UNIVERSITAS
GADJAH MADA
Otomatisasi Pelaporan Insiden Keamanan Berbasis n8n dan Large Language Model
Dzaki Maulana Asif, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR PUSTAKA

[1] R. Sugumar, "Next-Generation Security Operations Center (SOC) Resilience: Autonomous Detection and Adaptive Incident Response Using Cognitive AI Agents," *International Journal of Technology Management & Humanities (IJTMH) e-ISSN*, vol. 10, no. 2, pp. 2454–566, 2024, doi: 10.21590/ijtmh.2024100210.

[2] S. A. Chamkar, M. Zaydi, Y. Maleh, and N. Gherabi, "Improving Threat Detection in Wazuh Using Machine Learning Techniques," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, Jun. 2025, doi: 10.3390/jcp5020034.

[3] R. Wiratama, A. Pirdhaus, E. R. Putri Bintoro, Z. Sari, and S. Syaifuddin, "Random Forest and LLM Synergies Framework for Autonomous DDoS Mitigation," *Jurnal Teknik Informatika (Jutif)*, vol. 7, no. 1, pp. 515–528, Feb. 2026, doi: 10.52436/1.jutif.2026.7.1.5300.

[4] R. van der Kleij, J. M. Schraagen, B. Cadet, and H. Young, "Developing decision support for cybersecurity threat and incident managers," *Comput. Secur.*, vol. 113, Feb. 2022, doi: 10.1016/j.cose.2021.102535.

[5] S. G. AboulEla and R. F. Kashef, "Leveraging large language models, graph neural networks, and explainable AI for revolutionizing the next-generation network intrusion detection systems," Oct. 01, 2025, *Springer*. doi: 10.1007/s10844-025-00964-2.

[6] Vectra AI, "2023 State of Threat Detection The Defenders' Dilemma," 2023. Accessed: Mar. 04, 2026. [Online]. Available: https://cdn.prod.website-files.com/64e50cbe2b6f932c04238c14/651abd08bdcf7f22afa6fb8a_2023-state-of-threat-detection.pdf

[7] P. Kearney, M. Abdelsamea, X. Schmoor, F. Shah, and I. Vickers, "Combating Alert Fatigue in the Security Operations Centre Author names and affiliations."

UNIVERSITAS
GADJAH MADA
Otomatisasi Pelaporan Insiden Keamanan Berbasis n8n dan Large Language Model
Dzaki Maulana Asif, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

[8] C. Zhong and A. Yayla, "Cognitive Impacts of Explainable AI in Cybersecurity Incident Response: Challenges and Propositions," *Information Systems Frontiers*, 2025, doi: 10.1007/s10796-025-10609-y.

[9] S. Arora and J. D. Hastings, "A Survey-Based Quantitative Analysis of Stress Factors and Their Impacts Among Cybersecurity Professionals," Sep. 2024, [Online]. Available: http://arxiv.org/abs/2409.12047

[10] Tines, "Voice of the SOC 2023," 2023. Accessed: Mar. 04, 2026. [Online]. Available: https://www.tines.com/reports/voice-of-the-soc-2023/

[11] E. A. Kenlie, C. N. Hendris, N. Nadia, and F. Adeta, "The Impact of Human Error in Cybersecurity Breaches: Understanding Behavioral Patterns and Mitigation Strategies," in *Proceedings - 6th International Conference on Informatics, Multimedia, Cyber and Information System, ICIMCIS 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 1045–1050. doi: 10.1109/ICIMCIS63449.2024.10956680.

[12] Tines, "Voice of the SOC Analyst © Tines," 2022.

[13] M. Kuypers and E. Patè-Cornell, "Documenting Cyber Security Incidents," 2015. [Online]. Available: http://capec.mitre.org/

[14] Christopher Crowley, "SANS SOC Survey 2025," 2025.

[15] S. Srinivas *et al.*, "AI-Augmented SOC: A Survey of LLMs and Agents for Security Automation," Dec. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/jcp5040095.

[16] L. Belcastro, C. Carlucci, C. Cosentino, P. Liò, and F. Marozzo, "Enhancing network security using knowledge graphs and large language models for explainable threat detection," *Future Generation Computer Systems*, vol. 176, Mar. 2026, doi: 10.1016/j.future.2025.108160.

UNIVERSITAS
GADJAH MADA
Otomatisasi Pelaporan Insiden Keamanan Berbasis n8n dan Large Language Model
Dzaki Maulana Asif, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

[17] O. O. Aramide, "AI-Driven Automated Incident Response and Remediation in Networks," *International Journal of Technology, Management and Humanities*, vol. 11, no. 02, pp. 1–9, May 2025, doi: 10.21590/ijtmh.11.02.09.

[18] Anitha Mareedu, "Autonomous Security Operations Centers (SOC): AI Agents for Threat Triage, Response, and Orchestration," *International Journal of Emerging Research in Engineering and Technology*, vol. 6, no. 2, May 2025, doi: 10.63282/3050-922x.ijeret-v6i2p108.

[19] C. P. Obeng, N. M. Narasinghe, R. Striker, and E. A. Vazquez, "Security Framework for Agentic Home AI in Preventive Healthcare: Cyber Threats Worth Noting," in *2025 Cyber Awareness and Research Symposium (CARS)*, IEEE, Oct. 2025, pp. 1–5. doi: 10.1109/CARS67163.2025.11337832.

[20] Raju Katukam, "AI-Driven Log Summarization for Security Operations Centers: A Web-Based Approach Using Gemini API," *International Journal of Emerging Research in Engineering and Technology*, vol. 6, 2025, doi: 10.63282/3050-922X.IJERET-V6I3P117.

[21] V. Akre, T. Kobbaey, G. Lazarov, K. Abdulsalam, W. Al-Sit, and J. Diab, "From Alert Fatigue to Augmented Defense: A Case for AI Copilots in Cybersecurity Operation Centers," in *2025 10th International Conference on Information Technology Trends (ITT)*, IEEE, Nov. 2025, pp. 282–287. doi: 10.1109/ITT69610.2025.11352895.

[22] A. Al Rashdi and S. Li, "OST: An AI enabled One-Stop Station Platform for Cyber Security Incident Reporting," 2025.

[23] M. Vasilakis, M. Tampouratzis, and A. Dimitriadis, "Integrated Threat Intelligence and Event Correlation with Wazuh, Suricata, and MISP," Institute of Electrical and Electronics Engineers (IEEE), Dec. 2025, pp. 1–5. doi: 10.1109/ciees66347.2025.11300009.

[24] F. A. Saputra *et al.*, "Jurnal Informatika Terpadu IMPLEMENTASI WAZUH SIEM UNTUK MANAJEMEN LOG EVENT DI PESANTREN

UNIVERSITAS
GADJAH MADA
Otomatisasi Pelaporan Insiden Keamanan Berbasis n8n dan Large Language Model
Dzaki Maulana Asif, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

TEKNOLOGI INFORMASI DAN KOMUNIKASI JOMBANG," *Jurnal Informatika Terpadu*, vol. 10, no. 2, pp. 146–155, 2024, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[25] P. V. Kumar *et al.*, "Automated Threat Detection and Response Using Security Orchestration, Automation, and Response (SOAR) and Endpoint Detection and Response," in *2025 OITS International Conference on Information Technology (OCIT)*, IEEE, Dec. 2025, pp. 498–502. doi: 10.1109/OCIT66168.2025.11400041.

[26] O. Volotovskyi, R. Banakh, and A. Piskozub, "DEVELOPMENT OF AN AGENT FOR NOTIFICATION ANALYSIS BASED ON ARTIFICIAL INTELLIGENCE USING N8N AND ELASTIC SECURITY SOFTWARE," *Cybersecurity: Education, Science, Technique*, vol. 3, no. 31, pp. 424–440, 2025, doi: 10.28925/2663-4023.2025.31.1031.

[27] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," *IEEE Access*, vol. 8, pp. 227756–227779, 2020, doi: 10.1109/ACCESS.2020.3045514.

[28] Logsign, "Security Information and Event Management (SIEM) Buyer's Guide An Unbiased SIEM Guide: How to Choose the Right SIEM Solution. Contents." [Online]. Available: https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

[29] Ivan Lee, "What is Security Information and Event Management (SIEM)?" Accessed: Mar. 12, 2026. [Online]. Available: https://www.wallarm.com/what/siem-whats-security-information-and-event-management-technology-part-1

[30] "SIEM Technologies - Streamline Your System Security Management." Accessed: Apr. 06, 2026. [Online]. Available: https://www.wallarm.com/what/siem-whats-security-information-and-event-management-technology-part-1

UNIVERSITAS
GADJAH MADA
Otomatisasi Pelaporan Insiden Keamanan Berbasis n8n dan Large Language Model
Dzaki Maulana Asif, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

[31] Swimlane, “Security Orchestration, Automation and Response (SOAR) Capabilities.”

[32] “Security, Orchestration, Automation & Response (SOAR) | Hayyan Horizons.” Accessed: Mar. 12, 2026. [Online]. Available: https://hayyan.com.jo/2024/10/06/security-orchestration-automation-response-soar/

[33] “SOAR Solutions Powered by Infoblox Partner Integrations.” Accessed: Apr. 06, 2026. [Online]. Available: https://www.infoblox.com/blog/security/soar-solutions-powered-by-infoblox-partner-integrations/

[34] “Architecture - Getting started with Wazuh · Wazuh documentation.” Accessed: Mar. 12, 2026. [Online]. Available: https://documentation.wazuh.com/current/getting-started/architecture.html

[35] “Components - Getting started with Wazuh · Wazuh documentation.” Accessed: Mar. 12, 2026. [Online]. Available: https://documentation.wazuh.com/current/getting-started/components/index.html

[36] “Query DSL | Elastic Docs.” Accessed: Mar. 12, 2026. [Online]. Available: https://www.elastic.co/docs/explore-analyze/query-filter/languages/query-dsl

[37] “Explore n8n Docs: Your Resource for Workflow Automation and Integrations | n8n Docs.” Accessed: Mar. 12, 2026. [Online]. Available: https://docs.n8n.io/

[38] M. A. K. Raiaan *et al.*, “A Review on Large Language Models: Architectures, Applications, Taxonomies, Open Issues and Challenges,” *IEEE Access*, vol. 12, pp. 26839–26874, 2024, doi: 10.1109/ACCESS.2024.3365742.

[39] “How LLMs Learn from the Internet: The Training Process.” Accessed: Mar. 13, 2026. [Online]. Available: https://blog.bytebytego.com/p/how-llms-learn-from-the-internet

UNIVERSITAS
GADJAH MADA
Otomatisasi Pelaporan Insiden Keamanan Berbasis n8n dan Large Language Model
Dzaki Maulana Asif, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

[40] S. Ekin, "Prompt Engineering For ChatGPT: A Quick Guide To Techniques, Tips, And Best Practices," Apr. 29, 2023. doi: 10.36227/techrxiv.22683919.v1.

[41] "Guide to Prompt Engineering (2026)." Accessed: Mar. 13, 2026. [Online]. Available: https://www.stackai.com/blog/guide-to-prompt-engineering

[42] Dhuha Sabri Ghazi, H. S. Hamid, M. J. Zaiter, and A. S. Ghazi Behadili, "Snort Versus Suricata in Intrusion Detection," *Iraqi Journal of Information and Communication Technology*, vol. 7, no. 2, pp. 73–88, Dec. 2024, doi: 10.31987/ijict.7.2.290.

[43] E. Stephani, F. Nova, E. Asri, and N. # Fitri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," 2020. [Online]. Available: http://jurnal-itsi.org

[44] I. Ghafir, J. Svoboda, and V. Prenosil, "A Survey on Network Security Monitoring Implementations."

[45] Z. Morić, V. Dakić, and T. Čavala, "Security Hardening and Compliance Assessment of Kubernetes Control Plane and Workloads," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, Jun. 2025, doi: 10.3390/jcp5020030.

[46] "Standalone - Trivy." Accessed: Mar. 14, 2026. [Online]. Available: https://trivy.dev/docs/latest/references/modes/standalone/

[47] "What is Falco? | Falco." Accessed: Mar. 14, 2026. [Online]. Available: https://falco.org/about/

[48] "Shipyard | The Docker Ecosystem Explained." Accessed: Apr. 06, 2026. [Online]. Available: https://shipyard.build/blog/docker-ecosystem/

[49] "What is Gotenberg? | Gotenberg." Accessed: Mar. 14, 2026. [Online]. Available: https://gotenberg.dev/docs/getting-started/introduction

[50] "Gotenberg, a stateless API for converting Markdown files, HTML files and Office documents to PDF." Accessed: Mar. 14, 2026. [Online]. Available:

UNIVERSITAS
GADJAH MADA
Otomatisasi Pelaporan Insiden Keamanan Berbasis n8n dan Large Language Model
Dzaki Maulana Asif, Ir. Nur Rohman Rosyid, S.T., M.T., D.Eng., IPM.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

https://thecodingmachine.io/gotenberg-a-stateless-api-for-converting-files-to-pdf

[51] "Telegram APIs." Accessed: Mar. 14, 2026. [Online]. Available: https://core.telegram.org/

[52] M. W. Hasyim, S. Pramono, and Sutrisno, "Web-Based Telegram Chatbot Management System: Create Chatbot Without Programming Language Requirements," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1096, no. 1, p. 012075, Mar. 2021, doi: 10.1088/1757-899x/1096/1/012075.

[53] A. A. Salih and A. M. Abdulazeez, "Evaluation of Classification Algorithms for Intrusion Detection System: A Review," *Journal of Soft Computing and Data Mining*, vol. 2, no. 1, pp. 31–40, Apr. 2021, doi: 10.30880/jscdm.2021.02.01.004.

[54] M. Tran and H. Nguyen, "The Use of Automated Techniques in Cybersecurity Opera-tions: Supporting Threat Detection and Information Assur-ance in Modern Information Systems."

[55] O. Owolafe and A. A. James, "Comparative Analysis of Wazuh, Graylog, and Elk Stack for Cyber Threat Detection and Response."