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

Abstract:

In incident management, responding effectively to cyberattacks is crucial, and security playbooks guide response and recovery actions. However, many organizations lack the resources and expertise to handle incidents, making playbook sharing essential. Current playbooks are often organization-specific, lacking machine readability and interoperability. This work proposes a semantic web-based approach to standardize playbooks, enhancing sharing capabilities. The proof-of-concept tool, SASP, employs Semantic MediaWiki for playbook management. The paper outlines key incident handler requirements, SASP's architecture, core components, and functionalities. A user-centric evaluation involving Security Operation Centre members demonstrates its effectiveness. The proposed solution addresses the critical need for standardized, shareable, and interoperable playbooks, offering potential improvements for organizations in enhancing their response capabilities against cyberattacks.

Introduction:

The contemporary landscape of cybersecurity demands robust incident management strategies to effectively counteract the escalating threat of cyberattacks. In this context, the paper titled "SASP: a Semantic web-based Approach for management of Sharable cybersecurity Playbooks" addresses a pivotal problem within incident response – the lack of standardized, shareable, and interoperable playbooks. As organizations grapple with limited resources and varying levels of expertise, the need for a comprehensive solution becomes increasingly apparent.

The problem at hand revolves around the organization-specific nature of existing playbooks, often hindering seamless collaboration and knowledge exchange between entities. These playbooks, while essential for guiding incident response and recovery actions, are typically not machine-readable, impeding their adaptability across diverse security infrastructures. Consequently, a critical gap exists in the collective ability of organizations to harness incident response best practices. To tackle this challenge, the paper proposes SASP, a pioneering semantic web-based approach that leverages a standardized and common vocabulary.

This solution aims to enhance the creation, sharing, and management of cybersecurity playbooks. SASP provides a structured framework to address the inherent limitations of traditional playbooks, ensuring they become not only machine-readable but also interoperable and easily shareable across different organizations. The innovative nature of SASP lies in its utilization of Semantic MediaWiki, serving as a proof-of-concept tool for playbook management. By establishing a standardized foundation for incident response knowledge, SASP offers a promising avenue to bolster organizations' capabilities in navigating the intricate landscape of cyber threats. This paper explores the identified problem within incident management and presents SASP as a forward-thinking solution, marking a significant stride towards collective resilience in the face of evolving cybersecurity challenges.

Related Works:

The incident management workflows are commonly organisation specific. In an organisation, Computer Security Incident Response Teams (CSIRTs) or Computer

Emergency Response Teams (CERTs) are mainly responsible for incident handling. The main objectives of incident handling are:

- ❖ Strategic protection of the entire infrastructure and assets and mitigate adversary damages.
- ❖ Finding the adversaries, understanding their behaviour and motivations, getting rid of them once they are in, and discovering their possible return.
- ❖ Ensure no confidential data is revealed while gaining as much information as possible.

MITRE Corporation recommends preparing cyber exercise playbooks for incident mitigation. MITRE ATT&CK offers a global knowledge base of adversary tactics. Various standards like OpenC2, IACD, and COPS, reviewed in [29], address cybersecurity response and recovery actions. The OASIS CACAO standard aims to share machine-readable playbooks, but challenges persist in capturing and sharing on established platforms. MISP and STIX adapt to CACAO, enabling playbook publication. Semantic web technologies, a standard for knowledge management, offer advantages. Nykanen proposed a knowledge management system using Semantic MediaWiki for cybersecurity risk but lacked a focus on incident response and recovery steps.

SASP: OVERVIEW AND DESIGN:

In conducting an empirical study for SASP, a group of experts was engaged in two interview rounds with Security Operation Centres (SOC) incident response teams from academia and industry, including representatives from security companies, a research institute, and a university. The interviews, totalling four sessions in each round, covered diverse aspects such as current playbook management approaches, strengths, weaknesses, and expectations. Participants provided insights into the limitations of existing tools supporting cybersecurity playbook knowledge management and articulated requirements for the development of a playbook management tool emphasizing sharing and workflow automation. Feedback from domain experts informed the design choices, architecture, and vocabulary of SASP, addressing issues like the lack of advanced knowledge management tools capable of capturing both human- and machine-readable Response and Recovery (R&R) playbooks, with an exploration of varied organizational approaches ranging from SOAR automation workflows to diagramming software for human-understandable representation.

The identified problem in the paper revolves around the inefficiencies and challenges associated with the creation, sharing, and management of cybersecurity playbooks in incident response. Traditional playbooks, often organization-specific and lacking machine readability, hinder collaboration and knowledge exchange. To address these issues, the proposed solution, SASP (Semantic web-based Approach for management of Sharable cybersecurity Playbooks), employs a semantic web-based approach with a standardized vocabulary. The solution aims to enhance the interoperability and shareability of playbooks across diverse organizations, providing a structured framework for incident response.

1. Semantic Web-Based Approach:

SASP leverages semantic web technologies to overcome the limitations of traditional playbooks. By adopting a common vocabulary, it facilitates machine readability and interoperability, ensuring that playbooks can be comprehended and utilized across various security infrastructures. The semantic approach allows for a standardized representation of incident response and recovery steps, promoting a shared understanding of best practices.

2. **MITRE Recommendations and ATT&CK:**

The solution aligns with MITRE Corporation's recommendations for cyber exercise playbooks. It acknowledges the significance of MITRE ATT&CK, a comprehensive knowledge base, in organizing adversary tactics and techniques. By integrating these insights into SASP, the solution ensures that playbooks are not only tailored to specific organizations but are also informed by real-world observations and best practices. This incorporation adds a layer of real-world relevance to the playbooks, enhancing their effectiveness.

3. **Semantic MediaWiki:**

We chose Semantic MediaWiki (SMW) to quickly develop SASP because it has a user-friendly web interface linked to the SMW core component, allowing us to use semantic technologies for our knowledge base. We started by creating an ontology, a structured way of organizing information, using a formal method for detailing response and recovery (R&R) actions and steps. Then, we gathered domain knowledge and integrated the ontology into SMW forms, templates, categories, and properties. To make things easier, we considered reusing existing data by aligning it with our ontology and translating it into our vocabulary. This allows us to input data directly into SMW using the web interface or a graphical user interface (GUI) we developed. We can also translate and import existing data from different sources into our knowledge base. This whole process is visualized in Figure 1 for a better understanding.

4. **MISP Integration:**

To address the challenge of sharing playbooks on established platforms, SASP integrates with MISP, a well-known sharing platform. MISP provides an object to capture textual Course of Action (CoA) playbooks, and SASP ensures compatibility with the CACAO playbook structure. This integration enables the seamless sharing of CACAO playbooks into MISP, fostering collaboration and knowledge dissemination among cybersecurity professionals.

5. **STIX Adaptation:**

Acknowledging the diversity of sharing platforms, SASP extends its compatibility to STIX, offering another avenue for sharing CACAO playbooks. This adaptability ensures that SASP is not limited to a single platform, increasing its versatility and usability in various organizational contexts.

6. **User-Centric Design and Evaluation:**

SASP's development and design are informed by user-centric principles, considering the requirements and perspectives of incident handlers from different Security Operation Centres. This ensures that the solution aligns with the practical needs of cybersecurity professionals, making it a user-friendly and effective tool in real-world scenarios.

the SASP solution addresses the multifaceted challenges in incident response and playbook management by embracing a semantic web-based approach. By integrating with existing standards, leveraging knowledge management principles, and prioritizing user-centric design, SASP stands as a promising advancement in the field of cybersecurity incident management. Its adaptability, compatibility with sharing platforms, and emphasis on both machine and human-readable representations position it as a comprehensive solution to enhance the collective response capabilities against cyber threats.

Conclusion:

In summary, SASP, our Semantic web-based Approach for Sharable Cybersecurity Playbooks, utilizes Semantic MediaWiki to overcome challenges in incident response. Aligned with MITRE recommendations and ATT&CK, SASP offers a standardized, machine-readable, and user-friendly solution. Shaped by insights from expert interviews, the tool caters to practical needs, providing flexibility in data entry through a web interface or GUI and ensuring compatibility with emerging cybersecurity standards. SASP serves as an innovative response to the complexities of cybersecurity playbook management, enhancing collaboration and knowledge exchange. The empirical study and feedback from domain experts have refined SASP into a valuable, comprehensive tool for incident responders, contributing to standardized, interoperable, and efficient cybersecurity incident management.

Discussion:

In the discussion, the efficacy of SASP is underscored through its integration of Semantic MediaWiki, addressing the intricate challenges of cybersecurity playbook management. The choice of Semantic web technologies empowers SASP to provide a standardized and interoperable framework, aligning with MITRE recommendations and ATT&CK. Expert interviews guided the iterative development, ensuring practicality and user-centric design. The tool's flexibility in data entry and compatibility with diverse sources enhances its adaptability. By filling the gaps in existing knowledge management tools, SASP emerges as a comprehensive solution for incident responders, fostering collaboration and knowledge sharing. The empirical study further validates its utility, marking a significant advancement in the quest for efficient and standardized incident response capabilities against evolving cyber threats.

Analysis:

The analysis reveals the strategic selection of Semantic MediaWiki for SASP's rapid development, ensuring a user-friendly interface for semantic technologies. The paper effectively discusses the ontology development, knowledge acquisition, and data importation processes. SASP's adaptability is highlighted through its capacity to reuse existing domain data and integrate with different sources. The emphasis on addressing limitations in current cybersecurity playbook management tools aligns with industry needs. The analysis underscores the paper's clarity in presenting SASP as an innovative and pragmatic solution, incorporating expert feedback and empirical validation to strengthen its role in advancing standardized and efficient incident response capabilities.

References:

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