# ABSTRAK

Penelitian ini mengatasi tantangan peningkatan kemampuan cyber threat intelligence organisasi dengan mengintegrasikan Large Language Models (LLMs) dan Hybrid Retrieval-Augmented Generation (RAG) dalam CTI Capability Maturity Model. Sistem CTI tradisional kesulitan memproses data ancaman berskala besar dan tidak terstruktur secara efisien sambil mempertahankan akurasi dan kemampuan penjelasan.

Studi mengimplementasikan framework AIM-CTI menggunakan sumber data OpenCTI dan arsitektur database ganda Neo4j, dievaluasi melalui 28 query yang dikurasi ahli meliputi lima kategori domain CTI. Hasil menunjukkan peningkatan performa signifikan dibandingkan sistem baseline, dengan framework mencapai tingkat keberhasilan 82% dan meningkatkan maturitas CTI organisasi dari 21,2% menjadi 35,8%. Evaluasi ahli manusia mengkonfirmasi aplikabilitas praktis sistem yang diusulkan.

Penelitian memvalidasi bahwa sistem CTI berbasis AI menunjukkan kemampuan analitis superior dibandingkan pendekatan tradisional, menyediakan organisasi framework sistematis untuk memajukan intelijen keamanan siber sambil mempertahankan pengawasan manusia dan kemampuan penjelasan.

**Kata kunci:** Deteksi Ancaman, Intelijen Ancaman Siber, LLM, Hybrid RAG