REFERENCES

[1] X. Li and V. K. Madisetti, "ERAD: Enhanced Ransomware Attack Defense System for Healthcare Organizations," *Journal of Software Engineering and Applications*, vol. 17, no. 05, pp. 270–296, 2024, doi: 10.4236/jsea.2024.175016.

[2] A. Husseis, J. L. Flores, A. Bregar, G. Mazzeo, and L. Coppolino, "Enhancing Cybersecurity Proactive Decision-Making Through Attack Tree Analysis and MITRE Framework," in *Proceedings - International Carnahan Conference on Security Technology*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICCST59048.2023.10726853.

[3] Eliando and A. Budi Warsito, "LockBit Black Ransomware On Reverse Shell: Analysis of Infection Ransomware LockBit Black di Dalam Reverse Shell: Analisis Infeksi," *Cogito Smart Journal*, vol. 9, no. 2, pp. 228–240, 2023.

[4] CISA, "Understanding Ransomware Threat Actors: LockBit," 2023. Accessed: Jan. 07, 2026. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

[5] V. Mahendra and B. Soewito, "Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber Implementation of the NIST Cybersecurity Framework and CIS Controls as Cybersecurity Risk Management," *Techno.COM*, vol. 22, no. 3, pp. 527–538, Aug. 2023.

[6] S. Lee, M. Tsai, and S. W. Shieh, "The Game of Spear and Shield in Next Era of Cybersecurity," *IEEE Trans. Reliab.*, vol. 73, no. 1, pp. 85–92, Mar. 2024, doi: 10.1109/TR.2023.3342874.

[7] A. Yousaf and J. Zhou, "From sinking to saving: MITRE ATT &CK and D3FEND frameworks for maritime cybersecurity," *Int. J. Inf. Secur.*, vol. 23, no. 3, pp. 1603–1618, Jun. 2024, doi: 10.1007/s10207-024-00812-4.

[8] M. M. Khan, "Enhancing Cybersecurity with CIS Controls," *Available online www.jsaer.com Journal of Scientific and Engineering Research 401 Journal of Scientific and Engineering Research*, vol. 10, no. 5, pp. 401–407, 2023, [Online]. Available: www.jsaer.com

[9] M. R. Rahman and L. Williams, “An investigation of security controls and MITRE ATT\&CK techniques,” Nov. 2022, [Online]. Available: http://arxiv.org/abs/2211.06500

[10] Z. Yu and Q. Miao, “Cybersecurity Survivability Testing Technology Based on ATT&CK and D3FEND,” in *Proceedings of the 2025 2nd International Conference on Generative Artificial Intelligence and Information Security, GAIIS 2025*, Association for Computing Machinery, Inc, Jun. 2025, pp. 272–277. doi: 10.1145/3728725.3728768.

[11] A. K. Dash, S. Shivananda, R. Singh, and M. Gupta, “Bridging the Gap: A Comparative Study of CIS and NIST Cybersecurity Frameworks,” in *Advances in Enterprise Technology Risk Assessment*, IGI Global, 2024, pp. 49–66. doi: 10.4018/979-8-3693-4211-4.ch003.

[12] S. Mavire, K. B. Muhwati, N. Kota, and J. A. Awoleye, “Mitigating Ransomware in the Energy and Healthcare Sectors through Layered Defense Strategies,” *International Journal of Scientific and Management Research*, vol. 08, no. 04, pp. 143–166, 2025, doi: 10.37502/ijsmr.2025.8609.

[13] B. Reuben-Owoh and E. Haig, “A Systematic Review of Voluntary Cybersecurity Standards and Frameworks,” *Int. J. Inf. Secur.*, vol. 24, no. 5, Oct. 2025, doi: 10.1007/s10207-025-01121-0.

[14] S. Tommy and M. I. Padli Nasution, “EVALUASI MANAJEMEN RISIKO KEAMANAN SIBER PADA INFRASTRUKTUR DIGITAL PEMERINTAH: STUDI KASUS PUSAT DATA NASIONAL (PDN),” *Jurnal Manajemen Ekonomi dan Bisnis (JMEB)*, vol. 4, 2025, doi: 10.61715.

[15] Eliando and Y. Purnomo, “LockBit 2.0 Ransomware: Analysis of infection, persistence, prevention mechanism,” *Cogito Smart Journal* |, vol. 8, no. 1, 2022.

[16] Microsoft, “Audit SAM,” Microsoft Learn. Accessed: Jan. 07, 2026. [Online]. Available: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/audit-sam

[17] Microsoft, “NTLM Overview,” Microsoft Learn. Accessed: Jan. 07, 2026. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/security/kerberos/ntlm-overview

[18] Microsoft, “Server Message Block (SMB) Overview,” Microsoft Learn. Accessed: Jan. 08, 2026. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview

[19] F. Saccone, P. Melillo, A. Sgueglia, A. Di Sorbo, and C. A. Visaggio, “The ransomware blueprint: Attack patterns and strategic variations across gangs,” *Journal of Information Security and Applications*, vol. 95, Dec. 2025, doi: 10.1016/j.jisa.2025.104264.

[20] CISA, “#StopRansomware: LockBit 3.0,” 2023. Accessed: Apr. 21, 2026. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a

[21] MITRE, “Use Alternate Authentication Material: Pass the Hash,” Mitre Corporation. Accessed: Jan. 08, 2026. [Online]. Available: https://attack.mitre.org/techniques/T1550/002/

[22] MITRE, “Impair Defenses: Disable or Modify Tools,” MITRE Corporation. Accessed: Jan. 08, 2026. [Online]. Available: https://attack.mitre.org/techniques/T1562/001/

[23] Microsoft, “Set-MpPreference,” Microsoft Learn. Accessed: Feb. 20, 2026. [Online]. Available: https://learn.microsoft.com/en-us/powershell/module/defender/set-mppreference?view=windowsserver2025-ps

[24] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, “MITRE ATT&CK®: Design and Philosophy,” 2020.

[25] N. Suk-On, N. Thiratitsakun, and K. Chimmanee, “Digital Forensic Analysis of Lockbit Ransomware Attack on Operational Technology,” in *8th International Conference on Information Technology 2024, InCIT 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 624–629. doi: 10.1109/InCIT63192.2024.10810564.

[26] MITRE, “MITRE D3FEND Knowledge Graph,” MITRE Corporation. Accessed: Jan. 04, 2026. [Online]. Available: https://d3fend.mitre.org/

[27] Microsoft, “Advanced security audit policy settings,” Microsoft Learn. Accessed: Feb. 22, 2026. [Online]. Available: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/advanced-security-audit-policy-settings

[28] Microsoft, “Direct host SMB over TCP/IP,” Microsoft Learn. Accessed: Jan. 23, 2026. [Online]. Available: https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/direct-hosting-of-smb-over-tcpip

[29] Microsoft, “Protect security settings with tamper protection,” Microsoft Learn. Accessed: Jan. 26, 2026. [Online]. Available: https://learn.microsoft.com/en-us/defender-endpoint/prevent-changes-to-security-settings-with-tamper-protection

[30] Microsoft, “Protect important folders with controlled folder access,” Microsoft Learn. Accessed: Jan. 28, 2026. [Online]. Available: https://learn.microsoft.com/en-us/defender-endpoint/controlled-folders

[31] Center for Internet Security, “CIS Critical Security Controls Version 8.1,” 2024.

[32] Oracle Corporation, “About Oracle VirtualBox.” Accessed: Feb. 11, 2026. [Online]. Available: https://www.virtualbox.org/manual/topics/Introduction.html#ct_about-virtualbox

[33] Microsoft, “Windows 11 available on October 5.” Accessed: Feb. 11, 2026. [Online]. Available: https://blogs.windows.com/windowsexperience/2021/08/31/windows-11-available-on-october-5/

[34] OffSec, “Kali Docs.” Accessed: Feb. 11, 2026. [Online]. Available: https://www.kali.org/docs/

[35] MITRE, “Mimikatz Software.” Accessed: Feb. 11, 2026. [Online]. Available: https://attack.mitre.org/software/S0002/

[36] Fortra, “Fortra Impacket.” Accessed: Feb. 12, 2026. [Online]. Available: https://github.com/fortra/impacket