As Wang (2023) notes, there are challenges to analysing logs due to the complex ways in which they can be written. One way to overcome this is by adopting a semantic approach to log analysis. This allows an interpretation of the context in which invents occur (Ekelhart, 2018), enhancing situational awareness of what may be happening in a system.

In my opinion, a more meaningful and consistent logging structure eliminates the risk of missed incidents and eases the burden of analysis after a significant event. By providing a context in which events have happened, the forensic picture built by logging is more accurate and less error-prone, with less reliance on human intuition.

References

Ekelhart, A. et al. (2018) Taming the logs - Vocabularies for semantic security analysis *Procedia computer science* 137(2019): 109–119. Available from: <https://www-sciencedirect-com.uniessexlib.idm.oclc.org/science/article/pii/S1877050918316156?via%3Dihub> [Accessed 29 August 2024].

Wang, W. et al. (2023) DeepUserLog: Deep Anomaly Detection on User Log Using Semantic Analysis and Key-Value Data *2023 IEEE 34th International Symposium on Software Reliability Engineering (ISSRE)*. IEEE. pp. 172–182. DOI: 10.1109/ISSRE59848.2023.00046