AI-ThreatIntel-Research: Ongoing Study

Author: Loksharan Saravanan
Contact: loksharan.soc@gmail.com
GitHub: github.com/loksharan-soc
Status: Ongoing Research / Work in Progress

1. Introduction

Cybersecurity threats are becoming increasingly complex and frequent, creating a critical need for automated and intelligent threat detection systems. Traditional threat intelligence methods often rely on manual analysis or static signature-based detection, which are insufficient for identifying evolving threats in real-time.

This study evaluates the following:

- Application of AI/ML techniques for threat detection and classification.
- Effectiveness of automated analysis on heterogeneous threat intelligence datasets (malicious URLs, malware samples, phishing campaigns).
- Integration of AI-driven insights with frameworks like MITRE ATT&CK.

Research Question: How can AI models enhance the speed, accuracy, and predictive capabilities of threat intelligence operations?

Note: This research is ongoing. The methodology, results, discussion, conclusion, references, and appendices are currently a work in progress and will be added in future versions.