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	**It contributes to the field of cybersecurity by proposing and testing a cost-effective SOC architecture designed for small and medium-sized businesses.**

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)**	Yes, the manuscript is important. It provides a cost-effective SOC architecture using open-source tools, helping organizations enhance their cybersecurity against increasing cyber-attacks. Yes Yes Yes Yes Yes	
Minor REVISION comments **1. Is language/English quality of the article suitable for scholarly communications?**	Yes	
Optional/General comments	Areas for Improvement: 1. Expand Testing Scenarios: Include more diverse cyber-attack scenarios to thoroughly test the SOC's capabilities. 2. Quantitative Metrics: Provide detailed metrics like detection times and false positive rates to better evaluate the system's performance. 3. Implementation Clarity: Add step-by-step instructions and visual aids to make the SOC setup process easier to understand and replicate.	

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:	**Arul Selvam P**
Department, University & Country	**Hindusthan College of Engineering and Technology, India**