Daftar Pustaka

[1] Abdelkarim, Amjad, &. H. O., Nasereddin and Hebah, "Intrusion Prevention System," vol. 3, pp. 432-434, 2011.

[2] Sulaiman, N. S. &. Nasir, A. &. Othman, W. &. Fahmy, S. &. Aziz, N. &. Yacob, A. &. Samsudin and Norfarina, "Intrusion Detection System Techniques : A Review," *Journal of Physics: Conference Series*, 2021.

[3] H. Hu, W. Ma and W. Luo, "A Method for Detecting Large-scale Network Anomaly Behavior," *ITM Web Conf*, vol. 17, no. 01012, 2018.

[4] G. Gustavo, G.-Z. Susana and D. Rodrigo, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, p. 4759, 2021.

[5] R. M. Arifianto, P. Sukarno and E. J. Musthofa, "An SSH Honeypot Architecture Using Port Knocking and Intrusion Detection System," *2018 6th International Conference on Information and Communication Technology (ICoICT)*, pp. 409-415, 2018.

[6] Ramadhan, Ilham, P. Sukarno, Nugroho and M. Arief, "Comparative Analysis of K-Nearest Neighbor and Decision Tree in Detecting Distributed Denial of Service," *2020 8th International Conference on Information and Communication Technology (ICoICT)*, pp. 1-4, 2020.

[7] N. T. Van, T. N. Thinh and L. T. Sach, "An anomaly-based network intrusion detection system using Deep learning," *2017 International Conference on System Science and Engineering (ICSSE)*, pp. 210-214, 2017.

[8] F. A. Vadhil, M. F. Nanne and M. L. Salihi, "Importance of Machine Learning Techniques to Improve the Open Source Intrusion Detection Systems," *Indonesian Journal of Electrical Engineering and Informatics*, vol. 9, p. 3, 2021.

[9] N. A. Stoian, "Machine Learning for anomaly detection in IoT networks," July 2020.

[10] P. Mehra, "A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems," *2012*.

[11] Guan and Tianshuai, "Machine Learning Based IDS Log Analysis".

[12] Zeek, "Zeek Documentation," Zeek, 19 November 2021. [Online]. Available: https://docs.zeek.org/en/master/logs/conn.html. [Accessed 19 11 2021].

[13] Venosa, Paula, &. Garcia, Sebastian, &. Díaz and Javier, "A Better Infected Hosts Detection Combining Ensemble Learning and Threat Intelligence," 2020.

[14] Son, S. &. Kwon and Youngmi, "Performance of ELK stack and commercial system in security log analysis," pp. 187-190, 2017.

[15] P. Mehra, "A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems," 2012.

[16] S. Mrdovic, A. Huseinovic and E. Zajko, "Combining static and live digital forensic analysis in virtual environment," *2009 XXII International Symposium on Information, Communication and Automation Technologies*, vol. XXII, pp. 1-6, 2009.

[17] Vielberth, Manfred, Pernul and Günther, *A Security Information and Event Management Pattern*, 2018.