Contribution ID: **38** Type: **Talk**

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

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.

Student or Postdoc?

PhD or DTech4

Primary authors: Mr MASETHE, Hlaudi Daniel (Tshwane University of Technology); MASETHE, Hlaudi (Tshwane University of Technology)

Co-author: Ms DLAMINI, MS (Tshwane University of Technology)

Presenter: MASETHE, Hlaudi (Tshwane University of Technology)

Session Classification: SA NREN

Track Classification: SA NREN