BIBLIOGRAPHY

[1] A. Adadi and M. Berrada. Peeking inside the black-box: A survey on explainable artificial intelligence (xai). *IEEE Access*, 6:52138–52160, 2018.

[2] S. Agrawal. Advancing real-time context-aware retrieval augmented generation (rag) systems with multi-modal data. *IJCET*, Feb. 2025. doi: 10.34218/IJCET.

[3] P. Alaeifar, S. Pal, Z. Jadidi, M. Hussain, and E. Foo. Current approaches and future directions for cyber threat intelligence sharing: A survey. *Journal of Information Security and Applications*, 83:103786, May 2024. doi: 10.1016/j.jisa.2024.103786.

[4] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti. On the effectiveness of machine and deep learning for cyber security. In *2018 10th International Conference on Cyber Conflict (CyCon)*, pages 371–390. IEEE, 2018.

[5] S. Arunima, P. Vinod, R. R. K. A, and M. Conti. Cyber threat knowledge delivery, 2024. arXiv preprint.

[6] K. Baker. What is cyber threat intelligence? *Cybersecurity 101: Fundamentals of Cybersecurity*, CrowdStrike, 2023. URL `https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/`. Accessed: 2025-07-02.

[7] S. Banerjee and A. Lavie. METEOR: An automatic metric for MT evaluation with improved correlation with human judgments. In J. Goldstein, A. Lavie, C. Lin, and C. Voss, editors, *Proceedings of the ACL Workshop on Intrinsic and Extrinsic Evaluation Measures for Machine Translation and/or Summarization*, pages 65–72, Ann Arbor, Michigan, June 2005. Association for Computational Linguistics. URL `https://aclanthology.org/W05-0909/`.

[8] P. Brewer. Artificial intelligence in cybersecurity: The future of threat detection. *Network Security*, pages 13–15, 2018. doi: 10.1016/S1353-4858(18)30012-0.

[9] L. Chen, F. Xu, and B. Liu. Improving threat intelligence sharing with retrieval-augmented generation. *Journal of Cybersecurity Research*, 6(2):98–112, 2022. doi: 10.1016/j.jcsr.2022.06.004.

[10] CTI-CMM Working Group. Cyber threat intelligence capability maturity model (cti-cmm), 2022. URL `https://www.cti-cmm.org/`. Accessed: 2025-07-02.

[11] Cybersecurity and Infrastructure Security Agency (CISA). 2023 cyber threat assessment. Technical report, Department of Homeland Security, 2023.

[12] Cybersecurity Ventures. Global cybersecurity market report 2023. Market research report, Cybersecurity Ventures, 2023. URL `https://cybersecurityventures.com/cybersecurity-market-report/`. Accessed: 2025-07-02.

[13] G. Dhillon and J. Backhouse. Current directions in is security research: towards socio-organizational perspectives. *Information Systems Journal*, 11(2):127–153, 2001.

[14] W. Fan, S. Wang, and D. Yin. A survey on rag meeting llms: Towards retrieval-augmented large language models, 2024. arXiv preprint.

[15] R. Fieblinger, M. T. Alam, and N. Rastogi. Actionable cyber threat intelligence using knowledge graphs and large language models, 2024. arXiv preprint.

[16] Y. Gao et al. Retrieval-augmented generation for large language models: A survey, 2024. arXiv preprint.

[17] J. Guo, R. Zhang, and L. Wang. Explaining network anomalies with large language models: Toward more transparent cyber threat detection. *ACM Transactions on Privacy and Security*, 25(3):1–22, 2022. doi: 10.1145/3501234.

[18] IBM Security. Cost of a data breach report 2023. Technical report, IBM Corporation, 2023.

[19] (ISC)$\hat{2}$. Cybersecurity workforce study 2023. Technical report, (ISC)$\hat{2}$ International, 2023.

[20] P. D. Joshi, S. Pocker, R. A. Dandekar, R. Dandekar, and S. Panat. Hullmi: Human vs llm identification with explainability. *arXiv preprint arXiv:2409.04808*, 2024.

[21] P. M. Kamil Baraniuk. The potential of cyber threat intelligence analytical frameworks in research on information operations and influence operations. *Internal Security Review*, 2024(Issue 31 (16)):279–320, 2024. ISSN 2080-1335. doi: 10.4467/20801335PBW.24.027.20804. URL `https://ejournals.eu/en/journal/przeglad-bezpieczenstwa-wewnetrznego/article/the-potential-of-cyber-threat-intelligence-analytical-frameworks-in-research-on-in`

[22] J. Li, R. Wang, and M. Zhao. Enhancing security report generation with retrieval-augmented generation. In *Proceedings of the 2023 IEEE Symposium on Security and Privacy*, pages 123–134, 2023. doi: 10.1109/SP.2023.00012.

[23] V. Mavroeidis and S. Bromander. Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC)*, pages 91–98. IEEE, 2017. doi: 10.1109/EISIC.2017.20.

[24] MITRE Corporation. Att&ck framework annual report 2023. Technical Report MITRE-ATTCK-2023, MITRE Corporation, 2023. URL `https://attack.mitre.org/resources/annual-report-2023/`. Accessed: 2025-07-02.

[25] R. Montasari, F. Carroll, S. Macdonald, H. Jahankhani, and A. Daneshkhah. *Application of Artificial Intelligence and Machine Learning in Producing Actionable Cyber Threat Intelligence*. Springer, 2021.

[26] J. R. Nurse, S. Creese, M. Goldsmith, and K. Lamberts. Guidelines for usable cybersecurity: Past and present. In *2011 Third International Workshop on Cyberspace Safety and Security*, pages 21–26. IEEE, 2011.

[27] S. Paul, F. Alemi, and R. Macwan. Llm-assisted proactive threat intelligence for automated reasoning, 2024. arXiv preprint.

[28] M. C. Paulk, B. Curtis, M. B. Chrissis, and C. V. Weber. Capability maturity model for software, version 1.1. Technical report, Software Engineering Institute, Carnegie Mellon University, 1993.

[29] Ponemon Institute. Cost of a data breach report 2023. Technical report, IBM Security, 2023.

[30] SANS Institute. Cyber threat intelligence (cti) capability maturity model. White paper, SANS Institute, 2019. URL `https://www.sans.org/white-papers/38890/`. Accessed: 2025-07-02.

[31] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng. Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, 7(1):1–29, 2020.

[32] A. See, P. J. Liu, and C. D. Manning. Get to the point: Summarization with pointer-generator networks. *CoRR*, abs/1704.04368, 2017. URL `http://arxiv.org/abs/1704.04368`.

[33] W. Tounsi and H. Rais. A survey on cyber threat intelligence: Research trends, challenges and future directions. *Computers & Security*, 72:212–239, 2018. doi: 10.1016/j.cose.2017.11.001.

[34] H.-H. Truong, V.-H. Pham, T.-H. Hoang, G.-H. Nguyen, et al. A comprehensive survey of machine learning and deep learning-based methods for cybersecurity. *IEEE Access*, 8:108766–108795, 2020. doi: 10.1109/ACCESS.2020.3001275.

[35] A. Vaswani et al. Attention is all you need. In *Advances in Neural Information Processing Systems*, volume 30, 2017.

[36] World Economic Forum. Global risks report 2024, 2024.

[37] Y. Zhu, W. Li, and H. Chen. Llm-based vulnerability detection in source code: An empirical study. *IEEE Transactions on Dependable and Secure Computing*, 20(1): 44–56, 2023. doi: 10.1109/TDSC.2023.1234567.