Automatic Analysis Tooling in Cybersecurity (Blog Post)

Hassan Alshehri

12/3/2023

Safeguarding an organization's information systems or digital infrastructure in the modern era requires a robust integrated plan that regularly assesses risk susceptibilities in internal and external environments and presents the outcomes in simplified forms. As such, manual processes are increasingly becoming ineffective in analyzing cybersecurity risks, suggesting the need for automated risk analysis tools to facilitate real-time identification, evaluation, and management of information systems' risks. The complexity and amount of data decision-makers should analyze have also increased considerably, making automation a necessity. Against this background, the present study investigated the concept of automated risk assessment tooling in cyber security to shed light on how they can be implemented, their features, advantages, challenges/limitations, and the projected future trends. A large health system in Michigan was used as the case study. The organization's failure to refine third-party access and risk management program attracted significant fines and penalties, suggesting the need for a health information privacy and security risk management program that can automatically detect, prevent, or mitigate a cybersecurity threat.

Since the study was more analytical than implementation-based, it used both primary and secondary data collection tools to fulfill its objectives. Interviews formed the primary data collection method used, whereby the views of cybersecurity experts and managers of companies that have implemented security risk management systems in their organizations were sought. Their responses helped in assessing the advantages and challenges/limitations of automating risk analysis tools. A thematic analysis was used to analyze the data obtained. Secondary data collection involved a review of available literature regarding the topic to understand the problem's background, as well as the meaning and implications of automated risk analysis

tooling. Online databases, such as Google Scholar, were used to retrieve credible and up-to-date sources concerning the subject topic.

Findings obtained indicate that risk analysis tools help organizations determine their cybersecurity status by providing relevant information regarding potential risks, threat impacts, and associated costs. Its benefits include the following:

- Minimizing human errors and biases.
- Improving accuracy and efficiency.
- Cost-effectiveness.
- Facilitating informed decision-making.

This finding suggests that having an automated risk analysis tool can help the organization monitor its systems in real-time and scan for susceptibilities swiftly to mitigate threats before they cause substantial damage. The accuracy and efficiency of its decision-making processes can also be improved because human errors would be minimized. Furthermore, automation reduces operational costs by increasing efficiency and reducing the number of employees needed to complete a task.

Despite these benefits, several downsides were also established, including the following:

- Possibility of these tools giving false positives.
- Misinforming the decision-makers and directing their attention to non-existent risks.
- Lack of flexibility associated with a human being and less proactivity.
- Need for regular updates to deal with emerging threats.

In conclusion, it has been established that the demand for innovative solutions that can automatically detect risks and take the necessary measures to prevent or mitigate them has increased considerably in the recent past due to heightened concerns about the evolving threats to

information systems and networks. The hospital in Michigan can benefit from automatic risk analysis tools through improved accuracy and efficiency, reduced human errors and biases, cost-effectiveness, and facilitating informed decision-making. However, regular updates would be needed to ensure that the tools are able to deal with emerging threats. The few drawbacks identified indicate the need for further studies to investigate the various ways in which the effectiveness of these tools can be improved and how the latest technologies, such as artificial intelligence and machine learning, can be exploited.