DAFTAR PUSTAKA

[1] Verizon Business, "Explore a preview of some of the cybersecurity data uncovered by this year's DBIR.," [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/#takeaways. [Diakses 14 Oktober 2024].

[2] BSSN Indonesia, "Lanskap Keamanan Siber Indonesia 2023," [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf. [Diakses 14 Oktober 2024].

[3] A. Anggraeni, J. G. A. Ginting dan S. Ikhwan, "Implementation of intrusion prevention system (IPS) to analyze triad CIA on network security attacks," *Jurnal Infotel,* pp. 277-286, 2022.

[4] C. Ankit dan S. S. Shrivastava, "Intrusion Classification and Detection System Using Machine Learning Models on NSL-KDD Dataset," dalam *Proceedings of Fifth International Conference on Computer and Communication Technologies*, Singapore, 2024.

[5] M. F. Alfawaid dan J. Prianggono, "PENERAPAN METODE MULTIPLE MACHINE LEARNING (HYBRID MODEL) UNTUK MENDETEKSI LINK PHISHING SEBAGAI UPAYA PREVENTIF DALAM MEMINIMALISIR KORBAN PENCURIAN DATA," *Jurnal Ilmu Kepolisian,* vol. 17, no. 3, 2023.

[6] D. Šuškalo, Z. Morić, J. Redžepagić dan D. Regvart, "COMPARATIVE ANALYSIS OF IBM QRADAR AND WAZUH FOR SECURITY INFORMATION AND EVENT MANAGEMENT," dalam *34TH DAAAM INTERNATIONAL SYMPOSIUM ON INTELLIGENT MANUFACTURING AND AUTOMATION*, Vienna, 2023.

[7] K. Jiyeon, K. Jiwon, K. Hyunjung, S. Minsun dan C. Eunjung, "CNN-Based Network Intrusion Detection against Denial-of-Service Attacks," *Electronics,* vol. 9, no. 6, pp. 1-21, 2020.

[8] O. Karahan dan B. Kaya, "Raspberry Pi Firewall and Intrusion Detection System," *Journal of Intelligent System: Theory and Application,* vol. 3, no. 2, pp. 21-24, 2020.

[9] J. B. Indonesia, “Peraturan Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi,” [Online]. Available: https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022. [Diakses 16 Oktober 2024].

[10] A. Wiranata, N. Karna, A. Irawan dan I. A. Prakoso, “Implementation and Analysis of Network Security in Raspberry Pi against DOS Attack with HIPS Snort,” dalam *2023 International Conference on Computer Science, Information Technology and Engineering (ICCoSITE)*, Jakarta, 2023.

[11] Kominfo, “Menkominfo Tegaskan Peretas Situs Melanggar Hukum,” [Online]. Available: https://www.kominfo.go.id/berita/berita-kominfo/detail/menkominfo-tegaskan-peretas-situs-melanggar-hukum. [Diakses 17 Oktober 2024].

[12] IEEE Std, IEEE Guide for Developing System Requirements Specifications, 1998, pp. pp.1-36.

[13] AWS, “Apa Itu SLA (Perjanjian Tingkat Layanan)?,” Amazon, [Online]. Available: https://aws.amazon.com/id/what-is/service-level-agreement/. [Diakses 17 Oktober 2024].

[14] S. Overby, L. Greiner dan L. G. Paul, “What is an SLA? Best practices for service-level agreements,” [Online]. Available: https://www.cio.com/article/274740/outsourcing-sla-definitions-and-solutions.html. [Diakses 17 Oktober 2024].

[15] W. Nanda, “Musuh Terbesar bagi Generasi Muda Hoaks dan Cyberbullying,” [Online]. Available: https://www.goodnewsfromindonesia.id/2024/04/19/musuh-terbesar-bagi-generasi-muda-hoaks-dan-cyberbullying. [Diakses 17 Oktober 2024].

[16] CNN Indonesia, “Bahaya Kebocoran Data Pribadi, Termasuk Dicatut Buat Pinjol,” [Online]. Available: https://www.cnnindonesia.com/teknologi/20240628135241-192-1115301/bahaya-kebocoran-data-pribadi-termasuk-dicatut-buat-pinjol#:~:text=Salah%20satu%20risiko%20dari%20kebocoran%20data%20pribadi,pinjaman%20online%20yang%20kurang%20baik%20sistem%20pemeriksaann. [Diakses 16 Oktober 2024].

[17] M. Suharto dan M. Apriyani, “Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional,” *Risalah Hukum,* vol. 17, no. 2, pp. 98-107, 2021.

[18] N. A. Solekha, “Analysis of NSL-KDD Dataset for Classification of Attacks Based on Intrusion Detection System Using Binary Logistics and Multinomial Logistics,” *Seminar Nasional Official Statistics 2022,* pp. 507-520, 2022.

[19] M. Ardiansyah, I. Suhardi dan A. Wahid, “Perancangan dan Analisis Intrusion Detection System Terhadap Serangan Probe Menggunakan Metode Signature Based,” *JIMU: Jurnal Ilmiah Multi Disiplin,* vol. 3, pp. 86-102, 2024.

[20] A. Alharbi, S. Alhaidari dan M. Zohdy, “Denial-of-Service, Probing, User to Root (U2R) & Remote to User (R2L) Attack Detection using Hidden Markov Models,” *International Journal of Computer and Information Technology,* vol. 7, no. 5, pp. 204-210, 2018.

[21] A. Bahaa, A. Abdelaziz, A. Sayed, L. Elfangary dan H. Fahmy, “Monitoring Real Time Security Attacks for IoT Systems Using DevSecOps: A Systematic Literature Review,” *Information,* vol. 12, pp. 1-23, 2021.

[22] P. gupta, “An Efficient Classifier for U2R, R2L, DoS Attack,” *International Journal of Recent Technology and Engineering (IJRTE) ,* vol. 9, no. 1, pp. 644-647, 2020.

[23] I. Syarif, “PANDUAN PENANGANAN INSIDEN SERANGAN DDOS,” [Online]. Available: https://csirt.batam.go.id/web/wp-content/uploads/2023/09/PANDUAN-PENANGANAN-INSIDEN-SERANGAN-DDOS.pdf. [Diakses 16 Maret 2025].

[24] K. V. K. Putri, “KERJA SAMA INDONESIA DENGAN ASEAN MENGENAI CYBER SECURITY DAN CYBER RESILIENCE DALAM MENGATASI CYBER CRIME,” *Rewang Rencang : Jurnal Hukum Lex Generalis,* vol. 2, no. 7, pp. 542-554, 2021.

[25] A. Kumar, K. Abhishek, M. Ghalib, A. Shankar dan X. Cheng, “Intrusion detection and prevention system for an IoT environment,” *Digital Communications and Networks,* vol. 8, no. 4, pp. 540-551, 2022.

[26] K. Coulibaly, “An overview of Intrusion Detection and Prevention Systems,” *Conrnell University,* 2020.

[27] I. Sarker, “Machine Learning: Algorithms, Real-World Applications and Research,” *SN Computer Science,* vol. 2, no. 160, 2021.

[28] Nurhayati, Busman dan R. P. Iswara, “PENGEMBANGAN ALGORITMA UNSUPERVISED LEARNING TECHNIQUE PADA BIG DATA ANALYSIS DI MEDIA SOSIAL SEBAGAI MEDIA PROMOSI ONLINE BAGI MASYARAKAT,” *JURNAL TEKNIK INFORMATIKA,* vol. 12, no. 1, pp. 79-96, 2019.

[29] A. E. S. Abduljabbar dan K. Sefer, “Enhancing network intrusion detection systems with combined network and host traffic features using deep learning: deep learning and IoT perspective,” *Discover Computing,* vol. 27, no. 1, 2024.

[30] R. Grosse, “Lecture 5: Multilayer Perceptrons,” Department of Computer Science, University of Toronto, 2018. [Online]. Available: https://www.cs.toronto.edu/~rgrosse/courses/csc321_2018/readings/L05%20Multilayer%20Perceptrons.pdf.

[31] K. Geeta dan K. Gulshan, “Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges,” *Soft Computing,* vol. 25, no. 15, pp. 9731-9763, 2021.

[32] H. Li, “The Naïve Bayes Method,” dalam *Machine Learning Methods*, Singapore, Springer Nature Singapore, 2024, pp. 67-75.

[33] S. Mallissery, S. Kolekar dan R. Ganiga, “Accuracy Analysis of Machine Learning Algorithms for Intrusion Detection System using NSL-KDD Dataset,” dalam *International Conference on Future Trends In Computing and Communication FTCC 2013*, Karnataka, 2013.

[34] T. Chen dan C. Guestrin, “XGBoost: A Scalable Tree Boosting System,” dalam *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Francisco, 2016.

[35] Amazon AWS, “Bagaimana XGBoost algoritma SageMaker AI bekerja,” [Online]. Available: https://docs.aws.amazon.com/id_id/sagemaker/latest/dg/xgboost-HowItWorks.html. [Diakses 17 Mei 2025].

[36] R. Saumya, K. Gurleen, D. Anish, Arunima, S. Akshit dan B. Anshika, “Research on Problems and Solutions of Overfitting in Machine Learning,” *Advances in Artificial-Business Analytics and Quantum Machine Learning,* vol. 1191, pp. 637-651, 2024.

[37] S. A. Rahmah, “REVIEW TERBARU TENTANG KLASTERISASI DATA MINING MENGGUNAKAN METODE K-MEANS: TANTANGAN DAN APLIKASI,” *Djtechno : Jurnal Teknologi Informasi ,* vol. 5, no. 2, pp. 297-303, 2024.

[38] G. G. Gustavo, S. G. Zarzosa dan R. Diaz, “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures,” *Cyber Situational Awareness in Computer Networks,* 2021.

[39] Microsoft Corporation, “Apa itu SIEM?,” [Online]. Available: https://www.microsoft.com/id-id/security/business/security-101/what-is-siem#:~:text=SIEM%20adalah%20bagian%20penting%20dari,efektif%20menyederhanakan%20alur%20kerja%20keamanan. [Diakses 17 Oktober 2024].

[40] H. S. A. Abdullah, “A comparison of several intrusion detection methods using the NSL-KDD dataset,” *Wasit Journal of Computer and Mathematics Science ,* vol. 3, no. 2, pp. 32-41, 2024.

[41] K. Scarfone dan P. Mell, GUIDE TO INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS), National Institute of Standards and Technology, 2007.

[42] d. khon, “snort3-plugin-ML,” GitHub, [Online]. Available: https://github.com/benzi96/snort3-plugin-ML.git. [Diakses 18 February 2025].

[43] T. Tan, H. Sama, G. Wijaya dan O. E. Aboagye, “Studi Perbandingan Deteksi Intrusi Jaringan Menggunakan Machine Learning: (Metode SVM dan ANN),” *Jurnal Teknologi dan Informasi (JATI) ,* vol. 13, no. 2, pp. 152-164, 2023.

[44] M. S. Hadi dan D. A. P. Putri, “IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) UNTUK DETEKSI DAN ANALISA

INSIDEN KEAMANAN PADA WEB SERVER," *Universitas Muhammadiyah Surakarta,* 2023.

[45] Zenarmor, "How to Install Snort on Ubuntu and Snort Configuration," Zenarmor, 3 April 2025. [Online]. Available: https://www.zenarmor.com/docs/linux-tutorials/how-to-install-and-configure-snort-on-ubuntu-linux. [Diakses February 2025].

[46] M. H. Zaib, "NSL-KDD Dataset," Kaggle, [Online]. Available: https://www.kaggle.com/datasets/hassan06/nslkdd. [Diakses 14 April 2025].

[47] Wazuh Inc., "Quickstart Instalation Wazuh," [Online]. Available: https://documentation.wazuh.com/current/quickstart.html. [Diakses 15 February 2025].