Initial Post

by Ashok Kumar Shanmugam - Monday, 18 July 2022, 5:19 AM
Number of replies: 1

The number and sophistication of cyberattacks are increasing, trying to make security management a herculean task. Security analysts must manage large amounts of inconsistent log data from a variety of sources (such as network devices like firewalls, routers/switches, web & database servers, etc.) in order to keep a focus on the systems they are in control of protecting.

(Ekelhart et al., 2018)

What is log management, and why is it so important?

Security log management involves making, sending, storing, analyzing, and getting rid of security log data while making sure it is private, correct, and available.

The Center for Internet Security lists log management as one of its critical security controls because this process is so important. It's important because if an organisation doesn't collect, store, and analyze yse system events, it leaves itself open to attack. This is also why many laws and standards, like the Federal Information Security Modernization Act, ISO 27001, HIPAA, Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, National Industrial Security Program Operating Manual, and PCI DSS, require log management for compliance and reporting. Logs are also needed to do general audits, set baselines, find operational trends and long-term problems, and perform general audits. (Micheal Cobb 2022).

Eight Security Log Retention Best Practices to Follow

1: Define Audit Categories

2: Monitor Logs

3: Consolidate Records

4: Practice Redundant Data Storage

5: Monitor Known Threats

6: Track Users

7: Evolve Event Monitoring

8: Report Reliably

Hackers are actively scanning networks for log-related vulnerabilities such as Log4j. Apache rated Log4Shell, a software vulnerability in ApacheLog4j 2, a modern Javascript Library for logging warning messages in applications, as critical due to the widespread use of JAVA across IT platforms/applications. (ncse Dec 2021)

Examples of Log4j CVE's - (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832)

References:

1. Ekelhart, A., Kiesling, E. and Kurniawan, K. (2018). Taming the logs - Vocabularies for semantic security analysis. Procedia Computer Science
2. Michael Cobb (2022): What is log management, and why is it so important? **https://www.techtarget.com/searchsecurity/tip/Security-log-management-and-logging-best-practices**
3. Auditboard (Dec 2021) Eight Security Log Retention Best Practices to Follow Available at:**https://www.auditboard.com/blog/security-log-retention-best-practices/**
4. What is log4j? (Dec 2021) Avalable at: **https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know** [Accessed July 16]

Maximum rating: -
PermalinkReplyExport to portfolio

In reply to Ashok Kumar Shanmugam

Re: Initial Post

by Beran Necat - Friday, 22 July 2022, 8:30 AM
Hi Ashok,

You will find this article useful for the discussion of this unit.

Ekelhart, A., Kiesling, E. and Kurniawan, K. (2018). Taming the logs - Vocabularies for semantic security analysis. Procedia Computer Science, 137, pp.109–119. doi:10.1016/j.procs.2018.09.011.
PermalinkShow parentReply

- **◀ Initial Post**
- **Initial Post ▶**