Cloud & Cyber Security Expo

Master Theme:
AI Threats, Human Risks & Cyber Resilience
Threats are evolving – and so must our defences. In 2026, cyber resilience requires not only tooling, but behavioural vigilance and cross-team intelligence, especially in a world of LLM-powered attack surfaces.

1. AI Security Risk & Resilience
AI is transforming business—and rewriting the threat model. This theme unpacks how organisations can defend against new classes of AI-enabled attacks while responsibly integrating AI into their security stack. Explore risks like model poisoning and adversarial AI, as well as governance frameworks for secure AI deployment.
Sub-Themes: Adversarial AI & model poisoning, red-teaming generative AI systems, secure AI deployment & governance, synthetic data & privacy risks, and trust-by-design in AI pipelines.

2. Runtime Cloud Security and Real-Time Protection
Static scans aren't enough. This theme explores the need for runtime visibility and protection across multi-cloud and containerised environments, where threats evolve faster than traditional controls can respond.
Sub-Themes: Cloud-native detection & response, workload protection platforms, runtime telemetry & threat intelligence, continuous compliance in ephemeral environments, and securing multi-cloud & hybrid infrastructure.

3. The Role of Cyber Security Frameworks in Risk Management
Cyber security frameworks serve as the strategic blueprint for resilience in an age of escalating digital threats. This theme explores how organisations are leveraging established and emerging frameworks to proactively identify, assess, and mitigate risks across hybrid environments.
Sub-Topics: Aligning frameworks like NIST, ISO/IEC 27001, and CIS with operational objectives, creating adaptive response protocols, and embedding continuous compliance to navigate regulatory complexity and evolving threat landscapes.

4. Strategic Implementation & The Future of Cyber Security
Cyber security has evolved from a reactive IT function to a board-level priority. This theme explores how enterprises can transition from fragmented tools to integrated, future-ready strategies.
Sub-Themes: Pairing security investments with business growth, building CISO-led transformation roadmaps and preparing for next-gen threats—from quantum risk to AI-

enabled adversaries.

5. Identity-Driven Security at Scale
Identity is the new perimeter—and scaling identity-first security models is now critical. This theme explores how organisations are deploying adaptive identity governance, zero trust principles, and privileged access management at enterprise scale.
Sub-Themes: Cloud-native IAM, federated identity challenges, biometric security, and integrating identity signals with threat detection for faster response and reduced risk surface.