**Peer responses – Unit 5**

Hi <STUDENT\_NAME>,  
  
Thank you for your informative post on the rationale behind logging and various related methods and security considerations.  
  
I would suggest leveraging the recommended references and discussions of Berger (2021) and Ekelhart et al. (2018), as well as contextualising your summary of findings to focus on the impact of the security vulnerabilities in Apache Log4j (Microsoft, 2021) and any other open source software used for logging.  
  
Moreover, some of your statements, such as 'With regulations like the GDPR, the UK Financial Conduct Authority or other countries monitoring watchdogs, it would be recommended that sensitive data is not recorded within the logs. Things like names, contact details and account numbers should not be written.', although they are correct, they do not have in-text citations to support them. Please provide them for the reader to build more confidence in such statements and to be able to review the related references and learn further.  
  
I hope this helps.  
  
Best regards,  
Marianne

**References**  
  
Berger (2021) What is Log4Shell? Dynatrace. Accessed on July 7th, 2022, from https://www.dynatrace.com/news/blog/what-is-log4shell/.

Ekelhart, A., Kiesling, E., & Kurniawan, K. (2018) Taming the logs-Vocabularies for semantic security analysis. *Procedia Computer Science*, 137: 109-119.

Microsoft (2021) Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability. Security. Accessed on July 7th, 2022, from [**https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/**](https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/).

Hi <STUDENT\_NAME>,

Thank you for your informative post on logging and its associated security vulnerabilities.  
  
I would suggest leveraging the recommended reference and discussions of Berger (2021) too, as well as providing a brief analysis of the impact of the security vulnerabilities in Apache Log4j (Microsoft, 2021) and any other open source software used for logging.  
  
Two of your statements, i.e., ‘Logging is often necessary to prove compliance and the integrity of governance processes.’ and ‘Last but not least however and as the log4j breach demonstrates, a mechanism which was in place to support logging turned out to be the weakest chain in the link reminding us that security should be considered in all different areas as any point in our systems can offer exploiting opportunities.’, although they are correct, they do not have in-text citations to support them. Please provide them for the reader to build more confidence in such statements and to be able to review the related references and learn further. Furthermore, please provide at least one example to contextualise your statement ‘Logging is often necessary to prove compliance and the integrity of governance processes.’.

I hope this helps.  
  
Best regards,  
Marianne

**References**  
  
Berger (2021) What is Log4Shell? Dynatrace. Accessed on July 7th, 2022, from https://www.dynatrace.com/news/blog/what-is-log4shell/.

Microsoft (2021). Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability. Security. Accessed on July 7th, 2022, from [**https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/**](https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/).