DAY 1 Tuesday 18 November 2025	
08:30	*Register; grab a coffee. Mix, mingle and say hello to peers old and new.*
09:00	**Ngāti Whātua Ōrākei - Mihi Whakatau** **Te Aroha Grace**
09:10	**Welcome remarks by Corinium and Chair's opening remarks** **Adwin Singh** Cybersecurity Domain Lead – CISO Office **Inland Revenue NZ**
09:20	**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!
09:30	**Navigating the Threat Landscape to Explore the Strategic Path Forward** Drawing on frontline reporting and incident trends, NCSC (formerly CERT) outlines the current state of New Zealand's threat landscape covering what's changing, what's persistent, and what's coming next. This session offers clarity on the risks facing Kiwi organisations and where leaders should focus attention to stay ahead. • The latest threat activity observed across sectors and systems • Patterns in attacker behaviour, tactics, and target profiles • Strategic implications for detection, response, and sector-wide resilience **Sarah Penman** Director of Enterprise Information Security NCSC & CISO **GCSB**
09:55	**Enabling Secure Innovation Without Sacrificing Compliance: A Practical Zero Trust Playbook for CISOs** (Powered by the Platform Engineering Operating Model and the HashiCorp Security Stack) Join Andrew Brydon, Field CTO at HashiCorp, as he shares a Zero Trust playbook for CISOs to accelerate innovation without compromising compliance. Learn how identity-driven security, automation, and policy-as-code can secure multi-cloud environments, meet sovereignty requirements, and enable teams to move faster while staying audit-ready. **Andrew Brydon** Field CTO ANZ **HashiCorp**
10:20	**Panel: AI in Cyber – What Are We *Really* Talking About?** This panel unpacks where organisations are truly using AI, what's working, what isn't, and how leaders are separating hype from value in practical, risk-aligned ways. • How would you assess the current level of AI implementation within your organisation? • What challenges have you encountered in adopting AI, and how have you addressed them? • What are the key criteria and considerations for evaluating AI technologies as part of a holistic cyber risk management strategy? • What indicators or benchmarks should organisations consider evaluating the effectiveness of AI-driven cyber defence initiatives? Moderator:

	Jason Wood Chair **ISACA Auckland** Panellists: **Deepak Veerasamy** CISO **Kainga Ora** **Andy Pace** Network & Information Security Manager **MediaWorks** **Francis Kaitano** Enterprise Security Architect **BNZ** **Scott Morris** Managing Director, Australia and New Zealand **Infoblox**
10:50	*Get refreshed! Morning coffee break*
11:20	**Plenary 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. Interviewer: **Bob Kombora** Head of IT Operations **Vulcan** Interviewee: **Colin James** Head of Information Security, Risk Management & Network Services **Southern Cross Health Society**
11:45	**Mitigating Risk within Multi-Cloud Environments** In this session, Wiz and The Instillery will share expert strategies for modernising data architecture and securing complex multi-cloud environments. Matt Ramsey and Jeremy Nees will outline the forward-thinking approaches successful Kiwi organisations are taking to re-imagine cloud security—moving beyond IaaS/PaaS to prioritise data security and AI security from day one. This session will explore real-world use cases in cloud risk prioritisation, implementing continuous compliance, and gaining unified visibility across diverse cloud platforms using tools like Wiz. Walk away with actionable insights to drive both operational efficiency and risk mitigation in your own cloud journey. **Matt Ramsey** Senior Solutions Engineer **Wiz** **Jeremy Nees** COO **The Instillery**
12:10	**Panel: Leading with Risk — How to Make Risk Your Ally** Risk can't just be understood — it must shape decisions, drive priorities, and speak the language of the business. This panel discusses the keys to embed risk thinking into decision-making, repositioning as a powerful tool for alignment, influence, and long-term value. • How are leading CISOs reframing cyber risk as business risk? • What does effective risk communication look like – up, down, and across the organisation? • How are leading CISOs using risk to manage conflicting prioritise and budget constraints? • What does good cyber risk governance look like; how it will leave your teams feeling empowered? Moderator **Kavita Chetty** Senior Manager Technology Risk **NZAA** Panellists **Ronald Chung** Head of Risk (Information, Technology & Cyber Security) **BNZ** **Laura Marshall** Head of Information Security **LIC** **Richard Harrison** Head of Cyber & Architecture **Foodstuffs SI**
12:40	**Operationalising AI in Cyber: Influence with Integrity** As AI rapidly transforms the cyber landscape, organisations face both unprecedented opportunities and new layers of complexity in defending against evolving threats. This session explores how to operationalise AI in cyber defence amid increasingly complex threat environments. Corne will unpack recent incidents impacting major organisations, examine practical ways to enhance cyber risk awareness and decision-making using AI and advanced monitoring tools and discuss how executives are navigating the unpredictable nature of AI - balancing innovation with integrity in every security decision.

	Corne Mare CISO Australia **Fortinet**	
13:05	*Lunch*	*Invitation-Only VIP Lunch Hosted by Snyk*
	Track A: **Leading Security Across the Enterprise**	**Track B:** **Technical & Operational Resilience**
	Track A Chair: **Adwin Singh** Cybersecurity Domain Lead – CISO Office **Inland Revenue NZ**	Track B Chair: **Tash Bettridge** Co-founder **NZNWS**
14:05	**Beyond Awareness: Activating Security through Safer Choices by Design** A cyber-conscious mindset and security-aware culture are non-negotiable. It is not just about ticking boxes with e-learning or phishing tests. Real success is when people instinctively make safer choices and even share tips with family and friends. That's when culture truly sticks. This session explores practical ways to embed that mindset and turn everyday behaviours into security habits. **Marek Jawurek** Head of Cyber Security Advisory **Ampol**	**The Unexpected Union: When GRC and Architects Come Together** Tick-box compliance is no longer enough. This presentation explores how organisations are moving beyond policy-driven approaches to build real and measurable cyber capability through their GRC functions. Learn how embedding technical thinking into risk frameworks, reporting and decision-making helps turn intent into action and drives stronger security outcomes. **Shawn Wang** Head of Cybersecurity Governance Risk & Architecture **Spark**
14:30	**Secure Innovation, Not Slower Innovation: A Playbook for CISOs** Digital transformation and AI aren't side projects; they're the growth engines of modern organisations. But the pace of change creates a tension: how do CISOs enable innovation without becoming the brake pedal? In this session, we'll explore a playbook for balancing ambition with assurance. Drawing on lessons from boardrooms and transformation programs across ANZ, we'll unpack how to align cyber with business strategy, translate risk appetite into clear decision guardrails, and leverage AI safely to accelerate, not hinder, innovation. The result: a pathway where security isn't a compliance afterthought, but a catalyst for resilient growth. • How to align digital transformation goals with cyber strategy. • Turning risk appetite into practical decision-making guardrails. • Where AI can safely speed up both defence and innovation. • Positioning cyber as an enabler of resilience and growth. **Andrew Philp** Field CISO, ANZ **Trend Micro**	**When IAM is Targeted, Everything Changes** Attackers are not "hacking in, they are logging in", they target your user accounts (like Active Directory) before anything else. Why? To break your recovery plans. This talk shows how they get in and how you can stop them. **Ben Mudie** Principal Security Engineer **Tenable**
14:55	**Cyber Crisis Leadership: Uniting Security and Leadership** Cyber incidents don't stay confined to the SOC — they quickly become whole-of-business events. This session explores how security leaders are aligning technical response with executive-level crisis management to ensure clarity, speed, and coordination when it matters most. • The anatomy of cyber disruption from a senior leadership lens – what makes it uniquely difficult	**Security Operations for Critical Infrastructure: Improving Visibility, Detection, and Resilience** Join Adarsh as he shares how security operations were enhanced within a critical infrastructure environment. This session will explore strategies for increasing log visibility in high-risk areas, aligning threat intelligence with detection workflows, and validating coverage through adversary simulation. It will also cover the application of structured frameworks to guide detection engineering, the use

	• How to build "muscle memory" for high-pressure response (beyond the plan) • Bridging the gap between security experts and executive decision-makers **Laura Jury** Resilience Specialist (Business Continuity) **Air New Zealand**	of meaningful metrics to track progress, and practical approaches to overcoming operational challenges **Adarsh Lal** Security Operations Lead **Mercury NZ**
15:20	**When Trust Becomes a Weapon: The Rise of Invisible Phishing Attacks** Phishing attacks are increasingly outsmarting traditional defenses by hijacking trusted infrastructure like Microsoft's Direct Send. These sophisticated threats first evade legacy email filters and then go a step further, bypassing even multi-factor authentication, to deliver dangerous emails directly to CxO inboxes. Leveraging hyper-personalised tactics and advanced social engineering, attackers circumvent email authentication checks and exploit internal mail flows—putting every executive's mailbox at risk. Blocking obvious spam is no longer enough; today's phishing is invisible, relentless, and requires modern security strategies built for today's evolving threat landscape. Toby Guthrie from Abnormal AI will share insights on real-world examples and targeted campaigns seen in the wild. **Toby Guthrie** Sales Engineering Manager APJ **Abnormal AI**	**Agentic AI in Action: Risk Reduction Through Automation** Most companies are trying to use AI to streamline their cyber defences. Discover how AI-powered automation can enable organisations to shift from reactive patching to proactive risk reduction. Learn how agentic AI can: • Continuously assess and contextualise risk across hybrid environments • Automate remediation workflows based on business impact and exploitability • Empower security teams to focus on strategic initiatives, not manual triage Agentic AI is reshaping the future of cyber risk operations, turning complexity into clarity, and risk into resilience. **Joanne McKenzie** Senior Technical Account Manager **Qualys**
15:45	*Get refreshed! Afternoon tea break*	
16:15	**Beyond the Phishing Test: Effective Strategies for Managing Human Risk** 68% of all data breaches are due to human error, and despite significant investments in technical safeguards, phishing and social engineering attacks remain the #1 threat to your organisation. This session will explore: • The critical shift from traditional security awareness to human risk management (HRM). • How social engineering and phishing—particularly via email—remain the primary vectors for breaches and ransomware, now amplified by AI technologies that make sophisticated attacks accessible to novice cybercriminals. • Explore frameworks to quantify human risk, establish meaningful benchmarks, and provide clear metrics to measure success. **Joe Gillett** Head of ANZ **KnowBe4**	**Frog-Proof Security: Elevating DevSecOps for Tomorrow's Challenges** What does the future hold for software supply chain security in 2026? As the types and volume of software entering organizations continue to evolve, DevSecOps teams face increasingly complex challenges, including: • How can organisations effectively manage what enters their systems? • How can remediation be accelerated without sacrificing accuracy? • How will the rise of AI reshape our threat landscape, and can DevOps and security unite without adding friction? In this session, we will explore key insights into the looming challenges of software supply chain security and how they will transform operational practices. By analysing recent high-profile supply chain attacks in npm, we will expose malicious threats and offer practical, actionable solutions to mitigate both current and emerging risks. As our attack surfaces shift alongside evolving technologies, join us to discover innovative strategies and capabilities that seamlessly reintegrate security into DevSecOps. **Shani Levy** Senior Solutions Engineer **JFrog**
16:40	**What CISOs Need to Ask in Today's Identity-Driven, As-a-Service Environment**	**From Orchard to Firewall: Building Cyber Resilience Across the Supply Chain**

	As organisations move to SaaS and cloud native or hybrid models, identity has become the new security boundary and a frequent source of risk when transitions expose gaps attackers are quick to exploit. This session exploresye the key questions CISOs should be asking, including: • What's really changing in how we manage and secure identity? • What have we seen go wrong and how can it be avoided? • Are we thinking clearly about trust, privilege, and lifecycle in cloud-based environments? • How do we reduce complexity while maintaining control? **Ivan Reutskiy** GM Security **2degrees**	Cyber resilience doesn't stop at the enterprise boundary — especially in a sector reliant on seasonal staff, contractors, and legacy tech. Join Bryan as he shares how one of Australasia's largest horticulture businesses manages cyber risk across a complex, distributed operation. • Managing cyber security across a sprawling, seasonal, and third-party-reliant operation. • Tackling the "unsexy" risks: shared passwords, insecure remote access, outdated SCADA/PLC systems • Setting up vendor controls, contract guardrails, and alignment with business risk appetite • Cultivating cyber awareness in an industry where IT is often invisible — until something breaks **Bryan Graham** CIO **Seeka**
17:05	**Track A Chair Closing Remark** **Adwin Singh** Cybersecurity Domain Lead – CISO Office **Inland Revenue NZ**	**Track B Chair Closing Remark** **Tash Bettridge** Co-founder **NZNWS**
17:10	**Cheers with Peers!**	

DAY 2

Wednesday 19 November 2025

08:30	*Register; grab a coffee. Mix, mingle and say hello to peers old and new.*
09:00	**Welcome remarks by Corinium and Chair's opening remarks** **Denise Carter-Bennett** Co-Chair **New Zealand Network for Women in Security (NZNWS)**
09:10	**Fireside Chat: Where To From Here? What A Good Cyber Strategy Looks Like In NZ** This fireside chat explores what defines an effective cyber strategy in the New Zealand context — from aligning with business priorities and building resilience to uplifting sector capabilities and navigating a lighter regulatory environment. A forward-looking conversation on what matters most now, and what's next. **Phil Ross** CISO **Air New Zealand** **Edd Barber** CISO **WEL Networks**
09:35	**Seeing Ahead: Turning DNS Data into a Predictive Defense** In today's rapidly evolving threat landscape, organisations must move beyond reactive security strategies and embrace predictive intelligence to stay ahead of adversaries. The rise of generative AI has dramatically lowered the barrier of entry for cybercriminals - enabling faster, more focused attacks that are harder to detect and easier to automate. This session explores how Infoblox leverages the untapped potential of DNS data to deliver actionable, predictive threat insights that empower security teams to anticipate and mitigate attacks before they materialise. By transforming DNS into a rich source of early warning signals, Infoblox enables organisations to proactively defend their environments, reduce dwell time, and strengthen their overall security posture. **Brad Ford** Security Specialist – ANZ **Infoblox**
10:00	**Panel: Is Trust Enough? Do We Need Stronger Cyber Regulations?** New Zealand's flexible, trust-based approach to cyber security has long been seen as a strength — but is it enough? With rising threats and growing interdependence, this panel explores whether the time has come for stronger, enforceable regulation, and what a proportionate, uniquely Kiwi model might look like. • Is voluntary compliance still working or are gaps widening across sectors? • What would smarter, targeted regulation look like? vs. more red tape? • Should New Zealand follow Australia's lead with sector-specific obligations such as SOCI Act? Moderator: **Rebecca Holdsworth** Head of Privacy & Responsible AI **One NZ** Panellists: **Kavita Chetty** Senior Manager Technology Risk **NZAA** **Deepak Veerasamy** CISO **Kainga Ora** **Scott Shearman** CISO **House of Travel**
10:35	*Get refreshed! Morning coffee break*
11:05	**Panel: Resilience Starts Within – Nurturing a Cyber-Aware Culture Across Your Organisation** This panel explores how security leaders are embedding a culture of cyber awareness across the organisation. From influencing behaviour to measuring impact, hear how organisations are moving beyond annual training to create lasting engagement and shared responsibility. • How does human behaviour and organisational culture influence the effectiveness of cyber security practices? • What strategies can foster a security-conscious mindset and encourage proactive digital habits? • How can organisations measure the real impact of security awareness efforts and adjust over time? • What does it take to turn employees into active defenders of your cyber environment? Moderator: **Lakshya Mehra** National Security Awareness and Phishing Lead **Health NZ** Panellists:

	Ronnie Rahman Head of Cyber & Risk **Hamilton City Council** **Brad Ward Able** Head of Digital Security & Assurance **Mitre 10** **Scott Shearman** CISO **House of Travel** **Joe Gillett** Head of ANZ **KnowBe4**
11:35	**Harnessing AI for a Stronger Security Posture** • Explore how AI is transforming modern security operations, enhancing threat detection, prevention, and response. • Understand the role of AI in enabling data-centric security strategies to prevent breaches and mitigate insider threats. • Learn how advanced techniques like real-time behavioral analysis, contextual policy enforcement, and adaptive controls strengthen security. **Johnny Yeo** Transformation Architect **Zscaler**
12:00	**Panel: Securing the Supply Chain in a Connected, Trust-Based Ecosystem** This panel explores how security leaders are navigating supply chain complexity, driving uplift among vendors with varying levels of maturity, and balancing commercial relationships with the need for assurance. • How are you gaining visibility into third-party and SaaS risk across your ecosystem? • How are you evolving vendor assessments to keep up with the pace of procurement and onboarding? • Where should organisations draw the line between shared responsibility and direct control? • How can mitigation strategies be tailored to address financial, reputational and operational risks linked to third-party vulnerabilities? Moderator: **Adwin Singh** Cyber Security Domain Lead – CISO Office **Inland Revenue NZ** Panellists: **Eli Hirschauge** Head of Info Security **ANZ** **Darren Beattie** Head of Information Security **Tower Insurance**
12:35	*Lunch*
13:30	*Prize Winner Announcement*
13:35	**Mapping NZ's Threat Landscape and Unmasking a Local Phishing Kit** Join Kamo for an unfiltered look inside New Zealand's cyber threat reality. From dissecting a real phishing kit found on local networks to uncovering how attacker tactics evolve, this session reveals what drives today's biggest risks including ransomware, credential theft, card fraud, DDoS and hacktivism, and how security leaders can stay one move ahead. Expect sharp insights, local relevance and practical takeaways that help CISOs turn intelligence into action and resilience. **Junaid Siddiqui** Pre-Sales Manager **Group-IB**
14:00	**Panel: Invest Smart, Secure Smart – Maximising the Value through Strategic Resource Allocation** Cyber security investment is a balancing act. The goal isn't to spend more, it's to spend wisely. This panel explores how security leaders are aligning investment with actual risk, avoiding overengineering, and prioritising what matters most. From risk assessments to board conversations, it's about building fit-for-purpose capability that protects what counts without paying for the platinum package when the essentials will do. • How do you prioritise investment toward high-value areas without overinvesting in low-risk domains? • What metrics or KPIs help demonstrate whether security send is driving real impact? • How can you balance the need for thorough evaluation with the urgency of fast-moving threats? • What are the key challenges in securing board support and how do you respond when the answer is no? Moderator: **Luke Taylor** CEO **SSS Cybersecurity Specialists** Panellists:

	Ashley Archibald CISO **Natural Hazards Commission** **Marek Jawurek** Head of Cyber Security Advisory **Ampol** **Hassham Idris** Manager Cyber Risk and Assurance **Ministry of Justice - New Zealand**
14:35	**OT Under Siege: Modernising Remote Access in Critical Infrastructure** OT is digitalising fast and remote access is now the softest target. Join us for a pragmatic walkthrough of the SANS 5 Critical Controls, with a special focus on securing remote access without slowing operations. We'll unpack common missteps (and why they happen), share lessons from the field, and show how to implement controls that both the security team and the engineers will actually support. **Tim Jackson** Head of Solutions Engineering **Dull**
14:50	**Panel: Diverse Cyber Leadership – Roles, Growth and Influence Beyond the Title** This panel explores the expanding ecosystem of cyber decision-makers — from heads of risk and GRC to operations leads, architects, and advisors — who are driving impact without necessarily holding the top title. Hear how they're shaping strategy, building capability, and influencing outcomes across diverse career paths. • What leadership roles are emerging beneath or alongside the CISO? • How can professionals grow influence without chasing a title? • How can organisations recognise and support non-linear career growth? Moderator: **Michael Karich** Deputy CISO **University of Auckland** Panellists: **Ronald Chung** Head of Risk (Information, Technology & Cyber Security) **BNZ** **Lakshya Mehra** National Security Awareness and Phishing Lead **Health NZ** **Francis Kaitano** Enterprise Security Architect **BNZ**
15:25	*Get refreshed! Afternoon Tea break*
15:55	**Landing Cyber Deliverables: Beyond Strategy to Impact** Bridging the gap between strategy and execution is one of the hardest parts of cyber leadership. This session explores how to turn high-level plans into clear, achievable actions that deliver measurable outcomes. From prioritisation and stakeholder alignment to delivery roadmaps and metrics that matter, it's about making cyber real across the organisation. **Edd Barber** CISO **WEL Networks**
16:20	**Fireside Chat: The Innovation Mindset – Cyber Leaders Who Dare to Think Differently** Innovation and security are often seen as opposing forces, but the most successful organisations find ways to balance both. This panel brings together forward-thinking cyber security leaders to explore how to foster creativity while maintaining the rigour needed to safeguard organisations. • What does an innovation mindset mean to you as a cyber leader and how have you applied it in practice? • How do you create space for experimentation and bold ideas in environments where minimising risk is the norm? • Can you share a moment where thinking differently led to a shift in your cyber strategy, tooling, or team culture? Speakers: **Shawn Wang** Head of Cybersecurity Governance Risk & Architecture **Spark** **Kane Narraway** Head of Enterprise Security **Canva**
16:45	**Day 2 Chairperson's Closing Remarks** **Denise Carter-Bennett** Co-Chair **New Zealand Network for Women in Security (NZNWS)**
16:50	**Close of CISO New Zealand 2025**