DAFTAR PUSTAKA

Ahmad, U. A., Saputra, R. E., & Harahap, R. M. (2021). *Implementasi High Availability Server Menggunakan Platform Haproxy (Studi Kasus: Aplikasi Zammad Untuk Online Help Desk) Implementation Of High Availability Server Using The Haproxy Platform (Case Study: Zammad Aplication For Online Helpdesk)*. *8*(5).

Calçada, A., & Bernardino, J. (2022). Experimental Evaluation of Low Code development, Java Swing and JavaScript programming. *ACM International Conference Proceeding Series*, 103–112. https://doi.org/10.1145/3548785.3548792

Cobb, M., & Wigmore, I. (2019, Juli 9). *Threat Intelligence (cyber threat intelligence)*. TechTarget. https://www.techtarget.com/whatis/definition/threat-intelligence-cyber-threat-intelligence

Dannana, S., Prabakaran, T., Rajasekaran, A. S., Kumareshan, N., Daniel Shadrach, S. F., & Kalyanchakravarthi, P. (2022). A Novel System Model for Managing Cyber Threat Intelligence. *MysuruCon 2022 - 2022 IEEE 2nd Mysore Sub Section International Conference*. https://doi.org/10.1109/MysuruCon55714.2022.9972703

Khan, Z. C., Mkhwanazi, T., & Masango, M. (2023). A Model for Cyber Threat Intelligence for Organisations. *6th International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, icABCD 2023 - Proceedings*. https://doi.org/10.1109/icABCD59051.2023.10220503

Mavroeidis, V., Eis, P., Zadnik, M., Caselli, M., & Jordan, B. (2021). On the Integration of Course of Action Playbooks into Shareable Cyber Threat Intelligence. *Proceedings - 2021 IEEE International Conference on Big Data, Big Data 2021*, 2104–2108. https://doi.org/10.1109/BigData52589.2021.9671893

MISP. (t.t.). *MISP Features and Functionalities*. MISP Project. Diambil 1 Januari 2024, dari https://www.misp-project.org/features/

misp.gitbooks.io. (2023). *MISP Book*. https://misp.gitbooks.io/misp-book/content/

Mokaddem, S., Wagener, G., Dulaunoy, A., & Iklody, A. (2019). *Taxonomy driven indicator scoring in MISP threat intelligence platforms*. http://arxiv.org/abs/1902.03914

Naik, N., Jenkins, P., Grace, P., & Song, J. (2022). Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model. *ISSE 2022 - 2022 8th IEEE International Symposium on Systems Engineering, Conference Proceedings*. https://doi.org/10.1109/ISSE54508.2022.10005490

Paine, K., Whitehouse, O., Firefly, B., Sellwood, J., & Shaw, A. (2023). *RFC 9424: Indicators of Compromise (IoCs) and Their Role in Attack Defence*. https://www.rfc-editor.org/info/rfc9424

Pinho, D., Aguiar, A., & Amaral, V. (2023). What about the usability in low-code platforms? A systematic literature review. *Journal of Computer Languages*, *74*. https://doi.org/10.1016/j.cola.2022.101185

Salamun, M. A., Muttaqin, F. Z., & Rosyid, N. R. (2023). Design and Implementation of Honeypot Indicator of Compromise (IoC) Profiling using Malware Information Sharing Platform (MISP). *AIP Conference Proceedings*, *2828*(1). https://doi.org/10.1063/5.0164216

Tuyishime, A., Basciani, F., Iovino, L., Izquierdo, J. L. C., Cabot, J., & Pierantonio, A. (2023). *Bridging Workflow Automation Tools and EMF Modeling Ecosystems*. 893–897. https://doi.org/10.1109/models-c59198.2023.00140

Yih, Y. H., Tunku, U., & Rahman, A. (2022). *SYSTEM INTEGRATION WITH MULTIPLE SYSTEM FLOW TOOLS A REPORT SUBMITTED TO*.

Zammad Foundation. (2024). *Zammad*. https://docs.zammad.org/en/latest/about/zammad.html