DAFTAR PUSTAKA

[1] M. Rosso, M. Campobasso, G. Gankhuyag, and L. Allodi, "Saibersoc: Synthetic attack injection to benchmark and evaluate the performance of security operation centers; saibersoc: Synthetic attack injection to benchmark and evaluate the performance of security operation centers." [Online]. Available: https://doi.org/10.1145/3427228.

[2] S. Roy, E. Panaousis, C. Noakes, A. Laszka, S. Panda, and G. Loukas, "Sok: The mitre attck framework in research and practice," 4 2023.

[3] S. Yulianto, B. Soewito, F. L. Gaol, and A. Kurniawan, "Enhancing cybersecurity resilience through advanced red-teaming exercises and mitre attck framework integration: A paradigm shift in cybersecurity assessment," *Cyber Security and Applications*, vol. 3, 12 2025.

[4] M. I. Abdullah, A. I. Abas, and A. I. Hajamydeen, "Effective soc response strategies using mitre attck," pp. 1–7, 2024.

[5] Y. Jiang, Q. Meng, F. Shang, N. Oo, L. T. H. Minh, H. W. Lim, and B. Sikdar, "Mitre attck applications in cybersecurity and the way forward," 2 2025.

[6] Defenxor, "Website Defenxor," https://www.defenxor.com, Jun. 2025, diakses: 18 Juni 2025.

[7] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. NIST Special Publication 800-61 Revision 2, Aug. 2012. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-61r2

[8] DSIEM, "DSIEM — The Open Source Distributed SIEM," https://www.dsiem.org/, accessed: Jul. 12, 2025.

[9] SanWieb, "sigWah," GitHub, 2025, Accessed: Jul. 12, 2025. [Online]. Available: https://github.com/SanWieb/sigWah/blob/master/ossec-rules/local_rules.xml