AI-Based Holistic Framework for Cyber Threat Intelligence Management

Abstract:

Cyber Threat Intelligence (CTI) is an important asset for organisations to facilitate the safeguarding of their systems against new and emerging cyber threats. CTI continuously provides up-to-date information which enables the design and implementation of better security measures and mitigation strategies. Organisations gather data from different sources either internal or external to the organisation, which are analysed, resulting in CTI. Nevertheless, the gathered data usually contain a large amount of content that is irrelevant to CTI or even to cybersecurity. Furthermore, most approaches concerning CTI management (e.g., gathering, analysis) involve simply gathering and storing the information without any enrichment such as classification or correlation. However, in order to obtain optimal results, organisations should be able to utilise all capabilities of CTI. Therefore, in this work, we propose Threat wise AI, a novel framework that enables the gathering, analysis, enrichment, storage, and sharing of CTI in an efficient and secure manner. In particular, we have developed a novel pipeline in Threat wise AI which incorporates different advanced tools, with distinct capabilities that interact with each other to provide a complete set of functionalities for the administration of the overall CTI lifecycle. The developed tools integrate various Python scripts and provide gathering and analysis functionalities of CTI. Furthermore, the proposed framework leverages the MISP platform for storing, enriching and sharing while also integrating Artificial Intelligence (AI) and Machine Learning (ML) algorithms for advanced data enrichment.