Collaborative Discussion 2: Peer Response

Response 1:

Dear Amrol,

I appreciate your post. You pointed out that an essential component of log management is the ISO 27001 regulation. Logs are necessary to establish an event chronology and spot patterns inside an organisation's network, as ISMS (2022) noted. Transparent and readily available log information creation is critical to every organisation's ICT strategy.

I share your concern regarding any mistakes that businesses could make when logging in. Ahola (2021) emphasised that 95% of cybersecurity vulnerabilities result from human error, citing IBM research. As noted by Berger (2021), attackers can remotely manipulate a machine by sending text messages to exploit this vulnerability. This vulnerability has received the highest-level severity score of 10 out of 10 from the Apache Software Foundation's Log4j 2 library. This is due to the simplicity with which malevolent attackers can take advantage of it and its potential for broad exploitation. The core elements of the Log4j vulnerability are still present despite ongoing mitigation attempts, and the harm it causes is still being felt.

You also mentioned the potential impact of software vulnerabilities on security. Security Journey (2023) says that to prevent any oversights in security logging and monitoring, Security Journey recommends that all significant security events be logged, log files be securely stored, precautions be taken to avoid unauthorised access or tampering, logs be regularly reviewed and analysed, real-time monitoring systems be established, a comprehensive incident response plan be created, and continuous improvement be pursued by reviewing past incidents and responding to emerging threats.

Cobb (2021) emphasises that log files are records of IT system occurrences that provide security teams with a crucial audit trail. They assist companies in recognising patterns in their operations, conducting general audits, and complying with rules and guidelines. However, logging can be challenging for large businesses that produce hundreds of gigabytes of data. Therefore, monitoring, assessing, and reacting to logs is essential to prevent aggressive and unlawful behaviour.

References:

- ISMS (2022). *ISO 27002:2022 – Control 8.15 – Logging*. [online] Available at: https://www.isms.online/iso-27002/control-8-15-logging/.
- Ahola, M. (2021). *The Role of Human Error in Successful Cyber Security Breaches*. [online] blog.usecure.io. Available at: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches.
- Berger, A. (2021). *What is Log4Shell? The Log4j vulnerability explained (and what to do about it)*. [online] Dynatrace news. Available at: https://www.dynatrace.com/news/blog/what-is-log4shell/.
- Security Journey (2023). *OWASP Top 10 Security Logging and Monitoring Failures Explained*. [online] Available at: https://www.securityjourney.com/post/owasp-top-10-security-logging-and-monitoring-failures-explained [Accessed 5 Dec. 2023].
- Cobb, M. (2021). *Security log management and logging best practices*. [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/tip/Security-log-management-and-logging-best-practices.

Response 2:

Hi Adesola,

I appreciate your comments about the challenges of managing security in information systems, which have become increasingly complex and vulnerable to security threats. As Ekelhart et al. (2018) pointed out, security analysts must constantly monitor their systems to identify suspicious activities, which involves dealing with high volumes of log data from various sources. However, current automated methods for aggregating and triggering alerts are limited, and manual inspection is still required to establish causal chains between events from different sources.

In this context, Quest Technology Management (2023) highlights the importance of log analytics, which is the process of gathering, analysing, and interpreting log entries generated by software applications, operating systems, and hardware components. Log analytics solutions are specialised software applications that centralise and analyse log data, providing valuable insights through visualisations, alerts, and reports. These solutions are essential for making informed decisions in modern IT environments.

I agree with your observation that we should consider the interdependencies between different platforms and services, as noted by Kosinski (2023). The Log4Shell vulnerability discovered in Log4j versions 2.14.1 and earlier is a critical security threat that enables terrible actors to gain almost complete control over vulnerable systems. Despite Apache's patch release in December 2021, Log4j is still one of the most widely used logging libraries globally. The attack involves an attacker configuring a server to transmit a JNDI lookup command to an application running on Log4j, instructing it to fetch and run the attacker's malicious code.

Finally, I agree with your assessment that advanced, automated, and context-aware log analysis is necessary to address the complexity and scale of modern information systems, as highlighted by Faife (2021). Security teams are currently rushing to patch the Log4Shell vulnerability, which could allow hackers to compromise millions of devices. If exploited, it allows remote code execution, allowing attackers to import malware and compromise machines.

References:

- Ekelhart, A., Kiesling, E. & Kurniawan, K. (2018). Taming the logs - Vocabularies for semantic security analysis. *Procedia Computer Science*, 137, pp.109–119. doi:https://doi.org/10.1016/j.procs.2018.09.011.
- Quest Technology Management (2023). *Harnessing the Power of Log Analytics for Your Business*. [online] Available at: https://questsys.com/ceo-blog/harnessing-the-power-of-log-analytics-for-your-business/ [Accessed 6 Dec. 2023].
- Kosinski, M. (2023). *How to detect and patch a Log4J vulnerability*. [online] IBM Blog. Available at: https://www.ibm.com/blog/how-to-detect-patch-log4j-vulnerability/.
- Faife, C. (2021). *'Extremely bad' vulnerability found in widely used logging system*. [online] The Verge. Available at: https://www.theverge.com/2021/12/10/22828303/log4j-library-vulnerability-log4shell-zero-day-exploit.