# Leverage Intrusion Detection System Framework for Cyber Situational Awareness System



| | |
|---|---|
| Title | Leverage Intrusion Detection System Framework for Cyber Situational Awareness System |
| Publication Type | Conference Paper |
| Year of Publication | 2017 |
| Authors | Masduki, B. W., Ramli, K., Salman, M. |
| Conference Name | 2017 International Conference on Smart Cities, Automation Intelligent Computing Systems (ICON-SONICS) |
| Keywords | Attack, composability, cyber situational awareness system, Cyberspace, decision making, Framework, GUI, intrusion detection system, Measurement, Metrics, Network, Organizations, Ports (Computers), pubcrawl, Resiliency, security, situational awareness, Threat, Tools |

Abstract

As one of the security components in cyber situational awareness systems, Intrusion Detection System (IDS) is implemented by many organizations in their networks to address the impact of network attacks. Regardless of the tools and technologies used to generate security alarms, IDS can provide a situation overview of network traffic. With the security alarm data generated, most organizations do not have the right techniques and further analysis to make this alarm data more valuable for the security team to handle attacks and reduce risk to the organization. This paper proposes the IDS Metrics Framework for cyber situational awareness system that includes the latest technologies and techniques that can be used to create valuable metrics for security advisors in making the right decisions. This metrics framework consists of the various tools and techniques used to evaluate the data. The evaluation of the data is then used as a measurement against one or more reference points to produce an outcome that can be very useful for the decision making process of cyber situational awareness system. This metric offers an additional Graphical User Interface (GUI) tools that produces graphical displays and provides a great platform for analysis and decision-making by security teams.

URL http://ieeexplore.ieee.org/document/8267823/
DOI 10.1109/ICON-SONICS.2017.8267823

Citation Key masduki_leverage_2017

attack composability cyber situational awareness system Cyberspace Decision Making framework GUI intrusion detection system Measurement Metrics Network Organizations Ports (Computers) pubcrawl Resiliency security situational awareness threat tools