

## DAFTAR PUSTAKA

- [1] Y. Lei, "Network Anomaly Traffic Detection Algorithm Based on SVM," 2017 *International Conference on Robots & Intelligent System (ICRIS)*, Huai An City, China, 2017, pp. 217-220, doi: 10.1109/ICRIS.2017.61.
- [2] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," 2018 *International Conference on Artificial Intelligence and Data Processing (IDAP)*, Malatya, Turkey, 2018, pp. 1-5, doi: 10.1109/IDAP.2018.8620728.
- [3] BSSN, 2021, Laporan Tahunan Monitoring Keamanan Siber, BSSN, Jakarta.
- [4] Othman, S. M., Alsohybe, N. T., Alwi, F. M. B., & Zahary, A. T. 2018. *Survey on intrusion detection system types*. *International Journal of Cyber-Security and Digital Forensics*. 7,4 (December. 2018), 444-462.
- [5] Bayu, P. Implementasi *Server Log Monitoring System* menggunakan Elastic Stack. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 6, no. 4, p. 1814-1824, feb. 2022. ISSN 2548-964X.
- [6] Einy, S., Oz, Navaei, Y. D. 2021. "The anomaly- and signature-based ids for network security using Hybrid Inference Systems,". *Mathematical Problems in Engineering*, 2021, 1–10. <https://doi.org/10.1155/2021/6639714>.
- [7] Wahyu, D. R., 2021, Implementasi Suricata IDPS Untuk Monitoring Jaringan Dengan Visualisasi Elk (Elasticsearch, Logstash, Kibana) Dan Notifikasi Melalui Bot Telegram, Univeersitas Muhammadiyah Surakarta, Surakarta.
- [8] E. Hodo et al., "Threat analysis of IoT networks using artificial neural network intrusion detection system," 2016 *International Symposium on Networks, Computers and Communications (ISNCC)*, Yasmine Hammamet, Tunisia, 2016, pp. 1-6, doi: 10.1109/ISNCC.2016.7746067.
- [9] K. Gupta, R. Ranjan Singh and M. Dixit, "Cross site scripting (XSS) attack detection using intrusion detection system," 2017 *International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, 2017, pp. 199-203, doi: 10.1109/ICCONS.2017.8250709.

- [10] Handika, V, 2020, Perancangan Sistem Monitoring Multiple Network Menggunakan Platform Elastic Stack (Studi Kasus: PT. Jedi Global Teknologi), Universitas Atma Jaya, Yogyakarta.
- [11] X. Hu and C. Xie, "Security Operation Center Design Based on D-S Evidence Theory," 2006 International Conference on Mechatronics and Automation, Luoyang, China, 2006, pp. 2302-2306, doi: 10.1109/ICMA.2006.257690.
- [12] Uppal, H. A. M., Javed, M., & Arshad, M. 2014. An overview of intrusion detection system (IDS) along with its commonly used techniques and classifications. *International Journal of Computer Science and Telecommunications*, 5(2), 20-24.
- [13] Anggoro, B. S. 2019. Implementasi Intrusion Prevention System Berbasis Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi (Doctoral dissertation, Program Studi Teknik Informatika FTI-UKSW).
- [14] Kuswanto, D, 2014, Unjuk Kerja Intrusion Prevention System (IDS) Berbasis *Suricata* Pada Jaringan Lokal Area Network Laboratorium TIA, Teknik Informatika Universitas Trunojoyo, Madura.
- [15] Kamal, M. R. 2022. Implementasi *Security Information And Event Management* (SIEM) Dengan Splunk Untuk Analisis Tren Ancaman Siber Pada Jaringan UII.
- [16] P. Shukla and S. Kumar, 2017, *Learning Elastic Stack 6.0*, vol. 53, no. 9. Packt Publishing, Birmingham.
- [17] Parluhutan, P, 2020, Analisis Serangan *SQL Injection* Pada *Web Server* Menggunakan Intrusion Detection System, Universitas Pembangunan Panca Budi, Medan.
- [18] "Near real-time search". *Elastic.co*. Diakses pada 15 Juli 2023. <https://www.elastic.co/guide/en/elasticsearch/reference/current/near-real-time.html/>.