Name: **ATHARVA ASHUTOSH DESHPANDE**

Paper Title: **AN ADAPTABLE APPROACH FOR SUCCESSFUL SIEM ADOPTION IN COMPANIES**

1. Describe, in your own words, the premise of the paper.
   ➔ The premise of the paper is to address the need for a standardized approach to implement Security Information and Event Management (SIEM) systems in corporations amidst increasing cyber threats.

2. What was this paper's contribution to the field of cybersecurity? What problem did this paper seek to solve?
   ➔ This paper contributed to cybersecurity by addressing the gaps in existing process models for implementing SIEM systems, such as the absence of key phases and the lack of neutrality in vendor-provided models. It also aimed to solve these problems by developing a methodology for implementing SIEM systems in corporate contexts, including evaluation, deployment, and operational phases.

3. What are the weaknesses of the paper, and how could they have been better addressed by the author(s)?
   ➔ The paper's weaknesses lie in its lack of comparison with existing models, limited discussion on the model's adaptability to diverse contexts, and insufficient transparency regarding the validation methodology. To improve, the authors could have conducted comparative analyses, discussed broader applicability, and incorporated feedback from a wider range of stakeholders, thereby strengthening the proposed procedure model's reliability and usefulness.

4. In what ways could this paper be extended on in future research efforts?
   ➔ In future research efforts, the paper could be extended by exploring the integration of automation and orchestration capabilities into SIEM systems to streamline incident response processes and improve overall security posture. Moreover, developing techniques to effectively integrate external threat intelligence feeds into SIEM systems to enhance threat detection and response capabilities based on real-time and contextualized information would be part of the future work.

5. If you were to redesign this, what would you add or redo to enhance this research?
   ➔ To enhance this research, I would suggest a few additions and revisions that include a discussion section that would speak about the long-term impact and sustainability of the developed procedure model. Further I would emphasize the iterative nature of the DSR approach by incorporating feedback from validation activities into subsequent iterations of the procedure model, fostering continuous improvement and refinement.

6. Is there anything that was unclear about this paper that you would have liked either more information or some clarity on?
   ➔ The paper provided a detailed overview of the evaluation, deployment, and operation phases of implementing a SIEM system. However, there were a few aspects that could benefit from more information or clarity which include clarifying the criteria used to conduct stakeholder analysis. More information on specific operational activities, such as incident management, log monitoring, system maintenance, and corresponding documentation would have provided a clearer understanding of how the SIEM system is managed and maintained post-implementation.