DAFTAR PUSTAKA

Alam, S., Lestari, S., Fauziyyah, A. K., & Dzulfikar. (2024). Implementasi Docker Container untuk Sistem Monitoring dan Pengontrolan Peralatan Listrik di Laboratorium Cerdas. *Jurnal Elektronik Ilmu Komputer Udayana*, *12*(3), 697–704.

Alshehri, M. (2021). Generic attribute scoring for information decay in threat information sharing platform. *Computers, Materials and Continua*, *67*(1), 917–931. https://doi.org/10.32604/cmc.2021.014848

Analisis, K. D., Tony, F. Van, & Yazid, S. (2024). *Perancangan Tim Security Operation Center Di Perusahaan Sektor Finansial : Studi Designing Security Operations Center Team In Financial Sector Company : Sace Study And Analysis*. *7*(2), 95–110.

Hidayat, M. R. T., Widiyasono, N., & Gunawan, R. (2025). OPTIMASI DETEKSI MALWARE PADA SIEM WAZUH MELALUI INTEGRASI CYBER THREAT INTELLIGENCE DENGAN MISP DAN DFIR-IRIS. *Jurnal Informatika Dan Teknik Elektro Terapan*, *13*(1). https://doi.org/10.23960/jitet.v13i1.5686

Nayyul. (2024). *IMPLEMENTASI SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR) SISTEM MENGGUNAKAN SHUFFLE DI POLITEKNIK CALTEX RIAU*.

Rasyid. (2024). *Integrasi wazuh dan suricata dengan notifikasi telegram*.

Rahayu, Y. D. P., & Trianto, N. (2021). Analisis Malware Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2.1. *Info Kripto*, *1*.

Sidi. (2024). *LAPORAN PROYEK AKHIR IMPLEMENTASI IDS / IPS MENGGUNAKAN OPNSENSE DAN EVENT LOG MANAGEMENT MENGGUNAKAN ELK IMPLEMENTASI IDS / IPS MENGGUNAKAN OPNSENSE DAN EVENT LOG MANAGEMENT*.

Zahira, Z. F. (2023). Implementasi Security Information and Event Management (SIEM) menggunakan Wazuh pada Politeknik Caltex Riau. *Nucl. Phys.*, *13*(1), 104–116.

Fikri. (2024). *MONITORING KEAMANAN JARINGAN*.

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). *Science And Engineering National Seminar*, *7*(7).

Yunia Pratama, R. (2020). Proyek Pengembangan Cyber Threat Intelligence

Platform Guna Mendukung Ketahanan Siber Indonesia. *Academia.Edu*. https://www.academia.edu/download/58070029/Proyek_Pengembangan_Cyber_Threat_Intelligent_Platform__.pdf

Harri Kalikka. (2024). *Utilization of Threat Information in Detection Process of Cybersecurity Anomalies*. 98.

TryHackMe. (2023). Cyber Threat Intelligence. [online]. Tersedia: https://tryhackme.com/room/threatintelligenceforsoc

Ramadhani, R., Christie, A., Dewani, A. A., Krisnawan, M., & Dhimaz Ardhana, R. (2025). Optimalisasi Intelijen Ancaman Siber di Security Operation Centers dengan Pemanfaatan Large Language Models (LLM) dan SIEM. *Jurnal Ilmiah Multidisipline*, *3*(5), 535–541. https://doi.org/10.5281/zenodo.15707795

Khalda, K., & Wibowo, D. K. (2025). Malware Behavior Analysis Using Static and Dynamic Analysis Approaches. *Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi*, *4*(1), 1–8. https://doi.org/10.20885/snati.v4.i1.1

Surya Rahmadani, D., Ariyadi, T., Novitasari, E., Pertiwiningsih, D., & Kunci, K. (2025). ANALISIS KINERJA WEB SERVER BERBASIS LINUX UBUNTU 22.04. *Jurnal Tera*, *5*(1). http://jurnal.undira.ac.id/index.php/jurnaltera/Page

Ulvi, K., Rasikha, G., Aulia, R., Rika, S., & Hidayani, M. (2026). Kajian Ancaman Malware dan Upaya Pencegahan melalui Penguatan Keamanan Sistem Komputer. *JIKUM: Jurnal Ilmu Komputer*, *2*(1), 108–110. https://doi.org/10.62671/jikum.v2i1.155