DAFTAR PUSTAKA

[1] F. Pangandaheng, J. B. Maramis, D. P. E. Saerang, L. O. H. Dotulong, And D. Soepeno, "Transformasi Digital: Sebuah Tinjauan Literatur Pada Sektor Bisnis Dan Pemerintah," *Jurnal Emba : Jurnal Riset Ekonomi, Manajemen, Bisnis Dan Akuntansi*, Vol. 10, No. 2, Jun. 2022, Doi: 10.35794/Emba.V10i2.41388.

[2] Y. Ginanjar, "Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara," *Jurnal Dinamika Global*, Vol. 7, No. 02, Pp. 291–312, Dec. 2022, Doi: 10.36859/Jdg.V7i02.1187.

[3] John Zorabedian, "Surging Data Breach Disruption Drives Costs To Record Highs," Https://Www.Ibm.Com/Think/Insights/Whats-New-2024-Cost-Of-A-Data-Breach-Report.

[4] S. A. Chamkar, Y. Maleh, And N. Gherabi, "Security Operations Centers: Use Case Best Practices, Coverage, And Gap Analysis Based On Mitre Adversarial Tactics, Techniques, And Common Knowledge," *Journal Of Cybersecurity And Privacy*, Vol. 4, No. 4, Pp. 777–793, Dec. 2024, Doi: 10.3390/Jcp4040036.

[5] R. Amami, M. Charfeddine, And S. Masmoudi, "Exploration Of Open Source Siem Tools And Deployment Of An Appropriate Wazuh-Based Solution For Strengthening Cyberdefense," In *2024 10th International Conference On Control, Decision And Information Technologies (Codit)*, Ieee, 2024, Pp. 1–7.

[6] Socradar, "Top 10 Best Free Cyber Threat Intelligence Sources And Tools In 2025," Https://Socradar.Io/. Accessed: Oct. 10, 2025. [Online]. Available: Https://Socradar.Io/Top-10-Free-Cyber-Threat-Intelligence-Sources-And-Tools-2025/

[7] M. Vielberth, F. Bohm, I. Fichtinger, And G. Pernul, "Security Operations Center: A Systematic Study And Open Challenges," *Ieee Access*, Vol. 8, Pp. 227756–227779, 2020, Doi: 10.1109/Access.2020.3045514.

[8] Kevin. Mclaughlin, *Cybersecurity Operations And Fusion Centers : A Comprehensive Guide To Soc And Tic Strategy*, 1st Edition. Boca Raton, Fl: Crc Press, 2024.

[9] E-Spincorp Documentation, "Setting Up A Comprehensive Open-Source Security Operations Center: A Practical Guide," Https://Www.E-Spincorp.Com/. Accessed: Oct. 10, 2025. [Online]. Available:

Https://Www.E-Spincorp.Com/Documentation/Open-Source-Soc-Setup-Guide/

[10] J. Forsberg And T. Frantti, “Technical Performance Metrics Of A Security Operations Center,” *Comput. Secur.*, Vol. 135, Dec. 2023, Doi: 10.1016/J.Cose.2023.103529.

[11] E. Du Bois And I. Horváth, “Abstract Prototyping In Software Engineering: A Review Of Approaches,” 2011.

[12] N. A. Rakhmawati, “Software Open Source, Software Gratis?,” *Juti: Jurnal Ilmiah Teknologi Informasi*, Pp. 13–18, Jan. 2006, Doi: 10.12962/J24068535.V5i1.A201.

[13] S. Salamun And S. Sukri, “Analisa Pemanfaatan Dan Peran Software Open-Source Bagi Mahasiswa Universitas Abdurrab,” *Jurnal Buana Informatika*, Vol. 12, No. 1, Pp. 49–57, May 2021, Doi: 10.24002/Jbi.V12i1.4145.

[14] L. Shitao And E. D. Martin, “Optimization And Zspore Analysis Of Affinity Purification Coupled With Tandem Mass Spectrometry In Mammalian Cells,” *J. Proteom. Genom. Res.*, Vol. 1, No. 1, Pp. 9–20, 2012, Doi: 10.14302/Issn.2326-0793.Jpgr-12-100.

[15] M. R. T. Hidayat, N. Widiyasono, And R. Gunawan, “Optimasi Deteksi Malware Pada Siem Wazuh Melalui Integrasi Cyber Threat Intelligence Dengan Misp Dan Dfir-Iris,” *Jurnal Informatika Dan Teknik Elektro Terapan*, Vol. 13, No. 1, Jan. 2025, Doi: 10.23960/Jitet.V13i1.5686.

[16] R. Kanna R, *Cybersecurity Threats And Incident Response: Real-World Case Studies On Network Security, Data Breaches, And Risk Mitigation*, 1st Ed. Bangalore, Karnataka, India: Deep Science Publishing, 2025. Doi: 10.70593/978-93-7185-133-6.

[17] M. Y. Darus, A. Ramli, Y. Mohd Yussoff, And B. Azni, “Cybersecurity Resilience — An Integrated Framework For Detection Of Threats And Response In The Digital Age: A Review Paper,” *Malaysian Journal Of Computing*, Vol. 10, No. 1, Pp. 2099–2116, Apr. 2025, Doi: 10.24191/Mjoc.V10i1.4520.

[18] Courage Ojo, Emmanuel Ayodeji Osoko, Joy Nnenna Okolo, And Mamudat Jaji, “Incident Response: A Structured Model From Detection To Containment And Recovery,” *World Journal Of Advanced Research And Reviews*, Vol. 24, No. 1, Pp. 1401–1407, Oct. 2024, Doi: 10.30574/Wjarr.2024.24.1.3148.

[19] A. Sutanto And A. Rakhman, “Experimental Evaluation Of Wazuh-Grafana Integration For Real-Time Cyber Threat Detection In Resource-Constrained Environments,” *Journal Of Applied Informatics And Computing*, Vol. 9, No. 5, Pp. 2783–2790, Oct. 2025, Doi: 10.30871/Jaic.V9i5.10404.

[20] M. Ammi, “Cyber Threat Hunting Case Study Using Misp,” *Journal Of Internet Services And Information Security*, Vol. 13, No. 2, Pp. 1–29, May 2023, Doi: 10.58346/Jisis.2023.I2.001.

[21] G. Dahlberg, “Exploring Incident Management: A Comparative Study Of Splunk Enterprise, Graylog Open And Syslog-Ng And Their Impact On Mean Time To Resolution (Mttr) An Experimental Study Of Incident Detection And Alerting Performance Across Basic, Intermediate, And Advanced Siem Systems.”

[22] O. Owolafe And A. J. Alabi, “Comparative Analysis Of Wazuh, Graylog, And Elk Stack For Cyber Threat Detection And Response,” In *International Conference For Internet Technology And Secured Transactions (Icitst-2024)*, Infonomics Society, Dec. 2024, Pp. 182–193. Doi: 10.20533/Icitst.2024.0015.

[23] M. Husák, J. Komárková, E. Bou-Harb, And P. Čeleda, “Survey Of Attack Projection, Prediction, And Forecasting In Cyber Security,” *Ieee Communications Surveys & Tutorials*, Vol. 21, No. 1, Pp. 640–660, 2019, Doi: 10.1109/Comst.2018.2871866.

[24] E. M. Hutchins, M. J. Cloppert, And R. M. Amin, “Intelligence-Driven Computer Network Defense Informed By Analysis Of Adversary Campaigns And Intrusion Kill Chains.”

[25] M. Khayat, E. Barka, M. A. Serhani, F. Sallabi, K. Shuaib, And H. M. Khater, “Advanced Techniques For Alert Management In Security Information And Event Management Systems With Ensembled Deep Learning, Hybrid Optimization, And Multi-Feature Extraction,” *Ieee Open Journal Of The Communications Society*, Vol. 6, Pp. 7349–7368, 2025, Doi: 10.1109/Ojcoms.2025.3603000.

[26] R. Ramadhani, A. Christie, A. A. Dewani, M. Krisnawan, And R. Dhimaz Ardhana, “Optimalisasi Intelijen Ancaman Siber Di Security Operation Centers Dengan Pemanfaatan Large Language Models (Llm) Dan Siem,” *Jurnal Ilmiah Multidisipline*, Vol. 3, No. 5, 2025, Doi: 10.5281/Zenodo.15707795.

[27] K. Bezas And F. Filippidou, “Comparative Analysis Of Open Source Security Information &Amp; Event Management Systems (Siems),” *The Indonesian Journal Of Computer Science*, Vol. 12, No. 2, Pp. 443–468, Apr. 2023, Doi: 10.33022/Ijcs.V12i2.3182.

[28] H. Kaur *Et Al.*, “Evolution Of Endpoint Detection And Response (Edr) In Cyber Security: A Comprehensive Review,” *E3s Web Of Conferences*, Vol. 556, P. 01006, Aug. 2024, Doi: 10.1051/E3sconf/202455601006.

[29] A. Hozouri, A. Mirzaei, And M. Effatparvar, “A Comprehensive Survey On Intrusion Detection Systems With Advances In Machine Learning, Deep

Learning And Emerging Cybersecurity Challenges," *Discover Artificial Intelligence*, Vol. 5, No. 1, P. 314, Nov. 2025, Doi: 10.1007/S44163-025-00578-1.

[30] H. Debar, M. Dacier, And A. Wespi, "A Revised Taxonomy For Intrusion-Detection Systems," *Ann. Telecommun.*, Vol. 55, No. 7–8, Pp. 361–378, Jul. 2000, Doi: 10.1007/Bf02994844.

[31] Barlyan Kurdianto, Yohanzah Febriyanto, And Yustian Servanda, "Intrusion Detection System Analysis To Improve Computer Network Security," *Journal Of Artificial Intelligence And Engineering Applications (Jaiea)*, Vol. 4, No. 3, Pp. 1855–1862, Jun. 2025, Doi: 10.59934/Jaiea.V4i3.1036.

[32] S. Ang, S. Huy, And M. Janarthanan, "Utilizing Ids And Ips To Improve Cybersecurity Monitoring Process," *Journal Of Cyber Security And Risk Auditing*, Vol. 2025, No. 3, Pp. 77–88, Jul. 2025, Doi: 10.63180/Jcsra.Thestap.2025.3.10.

[33] Dwi Putri Amanda And Eriene Dheanda Absharina, "Implementasi Ai-Powered Intrusion Detection Systems Untuk Mendeteksi Ancaman Keamanan Pada Big Data," *Simtek : Jurnal Sistem Informasi Dan Teknik Komputer*, Vol. 10, No. 1, Pp. 29–33, Apr. 2025, Doi: 10.51876/Simtek.V10i1.1381.

[34] R. V. Rishika, B. A. Pratomo, And S. C. Hidayati, "Network Intrusion Detection System With Time-Based Sequential Cluster Models Using Lstm And Gru," *Juti: Jurnal Ilmiah Teknologi Informasi*, Pp. 1–12, Feb. 2025, Doi: 10.12962/J24068535.V23i1.A1241.

[35] M. Ahmed And Q. Abdullah, "Network Intrusion Detection Systems: Machine Learning-Based Attack And Remedy Strategies – A Review," *Al-Salam Journal For Engineering And Technology*, Vol. 4, No. 2, Pp. 11–29, Aug. 2025, Doi: 10.55145/Ajest.2025.04.02.002.

[36] M. Farhan *Et Al.*, "Network-Based Intrusion Detection Using Deep Learning Technique," *Sci. Rep.*, Vol. 15, No. 1, P. 25550, Jul. 2025, Doi: 10.1038/S41598-025-08770-0.

[37] M. K. Paul Kirvansean, "What Is Extended Detection And Response (Xdr)?," Https://Www.Techtarget.Com/Searchsecurity/Definition/Extended-Detection-And-Response-Xdr.

[38] Anne Aarness, "Extended Detection And Response (Xdr) Explained," Https://Www.Crowdstrike.Com/En-Us/Cybersecurity-101/Endpoint-Security/Extended-Detection-And-Response-Xdr/.

[39] Ibm, "What Is Extended Detection And Response (Xdr)?," Https://Www.Ibm.Com/Think/Topics/Xdr?

[40] G. Ahn, J. Jang, S. Choi, And D. Shin, “Research On Improving Cyber Resilience By Integrating The Zero Trust Security Model With The Mitre Att&Ck Matrix,” *Ieee Access*, Vol. 12, Pp. 89291–89309, 2024, Doi: 10.1109/Access.2024.3417182.