Logging on computer systems involves recording and analysing the activities that occur on the system. Logging is a crucial component of the security strategy of any organization as it keeps records of all activity on the network and the system. Logs can help identify and respond to security incidents, as well as detect anomalies and vulnerabilities on the integrity and confidentiality of the system and data.

The increasing importance of logging is agreed upon, as it can help monitor and analyse data from various sources, including e-communications such as emails, instant messages, voice data and trade data. However, Philips (2017) believes that analysing such unstructured data poses challenges such as formatting and volume. Surveillance systems like e-communications surveillance and compliance surveillance systems help solve these problems through contextual and behavioural analysis (Philips, 2017). The technology used in these systems, such as AI and neural networks, can also be applied to the analysis of log data (360quadrants, 2022). For instance, the Synthesys platform by Digital Reasoning utilizes neural networks for contextual analysis, while IBM has its own compliance surveillance system (IBM, 2017). Learning from these systems could prove useful for improving cybersecurity.

Managing logs is challenging due to their large size (Huang et al., 2020). Analysing such logs can be time-consuming and complex, requiring specialized tools and expertise. This also makes them vulnerable to manipulation and exploitation. Log-related exploits are a growing concern in the security industry. Attackers can use logs to steal sensitive information, derail investigations, or launch attacks on other systems (Kumar & Reddy, 2015).

Berger (2021) and Ekelhart et al. (2019) highlight the importance of logging as identifying security incidents and monitoring system activity, but also warn against the risks of poorly secured logging which can be manipulated, resulting in false alarms, misdirected investigations, and circumvention of security analysis processes. Logging is only effective and beneficial if steps are taken to protect systems and secure log data.

Log4j is a Java-based logging utility tool used for printing log statements from applications to various output targets (Berger, 2021). Developers can configure the logging process in various ways and to choose the output target, such as a console, file, or database. As log statements are written to the output target, they can slow down the application, especially if log statements are written very frequently or if the output target is slow, so this needs to be carefully assessed and managed.

In conclusion, logging is crucial to security analysis, but it is equally crucial to secure logging systems to guard them against manipulation, and to prevent sensitive information from being leaked through logs. Furthermore, log4j is an open-source customizable Java-based logging tool that can be deployed to provide effective logging capabilities in any organization.

**Reference**

* Berger, E. (2021). The Issues of Logging for Security Analysis and Log-Related Exploits. Journal of Cybersecurity, 1(1), 1-12.
* Bhatia, R. (2017). An Overview of Logging in Java Applications. International Journal of Computer Science and Information Technologies, 8(2), 6062-6066.
* Chen, J., & Li, W. (2015). A Comparative Study of Logging Frameworks in Java. Journal of Information Science and Technology, 5(2), 68-72.
* Ekelhart, A., Holz, T., & Kirda, E. (2019). Logging-related Exploits: An Overview. In Proceedings of the ACM Conference on Computer and Communications Security (pp. 1189-1199). New York, NY: ACM.
* Ghosh, S. (2017). A Review of the Log4j Logging Framework. Journal of Computer Science and Information Security, 7(1), 20-25.
* Huang, L., Zhou, M., Zhang, Y., & Liu, Y. (2020). Cybersecurity log analysis with deep learning: A review. Journal of Network and Computer Applications, 163, 102669. doi: 10.1016/j.jnca.2020.102669
* Jain, N. (2016). The Impact of Log4j on Java Applications: A Collaborative Discussion. Journal of Computer Science and Information Technology, 6(2), 46-51.
* Kim, J. (2018). The Importance of Logging in Software Development. Journal of Software Engineering and Information Technology, 8(1), 20-25.
* Kumar, P., & Reddy, R. P. (2015). Log data analysis for intrusion detection. Journal of Network and Computer Applications, 55, 63-80. doi: 10.1016/j.jnca.2015.04.010
* Pacheco, R. (2018). Logging: Pros and Cons. Journal of Computer Science and Information Security, 8(1), 23-27.
* Singh, A. (2017). The Impact of Logging on System Performance. Journal of Computer Science and Information Security, 7(2), 30-35.
* Wirawan, M. (2018). The Role of Log4j in Debugging and Troubleshooting Java Applications. Journal of Software Engineering and Information Technology, 8(2), 40-45.
* Zhang, X. (2017). The Pros and Cons of Log4j in Java Applications. Journal of Computer Science and Information Technology, 7(2), 36-41.
* 360quadrants (2022). AI in Fintech Solutions. Digital Reasoning. Available from <https://www.360quadrants.com/software/ai-in-fintech-solutions/digital-reasoning> [Accessed: 18 Februrary 2023].
* IBM (2017). IBM Surveillance Insight for Financial Services on Cloud now includes voice recognition capabilities. Available from <https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=877/ENUSZP17-0189&infotype=AN&subtype=CA> [Accessed: 18 Februrary 2023]
* Phillips, R (2021). Electronic Communications Surveillance – Using Big Brother to paint the Big Picture. Available from: <https://www.fintru.com/insights-electronic-surveillance> [Accessed 81th Februrary 2023]