DAFTAR PUSTAKA

Afek, Y., Berger, H., & Bremler-Barr, A. (2025). *POPS: From History to Mitigation of DNS Cache Poisoning Attacks*. https://doi.org/10.48550/arXiv.2501.13540

Agrawal, R., Stokes, J. W., Rist, L., Littlefield, R., Fan, X., Hollis, K., Coppedge, Z., Chesterman, N., & Seifert, C. (2022). *Long-Term Study of Honeypots in a Public Cloud*. https://doi.org/10.1109/DSN-S54099.2022.00011

Alexander Djo Njoera, Y., Nyoman Buda Hartawan, I., Agung Gede Bagus Ariana, A., & Dwi Krisna, E. (2024). *The analysis of honeypot performance using Grafana Loki and ELK Stack visualization*. *Informatika Dan Sains*, *14*, 2024. https://doi.org/10.54209/infosains.v14i03

Alkhwaja, I., Albugami, M., Alkhwaja, A., Alghamdi, M., Abahussain, H., Alfawaz, F., Almurayh, A., & Min-Allah, N. (2023). Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming. *Applied Sciences (Switzerland)*, *13*(10). https://doi.org/10.3390/app13105979

Alotaibi, A., & Rassam, M. A. (2023). Adversarial Machine Learning Attacks against Intrusion Detection Systems: A Survey on Strategies and Defense. In *Future Internet* (Vol. 15, Issue 2). MDPI. https://doi.org/10.3390/fi15020062

Alqahtani, A., & Sheldon, F. T. (2022). A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook. In *Sensors* (Vol. 22, Issue 5). MDPI. https://doi.org/10.3390/s22051837

Arshad, A., Rehman, A. U., Javaid, S., Ali, T. M., Sheikh, J. A., & Azeem, M. (2021). *A systematic literature review on phishing and anti-phishing techniques. Pakistan Journal of Engineering and Technology*, 4, 163–168. https://doi.org/10.48550/arXiv.2104.01255

Babanov, V. (December 2024). Internals of Defense-In-Depth Strategy in Cybersecurity. Security and Defense(2), 37-42. https://doi.org/10.70265/PNEZ3158

Badan Siber dan Sandi Negara. (2023). Laporan tahunan layanan Honeynet BSSN tahun 2023. Badan Siber dan Sandi Negara. https://www.bssn.go.id/honeynet-project/

Balarezo, J. F., Wang, S., Chavez, K. G., Al-Hourani, A., & Kandeepan, S. (2022). A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. In *Engineering Science and Technology, an International Journal* (Vol. 31). Elsevier B.V. https://doi.org/10.1016/j.jestch.2021.09.011

Byun, H., Kim, J., Jeong, Y., Seok, B., Gong, S., & Lee, C. (2024). A Security Analysis of Cryptocurrency Wallets against Password Brute-Force Attacks. *Electronics (Switzerland)*, *13*(13). https://doi.org/10.3390/electronics13132433

Cen, M., Jiang, F., Qin, X., Jiang, Q., & Doss, R. (2024). Ransomware early detection: A survey. In *Computer Networks* (Vol. 239). Elsevier B.V. https://doi.org/10.1016/j.comnet.2023.110138

Chen, Z., Simsek, M., Kantarci, B., Bagheri, M., & Djukic, P. (2024). *Machine learning-enabled hybrid intrusion detection system with host data transformation and*

an advanced two-stage classifier. Computer Networks, 250, 110576. https://doi.org/10.1016/j.comnet.2024.110576

Chou, F. K. Y., Chen, A. P. S., & Lo, V. C. L. (2021). Mindless response or mindful interpretation: Examining the effect of message influence on phishing susceptibility. *Sustainability (Switzerland)*, *13*(4), 1–25. https://doi.org/10.3390/su13041651

Cisco. (2026). *Snort intrusion prevention system*. https://www.snort.org/

Coppolino, L., Sgaglione, L., D'antonio, S., Magliulo, M., Romano, L., & Pacelli, R. (2022). Risk Assessment Driven Use of Advanced SIEM Technology for Cyber Protection of Critical e-Health Processes. *SN Computer Science*, *3*(1). https://doi.org/10.1007/s42979-021-00858-4

Cowrie (2026). *Cowrie SSH/Telnet honeypot*. https://github.com/cowrie/cowrie

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Diana, L., Dini, P., & Paolini, D. (2025). *Overview on Intrusion Detection Systems for Computers Networking Security. Computers*, 14(3), 87. https://doi.org/10.3390/computers14030087

Dionaea (2026). *Dionaea honeypot*. https://github.com/DinoTools/dionaea

Einy, S., Oz, C., & 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

Elastic. (2026). *Elastic documentation*. https://www.elastic.co/docs

Elrawy, M. F., Hadjidemetriou, L., Laoudias, C., & Michael, M. K. (2023). Detecting and classifying man-in-the-middle attacks in the private area network of smart grids. *Sustainable Energy, Grids and Networks*, *36*, 101167. https://doi.org/10.1016/j.segan.2023.101167

Fadhlurrohman, M., Muliawati, A., & Hananto, B. (2021). Analisis Kinerja Intrusion Detection System pada Deteksi Anomali dengan Metode Decision Tree Terhadap Serangan Siber. *Jurnal Ilmu Komputer Dan Agri-Informatika*, *8*(2), 90–94. https://doi.org/10.29244/jika.8.2.90-94

Fatemeh Deldar and Mahdi Abadi. 2023. *Deep Learning for Zero-day Malware Detection and Classification: A Survey*. ACM Comput. Surv. 56, 2, Article 36 (February 2024), 37 pages. https://doi.org/10.1145/3605775

Forsberg, J., & Frantti, T. (2023). *Technical Performance Metrics of a Security Operations Center. Computers and Security*, 135, Article 103529. https://doi.org/10.1016/j.cose.2023.103529

Fortinet. (2024). Essential metrics to track for successful security operations. Fortinet. Retrieved April 12, 2026, from https://www.fortinet.com/uk/resources/cyberglossary/secops-metrics

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14). https://doi.org/10.3390/s21144759

Hafiz, M., & Soewito, B. (2022). *Information Security Systems Design Using SIEM, SOAR and Honeypot*. https://doi.org/10.31004/jptam.v6i2.4850

Hiesgen, R., Nawrocki, M., Barcellos, M., Kopp, D., Hohlfeld, O., Chan, E., Dobbins, R., Doerr, C., Rossow, C., Thomas, D. R., Jonker, M., Mok, R., Luo, X., Kristoff, J., Schmidt, T. C., Wählisch, M., & Claffy, K. (2024). The Age of DDoScovery: An Empirical Comparison of Industry and Academic DDoS Assessments. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, 259–279. https://doi.org/10.1145/3646547.3688451

Holbel, R., Yerby, J., & Smith, W. (2024). UTILIZING VIRTUALIZED HONEYPOTS FOR THREAT HUNTING, MALWARE ANALYSIS, AND REPORTING. *Issues In Information Systems*. https://doi.org/10.48009/1_iis_2024_122

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation.

Ilg, N., Duplys, P., Sisejkovic, D., & Menth, M. (2023). *A Survey of Contemporary Open-Source Honeypots, Frameworks, and Tools*. https://doi.org/10.1016/j.jnca.2023.103737

Issa, M. M., Aljanabi, M., & Muhialdeen, H. M. (2024). Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations. In *Journal of Intelligent Systems* (Vol. 33, Issue 1). Walter de Gruyter GmbH. https://doi.org/10.1515/jisys-2023-0248

Kampourakis, V., Kambourakis, G., Chatzoglou, E., & Zaroliagis, C. (2022). Revisiting man-in-the-middle attacks against HTTPS. *Network Security*, *2022*(3). https://doi.org/10.12968/S1353-4858(22)70028-1

Kocaogullar, Y., Cetin, O., Arief, B., Brierley, C., Pont, J., Hernandez-Castro, J. (2025). *Hunting High or Low: Evaluating the Effectiveness of High-Interaction and Low-Interaction Honeypots*. In: Mehrnezhad, M., Parkin, S. (eds) Socio-Technical Aspects in Security. STAST 2022. Lecture Notes in Computer Science, vol 13855. Springer, Cham. https://doi.org/10.1007/978-3-031-83072-3_2

Kubba, A. A., Al Mutasim, O. M., Talib, M. A., & Nasir, Q. (2025). *A Systematic Review of Honeypot Data Collection, Threat Intelligence Platforms, and AI/ML Techniques*. https://ssrn.com/abstract=5242873

Liu, S., Peng, G., Zeng, H., & Fu, J. (2024). A survey on the evolution of fileless attacks and detection techniques. *Computers & Security*, *137*, 103653. https://doi.org/10.1016/j.cose.2023.103653

Louca, C., Peratikou, A., & Stavrou, S. (2023). A novel Evil Twin MiTM attack through 802.11v protocol exploitation. *Computers & Security*, *130*, 103261. https://doi.org/10.1016/j.cose.2023.103261

ManageEngine. (2025, January). 6+ Tren Cybersecurity 2025 di Indonesia yang Wajib Anda Ketahui.

Https://Blogs.Manageengine.Com/Id/2025/01/15/Tren-Cybersecurity-Di-Indonesia-Yang-Wajib-Anda-Ketahui.Html. https://blogs.manageengine.com/id/2025/01/15/tren-cybersecurity-di-indonesia-yang-wajib-anda-ketahui.html

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 March). https://doi.org/10.1371/journal.pone.0301183

Meurs, T., Cartwright, E., Cartwright, A., Junger, M., & Abhishta, A. (2024). Deception in double extortion ransomware attacks: An analysis of profitability and credibility. *Computers and Security*, *138*. https://doi.org/10.1016/j.cose.2023.103670

Mohale, V. Z., & Obagbuwa, I. C. (2025). Evaluating machine learning-based intrusion detection systems with explainable AI: enhancing transparency and interpretability. *Frontiers in Computer Science*, *7*. https://doi.org/10.3389/fcomp.2025.1520741

Mohd Fuzi, M. F., Mazlan, M. F., Jamaluddin, M. N. F., & Abd Halim, I. H. (2024). Performance analysis of network intrusion detection using T-Pot honeypots. *Journal of Computing Research and Innovation*, *9*(2), 348–360. https://doi.org/10.24191/jcrinn.v9i2.477

Morić, Z., Dakić, V., & Regvart, D. (2025). Advancing Cybersecurity with Honeypots and Deception Strategies. *Informatics*, *12*(1). https://doi.org/10.3390/informatics12010014

Nosyk, Y., Hureau, O., Fernandez, S., Duda, A., & Korczy´nski, M. K. (2023). *Unveiling the Weak Links: Exploring DNS Infrastructure Vulnerabilities and Fortifying Defenses*. https://doi.org/10.1109/EuroSPW59978.2023.00067

Open Information Security Foundation (OISF). (2026). *Suricata: Open source threat detection engine*. https://suricata.io/

Oliveira, S., Leal, A. B., Teixeira, M., & Lopes, Y. K. (2023). *A classification of cybersecurity strategies in the context of discrete event systems*. Annual Reviews in Control, 56, 100907. https://doi.org/10.1016/j.arcontrol.2023.100907

OWASP. (2021). A03:2021 – Injection. Https://Owasp.Org/Top10/A03_2021-Injection/. https://owasp.org/Top10/A03_2021-Injection/

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *ACM Computing Surveys*, *54*(11s), 1–37. https://doi.org/10.1145/3514229

Pamungkas, B. S., & Sembiring, I. (2023). ANALISIS SERANGAN CYBER MENGGUNAKAN HONEYPOT PADA WEB BERBASIS CLOUD. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *4*(3), 1284–1295. https://doi.org/10.35870/jimik.v4i3.325

Pamungkas, C., Hendradi, P., Sasongko, D., & Ghifari, A. (2023). Analysis of Brute Force Attacks Using National Institute Of Standards And Technology (NIST) Methods on Routers. *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, *5*(2), 115–125. https://doi.org/10.20895/inista.v5i2.1039

Paul, A., Sharma, V., & Olukoya, O. (2024). SQL injection attack: Detection, prioritization & prevention. *Journal of Information Security and Applications*, *85*. https://doi.org/10.1016/j.jisa.2024.103871

Pinto, A., Herrera, L. C., Donoso, Y., & Gutierrez, J. A. (2023). Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. In *Sensors* (Vol. 23, Issue 5). MDPI. https://doi.org/10.3390/s23052415

Pittman, J. M. (2023). *Machine learning and port scans: A systematic review*. arXiv. https://doi.org/10.48550/arXiv.2301.13581

Pöhn, D., & Hommel, W. (2022). *TaxIdMA: Towards a taxonomy for attacks related to identities*. *In Proceedings of the 17th International Conference on Availability, Reliability and Security* (ARES 2022) (pp. 1–13). Association for Computing Machinery (ACM). https://doi.org/10.1145/3538969.3544430

Priya, V. S. D., & Chakkaravarthy, S. S. (2023). Containerized cloud-based honeypot deception for tracking attackers. *Scientific Reports*, *13*(1). https://doi.org/10.1038/s41598-023-28613-0

Ramadhan, M. R., Santoso, J. D., Mulyatun, S., Komputer, T., Amikom Yogyakarta, U., Utara, J. R., & Coresponding Author, Y. (2024). Implementasi Intrusion Detection System (Ids) Menggunakan Jejaring Sosial Sebagai Media Notifikasi Dengan Menggunakan Snort. In *BHATARA: Jurnal Multidisiplin* (Vol. 1, Issue 1). https://doi.org/10.59095/jmb.v1i1.81

Ruindungan, J. D., Sompie, S. R. U. A., & Najoan, X. B. N. (2025). Analisis kerentanan terhadap serangan Denial of Service pada website Universitas Sam Ratulangi. Jurnal Teknik Informatika, 20(1), 39–50. https://ejournal.unsrat.ac.id/v3/index.php/informatika/article/view/56730

SecurityHive. (2025, July 14). *Best Honeypot Solutions in 2025 (including open-source!)*. Https://Www.Securityhive.Io/Blog/Best-Honeypot-Solutions-in-2025. https://www.securityhive.io/blog/best-honeypot-solutions-in-2025

Shah, S. S. H., Ahmad, A. R., Jamil, N., & Khan, A. ur R. (2022). Memory Forensics-Based Malware Detection Using Computer Vision and Machine Learning. *Electronics (Switzerland)*, *11*(16). https://doi.org/10.3390/electronics11162579

Spahn, N., Hanke, N., Holz, T., Kruegel, C., & Vigna, G. (2023). Container Orchestration Honeypot: Observing Attacks in the Wild. *ACM International Conference Proceeding Series*, 381–396. https://doi.org/10.1145/3607199.3607205

Srinivasa, S., Pedersen, J. M., & Vasilomanolakis, E. (2022). Interaction matters: a comprehensive analysis and a dataset of hybrid IoT/OT honeypots. *ACM International Conference Proceeding Series*, 742–755. https://doi.org/10.1145/3564625.3564645

Su, Y., Xiong, D., Qian, K., & Wang, Y. (2024). A Comprehensive Survey of Distributed Denial of Service Detection and Mitigation Technologies in Software-Defined Network. In *Electronics (Switzerland)* (Vol. 13, Issue 4). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics13040807

Telegram. (2026). *Telegram Bot API*. https://core.telegram.org/bots/api

Telekom Security. (2024). *T-Pot - The All In One Multi Honeypot Platform*. Https://Github.Com/Telekom-Security/Tpotce. https://github.com/telekom-security/tpotce

Uetz, R., Herzog, M., Hackländer, L., Fkie, F., Schwarz, S., & Henze, M. (2024). *You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks*. https://www.usenix.org/conference/usenixsecurity24/presentation/uetz

Ullrich, J. (2024). *The Top 10 Not So Common SSH Usernames and Passwords*. SANS Internet Storm Center. https://isc.sans.edu/diary/31360

UnderDefense. (2024). *SOC Metrics: Key Performance Indicators for Modern Security Operations*. https://underdefense.com/blog/soc-metrics/

Verizon. (2023). *2023 Data Breach Investigations Report*. https://www.verizon.com/business/resources/Ta5a/reports/2023-dbir-public-sector-snapshot.pdf

VirusTotal. (2026). *VirusTotal API documentation*. https://docs.virustotal.com/

Wang, S., Tu, C., Zhang, Y., Zhang, M., & Xue, P. (2026). Mapping Cyber Bot Behaviors: Understanding Payload Patterns in Honeypot Traffic. Sensors, 26(1), 11. https://doi.org/10.3390/s26010011

Wazuh. (2026). *Wazuh documentation*. https://documentation.wazuh.com/

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.

Xu, J., Ni, M., Zhu, D., & Yu, X. (2023). Overview of SQL Injection Attack Detection Techniques. *Proceedings of the 2023 International Conference on Communication Network and Machine Learning*, 215–225. https://doi.org/10.1145/3640912.3640956

Yandiputra Sunardi, G., Kania Ningsih, A., & Anggoro Universitas Jenderal Achmad Yani, S. (2024). SISTEM MONITORING SERANGAN JARINGAN MENGGUNAKAN INTRUSION DETECTION SYSTEM (IDS) DENGAN NOTIFIKASI TELEGRAM. In *Jurnal Ilmiah Sain dan Teknologi* (Vol. 2, Issue 3). https://doi.org/10.572349/scientica.v2i3.1086

Yelp. (2024). *ElastAlert - Easy & Flexible Alerting With Elasticsearch*. Https://Elastalert.Readthedocs.Io/En/Latest/. https://elastalert.readthedocs.io/en/latest/

Zeek Project. (2026). *Zeek network security monitor*. https://zeek.org/