ABSTRACT

This research addresses the challenge of enhancing organizational cyber threat intelligence capabilities by integrating Large Language Models (LLMs) and Hybrid Retrieval-Augmented Generation (RAG) within the CTI Capability Maturity Model. Traditional CTI systems struggle to process large-scale, unstructured threat data efficiently while maintaining accuracy and explainability.

The study implements the AIM-CTI framework using OpenCTI data sources and Neo4j dual database architecture, evaluated through 28 expert-curated queries across five CTI domain categories. Results demonstrate significant performance improvements over baseline systems, with the framework achieving an 82% success rate and increasing organizational CTI maturity from 21.2% to 35.8%. Human expert evaluation confirmed the practical applicability of the proposed system.

The research validates that AI-enhanced CTI systems demonstrate superior analytical capabilities compared to traditional approaches, providing organizations with a systematic framework to advance their cybersecurity intelligence while maintaining human oversight and explainability.

Keywords: Cyber Threat Intelligence, LLM, Hybrid RAG, Threat Detection