DAFTAR PUSTAKA

Ali G, Shah S, ElAffendi M. 2025. Enhancing cybersecurity incident response: AI-driven optimization for strengthened advanced persistent threat detection. *Results Eng*. 25:104078. https://doi.org/10.1016/J.RINENG.2025.104078.

Aljahdali AO, Alsulami R. 2025. STREAMLINING THREAT RESPONSE AND AUTOMATING CRITICAL USE CASES WITH SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR). *J Digit Secur Forensics*. 2(1):36–57–36–57. https://doi.org/10.29121/DIGISECFORENSICS.V2.I1.2025.45.

Ammi M, Jama YM. 2023. Cyber Threat Hunting Case Study using MISP. *J Internet Serv Inf Secur*. 13(2):1–29. https://doi.org/10.58346/JISIS.2023.I2.001.

Anggara TR. 2023. Strategi Implementasi SIEM untuk Mengurangi Risiko terhadap Kebocoran Informasi. *J Teknol Terpadu*. 9(2):101–107. https://doi.org/10.54914/JTT.V9I2.756.

Anggraini I, Widhiantoro D. 2025. Mengenal SIEM dan SOAR: Pilar Utama Keamanan Informasi Modern. *Semin Nas Inov Vokasi*. 4:1166–1174. [diakses 2025 Agu 22]. https://prosiding.pnj.ac.id/index.php/sniv/article/view/4170.

Badan Siber dan Sandi Negara. 2025 Feb. Lanskap Keamanan Siber Indonesia 2024. *Lap Tah Has Monit 2024*., siap terbit. [diakses 2025 Agu 22]. https://www.bssn.go.id/wp-content/uploads/2025/02/LANSKAP-KEAMANAN-SIBER-2024-1.pdf.

Basta A, Basta N, Anwar W, Essar MI. 2024. *Open-Source Security Operations Center (SOC): A Complete Guide to Establishing, Managing, and Maintaining a Modern SOC*. Ed ke-1. Wiley. [diakses 2025 Agu 9]. https://unidel.edu.ng/focelibrary/books/Open-Source Security Operations Center (SOC) (etc.) (Z-Library).pdf.

Bridges RA, Rice AE, Oesch S, Nichols JA, Watson C, Spakes K, Norem S, Huettel M, Jewell B, Weber B, *et al.* 2023. Testing SOAR tools in use. *Comput Secur*.

129:103201. https://doi.org/10.1016/j.cose.2023.103201.

Debar H. 2021. *Security Operations & Incident Management Knowledge Area Version 1.0.2*. 1.0.2. Chivers H, editor. The Cyber Security Body of Knowledge (CyBOK). [diakses 2025 Agu 9]. https://www.cybok.org/media/downloads/Security_Operations_Incident_Management_v1.0.2.pdf.

EC-Council. 2022 Mei 24. Week Four of EC-Council Certified Incident Handler (ECIH) Version 2 Self-Study Training - The Security Noob. [diakses 2025 Agu 22]. https://thesecuritynoob.com/course/week-four-of-ec-council-certified-incident-handler-ecih-version-2-self-study-training/.

Frikky. 2020. Shuffle Configuration Documentation. [diakses 2025 Agu 10]. https://shuffler.io/docs/configuration.

Harahap AHH, Andani CD, Christie A, Nurhaliza D, Fauzi A. 2023. Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *J Manaj dan Pemasar Digit*. 1(2):73–83. https://doi.org/10.38035/JMPD.V1I2.34.

Heluka HD, Sulistyo W. 2023. Perancangan Dan Implementasi Security Information and Event Management (SIEM) pada Layanan Virtual Server. *Progresif J Ilm Komput*. 19(2):912–922. https://doi.org/10.35889/PROGRESIF.V19I2.1353.

Ilmi A, Seta HB, Pradnyana IWW. 2022. Evaluasi Risiko Celah Keamanan Menggunakan Metodologi Open-Source Security Testing Methodology Manual (OSSTMM) Pada Aplikasi Web Terbaru Fakultas Ilmu Komputer UPN Veteran Jakarta. *Inform J Ilmu Komput*. 18(2):190–197. https://doi.org/10.52958/IFTK.V18I2.4672.

IRIS. 2024 Des 3. IRIS Documentation. [diakses 2025 Agu 10]. https://docs.dfir-iris.org/latest/.

Ismail, Kurnia R, Brata ZA, Nelistiani GA, Heo S, Kim Hyeongon, Kim Howon. 2025. Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic Artificial Intelligence. *Inf 2025, Vol 16, Page 365*. 16(5):365. https://doi.org/10.3390/INFO16050365.

Johansen G. 2022. *Digital Forensics and Incident Response Incident response tools and techniques for effective cyber threat response*. Ed ke-3. Packt Publishing. [diakses 2025 Agu 9]. https://itbooks.ir/assets/files/books/cybersecurity/digital-forensics-and-incident-response.pdf.

Jumiaty BS. 2024. SIEM and Threat Intelligence: Protecting Applications with Wazuh and TheHive. *Int J Adv Comput Sci Appl*. 15(9):239–251. https://doi.org/10.14569/IJACSA.2024.0150923.

Kaspersky. 2025 Feb 19. Kaspersky reports nearly 900 million phishing attempts in 2024 as cyber threats increase. [diakses 2025 Agu 23]. https://www.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase.

Knerler K, Parker I, Zimmerman C. 2022. *11 Strategies of a World-Class Cybersecurity Operations Center*. Ed ke-2. MITRE. [diakses 2025 Agu 9]. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf.

Kovacevic B. 2023. *Security Orchestration, Automation, and Response for Security Analysts: Learn the secrets of SOAR to improve MTTA and MTTR and strengthen your organization's security posture*. Ed ke-1. Packt Publishing. [diakses 2025 Agu 9]. https://www.cliffsnotes.com/study-notes/16509350.

Naraduhita B, Bumbungan MTE. 2025 Jun. Leveraging LLM Integration with Wazuh and Jira for Automated Cyberattack Detection and Incident Response. [diakses 2025 Agu 28]. https://www.researchgate.net/publication/392734102_Leveraging_LLM_Integra tion_with_Wazuh_and_Jira_for_Automated_Cyberattack_Detection_and_Incident_Response.

Pulyala SR, Desetty AG, Jangampet VD. 2019. The Impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) Efficiency: A Comprehensive Analysis. *Turkish J Comput Math Educ*. 10(3):1545–1549. https://doi.org/10.61841/TURCOMAT.V10I3.14323.

Purnomosidi B. 2025 Agu 8. Cyber Threat Intelligence: Menuju Strategi Keamanan Proaktif. *KEDAULATAN RAKYAT*., siap terbit. [diakses 2025 Agu 10]. https://www.utdi.ac.id/terbitan/180/cyber-threat-intelligence-menuju-strategi-keamanan-proaktif.

Rafeli AI, Seta HB, Widi IW. 2022. Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ. *Inform J Ilmu Komput*. 18(2):97–103. https://doi.org/10.52958/IFTK.V18I2.4632.

Ramadoni, Amirudin MZ, Fahmi R, Utami E, Mustafa MS. 2021. Evaluasi Penggunaan Prometheus dan Grafana Untuk Monitoring Database Mongodb. *J Inform Polinema*. 7(2):43–50. https://doi.org/10.33795/JIP.V7I2.530.

Ropi Taofiq Hidayat M, Widiyasono N, Gunawan R. 2025. Optimasi Deteksi Malware pada SIEM Wazuh melalui Integrasi Cyber Threat Intelligence dengan MISP dan DFIR-IRIS. *J Inform dan Tek Elektro Terap*. 13(1):2830–7062. https://doi.org/10.23960/JITET.V13I1.5686.

Sagita IPWA. 2024. Implementasi Security Orchestration, Automation, and Response dengan Wazuh & Shuffle untuk Otomasi Respon SOC di Departemen Teknologi Informasi Institut Teknologi Sepuluh Nopember. [diakses 2025 Mei 7]. https://repository.its.ac.id/106448/.

Saputra FA, Rizky Dharmawan T, Rustianto A. 2024. Implementasi Wazuh SIEM untuk Manajemen Log Event di Pesantren Teknologi Informasi dan Komunikasi Jombang. *J Inform Terpadu*. 10(2):146–155. https://doi.org/10.54914/JIT.V10I2.1435.

Shea S. 2024 Feb 5. What is SOAR (Security Orchestration, Automation and Response)? | Definition from TechTarget. [diakses 2025 Agu 22]. https://www.techtarget.com/searchsecurity/definition/SOAR.

Trend Micro. 2025 Mar 25. Trend 2025 Cyber Risk Report | Trend Micro (US). [diakses 2025 Agu 22]. https://www.trendmicro.com/vinfo/us/security/news/threat-landscape/trend-2025-cyber-risk-report.

Universitas Pembangunan Nasional Veteran Jakarta. 2024. UPA Teknologi Informasi dan Komunikasi. [diakses 2025 Agu 22]. https://upatik.upnvj.ac.id/.

Vaswani A, Brain G, Shazeer N, Parmar N, Uszkoreit J, Jones L, Gomez AN, Kaiser Ł, Polosukhin I. 2023. Attention Is All You Need.

Wazuh. 2025. Wazuh Documentation. [diakses 2025 Agu 11]. https://documentation.wazuh.com/current/index.html.