Application of Game Theoretic Model for Cyber Threat Intelligence Framework

Manas Kumar Yogi[1], Dwarampudi Aiswarya[1], and Jyotir Moy Chatterjee[2]

[1]Pragati Engineering College
[2]Graphic Era Deemed to be University

January 30, 2024

Abstract

In the ever-evolving landscape of cybersecurity, the application of game theoretic models has emerged as a powerful and innovative approach to enhance our understanding and management of cyber threats. This abstract explores the application of a variant of game theoretic models within the context of a Cyber Threat Intelligence (CTI) framework. With the proliferation of cyber-attacks targeting critical infrastructure, sensitive data, and national security, it has become imperative to develop proactive and adaptive strategies for threat detection, mitigation, and response. The variant of game theoretic models discussed in this abstract departs from traditional game theory by incorporating elements of dynamic adaptation and machine learning. This adaptation enables the framework to model and analyze the intricate and rapidly changing interactions between threat actors and defenders in real-time, thereby providing a more accurate representation of the evolving threat landscape. By leveraging machine learning algorithms, the model can continuously learn and adapt to new threats and tactics, making it a versatile tool for CTI. This abstract also explores the practical applications of the variant model in various aspects of cybersecurity, including threat actor profiling, vulnerability assessment, and decision support for incident response. By considering the strategic motivations and behaviors of threat actors, organizations can make informed decisions regarding resource allocation, risk assessment, and security investments. The integration of this variant of game theoretic models into CTI holds great potential to revolutionize our approach to cybersecurity, enabling organizations to stay one step ahead of adversaries. As the digital world becomes increasingly complex, the ability to predict, mitigate, and adapt to cyber threats is crucial for safeguarding critical assets and ensuring the resilience of digital infrastructure. This paper highlights the significance of this innovative approach and its potential to shape the future of cyber threat intelligence and cybersecurity practices.

Hosted file

`Final Manuscript Application-of-Game-Theoretic-Model-for-Cyber-Threat-Intelligence-Framework-26-9-2023` available at https://authorea.com/users/655920/articles/708564-application-of-game-theoretic-model-for-cyber-threat-intelligence-framework