DAFTAR PUSTAKA

Abu, S., Selamat, S. R., Ariffin, A. F. M., & Yusof, R. (2018). Cyber Threat Intelligence – Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*, 371–379. https://api.semanticscholar.org/CorpusID:4882915

Alanda, A., Mooduto, H. A., & Hadi, R. (2023). JITCE (Journal of Information Technology and Computer Engineering) Real-time Defense Against Cyber Threats: Analyzing Wazuh's Effectiveness in Server Monitoring. *JITCE*, 56–62. https://doi.org/10.25077/jitce.7.02.56-62.2023

Alexandru STAN, M. (2021). *Automation of Log Analysis Using the Hunting ELK Stack* (Vol. 3, Issue 1).

Anam, F. C., Sasmita, G. M. A., & Pratama, I. P. A. E. (2023). Implementation of Security Information and Event Management (SIEM) for Monitoring IT Assets Using Alienvault OSSIM (Case Study: Udayana University Information Resources Unit). *JITTER : Jurnal Ilmiah Teknologi Dan Komputer*, *4*(3). https://doi.org/10.24843/jtrti.2023.v04.i03.p03

DFIR IRIS. (2023). Incident Response Information Sharing with DFIR IRIS: Enhancing Cybersecurity Investigations. *Threat Intelligence Lab*. https://blog.dfir-iris.org

Dyan Heluka, H., & Sulistyo, W. (2023). *Perancangan Dan Implementasi Security Information and Event Management (SIEM) pada Layanan Virtual Server*.

Farrel, F. I. F., Is Mardianto, S.Si, M.Kom, & Ir. Adrian Sjamsul Qamar, MTI. (2024). Implementation of Security Information & Event Management (SIEM) Wazuh with Active Response and Telegram Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System. *Intelmatics*, *4*(1), 1–7. https://doi.org/10.25105/itm.v4i1.18529

Fernandes, R., Bugla, S., Pinto, P., & Pinto, A. (2023). On the Performance of Secure Sharing of Classified Threat Intelligence between Multiple Entities. *Sensors*, *23*(2). https://doi.org/10.3390/s23020914

Gillard, S., David, D. P., Mermoud, A., & Maillart, T. (2023). Efficient collective action for tackling time-critical cybersecurity threats. *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyad021

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

Gupta, S., Sasidharan, D., & Joseph, S. (2021). *THE CHALLENGES IN LEVERAGING CYBER THREAT INTELLIGENCE*.

Hapsari, R. D., & Pambayun, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1). https://doi.org/10.33701/jk.v5i1.3208

IBM. (2024). *What is Security Information and Event Management (SIEM)?* IBM. https://www.ibm.com/id-en/topics/siem

Jeon, S. E., Lee, S. J., Lee, E. Y., Lee, Y. J., Ryu, J. H., Moon, J. H., Yi, S. M., & Lee, I. G. (2023). An Effective Threat Detection Framework for Advanced Persistent Cyberattacks. *Computers, Materials and Continua*, *75*(2). https://doi.org/10.32604/cmc.2023.034287

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/https://doi.org/10.1016/j.inffus.2023.101804

Laksmiati, D. (2021). IMPLEMENTASI WAZUH 4.0 UNTUK PERLINDUNGAN KEAMANAN INTEGRITAS FILE. In *Jurnal AKRAB JUARA* (Vol. 6).

Murti Adi Santoso, W., Qotrun Nada, N., Gedung Lantai, S. B., & Sidodadi Timur, J. (2022). Monitoring Threats Menggunakan Huntbox dengan Metode MDR (Managed Detection and Response) pada Security Operation Center (SOC). In *Science And Engineering National Seminar* (Vol. 7, Issue 7).

Mycek, A. (2023). Monitoring, Management, and Analysis of Security Aspects of IaaS Environments. *Journal of Telecommunications and Information Technology*, *4*, 108–116. https://doi.org/10.26636/jtit.2023.4.1419

Roberts, A. (2021). Cyber Threat Intelligence – What Does It Even Mean? In *Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers* (pp. 17–36). Apress. https://doi.org/10.1007/978-1-4842-7220-6_2

Sani, J. (2023). Improved Log Monitoring using Host-based Intrusion Detection System. *AIJMR-Advanced International Journal of Multidisciplinary Research*, *1*(1), 15–22.

Sheeraz, M., Paracha, M. A., Haque, M. U., Durad, M. H., Mohsin, S. M., Band, S. S., & Mosavi, A. (2023). Effective Security Monitoring Using Efficient SIEM Architecture. *Human-Centric Computing and Information Sciences*, *13*. https://doi.org/10.22967/HCIS.2023.13.023

Spyros, A., Papoutsis, A., Koritsas, I., Mengidis, N., Iliou, C., Kavallieros, D., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2022). Towards Continuous Enrichment of Cyber Threat Intelligence: A Study on a Honeypot Dataset. *Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience, CSR 2022*, 267–272. https://doi.org/10.1109/CSR54599.2022.9850295

Wazuh. (2024). *The Open Source Security Platform | Wazuh*. Web. https://documentation.wazuh.com/current/index.html

Widyatono, D. P., & Sulistyo, W. (2023). Pemodelan Instrusion Prevention System Untuk Pendeteksi Dan Pencegahan Penyebaran Malware Menggunakan Wazuh. *Journal of Information Technology Ampera*, *4*(1), 113–127. https://journal-computing.org/index.php/journal-ita/index

Zohra, F., & Zerrouk, C. (2024). *NETWORK INTRUSION DETECTION SYSTEM FOR DENIAL-OF-SERVICE ATTACK DETECTION IN 5G*.