SASP: a Semantic web-based Approach for management of Sharable cybersecurity Playbooks

This paper describes about SASP architectural design, and its essential features and components are the incident handlers' primary requirements. Next, we talk about the solution's future potential and the findings of our user-centric assessment, which was done on employees of several Security Operation Centres. We propose employing a semantic web-based method to record incident response and recovery procedure knowledge in order to facilitate playbook sharing using a shared, standardised vocabulary. We present SASP, a proof-of-concept application for playbook management based on Semantic MediaWiki, to better illustrate our methodology.

Reference:

Mehdi Akbari Gurabi, Avikarsha Mandal, Jan Popanda, Robert Rapp, and Stefan Decker. 2022. SASP: a Semantic web-based Approach for management of Sharable cybersecurity Playbooks. In The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3538969. 3544478