Review Form 1.7

Journal Name:	**Journal of Engineering Research and Reports**
Manuscript Number:	**Ms_JERR_118983**
Title of the Manuscript:	**Building a Security Operations Center With Incident Response Capabilities**
Type of the Article	

General guideline for Peer Review process:

This journal's peer review policy states that **NO** manuscript should be rejected only on the basis of '**lack of Novelty'**, provided the manuscript is scientifically robust and technically sound.
To know the complete guideline for Peer Review process, reviewers are requested to visit this link:

(https://www.journaljerr.com/index.php/JERR/editorial-policy)

Review Form 1.7

PART 1: Review Comments

	Reviewer's comment	**Author's comment** *(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Compulsory REVISION comments **1. Is the manuscript important for scientific community?** (Please write few sentences on this manuscript) **2. Is the title of the article suitable?** (If not please suggest an alternative title) **3. Is the abstract of the article comprehensive?** **4. Are subsections and structure of the manuscript appropriate?** **5. Do you think the manuscript is scientifically correct?** **6. Are the references sufficient and recent? If you have suggestion of additional references, please mention in the review form.** **(Apart from above mentioned 6 points, reviewers are free to provide additional suggestions/comments)**	**1:** The manuscript is significant for the scientific community as it addresses the critical and growing need for robust cybersecurity measures in organizations of all sizes. It presents a scalable Security Operations Center (SOC) architecture using low-cost, open-source tools, making advanced cybersecurity accessible to small and medium-sized enterprises (SMEs). The detailed implementation and validation of this architecture, using tools like Wazuh, TheHive, and Suricata, provide a practical framework for detecting and responding to common cyber threats. This research contributes valuable insights and practical solutions to the field of cybersecurity, promoting the adoption 2: Title is week it should be like ""Building a Scalable Security Operations Center for Small and Medium-Sized Enterprises Using Open-Source Tools" 3: Yes 4:yes but in research methodology provide methodology in detail 5: Yes, the manuscript appears to be scientifically correct. It proposes a scalable SOC architecture using low-cost, open-source tools and validates its implementation against various cybersecurity scenarios. The detection and response results are documented, showing that the proposed system effectively identifies and responds to different types of cyber threats. The architecture's comparison with existing literature demonstrates its unique contributions, such as standalone threat intelligence and compliance monitoring components, enhancing its scientific rigor and practical relevance . **6: Week References are use author can add more references such as :** Papalkar, R. R., & Alvi, A. S. (2023). Review of unknown attack detection with deep learning techniques. In Artificial Intelligence, Blockchain, Computing and Security Volume 1 (pp. 989-997). CRC Press. Papalkar, R. R., & Alvi, A. S. (2022). Analysis of defense techniques for DDos attacks in IoT–A review. ECS Transactions, 107(1), 3061.	
Minor REVISION comments **1. Is language/English quality of the article suitable for scholarly communications?**	good	
Optional/General comments	Accept with revision as per suggested above	

Review Form 1.7

PART 2:

	Reviewer's comment	**Author's comment** *(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Are there ethical issues in this manuscript?	*(If yes, Kindly please write down the ethical issues here in details)*	

Reviewer Details:

Name:	**Rahul Rajendra Papalkar**
Department, University & Country	**VIshwakarma University, India**