


# Summary Post

◀ Initial Post

Display replies in nested form

Settings ▾



Summary Post

by [Lauren Pechey](#) - Saturday, 19 July 2025, 7:06 PM

### Balancing the Benefits and Risks of Security Logging

Across our posts, it's clear we all agree that logging is vital for network security monitoring, threat detection, and compliance. As Berger (2023) and Nyangaresi et al. (2024) explain, robust logging gives security teams the visibility needed to detect anomalies and respond effectively. Lauren highlighted how logs support forensic investigations and legal processes (Ahmed et al., 2020), while Victor reminded us that logging must be carefully controlled to avoid becoming an attack vector itself.

Cases like the Uber breach and exposed Elasticsearch clusters show how excessive or mismanaged logging can leak credentials or sensitive data. Best practice is not just about collecting as much data as possible, but doing so strategically: encrypting logs, excluding sensitive information by default, enforcing strict access controls, and using Write-Once-Read-Many storage to preserve integrity and prevent tampering.

Altogether, our discussion underlines that secure, minimalistic, and governed logging strikes the best balance — ensuring logs remain a powerful security asset instead of a hidden liability.

### References

Ahmed, F., Jahangir, U., Rahim, H., Ali, K., & Agha, D.-e.-S. (2020) 'Centralized log management using Elasticsearch, Logstash and Kibana', *2020 International Conference on Information Science and Communication Technology (ICISCT)*, Karachi, Pakistan, 27–28 November. IEEE, pp. 1–7.

Berger, J. (2023) *What is Log4Shell? The Log4j vulnerability explained (and what to do about it)*, Dynatrace News. Available at: <https://www.dynatrace.com/news/blog/what-is-log4shell/> (Accessed: 6 July 2025).

Li, H., Shang, W., Adams, B., Sayagh, W., & Hassan, A. (2021) 'A qualitative study of the benefits and costs of logging from developers' perspectives', *IEEE Transactions on Software Engineering*, 47(12), pp. 2858–2873. <https://doi.org/10.1109/TSE.2020.2970422>

Nyangaresi, V. O., Alsolami, E., & Ahmad, M. (2024) 'Trust-enabled energy efficient protocol for secure remote sensing in supply chain management', *IEEE Access*, 12(1), pp. 113553–113564. <https://doi.org/10.1109/ACCESS.2024.344261>

Maximum rating: -

[Permalink](#) [Edit](#) [Delete](#) [Reply](#)

◀ Initial Post

You are logged in as Lauren Pechey (Log out)

[Policies](#)

Powered by Moodle





Chat to us!