TUGAS AKHIR

IMPLEMENTASI *WORKFLOW* OTOMATIS MENGGUNAKAN N8N UNTUK DETEKSI DAN RESPONS ANCAMAN *MALWARE* DAN *PHISHING*

Sebagai salah satu syarat untuk memperoleh gelar Sarjana S-1

Program Studi Informatika

Disusun Oleh :

MUHAMMAD ROFI'FACHRUDDIN

NIM 21106050052

PROGRAM STUDI INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2025

LEMBAR PENGESAHAN

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-2480/Un.02/DST/PP.00.9/12/2025

Tugas Akhir dengan judul : Implementasi Workflow Otomatis Menggunakan N8n Untuk Deteksi dan Respons Ancaman Malware dan Phishing

yang dipersiapkan dan disusun oleh:

Nama	: MUHAMMAD ROFI'FACHRUDDIN
Nomor Induk Mahasiswa	: 21106050052
Telah diujikan pada	: Rabu, 10 Desember 2025
Nilai ujian Tugas Akhir	: A-

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED

Valid ID: 6940f3ed2cc47

Penguji I

Dr. Agung Fatwanto, S.Si., M.Kom.
SIGNED

Valid ID: 6940798912456

Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED

Valid ID: 6938d402b1c5

Yogyakarta, 10 Desember 2025
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 694257c983a3f

LEMBAR PERNYATAAN

SURAT PERNYATAAN KEASLIAN/BEBAS PLAGIASI

Yang bertanda tangan di bawah ini:

Nama	: Muhammad Rofi'Fachruddin
NIM	: 21106050052
Program Studi	: Informatika
Fakultas	: Sains dan Teknologi

Dengan ini menyatakan bahwa isi tugas akhir saya yang berjudul "Implementasi Workflow Otomatis Menggunakan N8n Untuk Deteksi dan Respons Ancaman Malware dan Phishing" merupakan hasil pekerjaan penulis sendiri, tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu perguruan tinggi, bukan duplikasi atau saduran dari karya orang lain, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain sepanjang pengetahuan penulis, kecuali yang secara tertulis diacu dalam tugas akhir ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 25 November 2025

Muhammad Rofi'Fachruddin

NIM. 21106050052

LEMBAR PERSETUJUAN TUGAS AKHIR

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi /Tugas Akhir
Lamp : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
Di Yogyakarta

Assalammualaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka saya selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Muhammad Rofi'Fachruddin
NIM : 21106050052
Judul Tugas Akhir: : Implementasi Workflow Otomatis Menggunakan N8n Untuk Deteksi dan Respons Ancaman Malware dan Phishing

Sudah dapat diajukan kembali kepada Program Studi Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara dapat segera di-*munaqasyah*-kan. Atas perhatiannya saya ucapkan terima kasih.

Wassalammualaikum wr. wb.

Yogyakarta, 25 November 2025
Pembimbing

Dr. Ir. Bambang Sugiantoro, M.T.,
IPU., ASEAN Eng.

INTISARI

Ancaman siber seperti *malware* dan *phishing* terus berkembang dengan kompleksitas tinggi, menjadikan metode penanganan manual tidak lagi efektif karena lambat dan rentan terhadap kesalahan manusia. Untuk mengatasi tantangan ini, diperlukan solusi yang mampu mendeteksi dan merespons insiden secara cepat dan terstruktur. Tugas akhir ini berfokus pada perancangan sistem *Security Orchestration, Automation, and Response* (SOAR) berbasis *open-source* menggunakan platform n8n sebagai *orkestrator* pusat untuk mengotomatisasi alur kerja keamanan siber.

Sistem ini dirancang dengan mengintegrasikan Wazuh sebagai agen deteksi ancaman pada *endpoint*, VirusTotal sebagai layanan intelijen ancaman eksternal, Google Gemini untuk analisis deskriptif berbasis kecerdasan buatan, serta Slack sebagai kanal notifikasi *real-time*. Pengujian dilakukan menggunakan 600 sampel data uji yang terdiri dari kategori *file* aman, *file malware*, tautan aman, dan tautan *phishing*.

Hasil pengujian menunjukkan bahwa sistem mampu bekerja dengan responsivitas tinggi dan akurat. Rata-rata waktu respons (*Mean Time to Response*) yang dicapai adalah 0,616 detik untuk *file* aman, 0,653 detik untuk tautan *phishing*, 0,655 detik untuk tautan aman, dan 4,771 detik untuk *file malware*. Tingkat akurasi deteksi keseluruhan mencapai 98,83%, dengan tingkat keberhasilan pengiriman notifikasi sebesar 100%. Implementasi *workflow* otomatis ini terbukti mampu meningkatkan efisiensi operasional sebesar 98,41% dibandingkan dengan estimasi waktu penanganan manual, sehingga sangat efektif dalam mendukung operasional keamanan siber.

Kata Kunci: SOAR, n8n, Wazuh, *Malware*, *Phishing*, Otomatisasi Keamanan.

ABSTRACT

Cyber threats such as malware and phishing continue to evolve with high complexity, rendering manual handling methods ineffective due to their slowness and susceptibility to human error. To address this challenge, a solution capable of detecting and responding to incidents quickly and structurally is required. This thesis focuses on designing an open-source Security Orchestration, Automation, and Response (SOAR) system using the n8n platform as a central orchestrator to automate cybersecurity workflows.

The system is designed by integrating Wazuh as a threat detection agent on endpoints, VirusTotal as an external threat intelligence service, Google Gemini for AI-based descriptive analysis, and Slack as a real-time notification channel. Testing was conducted using 600 test data samples consisting of safe files, malware files, safe links, and phishing links categories.

The test results demonstrate that the system performs with high responsiveness and accuracy. The achieved Mean Time to Response (MTTR) is 0.616 seconds for safe files, 0.653 seconds for phishing links, 0.655 seconds for safe links, and 4.771 seconds for malware files. The overall detection accuracy rate reached 98.83%, with a notification delivery success rate of 100%. The implementation of this automated workflow proved capable of increasing operational efficiency by 98.41% compared to manual handling estimates, making it highly effective in supporting cybersecurity operations.

Keywords: SOAR, n8n, Wazuh, Malware, Phishing, Security Automation.

HALAMAN PERSEMBAHAN

Karya ini penulis persembahkan kepada Bapak dan Ibu tercinta, atas segala doa, kasih sayang, dukungan, serta pengorbanan yang tiada henti. Semoga karya ini menjadi bentuk bakti dan rasa terima kasih penulis kepada Bapak dan Ibu.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas rahmat, karunia, dan hidayah-Nya, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul "Implementasi *Workflow* Otomatis Menggunakan n8n untuk Deteksi dan Respons Ancaman *Malware* dan *Phishing*" dengan baik. Tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga.

Dalam proses penyusunan tugas akhir ini, penulis banyak mendapatkan bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah SWT, atas limpahan rahmat dan hidayah-Nya.
2. Kedua orang tua tercinta, atas doa, kasih sayang, dukungan moril dan materil, serta motivasi yang tiada henti
3. Adik saya Muhammad Fahmi Alwi serta kedua kakek dan nenek, yang selalu memberikan perhatian, dorongan, serta semangat yang tak ternilai.
4. Bapak Prof. Noorhaidi, M.A., M.Phil., Ph.D., selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
5. Ibu Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi.
6. Bapak Dr. Muhammad Mustakim, S.T., M.T., selaku Ketua Program Studi Informatika.
7. Bapak Dr. Ir. Sumarsono, S.T., M.Kom., selaku Dosen Pembimbing Akademik yang selalu membantu dan mengarahkan penulis selama proses perkuliahan.
8. Bapak Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng., selaku Dosen Pembimbing Tugas Akhir yang selalu membantu dan memberikan arahan dalam menyelesaikan penulisan tugas akhir ini.
9. Bapak/Ibu Dosen di Program Studi Informatika, yang telah memberikan ilmu, pengetahuan, dan pengalaman berharga selama penulis menempuh pendidikan.

10. Rekan-rekan mahasiswa dan sahabat seperjuangan, yang senantiasa memberikan semangat, kebersamaan, dan dukungan moral dalam menghadapi setiap tantangan.
11. Seluruh pihak yang telah membantu, baik secara langsung maupun tidak langsung, yang tidak dapat penulis sebutkan satu per satu, namun kontribusinya sangat berarti dalam penyusunan karya ini.

Penulis menyadari bahwa tugas akhir ini masih jauh dari sempurna, baik dari segi isi maupun penyajiannya. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari berbagai pihak untuk perbaikan di masa yang akan datang.

Akhir kata, penulis berharap semoga tugas akhir ini dapat memberikan manfaat, baik bagi penulis sendiri, bagi dunia akademik, maupun bagi pembaca yang berminat mendalami bidang keamanan siber dan otomatisasi sistem.

Sleman, 27 November 2025

Muhammad Rofi'Fachruddin

MOTTO

"The first and greatest victory is to conquer yourself."

"Kemenangan pertama dan terbesar adalah menaklukkan diri sendiri."

— Plato (427–347 SM)

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era digital yang semakin kompleks, ancaman siber seperti *malware* dan *phishing* berkembang pesat dan menjadi isu yang sangat krusial dalam keamanan jaringan. Berdasarkan laporan dari AV-TEST Institute, tercatat lebih dari 450.000 varian *malware* dan program tidak diinginkan (PUA) baru muncul setiap hari sepanjang tahun 2024, sehingga jumlah totalnya melebihi 60 juta varian unik per tahun [1]. Sementara itu, laporan FBI Internet Crime Complaint Center (IC3) menunjukkan bahwa *phishing* merupakan kejahatan siber terbanyak dengan 193.407 kasus dan kerugian mencapai USD 16,6 miliar, naik 33% dari tahun sebelumnya [2]. Di Indonesia, selama 2024 Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak 241 dugaan insiden kebocoran data, serta lebih dari 26 juta aktivitas *phishing* yang tersebar di berbagai sektor, termasuk sektor pemerintahan dan infrastruktur kritikal. Selain itu, jumlah *traffic* anomali yang terpantau mencapai lebih dari 330 juta aktivitas, mengindikasikan bahwa ancaman siber di Indonesia mengalami peningkatan yang signifikan [3]. Tren ini mengindikasikan bahwa ekosistem jaringan informasi saat ini sangat rentan terhadap serangan yang semakin kompleks, sehingga dibutuhkan sistem deteksi dan respons yang mampu beroperasi secara otomatis dan *real-time*.

Kebutuhan akan respons cepat terhadap ancaman siber didasari oleh ketidakmampuan sistem manual dalam mendeteksi dan menanggapi insiden secara efisien. Pendekatan berbasis tenaga manusia cenderung memakan waktu lama, rawan kesalahan, dan tidak mampu menangani volume data yang besar secara simultan. Ilca et al. [4] dalam penelitiannya menyatakan bahwa sistem pertahanan siber berbasis *open-source* yang terintegrasi dengan modul deteksi dan respons otomatis memiliki efektivitas jauh lebih tinggi dibanding metode tradisional, terutama dalam organisasi kecil dan

menengah (SME). Dengan demikian, pendekatan otomatisasi *workflow* menjadi solusi yang layak dikembangkan.

Salah satu alat yang memiliki potensi besar dalam membangun sistem respons otomatis adalah n8n, yakni platform *workflow automation open-source* yang memungkinkan penggunanya merancang *workflow* secara visual tanpa harus menulis kode secara eksplisit. N8n mendukung integrasi dengan berbagai layanan pihak ketiga seperti Wazuh, VirusTotal, serta platform kolaborasi seperti Slack. Dalam sistem ini, Wazuh bertugas mendeteksi *file* mencurigakan atau aktivitas abnormal dalam sistem, yang selanjutnya dikirim ke n8n melalui *webhook* untuk dianalisis lebih lanjut. N8n kemudian mengotomatisasi proses pengambilan data seperti *hash file* atau URL dan memverifikasinya melalui VirusTotal API. Berdasarkan hasil pemindaian VirusTotal, sistem akan menentukan status *file* atau URL dan secara otomatis mengirimkan laporan ke Slack, sehingga eskalasi dan dokumentasi insiden berjalan cepat dan terstruktur.

Pemilihan n8n sebagai alat automasi *workflow* didasari oleh beberapa pertimbangan strategis. Pertama, n8n terdapat pilihan untuk *self-hosting* dan bebas lisensi, menjadikannya cocok digunakan oleh institusi pendidikan, lembaga pemerintah, maupun UMKM yang memiliki keterbatasan anggaran. Kedua, n8n memiliki antarmuka visual yang mempermudah proses pengembangan dan pemeliharaan *workflow*. Ketiga, fleksibilitas integrasi n8n memungkinkan penggabungan beragam sistem keamanan siber dalam satu platform terpusat. Adapun Wazuh dipilih karena kemampuannya dalam melakukan File Integrity Monitoring (FIM), deteksi *rule-based*, dan kemampuan eskalasi peristiwa keamanan melalui REST API. VirusTotal, sebagai mesin intelijen ancaman, mendukung pemindaian *hash* dan URL dari ratusan antivirus dan *machine learning engine*, sehingga memperkuat validasi data secara cepat dan kredibel.

Berdasarkan permasalahan tersebut, tugas akhir ini berupaya untuk menjawab pertanyaan utama yaitu bagaimana merancang sistem respons

ancaman *malware* dan *phishing* secara otomatis dan real-time menggunakan integrasi antara Wazuh, n8n, dan VirusTotal, serta bagaimana hasil analisis dan eskalasi dapat dikirim ke platform kolaborasi seperti Slack. Tugas akhir ini bertujuan membangun prototipe sistem keamanan informasi yang mampu mempercepat proses deteksi dan respons, serta memberikan kontribusi nyata bagi peningkatan ketahanan siber, baik pada skala individu maupun organisasi. Dengan solusi berbasis automasi *workflow* ini, diharapkan sistem keamanan siber dapat bergerak lebih proaktif, efisien, dan adaptif terhadap ancaman yang terus berkembang.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka rumusan masalah dalam tugas akhir ini dapat dirumuskan sebagai berikut:

1. Bagaimana merancang dan mengimplementasikan sistem otomatis berbasis n8n yang terintegrasi dengan Wazuh dan VirusTotal untuk deteksi ancaman siber?

2. Bagaimana efektivitas sistem tersebut ditinjau dari tingkat akurasi deteksi dan kecepatan waktu respons dalam menangani insiden?

1.3 Batasan Masalah

Untuk menjaga fokus dan keterukuran tugas akhir, batasan-batasan yang diterapkan dalam tugas akhir ini adalah sebagai berikut:

1. Implementasi sistem dilakukan pada lingkungan uji terkontrol menggunakan infrastruktur simulasi, bukan diterapkan pada lingkungan produksi perusahaan nyata atau jaringan publik skala besar.

2. Sistem yang dibangun merupakan purwarupa sebagai pembuktian konsep, sehingga aspek kepatuhan regulasi industri dan standar layanan komersial tidak menjadi fokus utama.

3. Tugas akhir ini membahas implementasi *workflow* otomatis menggunakan n8n yang terintegrasi dengan Wazuh sebagai sistem *monitoring* dan VirusTotal sebagai layanan analisis eksternal.

4. Sistem dirancang khusus sebagai solusi *alerting*. Tindakan mitigasi eksekusi aktif (seperti mematikan jaringan, isolasi *host*, atau menghapus *file* secara otomatis) tidak dibahas dalam tugas akhir ini dan masih memerlukan intervensi manual.

5. Pengujian keamanan dilakukan menggunakan sampel malware yang sudah diketahui dalam volume trafik simulasi yang terbatas. Tugas akhir ini tidak mencakup pendeteksian serangan jenis Zero-Day maupun uji ketahanan terhadap beban trafik ekstrem.

1.4 Tujuan Pengembangan

Tujuan dari tugas akhir ini adalah:

1. Membangun *workflow* otomatis berbasis n8n untuk mendeteksi dan melakukan respons terhadap ancaman *malware* dan *phishing* secara *real-time*.

2. Mengintegrasikan sistem deteksi ancaman Wazuh, layanan analisis reputasi VirusTotal, dan media notifikasi seperti Slack ke dalam satu *pipeline* kerja otomatis.

3. Mengevaluasi efektivitas *workflow* dalam merespons ancaman siber dengan mengukur waktu respons dan tingkat akurasi notifikasi

1.5 Manfaat Pengembangan

Tugas akhir ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Menambah literatur dan wawasan ilmiah dalam bidang keamanan siber, khususnya terkait penerapan sistem otomatis berbasis *workflow* untuk respons ancaman siber.

2. Memberikan solusi praktis berupa arsitektur sistem keamanan berbasis *open-source* yang dapat diterapkan oleh individu, organisasi kecil, maupun institusi pendidikan tanpa memerlukan biaya lisensi.

3. Mendukung upaya peningkatan ketahanan siber nasional dengan menghadirkan pendekatan respons ancaman yang adaptif, cepat, dan efisien di tengah keterbatasan sumber daya manusia dan finansial.

BAB V
PENUTUP

5.1 Kesimpulan

Tugas akhir ini berhasil merancang dan mengimplementasikan *workflow* otomatis menggunakan platform n8n yang terintegrasi dengan Wazuh sebagai sistem *monitoring* dan VirusTotal sebagai layanan analisis eksternal. Berdasarkan data hasil pengujian, dapat ditarik kesimpulan sebagai berikut:

1. Rata-rata waktu respons sistem untuk deteksi *File* Aman, Tautan Aman, dan Tautan *Phishing* masing-masing adalah 0,616 detik, 0,655 detik, dan 0,653 detik. Untuk deteksi *File Malware*, rata-rata waktu respons adalah 4,771 detik.
2. Tingkat akurasi deteksi sistem secara keseluruhan mencapai rata-rata 98,83%. Pada skenario pengujian *file*, sistem mencapai akurasi 100%, sedangkan pada skenario tautan, akurasi tercatat sebesar 97,67%.
3. Berdasarkan perbandingan waktu respons sistem dengan estimasi waktu manual, sistem memberikan tingkat efisiensi waktu sebesar 98,41%.
4. Seluruh notifikasi hasil deteksi berhasil terkirim ke kanal Slack dengan tingkat keberhasilan 100%.

5.2 Saran

Berdasarkan hasil tugas akhir dan kendala yang ditemukan selama pengujian, terdapat beberapa saran untuk pengembangan sistem di masa mendatang:

1. Menambahkan fitur mitigasi aktif seperti isolasi *file* berbahaya otomatis atau karantina surel, agar sistem tidak hanya mendeteksi tetapi juga mencegah dampak serangan secara langsung.

2. Mengintegrasikan kanal notifikasi tambahan selain Slack, seperti Telegram atau Microsoft Teams, serta menghubungkan sistem dengan platform tiket untuk manajemen insiden yang lebih terstruktur
3. Memperluas variasi sampel pengujian dan melakukan uji beban untuk memverifikasi stabilitas sistem dalam menangani volume trafik yang besar.

DAFTAR PUSTAKA

[1] "Malware Statistics & Trends Report | AV-TEST." Diakses: 4 Agustus 2025. [Daring]. Tersedia pada: https://www.av-test.org/en/statistics/malware/

[2] Federal Bureau of Investigation (FBI) dan Internet Crime Complaint Center (IC3), "2024 IC3 Annual Report." Federal Bureau of Investigation (FBI), 2024.

[3] Badan Siber dan Sandi Negara (BSSN), "Lanskap Keamanan Siber 2024." Badan Siber dan Sandi Negara (BSSN), 2024.

[4] L. F. Ilca, O. P. Lucian, dan T. C. Balan, "Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response," *Sensors*, vol. 23, no. 15, hlm. 6757, Jul 2023, doi: 10.3390/s23156757.

[5] D. Craigen, N. Diakun-Thibault, dan R. Purse, "Defining Cybersecurity," *Technol. Innov. Manag. Rev.*, vol. 4, no. 10, hlm. 13–21, 2014.

[6] F. Schiliro, "Towards a Contemporary Definition of Cybersecurity," 5 Februari 2023, *arXiv*: arXiv:2302.02274. doi: 10.48550/arXiv.2302.02274.

[7] M. G. Cains, L. Flora, D. Taber, Z. King, dan D. S. Henshel, "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation," *Risk Anal.*, vol. 42, no. 8, hlm. 1643–1669, Agu 2022, doi: 10.1111/risa.13687.

[8] "Apa itu Keamanan Siber? - Penjelasan tentang Keamanan Siber - AWS," Amazon Web Services, Inc. Diakses: 5 Agustus 2025. [Daring]. Tersedia pada: https://aws.amazon.com/id/what-is/cybersecurity/

[9] S. Kramer dan J. C. Bradfield, "A general definition of malware," *J. Comput. Virol.*, vol. 6, no. 2, hlm. 105–114, Mei 2010, doi: 10.1007/s11416-009-0137-1.

[10] A. P. Namanya, A. Cullen, I. U. Awan, dan J. P. Disso, "The World of Malware: An Overview," dalam *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, Barcelona, Spain: IEEE, Agu 2018, hlm. 420–427. doi: 10.1109/FiCloud.2018.00067.

[11] "What is Malware? | IBM." Diakses: 5 Agustus 2025. [Daring]. Tersedia pada: https://www.ibm.com/think/topics/malware

[12] P. Maniriho, A. N. Mahmood, dan M. J. M. Chowdhury, "A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends and challenges," *Future Gener. Comput. Syst.*, vol. 130, hlm. 1–18, Mei 2022, doi: 10.1016/j.future.2021.11.030.

[13] E. E. Lastdrager, "Achieving a consensual definition of phishing based on a systematic review of the literature," *Crime Sci.*, vol. 3, no. 1, hlm. 9, Des 2014, doi: 10.1186/s40163-014-0009-y.

[14] M. Butavicius, K. Parsons, M. Pattinson, dan A. McCormac, "Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails," 28 Mei 2016, *arXiv*: arXiv:1606.00887. doi: 10.48550/arXiv.1606.00887.

[15] M. Jari, "An Overview of Phishing Victimization: Human Factors, Training and the Role of Emotions," dalam *Computer Science and*

Information Technology, Jul 2022, hlm. 217–228. doi: 10.5121/csit.2022.121319.
[16] "Definition of Security Orchestration, Automation and Response (SOAR) - Gartner Information Technology Glossary," Gartner. Diakses: 5 Agustus 2025. [Daring]. Tersedia pada: https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar
[17] M. Vielberth, "Security Information and Event Management (SIEM)," dalam *Encyclopedia of Cryptography, Security and Privacy*, S. Jajodia, P. Samarati, dan M. Yung, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2021, hlm. 1–3. doi: 10.1007/978-3-642-27739-9_1681-1.
[18] G. González-Granadillo, S. González-Zarzosa, dan R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, no. 14, hlm. 4759, Jul 2021, doi: 10.3390/s21144759.
[19] "n8n Press | Automate without limits." Diakses: 5 Agustus 2025. [Daring]. Tersedia pada: https://n8n.io/press/
[20] A. F. Mahmud dan S. Wirawan, "Phishing Website Detection Using Machine Learning Classification Method," *SISTEMASI*, vol. 13, no. 4, hlm. 1368, Jul 2024, doi: 10.32520/stmsi.v13i4.3456.
[21] A. D. Harahap, D. Juardi, dan A. S. Y. Irawan, "RANCANG BANGUN SISTEM PENDETEKSI LINK PHISHING MENGGUNAKAN ALGORITMA RANDOM FOREST BERBASIS WEB," *J. Inform. Dan Tek. Elektro Terap.*, vol. 12, no. 3, Agu 2024, doi: 10.23960/jitet.v12i3.4858.
[22] V. A. Windarni, A. F. Nugraha, S. T. A. Ramadhani, D. A. Istiqomah, F. M. Puri, dan A. Setiawan, "DETEKSI WEBSITE PHISHING MENGGUNAKAN TEKNIK FILTER PADA MODEL MACHINE LEARNING," *Inf. Syst. J.*, vol. 6, no. 01, Agu 2023, doi: 10.24076/infosjournal.2023v6i01.1268.
[23] Dieta Wahyu Asry, Eko Siswanto, Dendy Kurniawan, dan Haris Ihsanil Huda, "Deteksi Malware Statis Menggunakan Deep Neural Networks Pada Portable Executable," *Tek. J. Ilmu Tek. Dan Inform.*, vol. 3, no. 1, hlm. 19–34, Mei 2023, doi: 10.51903/teknik.v3i1.325.
[24] H. Hartinah, A. W. Paundu, dan A. A. Ilham, "Deteksi Malware Ransomware Berdasarkan Panggilan API dengan Metode Ekstraksi Fitur N-gram dan TF-IDF," *J. Edukasi Dan Penelit. Inform. JEPIN*, vol. 9, no. 1, hlm. 50, Apr 2023, doi: 10.26418/jp.v9i1.58721.