

DAFTAR PUSTAKA

- Accorsi, R. (2013). A secure log architecture to support remote auditing. *Mathematical and Computer Modelling*, 57(7), 1578–1591. <https://doi.org/https://doi.org/10.1016/j.mcm.2012.06.035>
- Agbeyangi, A. O., & Suleman, H. (2023). Patterns for Software Systems in Low-Resource Environments. *Proceedings of the 30th Conference on Pattern Languages of Programs (PLoP)*, 1–11.
- Ahmad, A., Saad, M., & Mohaisen, A. (2019). Secure and transparent audit logs with BlockAudit. *Journal of Network and Computer Applications*, 145, 102406. <https://doi.org/https://doi.org/10.1016/j.jnca.2019.102406>
- Badan Siber dan Sandi Negara. (2024). Lanskap Keamanan Siber Indonesia. *Id-SIRTII /CC*, (70), 1–107. bit.ly/44bzpHM
- Basari, K., & Aldianto, L. (2025). Adopting Security Operation Center: Insights from the Indonesian Financial Sector. *International Journal of Current Science Research and Review*, 08(03), 1051–1066. <https://doi.org/10.47191/ijcsrr/v8-i3-08>
- Bautista Villalpando, L. E., April, A., & Abran, A. (2014). Performance analysis model for big data applications in cloud computing. *Journal of Cloud Computing*, 3(1), 19. <https://doi.org/10.1186/s13677-014-0019-z>
- Chandra, C., Mulya, D. P., & Faradika, F. (2025). Deteksi Serangan Siber Menggunakan Machine Learning: Studi Pada Sistem Informasi Akademik. *Jurnal Sistem Informasi Dan Informatika*, 3(2), 106–110.
- Enjam, G. R. (2023). Optimizing PostgreSQL for High-Volume Insurance Transactions & Secure Backup and Restore Strategies for Databases. *International Journal of Emerging Trends in Computer Science and Information Technology*, 4(1), 104–111.
- Ferraiolo, D. F., & Kuhn, D. R. (1992). Role-Based Access Control (RBAC). *Proceedings of the 15th National Computer Security Conference*, 554–563. https://doi.org/10.1007/978-1-4842-8593-0_5
- Firdyanto Rushendra, T. R. (2024). Implementation of Intrusion Detection System with Rule-Based Method on Website. *Journal of Computer Networks, Architecture and High Performance Computing*, (Vol. 6 No. 3 (2024): Articles Research Volume 6 Issue 3, July 2024), 1245–1252. <https://jurnal.itscience.org/index.php/CNAPC/article/view/4256/3331>
- Gilang Patoni, Yusuf Muhyidin, & Dayan Singasatia. (2024). Implementasi Wazuh Pada Ubuntu Server Untuk Mendeteksi Serangan Brute Force Hydra. *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika*, 2(5 SE-Articles), 145–156. <https://doi.org/10.61132/mercurius.v2i5.290>
- Haryanto, B., & Chandra, D. W. (2024). Implementasi Wazuh Integritas File untuk

- Perlindungan Keamanan Berdasarkan Aktivitas Log di BTSI UKSW. *Jurnal Indonesia: Manajemen Informatika Dan Komunikasi*, 5(1), 183–192.
- Heluka, H. D., & Sulisty, W. (2023). Perancangan dan implementasi Security Information and Event Management (SIEM) pada layanan virtual server. *Progresif: Jurnal Ilmiah Komputer*, 19(2), 912–922.
- Hussain, A., & Mkpojiogu, E. (2015). AN APPLICATION OF THE ISO/IEC 25010 STANDARD IN THE QUALITY-IN-USE ASSESSMENT OF AN ONLINE HEALTH AWARENESS SYSTEM. *Jurnal Teknologi (Sciences and Engineering)*, 5, 9–13.
https://www.researchgate.net/publication/283767184_An_application_of_the_ISOIEC_25010_standard_in_the_quality-in-use_assessment_of_an_online_health_awareness_system
- ISO/IEC. (2011). *ISO/IEC 25010:2011 - Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*. <https://www.iso.org/standard/35733.html>
- ISO/IEC. (2023). *ISO/IEC 25010:2023(en), Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model*. <https://www.iso.org/obp/ui#iso:std:iso-iec:25010:ed-2:v1:en>
- Jones, M., Bradley, J., Sakimura, N., Jones, M., Bradley, J., & Sakimura, N. (2015). *JSON Web Token (JWT)*. <https://doi.org/10.17487/RFC7519>
- Kampanakis, P., & Yavuz, A. A. (2015). BAFi: a practical cryptographic secure audit logging scheme for digital forensics. *Security and Communication Networks*, 8(17), 3180–3190. <https://doi.org/https://doi.org/10.1002/sec.1242>
- Kent, K., & Souppaya, M. (2006). *Guide to Computer Security Log Management. Nist Special Publication*.
- Khaerunnisa, L. S., Al Qodr, M. R. S., Putri, J. W. D., Firdaus, J. R., & Rozikin, C. (2025). OPTIMASI PROSES DATA WAREHOUSE MENGGUNAKAN PARTISI DAN INDEXING PADA POSTGRESQL UNTUK MENINGKATKAN PERFORMA QUERY. *Jurnal Informatika Dan Teknik Elektro Terapan*, 13(3S1).
- Knerler, K., Ingrid, P., & Zimmerman, C. (2024). *11 Strategies of a World-Class Cybersecurity Operations Center* (Vol. 2). MITRE. <https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf>
- Knerler, K., Parker, I., & Zimmerman, C. (2023). *11 Strategies of a World-Class Cybersecurity Operations Center*. MITRE.
- Konstantinos, B., & Foteini, F. (2023). Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs). *Indonesian Journal of Computer Science*, 12(1), 443–468.

<https://doi.org/https://doi.org/10.33022/ijcs.v12i2.3182>

- Lisnevskiy, R., Amanzholova, S., Akhmetzhanova, J., Ikembayeva, A., & Naumova, D. (2025). Development of an integrated network threat detection system based on Wazuh, Suricata and Telegram Bot. *CISN*.
- Lodderstedt, T., Bradley, J., Labunets, A., Fett, D., Lodderstedt, T., Bradley, J., Labunets, A., & Fett, D. (2025). *Best Current Practice for OAuth 2.0 Security*. <https://doi.org/10.17487/RFC9700>
- Mansur, Hidayasari, N., Kasmawi, & Efendi, Z. (2026). Wazuh-Based Security Monitoring for Public Service Web Systems: Detection Effectiveness, Alert Latency, and Resource Overhead. *Journal of Embedded Systems, Security and Intelligent Systems*, 7(2), 83–98. <https://doi.org/10.59562/JESSI.V7I2.2636>
- Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *Plos One*, 19(3), e0301183.
- Nafal Adi Syamaidzar Laudza, & Sofyan, H. (2024). Quality Evaluation of Academic Information Systems with ISO / IEC 25010 Standards (Case Study: ABC University). *Jurnal Informatika Dan Teknologi Informasi*, 21(2), 209–223. <https://doi.org/10.31515/telematika.v21i2>
- Naser, S. M., & Ali, Y. H. (2022). Systematic Review on Cyber-Security Applications. *Iraqi Journal of Computers, Communications, Control and Systems Engineering*, 22(4), 28–36. <https://doi.org/10.33103/uot.ijccce.22.4.3>
- Nugraha, F., Khalimi, T., & Herwanto, H. (2025). Implementasi Security Information and Event Management (SIEM) pada Sistem Akademik Universitas Kuningan. *Buffer Informatika*, 11(1), 71–77.
- Putra, W. P., Burjulus, R., Al Hilmi, M. A., & Sumarudin, A. (2024). Implementasi Sistem Manajemen Log untuk Penanggulangan Serangan Server dengan SIEM. *IKRA-ITH Informatika: Jurnal Komputer Dan Informatika*, 8(3), 23–30.
- Rafi, S., Akbar, M. A., & Khan, A. A. (2025). Assessing Software Product Quality in DevOps: An ISO 25010:2023 Perspective. *Proceedings of the 2025 29th International Conference on Evaluation and Assessment in Software Engineering Companion, EASE Companion '25*, 10–16. <https://doi.org/10.1145/3727967.3756847>
- Ravanello, A., Desharnais, J.-M., Villalpando, L. E. B., April, A., & Gherbi, A. (2014). Performance Measurement for Cloud Computing Applications Using ISO 25010 Standard Characteristics. *2014 Joint Conference of the International Workshop on Software Measurement and the International Conference on Software Process and Product Measurement*, 41–49. <https://doi.org/10.1109/IWSM.Mensura.2014.33>
- Rojas, H., Renteria, R., & Martinez, V. (2025). Understanding Performance Efficiency in ISO/IEC 25000: A Systematic Literature Review. *JOIV*:

- International Journal on Informatics Visualization*, 9(6), 2405–2417.
<https://doi.org/10.62527/JOIV.9.6.3074>
- Rosa, L., Alves, P., Cruz, T., Simões, P., & Monteiro, E. (2015). A Comparative Study of Correlation Engines for Security Event Management. *International Conference on Cyber Warfare and Security (ICCWS)*, 11.
- Runeson, P., & Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering*, 14(2), 131–164. <https://doi.org/10.1007/s10664-008-9102-8>
- Shafiyah, A., Nama, G. F., & Pradipta, R. A. (2024). 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*, 12(2).
- Sheffer, Y., Hardt, D., Jones, M., Sheffer, Y., Hardt, D., & Jones, M. (2020). *JSON Web Token Best Current Practices*. <https://doi.org/10.17487/RFC8725>
- Sijabat, D. R., & Evo, S. (2023). Perancangan Security Information and Event Management (SIEM) untuk mendeteksi insiden pada situs web. *J-INTECH*, 11(1), 10–17.
- Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. *Information Processing & Management*, 45(4), 427–437. <https://doi.org/https://doi.org/10.1016/j.ipm.2009.03.002>
- Sommerville, I. (2016). *TENTH edition Tenth Edition* (10th Editi). Pearson Education Limited.
- Stallings, W. (2011). the William Stallings Books on Computer Data and Computer Communications , Eighth Edition. In *Network* (Vol. 139, Number 3). <https://doi.org/10.1007/11935070>
- Sugiyono, D. (2013). *Metode penelitian pendidikan pendekatan kuantitatif, kualitatif dan R&D*.
- Sulthan, M., Rahmatullah, A., Muhandhatul Nabila, A., Dewi, S. S., Datry, V., & Azaruddin, F. A. (2024). Implementasi SIEM dan IDS Dalam Monitoring Terhadap Ancaman Serangan Pada WEB Server. *SABER: Jurnal Teknik Informatika, Sains Dan Ilmu Komunikasi*, 2(1), 130–137. <https://doi.org/10.59841/SABER.V2I1.666>
- Svelte Documentations. (2026). *Introduction - SvelteKit Docs*. <https://svelte.dev/docs/kit/introduction>
- Toktomusheva, G. (2025). *Indexing in PostgreSQL: Performance Evaluation and Use Cases*.
- Wazuh Documentation. (2026). *Quickstart - Wazuh documentation*. <https://documentation.wazuh.com/current/quickstart.html>

- Zahid, H., Hina, S., Hayat, M. F., & Shah, G. A. (2023). Agentless Approach for Security Information and Event Management in Industrial IoT. *Electronics* 2023, Vol. 12, Page 1831, 12(8), 1831. <https://doi.org/10.3390/ELECTRONICS12081831>
- Zain, A. R., Oktivasari, P., Soelaiman, N. F., & Umam, F. W. (2023). Implementasi Intrusion Detection System (Ids) Suricata Dan Management Log Elk Stack Untuk Pendeteksian Kegiatan Mining. *Jurnal Poli-Teknologi*, 22(1), 23–29.

