Journal of Information Technology and Computer Science (INTECOMS)
Volume 9 Nomor 2, Tahun 2026
e-ISSN : 2614-1574
p-ISSN : 2621-3249

SIMULASI MITIGASI ZERO-TOUCH PADA SERANGAN BRUTE FORCE SSH DAN RDP BERBASIS ORKESTRASI SIEM WAZUH

ZERO-TOUCH MITIGATION SIMULATION ON SSH AND RDP BRUTE FORCE ATTACKS BASED ON WAZUH SIEM ORCHESTRATION

Putu Dedi Juliana[1], Arya Adhyaksa Waskita[2], Ferhat Aziz[3]
Teknik Informatika, Universitas Pamulang[1,2,3]
putudediip@gmail.com[1]

ABSTRACT

Remote server administration via Secure Shell (SSH, port 22) and Remote Desktop Protocol (RDP, port 3389) on public-sector infrastructure particularly the Electronic Procurement Service (LPSE) of Mahakam Ulu Regency inherently expands the attack surface against credential-guessing techniques mapped to MITRE ATT&CK T1110. Analyst-dependent mitigation models lengthen the gap between repeated logon-failure detection and containment, creating an exploitable window for adversaries. This study designs and validates an automated-mitigation simulation prototype grounded in Wazuh Active Response semantics within a Security Information and Event Management (SIEM) framework. A client–server architecture (React/Vite frontend; Node.js/Express backend with JSON persistence) executes three functional test scenarios: single-source SSH brute force, single-source RDP brute force, and multi-source attacks rotating across three IP addresses. Each scenario applies a threshold of ten authentication failures to trigger detection rules 5710 (SSH) and 60122 (RDP) annotated with T1110, followed by Active Response execution analogous to firewall-drop (Linux) and netsh.exe (Windows). Results demonstrate a discrete Mean Time to Respond (MTTR) of one simulation tick across all three scenarios, with an IP-isolation success rate of 100% against the modelled source pool. The validated prototype serves as a conceptual blueprint for planning SIEM deployment on public infrastructure without incurring production-service disruption risk.

Keywords: *Automated Mitigation; Brute-Force Attack; Wazuh Active Response; SIEM Simulation; Mean Time To Respond*

ABSTRAK

Administrasi server berbasis Secure Shell (SSH, port 22) dan Remote Desktop Protocol (RDP, port 3389) pada infrastruktur layanan publik, khususnya Layanan Pengadaan Secara Elektronik (LPSE) Kabupaten Mahakam Ulu, secara inheren memperluas permukaan serangan terhadap Teknik *brute force* (MITRE ATT&CK T1110). Model mitigasi manual yang bergantung pada analis memperpanjang jarak antara deteksi kegagalan logon berulang dan kontainmen, sehingga membuka *jendela eksploitasi* yang dapat dimanfaatkan penyerang. Penelitian ini merancang dan memvalidasi prototipe simulasi mitigasi otomatis berbasis semantic *Active Response* Wazuh dalam kerangka Security Information and Event Management (SIEM). Arsitektur klien–pelayan (*React/Vite* pada sisi klien; *Node.js/Express* dengan persistensi JSON pada sisi pelayan) menjalankan tiga skenario pengujian fungsional: serangan *brute force* bersumber tunggal pada SSH, bersumber tunggal pada RDP, dan multi-sumber dengan tiga alamat IP berotasi. Setiap skenario menggunakan ambang 10 kegagalan autentikasi untuk memicu aturan deteksi 5710 (SSH) dan 60122 (RDP) beranotasi T1110, dilanjutkan eksekusi *Active Response* berupa *firewall-drop* (Linux) dan netsh.exe (Windows). Hasil pengujian menunjukkan Mean Time to Respond (MTTR) diskret sebesar satu *tick* simulasi pada ketiga skenario, dengan rasio keberhasilan isolasi alamat IP mencapai 100% terhadap himpunan sumber yang dimodelkan. Prototipe yang tervalidasi berfungsi sebagai cetak biru konseptual bagi perencanaan penerapan SIEM pada infrastruktur publik tanpa risiko gangguan layanan produksi.

Kata Kunci: Mitigasi Otomatis; Serangan *Brute Force*; Wazuh *Active Response*; Simulasi SIEM; *Mean Time To Respond*

PENDAHULUAN

Ketersediaan layanan digital pemerintahan yang andal merupakan prasyarat utama dalam implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia, termasuk dalam pengelolaan Layanan Pengadaan Secara Elektronik (LPSE) di tingkat kabupaten. LPSE Kabupaten Mahakam Ulu, sebagai infrastruktur pengadaan barang dan jasa pemerintah daerah, bergantung pada ketersediaan server secara kontinu (24/7) serta terjaminnya integritas dan kerahasiaan data pengadaan. Operasional dan

pemeliharaan server tersebut memerlukan akses administratif jarak jauh: pada lingkungan berbasis Linux, Secure Shell (SSH) dengan port standar 22 menjadi mekanisme utama sesi terminal terenkripsi, sedangkan pada lingkungan berbasis Windows, Remote Desktop Protocol (RDP) dengan port standar 3389 menyediakan antarmuka grafis jarak jauh. Kedua protokol ini merupakan komponen fungsional yang tidak dapat dihilangkan dari tata kelola infrastruktur modern, namun sekaligus menempatkan titik autentikasi pada posisi yang secara struktural mudah dijangkau dari jaringan eksternal, khususnya internet.

Keterbukaan layanan autentikasi jarak jauh secara inheren memperluas permukaan serangan infrastruktur. Di antara pola ancaman yang paling persisten terhadap protokol-port tersebut adalah serangan *brute force*, yang dalam kerangka taktik dan teknik MITRE ATT&CK dikelompokkan sebagai teknik T1110 (*Brute Force*). Serangan ini dilaksanakan melalui percobaan berulang terhadap kombinasi kredensial secara ekshaustif, berbasis kamus, maupun hibrida menggunakan perangkat lunak otomatis yang mampu menghasilkan volume percobaan login sangat tinggi dalam rentang waktu singkat (Singh et al., 2024). Apabila berhasil, penyerang memperoleh akses tidak sah ke lapisan sistem operasi maupun aplikasi, dengan konsekuensi yang berpotensi meliputi pemalsuan atau pembocoran data pengadaan, pemasangan muatan berbahaya, eskalasi hak akses, dan gangguan ketersediaan layanan. Pada konteks server LPSE yang menampung data sensitif pengadaan pemerintah daerah, risiko tersebut bukan bersifat teoretis semata, melainkan relevan secara langsung dan operasional.

Pendekatan mitigasi konvensional yang mengandalkan pemantauan manual berkas log atau pemblokiran alamat IP secara ad hoc oleh administrator menunjukkan keterbatasan struktural yang signifikan. Model semacam ini bersifat reaktif, memerlukan ketersediaan sumber daya manusia dalam jangka waktu panjang, dan rentan terhadap keterlambatan antara kemunculan indikator kompromi dengan tindakan pertahanan yang efektif (Jalalvand et al., 2024). Keterlambatan inilah yang menciptakan *jendela eksploitasi* interval temporal di mana penyerang dapat melanjutkan percobaan atau mengeksploitasi akses parsial sebelum pertahanan sepenuhnya diterapkan. Kajian literatur menunjukkan bahwa banyak implementasi SIEM masih berhenti pada tahap korelasi log pasif dan analisis pasca-insiden, sehingga nilai tambah utama terbatas pada visibilitas retrospektif, bukan pada penutupan kontainer ancaman secara real-time (González-Granadillo et al., 2021; Skopik et al., 2022).

Pergeseran paradigma menuju *active defense* dan orkestrasi respons berbasis Security Information and Event Management (SIEM) membuka kemungkinan untuk menyatukan agregasi peristiwa, penalaran berbasis aturan, dan eksekusi respons terkendali dalam satu rantai keputusan yang beroperasi pada kecepatan mesin. Platform Wazuh, sebagai solusi SIEM sumber terbuka yang telah banyak divalidasi dalam konteks operasional, menyediakan mekanisme *Active Response* yang memungkinkan pemicu tindakan pertahanan berbasis aturan seperti pemblokiran alamat IP melalui *firewall-drop* pada Linux atau `netsh.exe` pada Windows secara otomatis setelah ambang deteksi terpenuhi (Alanda et al., 2023; Wazuh Team, n.d.). Kemampuan ini secara konseptual mendekatkan postur keamanan pada model *zero-touch mitigation*: respons terjadi pada skala dan kecepatan mesin tanpa ketergantungan pada intervensi operator di setiap insiden. Kajian terkini juga menekankan bahwa integrasi Wazuh dengan kerangka taktis MITRE ATT&CK memungkinkan kontekstualisasi ancaman yang lebih kaya, memperkuat kapasitas triase analis SOC (Winkler & Sharma, 2025).

Meskipun demikian, validasi orkestrasi mitigasi otomatis pada infrastruktur publik yang kritis menghadapi kendala etis dan operasional yang nyata: eksperimen langsung pada server LPSE yang sedang beroperasi berpotensi mengganggu ketersediaan layanan pengadaan dan melanggar kewajiban kerahasiaan data. Kesenjangan ini mendorong kebutuhan terhadap lingkungan validasi terkendali yang mempertahankan relevansi domain namun meniadakan risiko produksi (Noor et al., 2023). Penelitian ini menjawab kesenjangan tersebut dengan merancang dan memvalidasi prototipe simulasi berfidelitas tinggi berarsitektur klien pelayan antarmuka *React/Vite* dan lapisan persistensi *Node.js*/JSON yang mereplikasi alur logis deteksi *brute force* SSH dan RDP, pembentukan peringatan dengan pemetaan ke aturan 5710 dan 60122 beranotasi T1110, serta eksekusi mitigasi otomatis bernarasi *firewall-drop* dan `netsh.exe`. Tujuan utama kajian ini adalah: (1) mendemonstrasikan konsistensi logika rantai *sense decide act* dalam analogi SIEM terkendali; (2) mengukur implikasi penurunan Mean Time to Respond (MTTR) dari materialisasi peringatan ke penegakan pemblokiran; dan (3) menawarkan cetak biru konseptual yang telah diverifikasi keamanan metodologisnya sebagai landasan perencanaan implementasi SIEM pada infrastruktur publik. Cakupan klaim penelitian ini secara eksplisit dibatasi pada konsistensi internal alur dan metrik prototipe, bukan pada kesetaraan numerik penuh dengan *deployment* Wazuh produksi.

METODE PENELITIAN

2.1 Desain Penelitian

Penelitian ini mengadopsi paradigma rekayasa sistem terapan (*applied systems engineering*) dengan strategi validasi melalui prototipe terkendali (*controlled prototyping*). Pendekatan ini dipilih berdasarkan dua pertimbangan utama: pertama, kebutuhan untuk memisahkan validasi logika orkestrasi respons otomatis dari risiko gangguan ketersediaan layanan pada infrastruktur LPSE yang sedang beroperasi; kedua, keterbatasan akses teknis dan legal terhadap log produksi nyata yang menyebabkan eksperimen langsung tidak dapat dipertanggungjawabkan secara etis. Simulasi berfidelitas tinggi diposisikan sebagai substitusi metodologis yang mempertahankan urutan kausal kejadian keamanan namun meniadakan dampak samping terhadap pengguna layanan publik (Ruambo et al., 2025). Klaim yang dihasilkan secara eksplisit mengacu pada perilaku artefak perangkat lunak dalam parameter yang terdefinisi, bukan pada pengukuran kinerja infrastruktur produksi.

2.2 Arsitektur Sistem Simulasi

Sistem simulasi dirancang mengikuti pola **klien–pelayan** dengan tiga lapisan tanggung jawab yang terpisah, sebagaimana diilustrasikan pada Gambar 1.

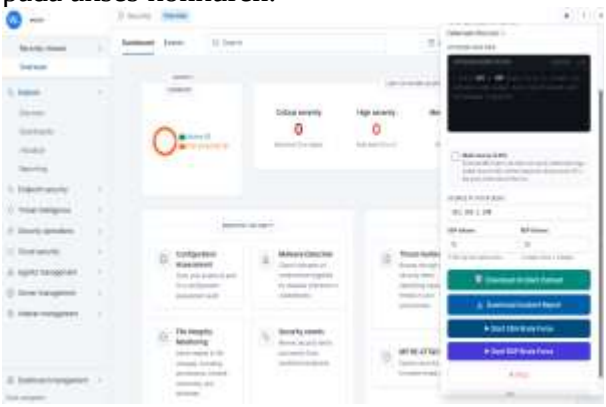
Lapisan Klien diimplementasikan sebagai *Single Page Application* (SPA) menggunakan *React 19* dan *Vite 5*. Lapisan ini menggabungkan peran dashboard investigasi (modul Discover, Security Events, Active Response, Incident Response) dan agen simulasi yang membangkitkan log kegagalan autentikasi bergaya produksi. Manajemen keadaan dilakukan melalui SimulationContext berbasis useReducer, yang memastikan satu sumber kebenaran (*single source of truth*) bagi seluruh modul visualisasi. Mesin simulasi diimplementasikan dalam *custom hook* useSimulation yang beroperasi dengan semantik waktu diskret: setiap *tick* merepresentasikan satu detik waktu simulasi.

Lapisan Pelayan diimplementasikan dengan *Node.js 18 LTS* dan kerangka *Express*. Pelayan menyediakan tiga *endpoint* RESTful: GET /api/logs untuk membaca keadaan persisten, POST /api/logs/update untuk menulis keadaan setelah setiap perubahan (*debounce* 500 ms), dan POST /api/logs/reset untuk mengembalikan

keadaan ke kondisi awal bersih antar skenario.

Lapisan Persistensi menggunakan berkas wazuh-alerts.json pada sistem berkas lokal, yang memungkinkan inspeksi manual untuk keperluan audit dan reproduksibilitas eksperimen tanpa bergantung pada memori sesi peramban.

Komunikasi antar lapisan mengikuti pola *polling* terkendali dengan interval ~1,5 detik disertai mekanisme *versioning* untuk mencegah kondisi balapan (*race condition*) pada akses konkuren.



Gambar 1. Arsitektur Simulasi

2.3 Skenario dan Parameter Pengujian

Pengujian dilaksanakan melalui tiga skenario fungsional dengan parameter baku yang seragam, sebagaimana dirangkum pada Tabel 1.

Parameter	Nilai	Keterangan
Ambang kegagalan autentikasi	10 percobaan	Sebelum peringatan *brut e force* dipicu
Interval diskret (*tick*)	1 detik	Satu langkah waktu simulasi
Durasi skenario	12 *tick*	Tick 1–10: log; Tick 10: alert; Tick 11: block; Tick 12: close
MTTR diskret (konfigurasi baku)	1 *tick*	Jarak pemicuan peringatan ke eksekusi pemblokiran
Format log SSH	sshd *Failed password for invalid user*	Bergaya log produksi Linux
Format log RDP	Windows Security Event ID 4625	*An account failed to log on*
Aturan SSH	Rule 5710 / Level 10	Anotasi MITRE ATT&CK T1110
Aturan RDP	Rule 60122 / Level 10	Anotasi MITRE ATT&CK T1110
Mitigasi SSH	firewall-drop (narasi Linux)	IP ditambahkan ke blockedIPs[]
Mitigasi RDP	netsh.exe (narasi Windows)	IP ditambahkan ke blockedIPs[]
Mode sumber multi	Round-robin 3 IP	Agregasi ambang kolektif

Skenario 1 (SSH, Sumber Tunggal): Satu alamat IP tetap (203.0.113.45) menghasilkan kegagalan autentikasi SSH pada port 22 hingga ambang tercapai, memicu Rule 5710 dan *firewall-drop*. Skenario 2 (RDP, Sumber Tunggal): Satu alamat IP tetap (198.51.100.78) menghasilkan kegagalan logon RDP pada port 3389 (Event ID 4625) hingga ambang tercapai, memicu Rule 60122 dan netsh.exe. Skenario 3 (Multi-Sumber, 3 IP): Tiga alamat IP (203.0.113.10–.12) berotasi *round-robin* per *tick* ; ambang dihitung secara kolektif; seluruh IP dalam pool diblokir serentak pada fase mitigasi.

2.4 Metrik Evaluasi

Dua metrik utama digunakan untuk mengevaluasi efektivitas sistem dalam batasan simulasi terkendali:

1. Mean Time to Respond (MTTR) Diskret dioperasionalkan sebagai jarak dalam satuan *tick* antara materialisasi peringatan (tick ke-10) dan eksekusi pemblokiran (tick ke-11). Metrik ini mengukur konsistensi temporal alur deteksi–mitigasi, bukan latensi infrastruktur produksi (Pitkar, 2025).
2. Rasio Keberhasilan Isolasi Alamat IP dinilai dengan memverifikasi bahwa setiap alamat dalam pool skenario: (i)

masuk ke struktur blockedIPs[] di backend, (ii) tercatat dalam riwayat *Active Response*, dan (iii) tampil konsisten di seluruh modul visualisasi.

Data dikumpulkan melalui inspeksi berkas wazuh-alerts.json, ekspor CSV (*Download Incident Dataset*), dan pengamatan visual pada modul investigasi menggunakan teknik triangulasi lintas modul.

HASIL DAN PEMBAHASAN

3.1 Implementasi dan Lingkungan Simulasi

Prototipe berhasil diinstansiasikan sebagai sistem klien–pelayan yang fungsional dan dapat diulang. Lapisan klien menghasilkan antarmuka mendekati *high-fidelity* dasbor Wazuh berbasis OpenSearch UI dengan modul investigasi utama: Discover, Security Events, Active Response, dan Incident Response. Lapisan persistensi memastikan keadaan insiden (log, peringatan, daftar IP terisolasi) dapat dimuat ulang setelah penyegaran sesi, menjadikan demonstrasi bersifat *repeatable*.

Skrip *Node.js* (generate-historical-data.js) mengisi lebih dari 5.000 entri log sintetis terkalibrasi dalam jendela 90 hari sebagai *noise* kontekstual yang merealismekan tampilan histogram temporal dan menguji mekanisme baca-tulis JSON.

Gambar 2. Tampilan Dasbor Utama Prototipe Modul Threat Hunting dengan KPI dan Histogram Log

3.2 Hasil Pengujian Skenario Serangan

3.2.1 Skenario 1: SSH Brute Force, Sumber Tunggal

Pada skenario pertama, sistem membangkitkan kegagalan autentikasi SSH dari IP 203.0.113.45. Pada Tick 1–9, sembilan log kegagalan bergaya sshd ditambahkan ke state.logs[] dan dapat diamati di modul Discover. Pada Tick 10, ambang tercapai; Rule 5710 dipicu (sshd: brute force trying to get access to the system, Level 10, Taktik TA0006, T1110) dan status berubah ke 'detected'. Pada Tick 11, IP 203.0.113.45 diblokir otomatis (firewall-drop) dan masuk ke state.blockedIPs[]. Pada Tick 12, insiden ditutup ('mitigated'). MTTR diskret: 1 tick. Verifikasi lintas modul mengkonfirmasi: Discover menampilkan 12 entri log, Security Events KPI Total Alerts=1/Auth Failures=10, Active Response satu baris Command History (Success), Incident Response *timeline* empat fase.

3.2.2 Skenario 2: RDP Brute Force, Sumber Tunggal

Pada skenario kedua, sistem membangkitkan log kegagalan logon Windows bergaya Event ID 4625 dari IP 198.51.100.78 pada port 3389. Alur temporal mengikuti struktur yang analog dengan Skenario 1, dengan perbedaan pada format log (EventID 4625: An account failed to log on. Logon Type: 3 (Network). Source: 198.51.100.78) dan aturan yang dipicu (Rule 60122: Windows: RDP brute force attack detected, Level 10, T1110). Pada fase mitigasi, narasi *Active Response* menggunakan netsh.exe advfirewall firewall add rule name='Block 198.51.100.78', mencerminkan konteks endpoint Windows. Verifikasi berkas JSON menunjukkan 12 entri logs[], satu entri alerts[], dan satu entri blockedIPs[] dengan command: "netsh.exe".

3.2.3 Skenario 3 : Brute Force Multi-Sumber

Pada skenario ketiga, tiga alamat IP (203.0.113.10, .11, .12) berotasi *round-robin* per *tick*. Penghitung *attempts* bertambah secara kolektif tanpa membedakan sumber. Pada Tick 10, ambang agregat terpenuhi; peringatan Rule 5710 dipicu dengan deskripsi "sshd: distributed brute force attack detected from multiple sources (3 IPs)". Pada Tick 11, ketiga IP diblokir serentak dengan *timestamp* identik (tidak ada iterasi manual). Verifikasi berkas JSON menunjukkan 14 entri logs[] (10 kegagalan + 3 log *Active Response* + 1 log penutupan) dan 3 entri blockedIPs[] membuktikan pemblokiran serentak tanpa intervensi operator.

Gambar 3. Modul Active Response Command History Skenario 3 dengan Tiga Baris Eksekusi *Firewall-Drop*.

3.1 Ringkasan Metrik dan Perbandingan Skenario

Tabel ini merangkum profil dan hasil agregat ketiga skenario pengujian.

Kode	Skenario	Protokol/Port	Rule ID	MTTR Diskret	IP Diblokir	Rasio Isolasi	Narasi Mitigasi
S1	SSH, sumber tunggal	SSH / 22	5710	1 *tick*	1 IP	100%	firewall-drop
S2	RDP, sumber tunggal	RDP / 3389	60122	1 *tick*	1 IP	100%	netsh.exe
S3	Multi-sumber (3 IP)	SSH / 22	5710	1 *tick*	3 IP	100%	firewall-drop

Tabel berikutnya menyajikan matriks keberhasilan pengujian fungsional berdasarkan kriteria yang ditetapkan pada desain skenario.

No	Aspek Uji	S1	S2	S3
1	Log kegagalan autentikasi terbangkit hingga ambang	✓	✓	✓
2	Peringatan terbentuk dengan Rule ID dan Level sesuai desain	✓	✓	✓
3	Anotasi MITRE ATT&CK T1110 hadir pada metadata peringatan	✓	✓	✓
4	Status berubah ke 'detected' pada tick pelanggaran ambang	✓	✓	✓
5	Eksekusi EXECUTE_BLOCK otomatis 1 tick setelah alert (MTTR=1)	✓	✓	✓
6	Jejak Active Response sesuai narasi (firewall-drop/netsh.exe)	✓	✓	✓
7	Seluruh IP skenario masuk blockedIPs[] di backend	✓	✓	✓
8	Konsistensi data lintas modul (Discover→Events→AR→IR)	✓	✓	✓
9	Reset antar skenario: tidak ada kontaminasi data	✓	✓	✓

Kode	Skenario	Protokol/Port	Rule ID	MTTR Diskret	IP Diblokir	Rasio Isolasi	Narasi Mitigasi
	10	S3: Pemblokiran 3 IP serentak (timestamp identik)			N/A	N/A	✓

Legenda: ✓ = kriteria terpenuhi; N/A = tidak berlaku untuk skenario ini.

3.3 Pembahasan

3.4.1 Efektivitas MTTR dan Keunggulan Respons Otomatis

MTTR diskret sebesar satu *tick* yang konsisten di ketiga skenario merupakan temuan sentral penelitian ini. Makna analitisnya bukan pengukuran latensi *netfilter* kernel produksi, melainkan bukti bahwa automasi menghapus jeda keputusan manusia pada setiap insiden yang memenuhi ambang sebuah keunggulan kritis dibandingkan model pemantauan manual yang rata-rata membutuhkan respons beberapa menit hingga puluhan menit (Jalalvand et al., 2024). Temuan ini konsisten dengan Alanda et al. (2023) yang mengkonfirmasi efektivitas Wazuh dalam respons real-time, dan Khandait et al. (2021) yang memvalidasi bahwa deteksi berbasis ambang log merupakan pendekatan efektif dan praktis untuk *brute force* SSH.

3.4.2 Keberhasilan Pemblokiran IP dan Konsistensi Lintas Modul

Rasio keberhasilan isolasi 100% pada ketiga skenario menunjukkan konsistensi internal rekayasa perangkat lunak yang solid. Pola *single source of truth* melalui SimulationContext memastikan tidak ada inkonsistensi data dari *reducer* ke presentasi maupun persistensi backend; konsistensi timestamp, Rule ID, teknik T1110, dan narasi perintah terverifikasi lintas empat modul investigasi. Suskalo et al. (2023) mencatat Wazuh unggul dalam fleksibilitas *Active Response* untuk lingkungan *resource-constrained*, sementara Park et al. (2021) dan Tiwari & Hubballi (2023) mengkonfirmasi bahwa deteksi ambang berbasis log SSH mencapai akurasi kompetitif dibandingkan pendekatan ML. Skenario multi-sumber juga mendemonstrasikan agregasi ambang kolektif yang menangani topologi terdistribusi sederhana tanpa mengubah arsitektur inti sejalan dengan rekomendasi Ruambo et al. (2025) mengenai pentingnya mempertimbangkan pola serangan terdistribusi pada layanan akses jarak jauh.

3.4.3 Keterbatasan dan Implikasi Praktis

Beberapa keterbatasan perlu diakui: prototipe tidak mereplikasi mesin aturan Wazuh produksi penuh (*decoder*, *ruleset engine*, indeks OpenSearch), pengujian terbatas pada *happy path* tanpa skenario positif palsu atau teknik evasi *low-and-slow*, dan data log bersifat sintetis terkalibrasi bukan log operasional LPSE aktual. Meskipun demikian, prototipe yang tervalidasi berfungsi sebagai cetak biru konseptual yang mengurangi ketidakpastian desain sebelum komitmen infrastruktur memungkinkan perencanaan konfigurasi Wazuh setelah tahapan *hardening*, kalibrasi ambang, dan validasi beban produksi. González-Granadillo et al. (2021) menekankan nilai utama SIEM terletak pada kemampuannya menutup lingkaran deteksi–respons; penelitian ini mendemonstrasikan penutupan lingkaran tersebut dalam simulasi terkendali, dengan Ismail et al. (2025) dan Chamkar et al. (2025) menunjukkan arah pengembangan lanjutan melalui integrasi pembelajaran mesin untuk mendeteksi pola ancaman yang lebih kompleks.

KESIMPULAN

Penelitian ini telah berhasil merancang dan memvalidasi prototipe simulasi mitigasi otomatis berarsitektur klien–pelayan (*React/Vite* pada sisi klien; *Node.js/Express* dengan persistensi JSON

pada sisi pelayan) sebagai representasi logis dari rantai *sense decide act* dalam kerangka Security Information and Event Management berbasis Wazuh *Active Response*. Tiga skenario fungsional yang diuji serangan *brute force* SSH bersumber tunggal, RDP bersumber tunggal, dan multi-sumber tiga alamat IP berotasi seluruhnya mengkonfirmasi konsistensi logika deteksi–mitigasi yang direkayasa: pemetaan ke aturan 5710 (SSH) dan 60122 (RDP) beranotasi MITRE ATT&CK T1110, disertai eksekusi *Active Response* bergaya *firewall-drop* (Linux) dan netsh.exe(Windows).

Metrik utama yang diukur menunjukkan hasil yang konsisten dan dapat direproduksi. Mean Time to Respond (MTTR) diskret dioperasionalkan sebagai jarak antara materialisasi peringatan dan eksekusi pemblokiran menyempit menjadi tepat satu *tick* simulasi pada ketiga skenario, merepresentasikan eliminasi jeda keputusan manusia yang menjadi pembeda utama antara respons manual dan respons terorkestrasi. Rasio keberhasilan isolasi alamat IP mencapai 100% terhadap seluruh sumber yang dimodelkan dalam desain skenario, termasuk pemblokiran serentak tiga IP pada skenario multi-sumber tanpa intervensi operator.

Klaim penelitian secara eksplisit dibatasi pada konsistensi internal alur prototipe dalam parameter simulasi yang terdefinisi; generalisasi ke lingkungan produksi memerlukan tahapan lanjutan berupa *hardening* konfigurasi, kalibrasi ambang berbasis pola operasional nyata, konfigurasi daftar putih administratif, pengujian beban, dan penyelarasan kebijakan tata kelola. Untuk penelitian selanjutnya, disarankan integrasi teknik pembelajaran mesin atau analitik perilaku ke dalam saluran SIEM guna mendeteksi pola *low-and-slow* yang berpotensi melewati ambang berbasis frekuensi sederhana, dengan tetap memperhatikan metrik positif palsu dan keterjelasan model agar solusi dapat dipertanggungjawabkan dalam konteks institusi pemerintahan.

DAFTAR PUSTAKA

Alanda, A., Mooduto, H. A., & Hadi, R. (2023). Real-time defense against cyber threats: Analyzing Wazuh's effectiveness in server monitoring. *Journal of Information Technology and Computer Engineering*, *7*(2), 56–62. https://doi.org/10.25077/jitce.7.2.56-62.2023

Chamkar, S. A., Zaydi, M., Maleh, Y., & Gherabi, N. (2025). Improving threat detection in Wazuh using machine learning techniques. *Journal of Cybersecurity and Privacy*, *5*(2), Article 34. https://doi.org/10.3390/jcp5020034

Fahrnberger, G. (2022). Realtime risk monitoring of SSH brute force attacks. In *Communications in Computer and Information Science*. Springer International Publishing. pp. 75–95. https://doi.org/10.1007/978-3-031-06668-9_8

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), Article 4759. https://doi.org/10.3390/s21144759

Ismail, Kurnia, R., Widyatama, F., Wibawa, I. M., Brata, Z. A., Ukasyah, Nelistiani, G. A., & Kim, H. (2025). Enhancing security operations center: Wazuh security event response with retrieval-augmented-generation copilot. *Sensors*, *25*(3), Article 870. https://doi.org/10.3390/s25030870

Jalalvand, F., Baruwal Chhetri, M., Nepal, S., & Paris, C. (2024). Alert prioritisation in security operations centres: A systematic survey on criteria and methods. *ACM Computing Surveys*, *57*(2), 1–36. https://doi.org/10.1145/3695462

Khandait, P., Tiwari, N., & Hubballi, N. (2021). Who is trying to compromise your SSH server? An analysis of

authentication logs and detection of brute-force attacks. In *Adjunct proceedings of the 2021 International Conference on Distributed Computing and Networking* (pp. 127–132). Association for Computing Machinery. https://doi.org/10.1145/3427477.3429772

López Velásquez, J. M., Martínez Monterrubio, S. M., Sánchez Crespo, L. E., & Garcia Rosado, D. (2023). Systematic review of SIEM technology: SIEM-SC birth. *International Journal of Information Security*, *22*(3), 691–711. https://doi.org/10.1007/s10207-022-00657-9

MITRE ATT&CK. (n.d.). *Brute force (T1110)*. MITRE Corporation. Retrieved April 9, 2026, from https://attack.mitre.org/techniques/T1110/

Noor, Z., Hina, S., Hayat, F., & Shah, G. A. (2023). An intelligent context-aware threat detection and response model for smart cyber-physical systems. *Internet of Things*, *22*, Article 100843. https://doi.org/10.1016/j.iot.2023.100843

Park, J., Kim, J., Gupta, B. B., & Park, N. (2021). Network log-based SSH brute-force attack detection model. *Computers, Materials & Continua*, *68*(1), 887–901. https://doi.org/10.32604/cmc.2021.015172

Pitkar, H. (2025). Cloud security automation through symmetry: Threat detection and response. *Symmetry*, *17*(6), Article 859. https://doi.org/10.3390/sym17060859

Ruambo, F. A., Masanga, E. E., Lufyagila, B., Ateya, A. A., Abd El-Latif, A. A., Almousa, M., & Abd-El-Atty, B. (2025). Brute-force attack mitigation on remote access services via software-defined perimeter. *Scientific Reports*, *15*, Article 18599. https://doi.org/10.1038/s41598-025-01080-5

Singh, S. K., Gautam, S., Cartier, C., Patil, S., & Ricci, R. (2024). Where the wild things are: Brute-force SSH attacks in the wild and how to stop them. In *Proceedings of the 21st USENIX Symposium on Networked Systems Design and Implementation (NSDI '24)*. USENIX Association. https://www.usenix.org/system/files/nsdi24-singh-sachin.pdf

Skopik, F., Landauer, M., & Wurzenberger, M. (2022). Blind spots of security monitoring in enterprise infrastructures: A survey. *IEEE Security & Privacy*, *20*(6), 18–26. https://doi.org/10.1109/MSEC.2021.3133764

Suskalo, D., Moric, Z., Redzepagic, J., & Regvart, D. (2023). Comparative analysis of IBM QRadar and Wazuh for security information and event management. In *Proceedings of the 34th DAAAM International Symposium* (pp. 96–102). DAAAM International. https://doi.org/10.2507/34th.daaam.proceedings.014

Tiwari, N., & Hubballi, N. (2023). Secure socket shell bruteforce attack detection with Petri net modeling. *IEEE Transactions on Network and Service Management*, *20*(1), 697–710. https://doi.org/10.1109/TNSM.2022.3212591

Wazuh Team. (n.d.). *Wazuh documentation*. Wazuh. Retrieved April 9, 2026, from https://documentation.wazuh.com/current/

Winkler, A. M., & Sharma, P. (2025). Proactive threat detection in enterprise systems using Wazuh: A MITRE ATT&CK evaluation. *Computers & Security*, *159*, Article 104702.

https://doi.org/10.1016/j.cose.2025.104702