Securing AI: Strategies for the Modern Threat Landscape

Artificial Intelligence (AI) is rapidly transforming various sectors, offering unprecedented capabilities and efficiencies. However, this advancement introduces new vulnerabilities and attack surfaces that cybercriminals can exploit. "Securing AI: Strategies for the Modern Threat Landscape" explores the multifaceted challenges associated with protecting AI systems, including adversarial attacks, data poisoning, and model theft. This session highlights the importance of developing robust security frameworks tailored to AI's specific needs. It emphasizes continuous monitoring and adaptive defense mechanisms to safeguard AI applications. Additionally, we will discuss the significance of collaboration between AI developers, cybersecurity experts, and policymakers to create comprehensive security strategies.

Pirabu Pathmasenan

Head of IBM Security Technical Sales Engineering, Canada & Caribbean (pirabu@ibm.com),

Pirabu Pathmasenan brings over 15 years of expertise across Data & Analytics, AI, Cybersecurity, Customer Success, and Consulting services. His career is marked by a commitment to innovation and simplification, helping clients achieve their business goals. Currently, Pirabu leads the Data & AI Technical Sales Engineering team for the Canadian market. Previously, he spearheaded Security Sales Engineering for the Canada & Caribbean market, guiding clients through their Data Protection and Privacy journeys to ensure robust security, privacy, and compliance. Before joining IBM, Pirabu played a pivotal role at TD Bank, driving the bank's digital transformation and advancing its Big Data & AI initiatives. Beyond his professional endeavors, Pirabu is a dedicated father of two and an enthusiastic sock designer. His passion for fashion led him to create "Velvet & White," a project that allows him to explore creativity in fashion.