## 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 | New Architecture for Security Operations / A Novel Study |

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 )

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<br><br>Is the manuscript important for scientific community?<br>(Please write few sentences on this manuscript)<br><br>Is the title of the article suitable?<br>(If not please suggest an alternative title)<br><br>Is the abstract of the article comprehensive?<br><br>Are subsections and structure of the manuscript appropriate?<br><br>Do you think the manuscript is scientifically correct?<br><br>Are the references sufficient and recent? If you have suggestion of additional references, please mention in the review form.<br><br>(Apart from above mentioned 6 points, reviewers are free to provide additional suggestions/comments) | Organizations are empowered to identify and avert possible attacks through the use of efficient detection systems. So it is important to develop such tools nowadays due to the growth of increasing users in the cyber world.<br><br>The tile says "Building security operations" the abstract says "proposes a SOC architecture with various components", The tile can be revisited.<br><br>Yes<br><br>Certain sub sections needs to be modified. For example the proposed architecture has to come under materials and methods sections .Only the experimental results to be findings and discussions. The subsections need to be rearranged.<br><br>Yes, But the scientific findings needs to be clearly stated<br><br>Few papers provided in the references are not cited in the paper<br><br>Check the word "preceding sections" can be used to mention the following sections<br>Image resolution has to be improved<br>The comparison of proposed with the existing architecture is not provided<br>Results sections needs to be revisited.<br>Section and sub sections to be properly framed<br>How to estimate the performance of the suggested architecture?<br>Dataset used for the research is not mentioned?<br>Clear explanation is needed for incident response capabilities | |

## Review Form 1.7

| | | |
|---|---|---|
| Minor REVISION comments<br><br>Is language/English quality of the article suitable for scholarly communications? | Check for Grammar mistakes and spelling mistakes | |
| Optional/General comments | The paper suggests an architecture for the detection of cyber attacks<br>All acronyms to be expanded For example SOC<br>Abstract is clearly stated<br>Literature review section ,the papers are not cited in the given order | |

**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: | **M.Sakthivanitha** |
| Department, University & Country | **Vels Institute of Science and Technology & Advanced Studies (VISTAS), India** |