Daftar Pustaka

[1] N. Miloslavskaya, "Analysis of siem systems and their usage in security operations and security intelligence centers," in *Advances in Intelligent Systems and Computing*, 2018. doi: 10.1007/978-3-319-63940-6_40.

[2] M. A. Shauma, Y. Purwanto, and A. Novianty, "Deteksi Anomali Trafik Menggunakan Algoritma Birch Dan Dbscan Pada Streaming Traffic," *eProceedings of Engineering*, vol. 3, no. 3, 2016.

[3] M. Majid and K. Ariffi, "Success Factors for Cyber Security Operation Center (SOC) Establishment," 2019. doi: 10.4108/eai.18-7-2019.2287841.

[4] A. A. Mughal, "Building and Securing the Modern Security Operations Center (SOC)," *International Journal of Business Intelligence and Big Data Analytics*, vol. 5, no. 1, 2022.

[5] N. Hidayah Ab Rahman and K. Kwang Raymond Choo, "A survey of information security incident handling in the cloud," 2015. doi: 10.1016/j.cose.2014.11.006.

[6] S. C. Sundaramurthy, J. Case, T. Truong, L. Zomlot, and M. Hoffmann, "A tale of three security operation centers," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2014. doi: 10.1145/2663887.2663904.

[7] D. Šuškalo, Z. Morić, J. Redžepagić, and D. Regvart, "COMPARATIVE ANALYSIS OF IBM QRADAR AND WAZUH FOR SECURITY INFORMATION AND EVENT MANAGEMENT," in *Annals of DAAAM and Proceedings of the International DAAAM Symposium*, 2023. doi: 10.2507/34th.daaam.proceedings.014.

[8] S. H. Sahir, *Metodelogi Penelitian*, 1st ed. Jogjakarta: KBM INDONESIA, 2021.

[9] S. Siyoto and A. Sodik, "Dasar Metodelogi Penelitian," *Literasi Media Publishing.*, vol. 3, no. 1, 2015.

[10] R. Pfau, "The Security Lifecycle," 2003.

[11] S. Schjolberg, *The History Of Cybercriime*, 3rd ed. Norderstedt : Cybercrime Research Institute GmbH, 2020.

[12] P. Baumard, *Cybersecurity in France*. 2017.

[13] I. Sofana and R. Primartha, *NETWORK SECURITY AND CYBER SECURITY*, vol. 1. Bandung: INFORMATIKA BANDUNG, 2019.

[14] R. Bidou, "Security Operation Center Concepts & Implementation," 2005.

[15] E. Novikova and I. Kotenko, "Analytical visualization techniques for security information and event management," in *Proceedings of the 2013 21st Euromicro*

International Conference on Parallel, Distributed, and Network-Based Processing, PDP 2013, 2013. doi: 10.1109/PDP.2013.84.

[16] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, 2021, doi: 10.3390/s21144759.

[17] S. S. Sekharan and K. Kandasamy, "Profiling SIEM tools and correlation engines for security analytics," in *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017*, 2017. doi: 10.1109/WiSPNET.2017.8299855.

[18] M. Cinque, D. Cotroneo, and A. Pecchia, "Challenges and Directions in Security Information and Event Management (SIEM)," in *Proceedings - 29th IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2018*, 2018. doi: 10.1109/ISSREW.2018.00-24.

[19] M. A. Hussein and E. K. Hamza, "Secure Mechanism Applied to Big Data for IIoT by Using Security Event and Information Management System (SIEM)," *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 6, 2022, doi: 10.22266/ijies2022.1231.59.

[20] Sander Dorigo, "Security Information and Event Management," Radboud University Nijmegen, Nijmegen, 2018.