DAFTAR PUSTAKA

[1] A. Sankar and F. K. A., "Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring," *2023 9th International Conference on Smart Computing and Communications (ICSCC)*, 2023.

[2] Check Point Research, "Cyber Threats Q2 2025: Sektor Pendidikan Jadi Target Utama," *Check Point Blog*, 2025. Cyber Threats Q2 2025: Sektor Pendidikan Jadi Target Utama

[3] Universitas Muhammadiyah Kotabumi (UMKO), "Serangan Siber ke Perguruan Tinggi Semakin Meningkat, Ketahanan Siber di Sektor Pendidikan Wajib Ditingkatkan," *UMKO News*, 2023. Serangan Siber ke Perguruan Tinggi Semakin Meningkat, Ketahanan Siber di Sektor Pendidikan Wajib Ditingkatkan - Universitas Muhammadiyah Kotabumi

[4] R. R. P. Reddy, "Enhancing Endpoint Security through Collaborative Zero-Trust Integration: A Multi-Agent Approach," International Journal of Computer Trends and Technology, vol. 72, no. 8, pp. 86–90, 2024, doi: 10.14445/22312803/ijctt-v72i8p112.

[5] Kipkoech Denzel, "A survey of security in zero trust network architectures," GSC Advanced Research and Reviews, vol. 22, no. 2, pp. 182–214, 2025, doi: 10.30574/gscarr.2025.22.2.0036.

[6] A. Stredler-brown, "20 2 3 4," pp. 292–315, 2023.

[7] A. Kamil, D. Rizaludin, and A. T. Ni'mah, "Implementasi Wazuh FIM (File Integrity Monitoring) untuk Perlindungan Keamanan Sistem Informasi pada Unit Kegiatan Mahasiswa di Universitas Trunojoyo Madura," Sains Data Jurnal Studi Matematika dan Teknologi, vol. 2, no. 2, pp. 80–92, 2024, doi: 10.52620/sainsdata.v2i2.127.

[8] Rangga Aditya, Yusuf Muhyidin, and Dayan Singasatia, "Implementasi Security Information And Event Management (SIEM) Untuk Monitoring Keamanan Server

Menggunakan Wazuh," Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika, vol. 2, no. 5, pp. 137–144, 2024, doi: 10.61132/merkurius.v2i5.289.

[9] A. Shafiyyah, G. F. Nama, and R. A. Pradipta, "Implementasi Wazuh Menggunakan Metode Ppdioo Di Sistem Keamanan Jaringan Psdku Universitas Lampung Waykanan Sebagai Deteksi Dan Respon Serangan Siber," Jurnal Informatika dan Teknik Elektro Terapan, vol. 12, no. 2, pp. 1–23, 2024, doi: 10.23960/jitet.v12i2.4074.

[10] Cisco Systems, *Network Design Methodology – PPDIOO Model*, CC Expert, 2023. https://www.ccexpert.us/network-design/network-design-methodology.html.

[11] Wazuh Documentation, "File Integrity Monitoring (FIM) Module," Wazuh Docs, 2025. Available: https://documentation.wazuh.com

[12] M. Zulfikri, M. Syahrir, and W. Kusuma, "Pelatihan Implementasi Security Event Monitoring Berbasis Wazuh / Siem Pada Aplikasi Command Center Pemerintah Provinsi Nusa Tenggara Barat," vol. 4, no. 1, pp. 21–30, 2025.

[13] C. Kurniawan and A. Triayudi, "File Integrity Monitoring as a Method for Detecting and Preventing Web Defacement Attacks," *Jurnal Online Informatika*, vol. 9, no. 2, pp. 276–285, 2024, doi: 10.15575/join.v9i2.1326.

[14] Pusdatin Kemendikdasmen. (2025). *CDT Talks #5: Ruang Siber Aman untuk Layanan Pendidikan Berkualitas*. https://pusdatin.kemendikdasmen.go.id/berita/cdt-talks-5-ruang-siber-aman-untuk-layanan-pendidikan-berkualitas

[15] R. Artha and B. Soewito, "Perancangan Ulang Topologi Jaringan Dengan Kerangka Kerja Ppdioo Network Topology Redesign With Ppdioo Framework," vol. 13, no. 1, pp. 34–41, 2023.

[16] F. Fachri, "optimasi keamanan web server terhadap serangan brute-force menggunakan penetration testing optimizing web server security for brute-force attacks using," vol. 10, no. 1, pp. 51–58, 2023, doi: 10.25126/jtiik.2023105872.

[17] M. R. Naeem, R. Amin, and M. Farhan, “Cyber security Enhancements with reinforcement learning : A zero-day vulnerabilityu identification perspective,” pp. 1–33, 2025, doi: 10.1371/journal.pone.0324595.

[18] M. Cen, X. Deng, F. Jiang, and R. Doss, “Computers & Security Zero-Ran Sniff : A zero-day ransomware early detection method based on zero-shot learning,” *Computers & Security*, vol. 142, no. April, p. 103849, 2024, doi: 10.1016/j.cose.2024.103849.

[19] K. Chanbuala, D. Puangpronpitag, E. Puangpronpitag, and S. Puangpronpitag, “Security Analysis and Mitigation of SSL Stripping , Homograph Redirection , and Keylogging Attacks : A Case Study on Thai Web Platforms,” vol. 15, no. 4, 2025.

[20] F. Tchakounté, J. Marie, K. Fotso, and V. Corneille, “An Architecture for Misconfiguration Patching of Web Services : A Case Study of Apache Server,” vol. 4523, pp. 37–56.

[21] R. Nair, K. R. Dodiya, and P. Lakhalani, “A Static Approach for Malware Analysis : A Guide,” no. December, 2023.

[22] Y. Safonov and M. Zernovic, “Enhancing Security Monitoring with AI-Enabled Log Collection and NLP Modules on a Unified Open Source Platform,” pp. 217–221, 2023, doi: 10.13164/eeict.2023.217.

[23] P. Okonkwor, O. Miriam, O. Raji, A. Samson, and T. Mabo, “Cybersecurity on a budget : Affordable cloud security tools for SMBs,” vol. 6, no. October, pp. 689–723, 2025, doi: 10.51594/csitrj.v6i9.2066.

[24] O. Dewangga, D. Pramudya, P. Hatta, and C. W. Budiyanto, “Modeling intrusion detection and prevention system to detect and prevent network attacks using wazuh pemodelan intrusion detection and prevention system untuk mendeteksi dan mencegah serangan jaringan,” vol. 6, no. 1, 2025.

[25] K. M. De Nobrega, A. Rutkowski, and C. Saunders, “Journal of Strategic Information Systems The whole of cyber defense : Syncing practice and theory,” *Journal of Strategic Information Systems*, vol. 33, no. 4, p. 101861, 2024, doi: 10.1016/j.jsis.2024.101861.

[26] P. D. I. Torino, “Study on Implementation and Optimization of Security Operation Center Using Open-source Tools,” no. December, 2024.