Report

Name: Md Sayem Mottakee
ID: 21301080

Paper Title: Integrated Network and Security Operation Center: A Systematic Analysis
Paper Link: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9729852

1 Summary

1.1 Motivation

The motivation behind this paper is to thoroughly examine the current state of the design of integrated Network Operation Centers (NOCs) and Security Operation Centers (SOCs). Furthermore, this paper seems to be focused on addressing the growing complexity of cybersecurity threats and the need for an improved integrated approach to network and security activities. The purpose of the hypothesis is to explore the advantages and disadvantages of combining NOCs and SOCs to improve the security level of organizations.

1.2 Contribution

The paper goes into detail about the integrated NOCs and SOCs architecture. The pros and cons of merging NOCs and SOCs within organization sectors are clearly and thoroughly looked at in this study. To help organizations combine their NOC and SOC, this paper looks at related material and pulls together the most important ideas. This research talks about interaction design, what it does, what you should think about when using it, and its limitations or areas to improve. This is especially helpful for organizations that are thinking about or are already integrating.

1.3 Methodology

To perform this analysis, they followed a few crucial steps:
Firstly, the researchers made specific research questions to guide their study, which will help them to focus on looking for and evaluating crucial aspects of the integration of NOCs and SOCs. They used the PRISMA statement to make their research cautious and genuine.
Secondly, by using a systematic approach, they searched for pieces of information. They chose databases from Scopus, IEEE Xplore, Science Direct, and Google Scholar that contain relevant articles in fields such as engineering, computer science, and cybersecurity using keywords related to NOCs, and SOCs to find the relevant articles and avoid wasting time on irrelevant sources.
Thirdly, the researchers carefully checked this information, getting rid of any duplicate or unnecessary pieces so that they could only use the best and most reliable sources to make sure that the data from their study was accurate and useful.
Fourthly, the researchers tried to make sense of all the data they had collected. They try to discover patterns, trends, and key information about how to connect Network Operation Centers (NOCs) and Security Operation Centers (SOCs). After putting all the pieces of knowledge together, they were able to conclude, find advantages, and disadvantages, and suggest what should be done.

1.4 Conclusion

In conclusion, this paper shows that NOCs and SOCs should collaborate to improve corporate cybersecurity. The researchers discussed about the benefits and areas to improve by combining data analyses and examining significant ideas, challenges, and prospects. Integrating NOCs and SOCs is crucial for protecting from cyberattacks, according to data. We need coordination, standardization, and automation to solve tool integration and automation issues to improve SOC operations.

2 Limitations

2.1 First Limitation

Tool Integration Challenges: The paper addresses the crucial challenge of integrating the tools that are used in SOCs. The majority of the challenges related to obtaining flawless operation of integrated SOCs result from the need to use unique tools for security activities. While different goods may not be able to work together or follow the same standards, this can make integration more difficult and waste time and security. To ease these worries and make the merging process more efficient, the study suggests using standardized and interoperable toolkits that can work with other programs.

2.2 Second Limitation

Insufficient Automation: Another important challenge that is brought up in the study is that SOC processes are not automated enough. Doing things like monitoring networks, threat scanning, and attack response manually can take longer, make errors, and waste time. The study suggests that not having automation makes it harder to scale and improve SOC activities, especially when there are large volumes of security alerts and incidents. To solve this problem, the researchers suggest investing more in automation technologies that can improve overall operational efficiency, speed up response times, and make SOC processes work better.

3 Synthesis

The flaws of this paper reveal new uses and directions for cybersecurity and also show how difficult it is to integrate NOCs and SOCs. Showing these limitations gives developers to choice for improving their cybersecurity and stability. By solving problems of tool integration, standardized and compatible tool sets can be used for clearer and more effective SOC systems to find and reduce cyber attacks. Standardized tools make it easier to integrate technology and share information between security professionals, automation tools make it easier to respond to attacks, reduce errors made by people, and free up security experts to study threats and come up with plans. Lastly, network and security teams need to work together to connect NOCs and SOCs. This method of working together makes it easier to respond to incidents and share responsibility for business safety. In conclusion, standardized tools, automation, and working together give organizations the confidence they need to handle modern threats. This will strengthen cybersecurity and inspire new security operations.