JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i3.9929

IMPLEMENTASI SISTEM DETEKSI MALWARE PADA SIEM WAZUH VIA SHUFFLE SOAR DI DISKOMINFOSTAN DI KOTA BEKASI

Sugiarto Catrio Mulyo Rachmanto[1*], Saludin Muis [2]

Universitas Bina Insani; Jl. Raya Siliwangi No.6, Bekasi, Jawa Barat; Telp (021) 82400924

Keywords:
Keamanan Siber, SIEM, Wazuh, SOAR, *Threat Intelligence*

Corespondent Email:
sugiarto.cmr@gmail.com

Abstrak. Keamanan infrastruktur teknologi informasi pada instansi pemerintah merupakan aspek kritis yang perlu mendapat perhatian serius, mengingat tingginya risiko ancaman siber yang dapat mengganggu keberlangsungan layanan publik. Penelitian ini bertujuan untuk merancang dan mengimplementasikan *framework* keamanan siber terintegrasi pada infrastruktur Dinas Komunikasi, Informatika, Statistik dan Persandian (Diskominfostandi) Kota Bekasi menggunakan SIEM Wazuh yang diintegrasikan dengan Shuffle SOAR, MISP, DFIR-IRIS, dan notifikasi Discord. Pengujian kerentanan dilakukan secara langsung pada sistem nyata menggunakan dua skenario serangan, yaitu *Cross-Site Scripting* (XSS) dan unggahan *webshell*, yang masing-masing dinilai menggunakan standar CVSS v3.1 dengan skor 6.1 (*Medium*) dan 9.8 (*Critical*). Setelah implementasi *framework* dilakukan, pengujian ulang menunjukkan bahwa sistem mampu mendeteksi ancaman secara otomatis, menghapus file berbahaya melalui fitur *Active Response* Wazuh, mencatat insiden di DFIR-IRIS, memperkaya data ancaman melalui MISP, serta mengirimkan notifikasi *real-time* ke Discord tanpa intervensi manual. Hasil implementasi dibuktikan dengan penurunan skor CVSS pada kerentanan XSS dari 6.1 menjadi 4.3 dan kerentanan *webshell* dari 9.8 menjadi 6.5, yang mencerminkan peningkatan signifikan dalam kemampuan deteksi dan respons insiden keamanan siber secara otomatis dan terintegrasi.

Abstract. *The security of information technology infrastructure in government agencies is a critical aspect that requires serious attention, given the high risk of cyber threats that can disrupt public services. This study aims to design and implement an integrated cybersecurity framework on the infrastructure of the Communication, Informatics, Statistics and Encryption Service (Diskominfostandi) of Bekasi City using Wazuh SIEM integrated with Shuffle SOAR, MISP, DFIR-IRIS, and Discord notifications. Vulnerability testing was conducted directly on the live system using two attack scenarios, namely Cross-Site Scripting (XSS) and webshell upload, each assessed using the CVSS v3.1 standard with scores of 6.1 (Medium) and 9.8 (Critical) respectively. Following the framework implementation, re-testing demonstrated that the system was capable of automatically detecting threats, deleting malicious files through Wazuh's Active Response feature, recording incidents in DFIR-IRIS, enriching threat data through MISP, and delivering real-time notifications to Discord without manual intervention. The effectiveness of the implementation was evidenced by a reduction in CVSS scores for the XSS vulnerability from 6.1 to 4.3 and the webshell vulnerability from 9.8 to 6.5, reflecting a significant improvement in the capability for automated and integrated cybersecurity incident detection and response.*

1. PENDAHULUAN

Keamanan siber (cybersecurity) merupakan garda terdepan dalam ekosistem digital saat ini, yang mencakup serangkaian praktik, teknologi, dan proses yang dirancang untuk melindungi perangkat, jaringan, serta data dari akses tidak sah maupun serangan digital yang berbahaya. Di tengah masifnya transformasi teknologi, tantangan keamanan siber tidak lagi hanya berfokus pada pencegahan statis, melainkan telah bergeser ke arah kemampuan deteksi dini dan respons cepat terhadap ancaman yang terus berevolusi secara kompleks [1].

Dinas Komunikasi, Informatika, Statistik, dan Persandian (Diskominfostandi) Kota Bekasi merupakan instansi vital yang mengelola infrastruktur teknologi informasi dan komunikasi untuk menunjang jalannya roda pemerintahan serta pelayanan publik di Kota Bekasi. Berdasarkan hasil observasi, ditemukan kendala signifikan berupa alert fatigue atau kelelahan peringatan yang dialami oleh para analis keamanan, serta proses manajemen insiden yang masih bersifat manual dan belum terintegrasi secara end-to-end.

Beberapa penelitian terdahulu menegaskan bahwa efektivitas pertahanan siber sangat bergantung pada integrasi sistem keamanan serta pemanfaatan otomatisasi. Penelitian oleh [2] menunjukkan bahwa penerapan open-source SIEM berbasis Wazuh mampu meningkatkan kemampuan pemantauan keamanan secara terpusat. [3] mengemukakan bahwa penggabungan kapabilitas SIEM dengan sumber Threat Intelligence eksternal berkontribusi signifikan dalam meningkatkan ketepatan korelasi event serta mengurangi tingkat false positive. [4] menjelaskan bahwa penerapan SOAR berperan penting dalam meningkatkan efisiensi penanganan insiden keamanan melalui otomasi proses respons.

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan pengembangan framework keamanan terintegrasi yang menggabungkan SIEM Wazuh untuk deteksi, MISP untuk pengayaan data ancaman, DFIR-IRIS untuk manajemen kasus, Shuffle SOAR sebagai pusat orkestrasi otomatisasi, dan Discord sebagai media notifikasi real-time. Tujuan penelitian ini adalah: (1) merancang framework keamanan siber terintegrasi menggunakan SIEM Wazuh; (2) mengimplementasikan integrasi Wazuh dengan Threat Intelligence; (3) menerapkan otomatisasi respons insiden; dan (4) mengimplementasikan mekanisme respons insiden secara otomatis menggunakan integrasi Wazuh, Shuffle, MISP, DFIR-IRIS, dan notifikasi Discord.

2. TINJAUAN PUSTAKA

2.1 Keamanan Siber (CyberSecurity)

Keamanan siber merupakan serangkaian upaya dan strategi yang dirancang untuk melindungi berbagai aset teknologi informasi dari berbagai bentuk ancaman digital, mencakup pengamanan informasi agar terhindar dari akses tidak sah, penyalahgunaan, perusakan, maupun pencurian data [5]

2.2 SIEM (Security Information and Event Management)

SIEM merupakan platform yang dirancang untuk mengumpulkan, mengintegrasikan, dan menganalisis data keamanan dari berbagai sumber telemetry. Sistem ini bekerja dengan melakukan agregasi log serta korelasi event keamanan guna mengidentifikasi aktivitas mencurigakan secara terpusat dan real-time [6].

2.3 Wazuh

Wazuh merupakan perangkat lunak keamanan berbasis open-source yang berfungsi sebagai sistem deteksi berbasis host dengan mengintegrasikan kemampuan XDR dan SIEM. Platform ini mampu melakukan analisis log, mendeteksi intrusi dan malware, memantau integritas file (FIM), serta mendukung respons aktif terhadap ancaman yang terdeteksi [7].

2.4 Shuffle SOAR

SOAR (Security Orchestration, Automation, and Response) merupakan platform yang dirancang untuk membantu tim keamanan dalam mengotomatisasi proses penanganan insiden melalui workflow visual berbasis playbook. Platform ini memungkinkan pengguna untuk membuat, mengatur, dan menjalankan alur kerja otomatis yang terdiri dari berbagai aksi keamanan [8].

2.5 MISP (Malware Information Sharing Platform)

MISP merupakan platform Threat Intelligence berbasis open-source yang dirancang untuk mengelola, menyimpan, dan membagikan informasi terkait ancaman keamanan secara terstruktur, termasuk Indicator of Compromise (IoC) [9].

2.6 DFIR-IRIS

DFIR-IRIS merupakan platform open-source yang dikembangkan untuk mendukung proses respons insiden keamanan melalui pengelolaan investigasi forensik digital dan pertukaran informasi ancaman secara terstruktur [10].

2.7 VirusTotal

VirusTotal adalah layanan pemindaian file dan URL berbasis cloud yang bekerja dengan menggunakan sejumlah besar mesin antivirus komersial dan open-source untuk menganalisis dan mendeteksi file maupun URL berbahaya secara komprehensif [11]. Dalam implementasinya pada penelitian ini, VirusTotal dimanfaatkan sebagai komponen verifikasi file berbahaya yang terintegrasi dengan Wazuh [12].

2.8 Discord

Discord dijelaskan sebagai platform komunikasi digital yang memungkinkan individu maupun organisasi membangun komunitas dan berinteraksi secara real-time melalui teks, suara, dan video dalam satu ruang terintegrasi yang disebut server. Awalnya dikenal sebagai aplikasi komunikasi untuk komunitas gim, Discord berkembang menjadi alat kolaborasi yang mendukung kebutuhan bisnis, pemasaran, serta pengelolaan komunitas secara profesional dengan fitur seperti channel terstruktur, manajemen peran (*roles*), serta integrasi dengan berbagai aplikasi pendukung. Platform ini dirancang untuk menciptakan komunikasi yang interaktif, terorganisir, dan mudah diakses melalui berbagai perangkat [13].

2.9 Ubuntu

Ubuntu Live Server merupakan edisi Ubuntu yang dirancang khusus untuk kebutuhan server, terutama bagi pengguna yang ingin menjalankan layanan berbasis internet seperti website, FTP, maupun layanan jaringan lainnya. Versi ini menyediakan paket server berbasis Linux yang mencakup berbagai layanan seperti web server, FTP server, serta dukungan jaringan seperti DNS server. Berbeda dengan versi desktop, Ubuntu Server menggunakan antarmuka berbasis command line (CLI) tanpa tampilan grafis, sehingga mampu memberikan efisiensi penggunaan sumber daya yang lebih tinggi dan performa yang optimal, khususnya pada server dengan beban kerja intensif. Selain itu, edisi server ini juga mendukung implementasi pada lingkungan komputasi awan (cloud), sehingga fleksibel untuk digunakan dalam berbagai skenario infrastruktur modern [14].

2.10 Threat Intelligence

Threat intelligence merupakan proses sistematis dalam mengumpulkan, menganalisis, dan menginterpretasikan informasi mengenai ancaman yang berpotensi membahayakan sistem dan infrastruktur teknologi informasi. Konsep ini tidak hanya berfokus pada pengumpulan data mentah terkait serangan, tetapi juga mengubah data tersebut menjadi informasi yang bernilai strategis untuk mendukung pengambilan keputusan dalam bidang keamanan. Threat intelligence membantu organisasi memahami siapa pelaku ancaman, bagaimana metode serangan dilakukan, serta apa tujuan yang ingin dicapai oleh penyerang. Informasi yang dihasilkan dapat berupa indikator kompromi (Indicator of Compromise/IoC) seperti alamat IP berbahaya,

domain mencurigakan, hash file malware, maupun pola serangan tertentu [15].

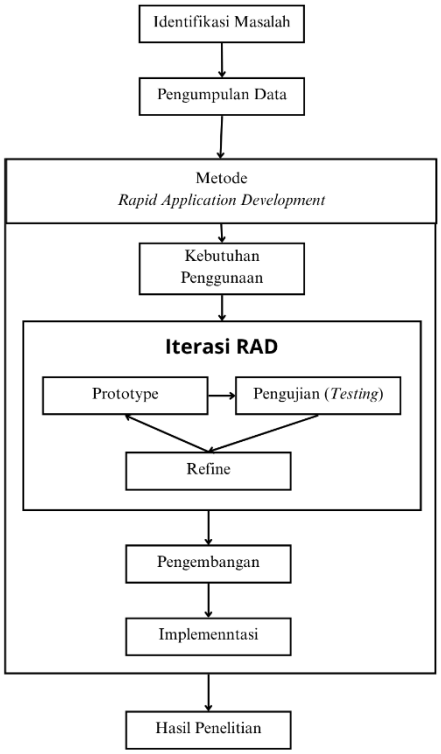
2.11 Rapid Application Development (RAD)

Rapid Application Development (RAD) merupakan metode pengembangan perangkat lunak yang berfokus pada pembuatan prototipe secara cepat melalui proses iteratif guna menghasilkan sistem yang sesuai dengan kebutuhan pengguna, dengan kelebihan seperti peningkatan kualitas hasil, efisiensi waktu dan biaya, serta kemampuan melakukan pembaruan secara cepat, meskipun memiliki keterbatasan seperti membutuhkan tim dengan keahlian tinggi dan hanya cocok untuk proyek yang dapat dimodularisasi, di mana tahapan utamanya meliputi perencanaan kebutuhan, desain sistem yang dilakukan secara berulang dengan melibatkan pengguna, proses pengembangan disertai pengumpulan umpan balik, hingga tahap implementasi sebagai penyelesaian akhir dari sistem yang dibangun [16].

3. METODE PENELITIAN

Model pengembangan sistem yang digunakan dalam penelitian ini adalah Rapid Application Development (RAD). Metode RAD dipilih karena menekankan pada kecepatan proses pembangunan sistem serta fleksibilitas dalam menyesuaikan kebutuhan yang dapat berubah selama proses pengembangan berlangsung.

Teknik pengumpulan data dilakukan melalui tiga cara: (1) Observasi langsung terhadap infrastruktur sistem jaringan serta sistem keamanan informasi di Diskominfostandi Kota Bekasi; (2) Wawancara dengan administrator IT untuk mengetahui kondisi sistem monitoring keamanan yang digunakan saat ini; dan (3) Studi pustaka dengan mengumpulkan referensi dari buku, jurnal ilmiah, artikel, dan dokumentasi resmi yang relevan.



Gambar 1. Kerangka Pemikiran

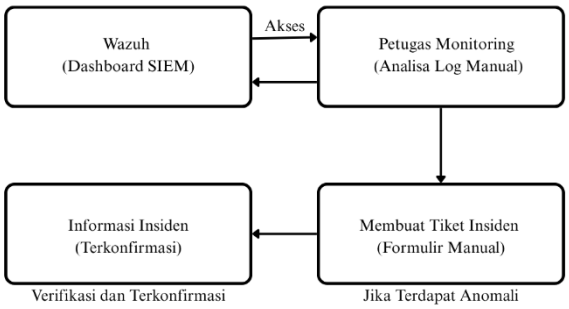
Tahapan penelitian mengikuti model RAD meliputi: (1) Identifikasi kebutuhan sistem keamanan terintegrasi; (2) Perancangan prototype framework yang mencakup konfigurasi Wazuh, Shuffle, MISP, DFIR-IRIS, dan Discord; (3) Pengujian sistem dengan simulasi serangan XSS dan webshell; (4) Penyempurnaan (refine) berdasarkan hasil pengujian; (5) Pengembangan dan finalisasi; serta (6) Implementasi pada lingkungan nyata Diskominfostandi.

Lingkungan implementasi menggunakan server Ubuntu Server 24.04 LTS dengan konfigurasi sebagai berikut: Wazuh Manager pada IP 10.100.0.154, Wazuh Agent pada IP 10.100.0.87 (server web aduansiber), MISP pada IP 10.100.0.140 (Docker), Shuffle SOAR pada IP 10.100.0.141 (Docker), dan DFIR-IRIS pada IP 10.100.0.142 (Docker).

4. HASIL DAN PEMBAHASAN

4.1 Analisis Infrastruktur Awal

Berdasarkan observasi yang dilakukan, infrastruktur awal Diskominfostandi Kota Bekasi masih mengandalkan proses monitoring dan penanganan insiden secara manual.



Gambar 2. Skema Infrastruktur Awal

Alur kerja yang berjalan adalah: Wazuh mengumpulkan log → petugas monitoring mengakses dashboard secara manual → melakukan analisis log → jika ditemukan anomali, petugas membuat tiket insiden manual → informasi insiden terkonfirmasi. Ketergantungan pada analisis manual ini menyebabkan keterlambatan dalam respons dan berpotensi terjadinya human error.

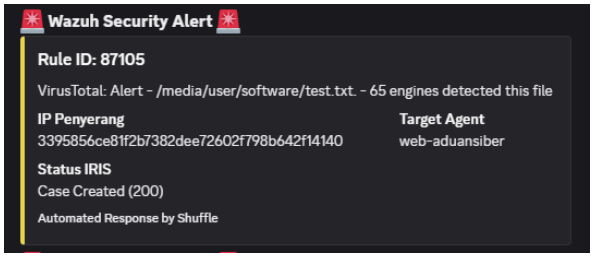
4.2 Pengujian Kerentanan Sistem

4.2.1. Skenario Cross-Site Scripting (XSS)

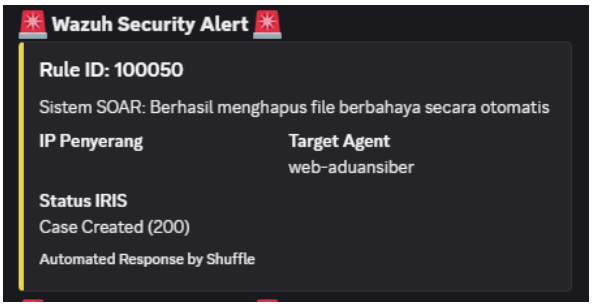
Pengujian XSS dilakukan dengan menyisipkan payload standar pada kolom input aplikasi web Diskominfostandi. Payload yang digunakan adalah id=<script>alert("xss")</script>. Hasil pengujian menunjukkan bahwa server merespons dengan mengembalikan halaman error 403 Forbidden, namun Wazuh tetap berhasil mendeteksi aktivitas tersebut dan menghasilkan alert "XSS Attempt Detected" pada dashboard. Hal ini mengindikasikan bahwa validasi input pada lapisan aplikasi belum sepenuhnya mampu menangani seluruh variasi payload XSS.

4.2.2. Skenario Unggahan Webshell

Pengujian webshell dilakukan dengan mengunggah file webshell melalui fitur unggah file pada aplikasi web. File yang diunggah diverifikasi melalui VirusTotal yang mengidentifikasinya sebagai malware dengan 62-66 engines terdeteksi. Wazuh secara otomatis mendeteksi file berbahaya tersebut dan langsung mengeksekusi Active Response untuk menghapus file tanpa intervensi manual. Alert kemudian diteruskan ke Shuffle SOAR dan notifikasi dikirimkan secara real-time ke Discord.



Gambar 3. Notifikasi VirusTotal Masuk Di Discord



Gambar 4. Notifikasi Active Response Deleted File Berbahaya Masuk Di Discord

Skenario unggahan webshell mengungkapkan kerentanan nyata pada lapisan validasi unggahan file di aplikasi web, di mana sistem belum mampu mencegah masuknya file berbahaya secara proaktif. Namun demikian, pengujian ini sekaligus membuktikan efektivitas sistem keamanan berlapis yang telah diimplementasikan — mulai dari deteksi oleh Wazuh, respons otomatis melalui *Active Response*, integrasi dengan VirusTotal untuk verifikasi ancaman, hingga penyampaian notifikasi *real-time* ke Discord. Alur respons yang berjalan secara otomatis ini secara signifikan memperpendek waktu penanganan insiden dibandingkan proses manual yang selama ini dilakukan

4.2.3. Penilaian Kerentanan dengan CVSS v3.1

Tabel 1. Hasil Penilaian Kerentanan Berdasarkan CVSS v3.1

No	Kerentanan	String Vector	CVSS	Level
1	Cross-Site Scripting (XSS)	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	6.1	Medium
2	Unrestricted File Upload (Webshell)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8	Critical

4.3 Implementasi Framework Keamanan Integrasi

Implementasi framework keamanan terintegrasi dilakukan dengan membangun ekosistem yang menghubungkan lima komponen utama. Pertama, konfigurasi rule custom Wazuh dilakukan pada direktori /var/ossec/etc/rules/ untuk mengenali pola serangan XSS (string <script>, alert(), onerror=) dan webshell. Kedua, Active Response dikonfigurasi pada file /var/ossec/etc/ossec.conf untuk secara otomatis menghapus file berbahaya yang terdeteksi. Ketiga, integrasi Wazuh ke Shuffle SOAR dilakukan melalui webhook HTTP POST dalam format JSON. Keempat, workflow otomatis Shuffle dirancang untuk mengorkestrasi alur respons insiden end-to-end: penerimaan alert → enrichment MISP → pembuatan case DFIR-IRIS → notifikasi Discord. Kelima, konfigurasi notifikasi real-time ke Discord menggunakan webhook platform Discord.

4.4 Pengujian Ulang Sistem Pasca-Implementasi

Pengujian ulang dilakukan dengan skenario serangan yang identik dengan pengujian awal. Hasil pengujian ulang XSS menunjukkan bahwa seluruh alur dari deteksi Wazuh hingga notifikasi Discord berjalan secara otomatis dalam hitungan detik. Pengujian ulang webshell menunjukkan bahwa file berbahaya berhasil dideteksi, dihapus otomatis oleh Active Response, case terbuat di DFIR-IRIS, dan notifikasi masuk ke Discord tanpa intervensi manual.

Tabel 2. Skor Kerentanan Sebelum Implementasi

Kerentanan	Skor	Level
Cross-Site Scripting (XSS)	6.1	Medium
Unrestricted File Upload (Webshell)	9.8	Critical

Tabel 3. Skor Kerentanan Sesudah Implementasi

Kerentanan	Skor	Level
Cross-Site Scripting (XSS)	4.3	Medium
Unrestricted File Upload (Webshell)	6.5	Medium

Penurunan skor CVSS pada kerentanan XSS dari 6.1 menjadi 4.3 terjadi karena adanya mekanisme deteksi dan notifikasi otomatis yang mempersingkat waktu respons. Penurunan skor webshell yang lebih signifikan dari 9.8 menjadi 6.5 mencerminkan efektivitas Active Response Wazuh yang secara otomatis menghapus file berbahaya segera setelah terdeteksi, sehingga dampak potensial berhasil ditekan secara substansial.

5. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa perancangan dan implementasi *framework* keamanan siber terintegrasi berbasis SIEM Wazuh pada infrastruktur

Diskominfostandi Kota Bekasi berhasil dilakukan secara menyeluruh, mencakup integrasi Wazuh, Shuffle SOAR, MISP, DFIR-IRIS, dan Discord yang bekerja secara otomatis dan berkesinambungan. Integrasi Wazuh dengan MISP sebagai platform *threat intelligence* terbukti meningkatkan kualitas deteksi ancaman melalui pengayaan data *alert* secara otomatis, sementara otomatisasi respons insiden melalui *Active Response* Wazuh dan *workflow* Shuffle SOAR berhasil mempersingkat waktu respons dari proses manual menjadi hitungan detik. Efektivitas implementasi ini dibuktikan secara kuantitatif dengan penurunan skor CVSS v3.1 pada kerentanan XSS dari 6.1 menjadi 4.3 dan kerentanan *webshell* dari 9.8 menjadi 6.5, yang mencerminkan peningkatan nyata dalam kemampuan deteksi dan respons insiden keamanan siber secara otomatis dan terintegrasi.

UCAPAN TERIMA KASIH

Segala puji bagi Allah SWT atas rahmat dan hidayah-Nya yang telah memberikan kemampuan kepada penulis untuk menyusun dan menyelesaikan artikel ini. Tidak lupa pula, penulis mengucapkan terima kasih kepada semua pihak yang terlibat dalam penyusunan, khususnya para pengguna aplikasi Sapawarga yang telah bersedia mengikuti pengujian.

DAFTAR PUSTAKA

[1] T. Setiadi *et al.*, *Sistem Informasi Cyber Security*. CV. Gita Lentera, 2024. [Online]. Available: https://books.google.co.id/books?id=ExALEQAAQBAJ

[2] R. Amami, M. Charfeddine, and S. Masmoudi, "Exploration of Open Source SIEM Tools and Deployment of an Appropriate Wazuh-Based Solution for Strengthening Cyberdefense," in *2024 10th International Conference on Control, Decision and Information Technologies (CoDIT)*, IEEE, 2024, pp. 1–7.

[3] A. Sutanto and A. Rakhman, "Experimental Evaluation of Wazuh-Grafana Integration for Real-Time Cyber Threat Detection in Resource-Constrained Environments," *Journal of Applied Informatics and Computing*, vol. 9, no. 5, pp. 2783–2790, 2025.

[4] P. Rathore and K. Kolhe, "Integrating Automation and Orchestration in Security Incident Handling: A Review of SOAR Frameworks and Platforms," in *The Unified International Conference on Emerging Technologies in Cyber-Physical Systems and Industrial AI*, Springer, 2024, pp. 529–551.

[5] V. A. Tandirerung and R. T. Mangesa, "Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas," *TEKNOVOKASI: Jurnal Pengabdian Masyarakat*, pp. 89–94, 2023.

[6] R. Boddu, R. Trent, and S. Lamppu, *Microsoft Unified XDR and SIEM Solution Handbook: Modernize and build a unified SOC platform for future-proof security*. Packt Publishing, 2024. [Online]. Available: https://books.google.co.id/books?id=X6n4EAAAQBAJ

[7] R. Gupta and S. Bassett, *Security Monitoring with Wazuh: A hands-on guide to effective enterprise security using real-life use cases in Wazuh*. Packt Publishing, 2024. [Online]. Available: https://books.google.co.id/books?id=hMH7EAAAQBAJ

[8] A. Thakker, A. More, and K. Kumar, "Automated Defense Against Application-Layer Attacks on Windows Systems Using Wazuh and Shuffle," *International Journal of Education, Science, Technology, and Engineering (IJESTE)*, vol. 8, no. 1, pp. 45–57, 2025.

[9] D. Chatziamanetoglou and K. Rantos, "Weighted quality criteria for cyber threat intelligence: assessment and prioritisation in the MISP data model," *Int. J. Inf. Secur.*, vol. 24, no. 4, p. 160, 2025, doi: 10.1007/s10207-025-01080-6.

[10] M. R. T. Hidayat, N. Widiyasono, and R. Gunawan, "OPTIMASI DETEKSI MALWARE PADA SIEM WAZUH MELALUI INTEGRASI CYBER THREAT INTELLIGENCE DENGAN MISP DAN DFIR-IRIS," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 1, 2025.

[11] K. van Liebergen, J. Caballero, P. Kotzias, and C. Gates, "A deep dive into the VirusTotal file feed," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, 2023, pp. 155–176.

[12] Wazuh, "VirusTotal Integration — Malware Detection," Wazuh Documentation.

[13] B. Wilson, *Discord For Business Success*. Publisher s21598, 2025. [Online]. Available:

https://books.google.co.id/books?id=ilVSEQAAQBAJ
[14] R. Petersen, *Ubuntu 24.04 LTS Server: Administration and Reference*. surfing turtle press, 2025.
[15] M. Lee, *Cyber threat intelligence*. John Wiley & Sons, 2023.
[16] S. T. M. K. Maria Atik Sunarti Ekowati and S. P. M. P. Dr. Fitri Rezeki, *Analisa dan Perancangan Sistem Informasi*. PT KIMHSAFI ALUNG CIPTA, 2025. [Online]. Available: https://books.google.co.id/books?id=qhZZEQAAQBAJ