In a world of ever-increasing cyber security threats (Trellix, 2023), logging has become essential for effective security monitoring. But in the wake of Log4Shell vulnerability (Berger, 2023), the real question becomes "if logging makes your system to be more vulnerable, is it still worth it?".

Logging is an essential part of a broader term called telemetry - which involves the automated collection and transmission of data for monitoring and analysis. Telemetry is useful in knowing what is happening within your system (Riedesel, 2021). It is even most useful in security for incidents tracking and investigation.

A semantic approach to security monitoring has been proposed, which aims to lift raw log data and model their context (Ekelharta, 2019). The benefit of this approach is that it links events to background knowledge, model causal relationships and provide context-specific interpretation. The semantic approach if well implemented can provide better threat detection and incident response.

In summary, while the log4Shell vulnerability might present the weak side of logging, the benefits of logging still outweighs the drawback. Organizations can still use logging as a powerful tool in their cybersecurity arsenal by embracing the semantic approach.

REFERENCES:

Trellix (2022). *2023 Threat Predictions Report*. Available at: **https://www.trellix.com/2023-threat-predictions/** [Accessed 19 November 2024].

Berger, A.(2023). *What is Log4Shell? The Log4j vulnerability explained (and what to do about it)*. Available at: **https://www.dynatrace.com/news/blog/what-is-log4shell/** [Accessed 19 November 2024].

Riedesel, J. (2021) *Software telemetry : reliable logging and monitoring*. Shelter Island, New York: Manning Publications Co.

Ekelhart, A., Kiesling, E. and Kurniawan, K. (2019). Taming the logs-Vocabularies for semantic security analysis. *Procedia Computer Science*, *137*, pp.109-119.