An Architectural Model for APT Detection

Authors : Nam-Uk Kim, Sung-Hwan Kim, Tai-Myoung Chung

Abstract : Typical security management systems are not suitable for detecting APT attack, because they cannot draw the big picture from trivial events of security solutions. Although SIEM solutions have security analysis engine for that, their security analysis mechanisms need to be verified in academic field. Although this paper proposes merely an architectural model for APT detection, we will keep studying on correlation analysis mechanism in the future.

Keywords : advanced persistent threat, anomaly detection, data mining

Conference Title : ICCCISE 2015 : International Conference on Computer, Communication and Information Sciences, and Engineering

Conference Location : London, United Kingdom

Conference Dates : February 16-17, 2015

Open Science Index, Computer and Information Engineering Vol:9, No:02, 2015 publications.waset.org/abstracts/23009.pdf