Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019), Stellenbosch University, South Africa, 28 February to 1 March 2019

Categorising cyber security threats for standardisation

Khan, ZC

Abstract:
Computer Security Incident Response Teams (CSIRTs) are responsible for data collection and analysis concerning cyber security threat incidents. In order to provide the best service support for cyber security breaches, information about how to classify encountered threats is required. A taxonomy can be used to provide an organisation of threats, while an ontology can be used to provide the organisation as well as complex relations among the threats. To assist with the representation and management of cyber security threats, this paper presents an ontology for categorising cyber security threats. The ontology can be used by CSIRTs for the collection of cyber threat information, to analyse the threats for reports, and to infer new knowledge about the cyber security threats that have been reported.