Challenges and Opportunities in Information Sharing during Cybersecurity Exercises

Chethiya Galkaduwa

January 2, 2024

Abstract

A key component of cybersecurity defense is effective information sharing, which promotes teamwork and quick reaction to emerging threats. However, putting strong information-sharing principles into practice might be difficult for practitioners. This summary paper explores cybersecurity specialists’ perceptions on information sharing during real-world international cybersecurity exercises (CDX) and looks at the barriers to the development of better information-sharing skills. The study intends to shed light on the difficulties faced by cybersecurity professionals and pinpoint areas where information-sharing procedures could be improved.

Introduction

A key component of cybersecurity defense is effective information sharing, which promotes teamwork and quick reaction to emerging threats. However, putting strong information-sharing principles into practice might be difficult for practitioners. This summary paper explores cybersecurity specialists’ perceptions on information sharing during real-world international cybersecurity exercises (CDX) and looks at the barriers to the development of better information-sharing skills. The study intends to shed light on the difficulties faced by cybersecurity professionals and pinpoint areas where information-sharing procedures could be improved.

Methods

The paper analyzes two actual live international CDX events that took place in 2018 and 2019. The exercises were created as hybrid events that included both reporting duties to fictitious legal authorities and real-time technical defense of operating systems. The participants, mostly junior cybersecurity experts from the military and critical infrastructure corporations, were split up into independent Blue Teams (BTs), which oversaw protecting their simulated enterprise infrastructures from Red Teams (RT). The management of attack reports, interactions with other teams, and internal communication flows were all observed by observers assigned to each team. Before and after the exercises, participants were given questionnaires to gauge their abilities, attitudes, and intended areas of development.[4]

Results and Discussion

The study identifies nine important barriers to information sharing during CDX events.

Factor 1: Teams tend to prioritize active defense and technical mitigation duties above reporting and information-sharing (RIS) tasks due to a restricted concentration on technical jobs. [1]

Factor 2: Reporters face difficulties due to the need for a variety of technical skills since they must assemble information from members of different teams with varying levels of experience to compile thorough attack reports. [1]
Factor 3: The lack of a standard terminology and taxonomy makes it difficult for team members to grasp attack descriptions, which can cause ambiguity and miscommunication. [1]

Factor 4: Lack of training and inconsistent reporting standards lead to uncertainty and inconsistent reporting practices because of fragmented knowledge of legal documents relating to reporting procedures. [1, 2, 37]

Factor 5: Lack of understanding of data exchange standards makes it difficult to provide threat intelligence in an organized manner and raises the possibility of reporting errors, like the mixing of text and numeric data in report forms. [1]

Factor 6: The effectiveness of information exchange is limited by the insufficient use of information-sharing platforms created for CDX events and the reliance on other communication methods. [1]

Factor 7: An overabundance of communication channels combined with the reporting officers’ enormous multitasking demands causes delays, insufficient information, and decreased quality of shared data. [1]

Factor 8: The size of the team has an impact on how well RIS tasks are completed; smaller teams sometimes have jobs that overlap, while larger teams need more coordination to acquire data, which makes it difficult to share information efficiently. [1]

Factor 9: The motivation and understanding of the usefulness of reporting skills in real-world cybersecurity scenarios are undermined by a hazy perspective of the advantages of information-sharing abilities outside of CDX events. [1]

The effectiveness of information sharing in cybersecurity defense can be improved by addressing these factors, such as prioritizing RIS tasks, fostering a common language, offering training on data exchange standards and information-sharing platforms, and outlining the advantages of information-sharing abilities.

Conclusion and Future Work

The study’s conclusions highlight the difficulties cybersecurity experts confront when exchanging information during CDX incidents and the requirement for improved information-sharing procedures. The effectiveness of information sharing in cybersecurity defense can be improved by addressing the identified factors, such as prioritizing RIS tasks, fostering a shared vocabulary and understanding, offering training on data exchange standards and information-sharing platforms, and outlining the advantages of these skills.

The development of automated analysis techniques to assess the quality of shared information, the investigation of specialized environments that streamline communication channels and CDX platforms for better information exchange, and further research into the inclusion of information-sharing abilities in cybersecurity curricula are some future research directions.

The study highlights the need for a positive attitude toward reporting and information sharing among cybersecurity specialists and emphasizes the need of efficient information sharing in cybersecurity defense. The cybersecurity community may improve collaboration, reaction capabilities, and overall resilience in the face of emerging threats by addressing the stated obstacles and encouraging a culture of information sharing.

References


