DOI: doi.org/10.47363/JAICC/ICAIC2025/2025(4)5

International Conference on
Artificial Intelligence and Cybersecurity (ICAIC 2025)

Conference Proceedings November 27-28, 2025 - Japan

AI-Driven Threat Detection and Response

Pietro Di Maria

GM & Co-Founder, Meridian Group | Assoc. Researcher, EDHEC Business School, Italy

Abstract

The increasing sophistication of the cyber threat landscape demands a systemic and cross-disciplinary approach that integrates Cyber Threat Intelligence (CTI) with Competitive Intelligence (CI). Traditional cybersecurity measures, often focused on detection and incident response, are no longer sufficient in environments characterized by asymmetrical threats, geopolitical tensions, and rapid technological change. To address these challenges, Kitsune (Meridian Group) has developed an operational model that merges CTI methodologies with CI practices, creating a comprehensive knowledge ecosystem designed to identify weak signals, anticipate emerging risks, and inform strategic decision-making processes. The proposed framework is structured along three key dimensions. First, data collection and enrichment, combining heterogeneous sources such as OSINT, HUMINT, technical feeds, and commercial intelligence, which are normalized and enriched to ensure interoperability and actionable insights. Second, multi-level threat analysis, spanning from the identification of indicators of compromise (IoCs) and adversary tactics, techniques, and procedures (TTPs) mapped to MITRE ATT&CK, to the evaluation of strategic risks related to state actors, cybercriminal groups, and geopolitical drivers. Third, competitive contextualization, where cyber threat insights are correlated with sectoral dynamics, business risks, and market trends, enabling organizations to transform threat intelligence into a lever of decision advantage. The integration of machine learning and predictive analytics further enhances the framework, enabling the identification of recurring patterns and advanced persistent threats (APTs), while simultaneously improving prevention, detection, and resilience. This convergence ensures that decision makers benefit from situational awareness not only in the cyber domain but also across strategic and competitive contexts. Such awareness allows for the optimization of cybersecurity investments, prioritization of defensive capabilities, and the proactive anticipation of market and reputational risks tied to the evolving threat environment. Empirical results from the Kitsune model indicate that the convergence of CTI and CI delivers dual value. On the one hand, it strengthens the organization? s ability to detect and mitigate threats in near real-time, reducing operational exposure and the potential impact of attacks. On the other hand, it fosters long-term resilience by embedding intelligence-driven perspectives into corporate strategy, risk management, and governance frameworks. This contribution aims to stimulate discussion on the necessity of bridging technical and strategic intelligence practices, highlighting how the integration of CTI and CI is increasingly becoming a differentiator in complex operating environments. By positioning cybersecurity not as a purely technical safeguard but as a strategic and competitive enabler, organizations can better navigate uncertainty, protect critical assets, and sustain a competitive advantage in the digital age.