PEER RESPONSES

Hello Iason,

Thanks for your informative post-

I agree that the Logging is required to fulfil compliance and regulatory requirements (like PCI-DSS) in many of the cases. It takes more than six months, on an average, for an enterprise to realize that the environment has been compromised. And it's only the retained logs which are helpful in analyzing the full impact of the breach. Also, the retained logs must be secured, centralized and archived for long term storage as per the requirement.

(Using Logs for Security & Compliance, 2016)

Application logs must be stored and becomes invaluable information for identifying incidents, monitoring and providing information for unusual conditions. It can also be used for audit trails and compliance monitoring.

(OWASP Cheat Sheet Series, N.D)

REFERENCES:

Using Logs for Security & Compliance: (2016)

https://www.rapid7.com/blog/post/2016/02/04/using-logs-for-security-compliance-part-2/

OWASP Cheat Sheet Series(N.D.)

https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

Hello Gokul,

Thanks for your detailed and informative post-

I agree that the logging is required for audit trails, identifying incidents, to fulfil compliance and regulatory requirements.

Retained logs are helpful in assessing the full impact of the breach as it takes a long time for the organization to realize that the environment has been attacked.

(Using Logs for Security & Compliance, 2016)

As you rightly mentioned that the logs come from different sources and in different formats, just to add to that point, the retained logs must be secured / encrypted, centralized and properly integrated. Depending on the compliance requirements, logs should be archived for long term storage.

Integrity & log data availability protection of log data can be done by:

- Limiting privilege access, protection through file encryption
- Data security for log-data in transit – from source to the log servers
- Avoiding logging unwanted sensitive data

(Philip, 2021)

REFERENCES:

1. Using Logs for Security & Compliance: (2016)

https://www.rapid7.com/blog/post/2016/02/04/using-logs-for-security-compliance-part-2/

2. Philip Duff (2021): Managing long term log retention

https://techcommunity.microsoft.com/t5/azure-storage-blog/managing-long-term-log-retention-or-any-business-data/ba-p/2494791