Defending and Leveraging AI: Strategies to Secure Intelligent Systems Against Emerging Threats.

AI is rapidly transforming the cybersecurity battlefield—both as a tool for defenders and a target for attackers. In this session, we explore actionable strategies to defend AI systems from emerging threats and leverage AI to boost your organization's cyber resilience.

Participants will learn how to identify and mitigate unique risks facing AI, including adversarial inputs, data poisoning, and model theft. The session also covers how AI can be used to strengthen security operations through automation, threat detection, and rapid response. With a spotlight on evolving AI regulations and guidance on extending frameworks like NIST, ISO, and CIS Controls, this session equips cybersecurity leaders with the knowledge to adapt traditional defenses and build robust, intelligent protection against AI-powered threats.

Sushila Nair

CISA, CISM, CDPSE, CISSP, GIAC

CEO, Cybernetic LLC

President of ISACA's Greater Washington, D.C. Chapter

Sushila Nair is the CEO of Cybernetic LLC and former Vice President of Capgemini's North American Cybersecurity practice, where she played a crucial role in driving secure digital transformation on a global scale. With over 30 years of experience in computing infrastructure, business, and security risk analysis, Sushila has established herself as a leading authority in the cybersecurity domain. Her career highlights include serving as Vice President responsible for global security offers at NTT DATA Services, a decade of leading her own IT and cybersecurity company across major UK cities, and serving as a Chief Information Security Officer (CISO) and trusted advisor to boards, where she honed her expertise in protecting organizations from evolving digital threats. Recognized through the top cybersecurity leader award by Security Magazine and Cyber Magazine, Sushila's influence in the industry is undeniable.

An esteemed thought leader, Sushila has shared her insights on prestigious platforms such as RSA Conference and ISACA's global events. Her active participation in ISACA's global emerging trends working group and her leadership as President of ISACA's Greater Washington, D.C. Chapter underscore her dedication to advancing the field of cybersecurity. In 2024, her commitment to nurturing the next generation of cybersecurity professionals and promoting diversity in the industry was honored with the prestigious ISACA Technology for Humanity Award.