Daftar Pustaka

[1] X. Yuan, C. Li and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," 2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, China, 2017, pp. 1-8, doi: 10.1109/SMARTCOMP.2017.7946998.

[2] Dayanandam, G., Rao, T.V., Bujji Babu, D., Nalini Durga, S. (2019). “DDoS Attacks—Analysis and Prevention”. In: Saini, H., Sayal, R., Govardhan, A., Buyya, R. (eds) Innovations in Computer Science and Engineering. Lecture Notes in Networks and Systems, vol 32. Springer, Singapore. https://doi.org/10.1007/978-981-10-8201-6_1 .

[3] Abhishta, A., van Heeswijk, W., Junger, M., Nieuwenhuis, L. J., & Joosten, R. (2020). “Why would we get attacked? An analysis of attacker's aims behind DDoS attacks”. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 11(2), 3-22.

[4] Y. Chen, K. Hwang and W. -S. Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," in IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649-1662, Dec. 2007, doi: 10.1109/TPDS.2007.1111.

[5] Aulia Arif Wardana, Parman Sukarno, and Muhammad Salman. 2024. “Collaborative Botnet Detection in Heterogeneous Devices of Internet of Things using Federated Deep Learning”. In Proceedings of the 2024 13th International Conference on Software and Computer Applications (ICSCA '24). Association for Computing Machinery, New York, NY, USA, 287–291. https://doi.org/10.1145/3651781.3651825 .

[6] M. Ozkan-Okay, R. Samet, Ö. Aslan and D. Gupta, "A Comprehensive Systematic Literature Review on Intrusion Detection Systems," in IEEE Access, vol. 9, pp. 157727-157760, 2021, doi: 10.1109/ACCESS.2021.3129336.

[7] O. Abouabdalla, H. El-Taj, A. Manasrah and S. Ramadass, "False positive reduction in intrusion detection system: A survey," 2009 2nd IEEE International Conference on Broadband Network & Multimedia Technology, Beijing, China, 2009, pp. 463-466, doi: 10.1109/ICBNMT.2009.5348536.

[8] Mirheidari, S.A., Arshad, S., Jalili, R. (2013). “Alert Correlation Algorithms: A Survey and Taxonomy”. In: Wang, G., Ray, I., Feng, D., Rajarajan, M. (eds) Cyberspace Safety and Security. CSS 2013. Lecture Notes in Computer Science, vol 8300. Springer, Cham. https://doi.org/10.1007/978-3-319-03584-0_14 .

[9] González-Granadillo G, González-Zarzosa S, Diaz R. “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures”. Sensors. 2021; 21(14):4759. https://doi.org/10.3390/s21144759 .

[10] S. OUIAZZANE, M. ADDOU and F. BARRAMOU, "A Multi-Agent Model for Network Intrusion Detection," 2019 1st International Conference on Smart Systems and Data Science (ICSSD), Rabat, Morocco, 2019, pp. 1-5, doi: 10.1109/ICSSD47982.2019.9003119.

[11] V. Shah and A. K. Aggarwal, "Heterogeneous Fusion of IDS Alerts for Detecting DOS Attacks," 2015 International Conference on Computing Communication Control and Automation, Pune, India, 2015, pp. 153-158, doi: 10.1109/ICCUBEA.2015.35.

[12] A. Azodi, D. Jaeger, F. Cheng and C. Meinel, "A New Approach to Building a Multi-tier Direct Access Knowledgebase for IDS/SIEM Systems," 2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 2013, pp. 118-123, doi: 10.1109/DASC.2013.48.

[13] Nespoli, P., & Gómez Mármol, F. (2018, April). “e-Health Wireless IDS with SIEM integration”. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC18), Barcelona, Spain (pp. 15-18).

[14] V. Vasilyev and R. Shamsutdinov, "Security Analysis of Wireless Sensor Networks Using SIEM and Multi-agent Approach," 2020 Global Smart Industry Conference (GloSIC), Chelyabinsk, Russia, 2020, pp. 291-296, doi: 10.1109/GloSIC50886.2020.9267830.

[15] S. D. Çakmakçı, H. Hutschenreuter, C. Maeder and T. Kemmerich, "A Framework For Intelligent DDoS Attack Detection and Response using SIEM and Ontology," 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICCWorkshops50388.2021.9473869.

[16] M. Hristov, M. Nenova, G. Iliev and D. Avresky, "Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT," 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA), Boston, MA, USA, 2021, pp. 1-5, doi: 10.1109/NCA53618.2021.9685977.

[17] T. Laue, C. Kleiner, K. -O. Detken and T. Klecker, "A SIEM Architecture for Multidimensional Anomaly Detection," 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, 2021, pp. 136-142, doi: 10.1109/IDAACS53288.2021.9660903.

[18] Johanes Raphael Nandaputra, Parman Sukarno, and Aulia Arif Wardana. 2024. Detection and Prevention System on Computer Network to Handle Distributed Denial-Of-Service (Ddos) Attack in Realtime and Multi-Agent. In Proceedings of the 2024 10th International Conference on Computer Technology Applications (ICCTA '24). Association for Computing Machinery, New York, NY, USA, 237–241. https://doi.org/10.1145/3674558.3674592 .

[19] Kumar, V., & Sangwan, O. P. (2012). “Signature based intrusion detection system using SNORT”. International Journal of Computer Applications & Information Technology, 1(3), 35-41.

[20] K. Wong, C. Dillabaugh, N. Seddigh and B. Nandy, "Enhancing Suricata intrusion detection system for cyber security in SCADA networks," 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), Windsor, ON, Canada, 2017, pp. 1-5, doi: 10.1109/CCECE.2017.7946818.