilience against sophisticated Bot and API threats across every environment. **Guy Brown** Staff Enterprise Security Architect, APAC **Fastly**	
14:25	**Panel: Quantum Computing – Is It a Risk or Not?** Quantum computing promises groundbreaking capabilities, but also the potential to break today's encryption and security assumptions. In this debate, leading experts will explore whether quantum is an imminent cyber risk, a distant concern, or an overhyped distraction. We will explore what security leaders should be doing now to prepare. Moderator: **Cathy Foley** Board Member & Former Australia's Chief Scientist **CSIRO** Panellists: **Adam Byrne** Group CSO **The Adecco Group** **Saba Bagheri** Cyber Threat Intelligence Manager **Bupa** **Dr Andreas Sawadsky** Technology & Innovation Manager **Quantum Brilliance**	
14:55	**Outsmarting Disruption: Threat-Led Security for Cyber Leaders** AI is amplifying both innovation and adversary capability, widening the gap between disruption and defence. To stay ahead, organisations must anchor their security strategy in threat intelligence that reveals intent, exposes tradecraft, and drives precise action. By leading with real-time insight, enterprises can prioritise what matters most, strengthen resilience, and outpace attackers in an environment where the rules are being rewritten. **Ash Smith** Principal Technology Strategist **CrowdStrike**	
15:20	**Fireside Chat: Where To From Here? Redefining Cyber Strategy for 2026 and Beyond** Has cyber really changed, or are we still fighting the same battles in new ways? This closing session pairs two perspectives, one deeply experienced and the other earlier in their career, to spark a candid conversation about what defines a "good" cyber strategy today. Together, we'll explore: • What has truly changed in cyber strategy over the past few years, and what hasn't? • Can you share a strategy that failed and the key lesson you took from it? • Where should organisations go "back to basics" and where is bold innovation needed? • If you had to define the top marker of a "good" strategy in 2026, what would it be? Moderator: **Chirag Joshi** Founder & CISO **7 Rules Cyber** Speakers:	

	Sanja Petrovic GM Cyber Security & Governance **HUB24** **Abhishek Singh** GM – Enterprises System, ICT, Data Analytics & Cyber Security **New Horizons**
15:45	**Chair's Closing Remarks**
15:55	**Close of CISO Sydney 2026 & Networking over tea** *Join us to reflect, connect, and network over tea*.