Daftar Pustaka

Afzaal, M., Di Sarno, C., D'Antonio, S., & Romano, L. (2012). An intrusion and fault tolerant forensic storage for a SIEM system. *8th International Conference on Signal Image Technology and Internet Based Systems, SITIS 2012r*, 579–586. https://doi.org/10.1109/SITIS.2012.89

Anastasov, I., & Davcev, D. (2014). SIEM implementation for global and distributed environments. *2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014*. https://doi.org/10.1109/WCCAIS.2014.6916651

ARSYAM, K. (2016). *Implementasi Manajemen Keamanan Jaringan Menggunakan Open Source Security Information Management (Ossim)*. Retrieved from https://repository.telkomuniversity.ac.id/pustaka/121650/implementasi-manajemen-keamanan-jaringan-menggunakan-open-source-security-information-management-ossim-.html

Bachane, I., Adsi, Y. I. K., & Adsi, H. C. (2017). Real time monitoring of security events for forensic purposes in Cloud environments using SIEM. *Proceedings - 2016 3rd International Conference on Systems of Collaboration, SysCo 2016*. https://doi.org/10.1109/SYSCO.2016.7831327

Bedwell, P. (2014). Finding a new approach to SIEM to suit the SME environment. *Network Security*, *2014*(7), 12–16. https://doi.org/10.1016/S1353-4858(14)70070-4

Briffaut, J., Clemente, P., Lalande, J.-F., & Rouzaud-Cornabas, J. (2013). Honeypot forensics for system and network SIEM design. In *Advances in Security Information Management Perceptions and Outcomes* (pp. 181–216). Retrieved from http://hal.archives-ouvertes.fr/hal-00677340/

Bryant, B. D., & Saiedian, H. (2017). A novel kill-chain framework for remote security log analysis with SIEM software. *Computers and Security*, *67*, 198–210. https://doi.org/10.1016/j.cose.2017.03.003

Cherdantseva, Y., & Hilton, J. (2013). Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. *... Dimensions of IS Administrator. IGI Global …*, 1–45. https://doi.org/10.4018/978-1-4666-4526-4.ch010

Fernandes, J. J. (2016). *SIEM : Your Complete IT Security Arsenal*.

Gartner. (2016). Security Information and Event Management (SIEM) - Gartner IT Glossary. Retrieved from IT Glossary website: http://www.gartner.com/it-glossary/security-information-and-event-management-siem/

Gartner. (2016). Security Information and Event Management (SIEM) - Gartner IT Glossary. *IT Glossary*. Retrieved from http://www.gartner.com/it-glossary/security-information-and-event-management-siem/

Hadiansyah, C., & Iskandar Ikbal. (2017). *Pembangunan Server Security Information Management Untuk Monitoring Keamanan Di Server Diskominfo Provinsi Jawa Barat*.

Irfan, M., Abbas, H., & Iqbal, W. (2015). Feasibility analysis for incorporating/deploying SIEM for forensics evidence collection in cloud environment. *2015 IEEE/ACIS 14th International Conference on Computer and Information Science, ICIS 2015 - Proceedings*, 15–21. https://doi.org/10.1109/ICIS.2015.7166563

ISACA. (2006). *Information Systems Audit and Control Association*.

ISO/IEC. (2009). *ISO/IEC 27000:2009 (E). Information technology - Security techniques - Information security management systems - Overview and vocabulary*.

McAfee, Beek, C., Frosst, D., Greve, P., Gund, Y., Moreno, F., … Weafer, V. (2017). *McAfee Labs Threats Report April 2017*. Santa Clara.

netwrix. (2016). *SIEM Efficiency Survey Report 2016*. Retrieved from http://netwrix.solutions-exchange.fr/wp-content/uploads/pdf/AnalysesTendances/2016_SIEM_Efficiency_Survey.pdf

OWASP. (2015). OWASP. Retrieved from https://www.owasp.org/index.php/Defense_in_depth

Palmer, G. (2001). *A Road Map for Digital Forensic Research* (Report fro). Utica, New York,.

Pratama, A., Wijaya, A., & D, R. N. H. (2016). *Penerapan Network Monitoring Menggunakan Security Information and Event Management (Siem) Berbasis Open Source di Universitas Bina Darma Palembang*.

Rihal, M., & Purnamasari, P. D. (2010). *Implementasi dan Analisa Security Information Management Menggunakan OSSIM Pada Sebuah Perusahaan* (universitas indonesia). Retrieved from http://lib.ui.ac.id/file?file=digital/20249100-R031079.pdf

Sean-Philip Oriyano. (2014). Introduction To Ethical Hacking. In *CEH v9 - Certified Ethical Hacking*.

Symantec. (2017). Internet Security Threat Report. In *Symantec Corporation World Headquarters*. Retrieved from https://www.symantec.com/security-center/threat-report

Tegal, W. (2016). *Peraturan Walikota Nomor 18 SOTK Dinas.pdf*. Retrieved from http://diskominfo.tegalkota.go.id/wp-content/uploads/2017/03/Perwal-Nomor-18-Tahun-2016-SOTK-Dinas.pdf

Vianello, V., Gulisano, V., Jimenez-Peris, R., Patiño-Martínez, M., Torres, R., Díaz, R., & Prieto, E. (2013). A scalable SIEM correlation engine and its application to the olympic games it infrastructure. *Proceedings - 2013 International Conference on*

Availability, Reliability and Security, ARES 2013, 625–629. https://doi.org/10.1109/ARES.2013.82

von Solms, B. (2006). Information Security - The Fourth Wave. *Computers and Security*, *25*(3), 165–168. https://doi.org/10.1016/j.cose.2006.03.004