World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:12, No:09, 2018

Anomaly Detection of Log Analysis using Data Visualization Techniques for Digital Forensics Audit and Investigation

Authors : Mohamed Fadzlee Sulaiman, Zainurrasyid Abdullah, Mohd Zabri Adil Talib, Aswami Fadillah Mohd Ariffin

Abstract : In common digital forensics cases, investigation may rely on the analysis conducted on specific and relevant exhibits involved. Usually the investigation officer may define and advise digital forensic analyst about the goals and objectives to be achieved in reconstructing the trail of evidence while maintaining the specific scope of investigation. With the technology growth, people are starting to realize the importance of cyber security to their organization and this new perspective creates awareness that digital forensics auditing must come in place in order to measure possible threat or attack to their cyber-infrastructure. Instead of performing investigation on incident basis, auditing may broaden the scope of investigation to the level of anomaly detection in daily operation of organization's cyber space. While handling a huge amount of data such as log files, performing digital forensics audit for large organization proven to be onerous task for the analyst either to analyze the huge files or to translate the findings in a way where the stakeholder can clearly understand. Data visualization can be emphasized in conducting digital forensic audit and investigation to resolve both needs. This study will identify the important factors that should be considered to perform data visualization techniques in order to detect anomaly that meet the digital forensic audit and investigation objectives.

Keywords : digital forensic, data visualization, anomaly detection , log analysis, forensic audit, visualization techniques
Conference Title : ICDFIE 2018 : International Conference on Digital Forensics, Investigation and Evidence
Conference Location : Rome, Italy
Conference Dates : September 17-18, 2018