Name: **ATHARVA ASHUTOSH DESHPANDE**

Paper Title: **A Survey on Threat Hunting in Enterprise Networks**

1. Describe, in your own words, the premise of the paper.
   - ➔ The premise of the paper is to address the escalating complexity of cyber threats, emphasizing the need for proactive defense strategies, particularly threat hunting, to counter advanced persistent threats. It categorizes existing threat hunting techniques, discusses standardization efforts, and identifies research gaps for improving cyber defense measures.

2. What was this paper's contribution to the field of cybersecurity? What problem did this paper seek to solve?
   - ➔ The paper contributes to the field of cybersecurity by providing a comprehensive survey and a detailed component-based architecture of threat hunting. It addresses the problem of evolving cyber threats by examining current state-of-the-art solutions in enterprise networks. Furthermore, the paper aimed to address the lack of in-depth studies and standardization efforts in threat hunting, and offering insights into methodologies, components, and open research challenges to enhance cybersecurity practices.

3. What are the weaknesses of the paper, and how could they have been better addressed by the author(s)?
   - ➔ The paper is weakened by the lack of empirical validation or experimental results to support the effectiveness of the proposed unified top-down architecture for threat hunting. Including empirical evidence or case studies demonstrating the implementation and performance of the architecture in real-world scenarios would enhance the credibility and applicability of the proposed framework. Additionally, the authors could have incorporated feedback from practitioners or experts in the field to validate the relevance and practicality of their proposed architecture and recommendations.

4. In what ways could this paper be extended on in future research efforts?
   - ➔ Future research efforts could be extended by conducting empirical studies or case studies to evaluate the effectiveness and real-world applicability of the proposed threat hunting architecture and methodologies in diverse Enterprise network environments. Additionally, exploring the integration of emerging technologies such as blockchain or quantum computing into threat hunting frameworks could offer novel approaches for enhancing cybersecurity defenses.

5. If you were to redesign this, what would you add or redo to enhance this research?
   - ➔ To enhance the research, I would have incorporated practical case studies, defined clear evaluation metrics, and thoroughly discussed the limitations of threat hunting techniques. Furthermore, exploring the integration of emerging technologies and

addressing standardization and collaborative efforts would enhance the overall practicality and effectiveness of threat hunting in Enterprise networks.

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 systematic and detailed component-based architecture of threat hunting. It would have been helpful to have more clarification on how the proposed solutions addressed the scalability and performance challenges associated with automated hypothesis generation and data representation. Additionally, a deeper discussion on the potential trade-offs and limitations of integrating AI-based tools for threat hunting, as well as the practical implementation considerations for integration with (X)SOAR systems, would provide a clearer understanding of the research findings.