World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:06, 2022

Using Social Network Analysis for Cyber Threat Intelligence

Authors : Vasileios Anastopoulos

Abstract : Cyber threat intelligence assists organizations in understanding the threats they face and helps them make educated decisions on preparing their defenses. Sharing of threat intelligence and threat information is increasingly leveraged by organizations and enterprises, and various software solutions are already available, with the open-source malware information sharing platform (MISP) being a popular one. In this work, a methodology for the production of cyber threat intelligence using the threat information stored in MISP is proposed. The methodology leverages the discipline of social network analysis and the diamond model, a model used for intrusion analysis, to produce cyber threat intelligence. The workings are demonstrated with a case study on a production MISP instance of a real organization. The paper concluded with a discussion on the proposed methodology and possible directions for further research.

Keywords : cyber threat intelligence, diamond model, malware information sharing platform, social network analysis
Conference Title : ICCTI 2022 : International Conference on Cyber Threat Intelligence
Conference Location : Paris, France
Conference Dates : June 23-24, 2022