**Peer – Response**

The article clearly outlines some of the key benefits of deploying SOC/SIEM in network security. By having a dedicated SOC/SIEM in network security system, businesses are able to continuously monitor the traffic flowing across their networks. This way, they have a better visibility of the threats to which their networks could be exposed to. The article however fails to show the differences between SIEM and SOC systems. SIEM is primarily used to collect aggregate log information. SOC on the other hand is a combination of people, processes, and technologies picked from the analysis done on SIEM. The two complement each other with SIEM doing the analysis work and SOC responding to any alerts (Akinrolabu, Agrafiotis, & Erola, 2018). It is also worth noting that SOC/SIEM systems have developed a highly advanced complex analysis method based on Artificial Intelligence (AI) and Machine Learning (ML). This helps to determine the aspects of the data that need further investigation and those that require immediate attention (González-Granadillo, González-Zarzosa, & Diaz, 2021).

I support the views expressed in the article. The application of SOC/SIEM security in business is quite beneficial mainly because it is cost effective, has a better collaboration, and offers continuous monitoring of the networks. SOC/SIEM also reduces the amount of time taken by the traditional systems to identify various threats and act on them (Mohanur Jagadeesan, 2020; Dietz, Vielberth, & Pernul, 2020). Consequently, the extent of the possible damage that could be incurred is also reduced.

References

Akinrolabu, O., Agrafiotis, I., & Erola, A. (2018, August). The challenge of detecting sophisticated attacks: Insights from SOC Analysts. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (pp. 1-9).

Dietz, M., Vielberth, M., & Pernul, G. (2020, August). Integrating digital twin security simulations in the security operations center. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-9).

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (siem): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759.

Mohanur Jagadeesan, P. R. (2020). *A Framework Design to Improve and Evaluate the Performance of Security Operation Center (SOC)* (Doctoral dissertation, Dublin, National College of Ireland).