Title: A risk management dissemination process of cybersecurity threat intelligence using STIX/TAXII platform

Authors: MS Dlamini[1] ; Hlaudi Daniel Masethe[2]

Institutions/Affiliations:
[1]Tshwane University of Technology, South Africa
[2]Tshwane University of Technology, South Africa

Corresponding author email address: Dan Masethe MasetheHD@tut.ac.za; MS Dlamini 205310206@tut4life.ac.za

Abstract

Cybersecurity threats in the 21st century bring difficult risk situations, with sophisticated attack experiences or advanced persistent threats (APTs) in which targeted and destructive attacks cannot be resolved with traditional cybersecurity approaches [1][2]. Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII) are established for the Cyber Threat Intelligence (CTI) risk management components such as dissemination, information gathering and threat analysis which maybe unified into security procedures for an organization [1]. Trading early warning of approaching cyber threats condition awareness information is relevant for organizations to endure as part of cyber domain [3]. The research study detects potential cyber threats with the aim of dissemination process for cyber threat information sharing using STIX/TAXII platform. The research use evaluation metrics of accuracy and effectiveness to test the performance of the proposed solutions.

Keywords – Cybersecurity; STIX; TAXII

References:

[1] O. C. Briliyant, N. P. Tirsa, and M. A. Hasditama, “Towards an Automated Dissemination Process of Cyber Threat Intelligence Data using STIX,” in *Proceedings - IWBIS 2021: 6th International Workshop on Big Data and Information Security*, 2021, pp. 109–114. doi: 10.1109/IWBIS53353.2021.9631850.

[2] Z. Iqbal, Z. Anwar, and R. Mumtaz, “STIXGEN-A novel framework for automatic generation of structured cyber threat information,” in *Proceedings - 2018 International Conference on Frontiers of Information Technology, FIT 2018*, 2019, pp. 241–246. doi: 10.1109/FIT.2018.00049.

[3] T. Kokkonen, J. Hautamaki, J. Siltanen, and T. Hamalainen, “Model for sharing the information of cyber security situation awareness between organizations,” in *2016 23rd International Conference on Telecommunications, ICT 2016*, 2016, pp. 1–5. doi: 10.1109/ICT.2016.7500406.