In my initial post, I discussed the two security technologies, Data Loss Prevention (DLP) and Security Incident and Event Management System (SIEMS).

Thank you, Kwok, Pearce, and Uvaraj, for your responses.

I agree with Uvaraj that DLP is an important component of every organisation as data is the greatest asset every organisation has. As rightfully stated, “Everyone in an organisation has a role to play ensuring the security of their data.” It is vital for everyone in the organisation to play their role as there are causes of data leaks that can occur in an organisation. These causes may include insider threats, extrusion by attackers, and unintentional or negligent data exposure. (What is Data Loss Prevention (DLP) | Data Leakage Mitigation | Imperva, 2022).

Thank you, Pearce, for your contribution and for identifying that DLP is categorised into the following groups: Network DLP, Endpoint DLP, and Cloud DLP. In addition to these groups, I would like to add Email DLP as part of the DLP software tools. Email DLP is used to monitor and filter emails between users within an organisation and external users based on a certain condition. (4 types of Data Loss Prevention (DLP) — Tricent, 2022).

Thank you, Kwok, for your insightful post on Security Incident Management and Event Management Systems (SIEMS) drawback regarding the log correlation. I do agree with you that this is a concern as SIEMS may provide false positives which may be misleading and cause a delay in response time in identifying the actual threat from the logs. Like firewalls require the correct initial configurations for optimum performance, a security incident and event management system also require the initial setup to reach its optimum performance while meeting the requirements of the organisation and the purpose this system has for it in order to identify the potential threats in an effective manner. (Villanueva, 2022)

References:

- Tricent. 2022. *4 types of Data Loss Prevention (DLP) — Tricent*. [online] Available at: <https://www.tricent.com/blog/dlp-types-of-data-loss-prevention> [Accessed 26 April 2022].
- Villanueva, M., 2022. *Pros and Cons of Implementing SIEM*. [online] Itsasap.com. Available at: <https://www.itsasap.com/blog/pros-cons-siem> [Accessed 26 April 2022].
- Learning Center. 2022. *What is Data Loss Prevention (DLP) | Data Leakage Mitigation | Imperva*. [online] Available at: <https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/> [Accessed 26 April 2022].