# KATA PENGANTAR

Buku ini dimulai dengan konteks yang kuat tentang peran Kecerdasan Artifisial (*Artificial Intelligence*) dan *Machine Learning* dalam kehidupan digital saat ini, yang tentunya langsung menarik perhatian pembaca. Tantangan serangan adversarial dipaparkan dengan lugas dan dampaknya dalam berbagai aplikasi kritis (keamanan, keuangan, kesehatan) sangat ditekankan. Buku ini secara eksplisit disebut sebagai "panduan komprehensif" untuk memahami dasar-dasar *Adversarial Machine Learning* dan membangun model yang tahan serangan.

Buku ini dengan jelas memfokuskan pada pemahaman serangan dan metode pertahanan adversarial, yang merupakan inti dari bidang ini. Buku ini dijanjikan akan membantu pengembang merancang model yang tidak hanya berkinerja tinggi tetapi juga tahan terhadap serangan. Buku secara jelas menyebutkan target audiens (peneliti, praktisi, mahasiswa) dan menyesuaikan bahasa yang digunakan sehingga mudah dipahami oleh mereka.

Harapan buku sebagai "bahan bacaan yang berharga" dan pendorong penelitian lebih lanjut realistis dan tidak berlebihan. Buku ini ditulis mengalir dengan baik, mulai dari konteks, identifikasi masalah, solusi yang ditawarkan, manfaat, target audiens, hingga harapan.

Secara keseluruhan, buku ini sangat baik. Ini secara efektif mengkomunikasikan pentingnya topik, solusi yang ditawarkan oleh