Name: **ATHARVA ASHUTOSH DESHPANDE**

Paper Title: **Cyber Security Operations Centre: Security Monitoring for protecting Business and supporting Cyber Defense Strategy**

1. Describe, in your own words, the premise of the paper.
   ➔ The premise of the paper is to outline the significance of a Cyber Security Operations Centre (CSOC) as a crucial business control for safeguarding ICT systems and supporting an organization's Cyber Defense Strategy. It proposes a comprehensive CSOC framework encompassing key components such as Log Collection, Analysis, Incident Response, Reporting, Personnel, and Continuous Monitoring.

2. What was this paper's contribution to the field of cybersecurity? What problem did this paper seek to solve?
   ➔ The main contribution of the paper towards cybersecurity is its comprehensive exploration of the importance of Cyber Security Operations Centers (CSOCs) in mitigating the escalating risks posed by cyberattacks in today's expansive digital landscape. The authors aimed to address the pressing need for organizations to establish a robust CSOC framework to effectively protect critical assets, respond swiftly to incidents, and ensure ongoing business continuity in the face of evolving cyber threats.

3. What are the weaknesses of the paper, and how could they have been better addressed by the author(s)?
   ➔ The weaknesses of the paper include a lack of empirical evidence or case studies to support the assertions made about the effectiveness of CSOCs and the proposed framework. To address these weaknesses, the authors could incorporate real-world examples of CSOC implementations, conduct surveys or interviews with practitioners to gather insights on challenges and best practices, and provide a more nuanced discussion on regulatory requirements impacting CSOC operations.

4. In what ways could this paper be extended on in future research efforts?
   ➔ For future work, the paper could be extended by conducting empirical studies to validate the proposed CSOC framework's effectiveness in diverse organizational contexts. Additionally, exploring emerging technologies such as artificial intelligence and machine learning for enhancing CSOC capabilities could be a valuable avenue for research.

5. If you were to redesign this, what would you add or redo to enhance this research?
   ➔ To enhance this research, I would add empirical evidence through case studies or real-world data to validate the effectiveness of CSOC frameworks in mitigating cyber threats. Furthermore, I would have included a comparative analysis of CSOC and SOAR. Finally, I would have explained the relevance and impact of external threat intelligence in a CSOC framework.

6. Is there anything that was unclear about this paper that you would have liked either more information or some clarity on?
   ➔ While the paper provided a comprehensive overview of the importance of CSOCs and the strategies that it would work on, it would have been better had the authors shared some insights regarding threat intelligence and roles of different personnel in the CSOC. Additionally, I would have liked to read more about particular software/tools that could be used. Finally, the paper could have included a section explaining the significance of threat escalation and ticket creation as a part of their framework. I would have liked to know if the CSOC was proposed considering the guidelines of NIST.