Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

Implementation of Suricata and Cyber Attack Analysis with SIEM for Attack Verification and Mitigation

Valentino Raffer*[1], Nelmiawati[2]

[1,2]Cyber Security Engineering, Batam State Polytechnic, Indonesia

Email: [1]valentino.4332001031@students.polibatam.ac.id

Abstract

The escalating complexity of cyber threats, encompassing web application exploitations, Denial-of-Service (DoS), and brute-force attacks, necessitates cloud infrastructures to deploy adaptive and automated defense mechanisms. Standalone conventional detection systems frequently fall short in delivering immediate responses to multi-vector attacks. This research aims to design and implement a robust Defense in Depth (DiD) security architecture that synergizes network visibility, application-level security, and automated incident response powered by Security Information and Event Management (SIEM). The experimental environment was constructed on a cloud server, utilizing the Damn Vulnerable Web Application (DVWA) as the evaluation target. The defensive framework integrates ModSecurity as a Web Application Firewall (WAF) at the application layer, Suricata as a Network Intrusion Detection System (NIDS) at the network layer, and Wazuh as the centralized SIEM orchestrator. Penetration testing was executed via Kali Linux, simulating critical attack vectors including DoS, authentication brute-force, and web-based injections (SQLi, XSS, and File Upload). The empirical results demonstrate the architecture's high efficacy in real-time threat detection and mitigation. ModSecurity instantaneously intercepted malicious application-layer payloads, while Wazuh successfully correlated logs from Suricata and ModSecurity to trigger its Active Response module. This automation seamlessly executed a full IP block via *iptables* upon reaching predefined threat thresholds. Ultimately, the integration of Wazuh, Suricata, and ModSecurity establishes a resilient Defense in Depth ecosystem, significantly minimizing incident response times and fortifying cloud server defenses without requiring manual administrative intervention.

Keywords : *Active Response, Cloud Security, Defense in Depth, ModSecurity, SIEM, Suricata, Wazuh.*

1. PENDAHULUAN

Seiring Transformasi digital mendorong banyak instansi dan perusahaan untuk mengandalkan infrastruktur internet dalam mempercepat arus komunikasi dan informasi. Meskipun demikian, adopsi teknologi yang masif ini berbanding lurus dengan eskalasi ancaman eksploitasi keamanan siber [1], [2]. Informasi rahasia perusahaan kini menjadi target eksploitasi oleh oknum tidak bertanggung jawab. Badan Siber dan Sandi Negara (BSSN) melaporkan tingginya tingkat insiden intrusi web, di mana serangan seperti *SQL Injection* (SQLi) dan *Cross-Site Scripting* (XSS) secara konsisten mendominasi statistik pelanggaran data (*data breaches*) [3]. Kerentanan pada aplikasi web umumnya diukur menggunakan standar *Open Web Application Security Project* (OWASP) *Top 10*, yang mengklasifikasikan celah keamanan paling kritis berdasarkan prevalensi, kemudahan eksploitasi, dan dampaknya [4], [5].

Dalam upaya memitigasi risiko tersebut, pemantauan jaringan yang berdiri sendiri tidak lagi memadai[6], [7]. Organisasi memerlukan sistem yang mampu memonitor aktivitas tingkat jaringan dan *host* secara terpadu[8]. *Intrusion Detection System* (IDS) seperti Suricata telah terbukti efektif dalam melakukan *deep packet inspection* dan mendeteksi anomali secara *real-time* [9], [10], [11]. Meskipun demikian, peringatan jaringan tanpa disertai konteks pada level sistem (log server) sering kali

P-ISSN: 2723-3863 https://jutif.if.unsoed.ac.id
E-ISSN: 2723-3871 DOI: https://doi.org/10.52436/1.jutif.6.6.3540

menyulitkan proses investigasi dan berpotensi menghasilkan tingkat peringatan palsu (*false positive*) yang tinggi [12], [13], [14].

Oleh karena itu, diperlukan integrasi log terpusat dan manajemen respons insiden menggunakan platform *Security Information and Event Management* (SIEM). Wazuh merupakan platform keamanan *open-source* yang memiliki kemampuan agregasi log tingkat lanjut [14], [15], *File Integrity Monitoring* (FIM), dan korelasi keamanan *endpoint*. Penelitian oleh Adrian (2026) [16] , Suryayusra (2026) [17] dan Dehan Pratama (2022) [18] mengonfirmasi bahwa penggabungan *Network Intrusion Detection System* (NIDS) Suricata dengan SIEM Wazuh mampu memberikan visibilitas keamanan berlapis (*multilayer architecture*). Log deteksi jaringan dari Suricata (berupa format eve.json) [19], [20] diteruskan kepada Wazuh Manager untuk dianalisis bersamaan dengan log sistem *web server*, sehingga administrator keamanan dapat melakukan triase insiden secara komprehensif.

Meskipun konsep integrasi SIEM telah banyak diteliti, masih terdapat kesenjangan implementasi deteksi hibrida pada lingkungan yang terkontainerisasi [21], serta minimnya pengujian komprehensif yang melibatkan kombinasi *Web Application Firewall* (WAF). Penelitian ini bertujuan untuk merancang, mengimplementasikan, dan mengevaluasi ekosistem *Defense in Depht Security* [22] dengan mengintegrasikan Wazuh SIEM, Suricata NIDS, dan ModSecurity WAF. Pengujian efektivitas arsitektur disimulasikan pada target *Damn Vulnerable Web App* (DVWA) menggunakan kerangka kerja OWASP [23]. Pengujian efektivitas deteksi disimulasikan menggunakan target *Damn Vulnerable Web App* (DVWA) dengan vektor serangan: *Brute Force, SQL Injection, File Upload, Cross-Site Scripting* (XSS), dan *Denial of Service* [5]. Integrasi teknologi ini diharapkan mampu menghasilkan sistem pemantauan yang tidak hanya tangguh dalam mendeteksi ancaman, tetapi juga mampu melakukan eskalasi mitigasi secara otomatis[24], [25].

2. STUDI LITERATUR

2.1. Vektor Serangan Aplikasi Web dan OWASP Top 10

Open Web Application Security Project (OWASP) adalah komunitas internasional yang secara berkala merilis dokumen *OWASP Top 10* [26], yaitu klasifikasi kerentanan aplikasi web paling kritis. Beberapa vektor serangan utama yang menjadi fokus mitigasi meliputi:

a. **SQL Injection (SQLi):** Teknik eksploitasi di mana penyerang menyisipkan perintah SQL berbahaya melalui input aplikasi untuk memanipulasi basis data di belakang (sisi peladen).
b. **Cross-Site Scripting (XSS):** Serangan injeksi berupa penyisipan skrip berbahaya (biasanya JavaScript) ke dalam halaman web yang dipercaya, yang kemudian dieksekusi oleh peramban pengguna lain.
c. **File Upload Vulnerability:** Eksploitasi yang terjadi ketika aplikasi web mengizinkan pengguna untuk mengunggah berkas tanpa validasi tipe, ukuran, atau konten yang memadai, memungkinkan penyusupan *malware* atau *web shell*.
d. **Denial of Service (DoS):** Upaya untuk menguras sumber daya komputasi atau jaringan pada server, sehingga layanan tidak dapat diakses oleh pengguna yang sah (*availability impact*).
e. **Brute-force Authentication:** Metode serangan berulang menggunakan metode *trial-and-error* (tebak-coba) secara otomatis untuk meretas kata sandi, kredensial login, atau kunci enkripsi.

2.2. Arsitektur *Defense in Depth*

Defense in Depth (DiD) merupakan strategi keamanan siber komprehensif yang mengadaptasi konsep pertahanan militer berlapis. Pendekatan ini dirancang sedemikian rupa sehingga apabila satu lapisan kendali keamanan berhasil ditembus oleh penyerang, lapisan perlindungan berikutnya akan mengintervensi untuk mencegah eskalasi eksploitasi [22]. Dalam konteks infrastruktur *cloud* dan aplikasi web, implementasi DiD modern mengombinasikan kontrol pada tingkat jaringan (*network-*

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

level), tingkat inang (*host-level*), dan tingkat aplikasi (*application-level*) secara terintegrasi untuk mendeteksi, menunda, dan merespons ancaman secara komprehensif.

2.3. *Security Information and Event Management* (SIEM) dan Wazuh

Security Information and Event Management (SIEM) adalah solusi keamanan yang memfasilitasi visibilitas menyeluruh terhadap infrastruktur TI melalui agregasi, normalisasi, dan korelasi log dari berbagai sumber secara *real-time*. Wazuh merupakan platform SIEM *open-source* tingkat lanjut yang mengintegrasikan kapabilitas *Extended Detection and Response* (XDR) [27]. Wazuh beroperasi menggunakan arsitektur *client-server*, di mana Wazuh Agent yang terpasang pada *endpoint* bertugas mengumpulkan metrik keamanan dan meneruskannya ke Wazuh Manager [28]. Salah satu keunggulan utama Wazuh adalah fitur *Active Response*, yang memungkinkan sistem untuk mengeksekusi skrip mitigasi otomatis (seperti modifikasi *iptables* untuk memblokir alamat IP) segera setelah *rule engine* mendeteksi anomali yang melampaui ambang batas keamanan [28].

2.4. *Network Intrusion Detection System (NIDS) Suricata*

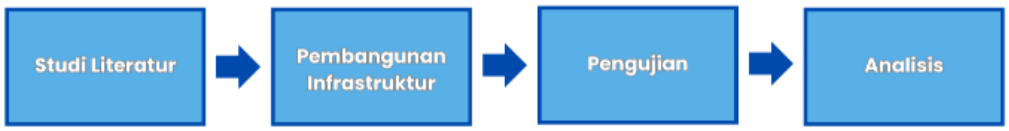
Suricata adalah *Network Intrusion Detection System* (NIDS) berkinerja tinggi yang berbasis sumber terbuka dan dikembangkan oleh Open Information Security Foundation (OISF) [29]. Sistem ini menggunakan metode *deep packet inspection* dan pencocokan tanda tangan (*signature-based matching*) untuk mengidentifikasi anomali pada lalu lintas jaringan. Berbeda dengan IDS konvensional, Suricata mendukung pemrosesan *multi-threading* [30] dan mampu menghasilkan *output* log terstruktur dalam format JSON (eve.json) [13], [19]. Format log standar ini sangat krusial untuk memudahkan proses integrasi (*parsing*) dan analisis lanjutan saat log diteruskan ke dalam mesin korelasi SIEM.

2.5. *Web Application Firewall* (WAF) ModSecurity

ModSecurity adalah *Web Application Firewall* (WAF) yang dirancang secara khusus untuk melindungi aplikasi web dari serangan tingkat lapisan aplikasi (Layer 7 OSI), seperti *SQL Injection, Cross-Site Scripting* (XSS), dan yang lainnya [31]. ModSecurity bekerja dengan cara mencegat lalu lintas HTTP/HTTPS dan menganalisis *header* serta *payload* dari setiap permintaan (kueri) sebelum diteruskan ke *web server* (*reverse proxy*). Efektivitas deteksi ModSecurity umumnya didukung oleh integrasi *OWASP ModSecurity Core Rule Set* (CRS), yang memberikan mekanisme penilaian anomali (*anomaly scoring*) [32]. Kueri yang menghasilkan skor anomali di atas ambang batas yang diizinkan akan secara otomatis ditolak, dan sistem akan mengembalikan status galat HTTP 403 (*Access Denied*) [33].

3. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimental dengan merancang infrastruktur cloud terisolasi guna memvalidasi kemampuan deteksi dan respons otomatis dari arsitektur keamanan yang diusulkan.



Gambar 1. Tahapan Penelitian

3.1. Studi Literatur

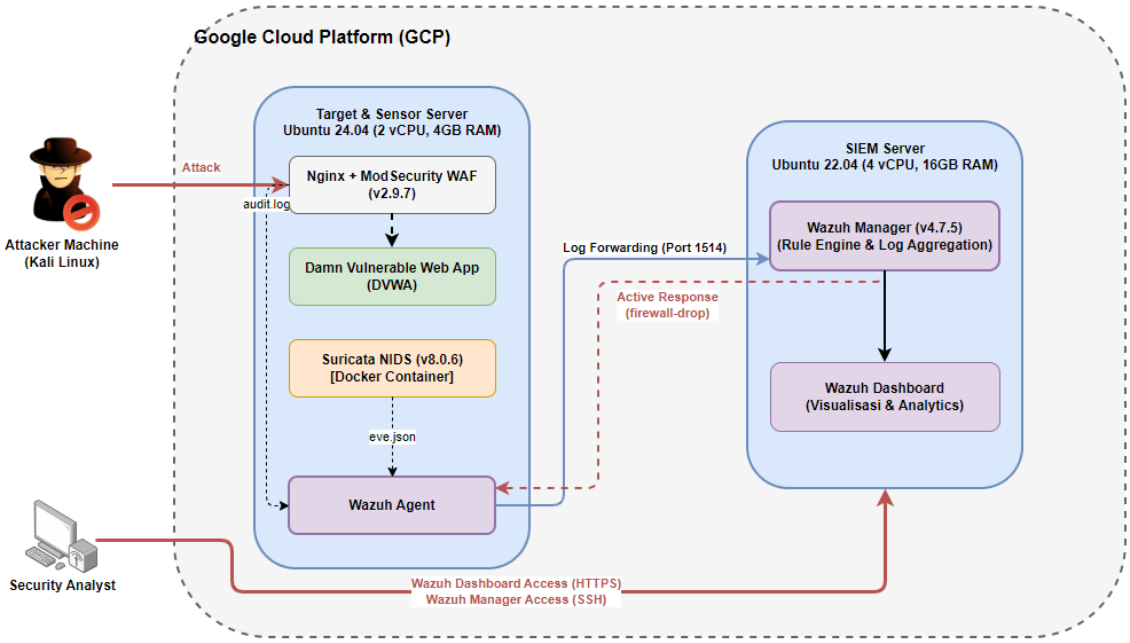
Pada tahapan ini, data dan informasi teknis terkait Wazuh SIEM, Suricata, dan ModSecurity dikumpulkan. Studi ini mengakumulasi referensi dari jurnal akademik, dokumentasi resmi sistem, serta pedoman keamanan standar industri guna menyusun kerangka kerja arsitektur pengujian.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

3.2. Pembangunan Infrastruktur

Pembangunan infrastruktur dilakukan menggunakan *Damn Vulnerable Web Application* (DVWA) sebagai *environment* target serangan dan ModSecurity sebagai *Web Application Firewall* (WAF). Infrastruktur ini dideploy di atas arsitektur *cloud* yang terdiri dari dua mesin utama:

- Target & Sensor Server: Server Linux yang menjalankan *stack* keamanan yang meliputi ModSecurity, Suricata, aplikasi web DVWA, dan Wazuh Agent.
- SIEM Server: Server independen yang menjalankan Wazuh Manager sebagai mesin korelasi log (*rule engine*) dan dasbor analitik keamanan.

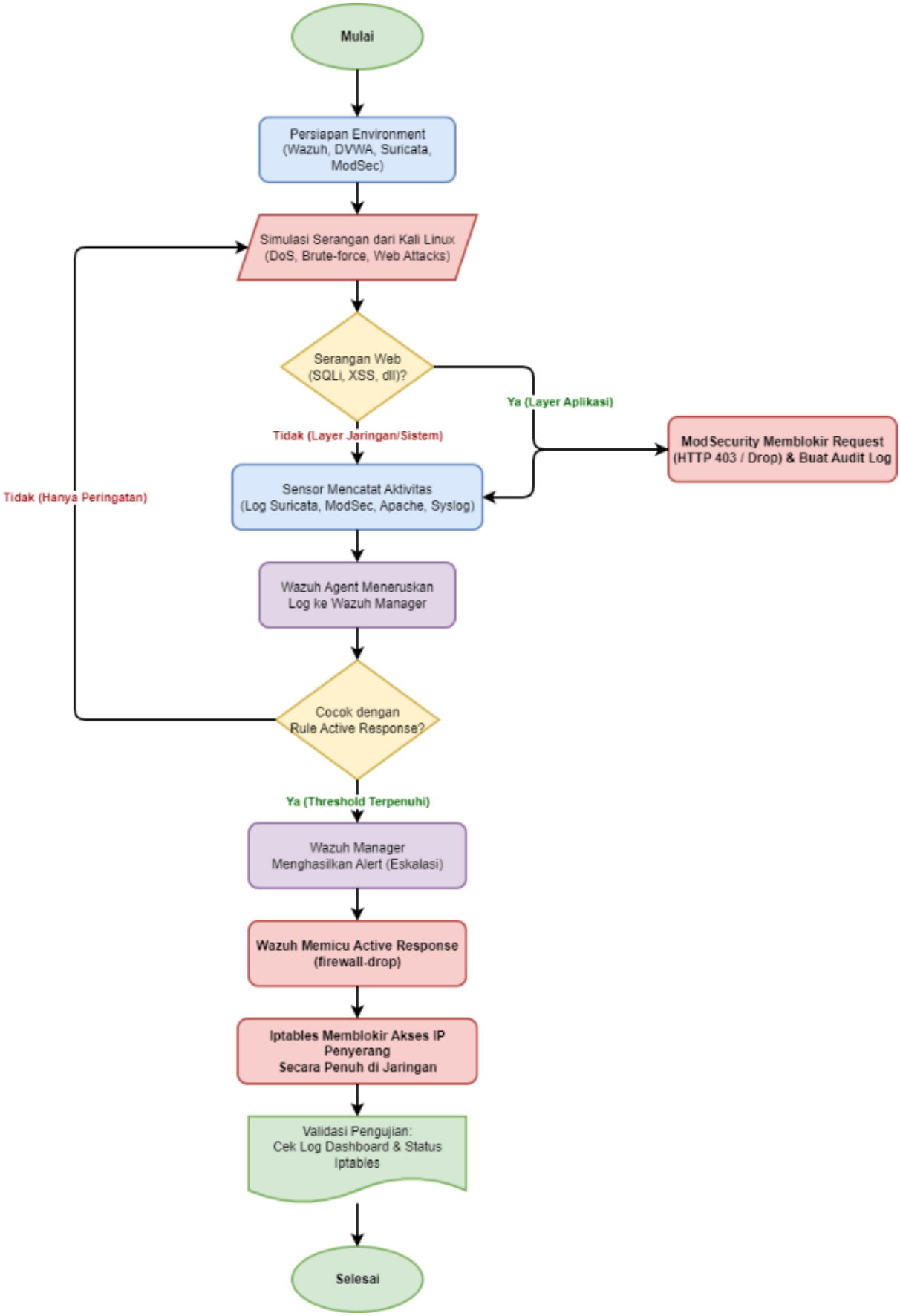


Gambar 2. Topologi Infrastruktur

3.3. Pengujian

Pengujian penetrasi diorkestrasikan dari mesin penyerang berbasis Kali Linux untuk meluncurkan berbagai vektor serangan (seperti DoS, eksploitasi web, dan *brute-force*) ke server DVWA. Data log hasil serangan dievaluasi untuk mengonfirmasi keberhasilan deteksi pada lapisan sensor, serta memastikan berjalannya mekanisme mitigasi (*Active Response* atau penolakan kueri WAF) sesuai dengan parameter *threshold* keamanan yang telah dikonfigurasi.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540



Gambar 3. Metode Pengujian

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

3.4. Analisis

Analisis komprehensif terhadap serangkaian pengujian membuktikan bahwa arsitektur keamanan *Defense in Depth* yang diterapkan mampu memberikan perlindungan secara *real-time* lintas vektor serangan. Sistem pertahanan terintegrasi ini tidak beroperasi secara pasif yang sekadar melakukan pencatatan (*logging*), melainkan mengeksekusi intervensi aktif sepersekian detik sebelum muatan berbahaya berhasil mengeksploitasi celah aplikasi target.

Pada pengujian eksploitasi kerentanan aplikasi web, visibilitas keamanan sistem terekam secara sangat presisi. Sebagai contoh, saat serangan *SQL Injection* diluncurkan, Suricata mendeteksi anomali lalu lintas HTTP pada pukul 23:07:31. Hanya dalam hitungan milidetik kemudian (23:07:31.088), ModSecurity mengambil alih peran mitigasi instan dengan menolak kueri (*Rejected a query*) dan mengembalikan status HTTP 403 *Access Denied*. Pemblokiran ini secara spesifik dipicu karena terlampauinya batas skor anomali lalu lintas jaringan (*Inbound Anomaly Score Exceeded*). Pola deteksi serupa juga terlihat pada ancaman *Cross-Site Scripting* (XSS) yang memicu peringatan "*XSS attempt*" dari Wazuh pada pukul 23:03:20. Pola pertahanan berlapis ini terbukti konsisten pada pengujian celah keamanan *File Upload*, di mana ModSecurity menolak muatan berbahaya melalui metode permintaan POST ke *endpoint* /DVWA/vulnerabilities/upload/ pada pukul 23:24:29.

Lebih jauh, sistem terbukti tangguh dalam menghadapi serangan yang menargetkan ketersediaan (*availability*) dan autentikasi. Pada simulasi serangan volumetrik berupa *Denial of Service* (DoS), dasbor Wazuh secara akurat merekam lonjakan lalu lintas yang mencapai 1.092 ketukan (*hits*). Analisis log menunjukkan bahwa ModSecurity tidak hanya memblokir kueri, tetapi sistem korelasi juga berhasil mengenali pola persisten dengan menghasilkan peringatan tingkat tinggi (*Rule Level 12*): "*Same IP Triggering Modsecurity Block 5 times within 10 minutes*" pada pukul 23:11:06.

Selanjutnya, efektivitas sistem respons otomatis diuji melalui serangan *Brute-force* menggunakan perangkat lunak Hydra untuk mengeksploitasi parameter autentikasi melalui HTTP GET. Berdasarkan log, penyerang memulai eksekusi perangkat Hydra pada pukul 23:19:10. Keunggulan mekanisme *real-time* dari Wazuh SIEM terbukti saat sistem memicu fitur *Active Response* dan mengeksekusi perintah *firewall-drop* pada pukul 23:19:14. Waktu respons (*response time*) yang hanya memakan waktu 4 detik tersebut seketika memblokir alamat IP sumber penyerang (36.69.81.173), sehingga seluruh akses peretas ke dalam infrastruktur terputus secara seketika.

Tabel 1. Hasil Log Deteksi dan Mitigasi Sistem Keamanan Terintegrasi

Waktu Kejadian	Jenis Serangan	Deskripsi Aturan	Eksekusi Mitigasi	Alamat Penyerang
Jul 12, 2026 @ 23:03:20	Cross-Site Scripting (XSS)	XSS (Cross Site Scripting) attempt (Level 6)	WAF Block (HTTP 403)	36.69.81.173
Jul 12, 2026 @ 23:07:31	SQL Injection (SQLi)	Suricata HTTP Traffic (Level 3) / ModSecurity: Rejected a query (Level 7)	WAF Block (HTTP 403)	36.69.81.173
Jul 12, 2026 @ 23:11:06	Denial of Service (DoS)	Same IP Triggering Modsecurity Block 5 times within 10 minutes (Level 12)	Penolakan lalu lintas massal	36.69.81.173
Jul 12, 2026 @ 23:19:14	Brute-force Authentication	Host Blocked by firewall-drop Active Response (Level 3)	Eksekusi Iptables (Blokir Penuh)	36.69.81.173
Jul 12, 2026 @ 23:24:29	File Upload Vulnerability	ModSecurity: Rejected a query (Level 7)	WAF Block (HTTP 403)	36.69.81.173

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

4. HASIL DAN PEMBAHASAN

Bagian ini memaparkan hasil evaluasi dari pengujian penetrasi terhadap arsitektur keamanan terintegrasi, yang difokuskan pada kemampuan sistem dalam mendeteksi dan memitigasi berbagai vektor serangan secara *real-time*. Sistem pertahanan yang diusulkan tidak sekadar beroperasi secara pasif (pencatatan log), melainkan melakukan intervensi aktif untuk memblokir muatan berbahaya sebelum berhasil mengeksploitasi aplikasi target.

4.1. Metode Ekstraksi dan Analisis Log

Untuk menjabarkan hasil mitigasi secara komprehensif, proses pemantauan dan analisis log dilakukan terpusat melalui antarmuka Wazuh Dashboard yang ditenagai oleh mesin pencari OpenSearch. Seluruh aktivitas jaringan dan sistem termasuk tangkapan *rule* dari sensor Suricata dan ModSecurity—diagregasi oleh Wazuh Agent dan diteruskan ke Wazuh Manager melalui *port* 1514. Penarikan data (*querying*) difokuskan pada indeks wazuh-alerts-* dengan menetapkan filter parameter agen target (contohnya, agent.name: "dvwa-testing"). Selain itu, filter rentang waktu absolut (*absolute time*) disinkronkan secara presisi dengan waktu peluncuran serangan dari mesin peretas (Kali Linux). Pendekatan ini memungkinkan ekstraksi *field* spesifik seperti rule.description, rule.level, data.srcip, dan timestamp untuk memvalidasi akurasi deteksi serta mengukur kecepatan *response time* dari sistem mitigasi.

4.2. Analisis Mitigasi Vektor Serangan

Agar Pada pengujian eksploitasi kerentanan aplikasi web khususnya *SQL Injection* (SQLi), *Cross-Site Scripting* (XSS), dan *File Upload* sistem menunjukkan kapabilitas pertahanan berlapis yang proaktif. Dalam simulasi SQLi dan XSS, anomali tersebut terdeteksi secara langsung dan bersamaan oleh sensor Suricata dan Wazuh. Dalam hitungan detik, ModSecurity mengambil alih peran mitigasi instan dengan mencegat kueri berbahaya tersebut dan mengembalikan status HTTP 403 (*Access Denied*). Pemblokiran ini terpicu akibat terlampauinya batas skor anomali (*Inbound Anomaly Score Exceeded*). Pola pertahanan yang sama terbukti efektif pada celah *File Upload*; saat penyerang mengirimkan muatan berbahaya melalui permintaan HTTP POST ke *endpoint* /DVWA/vulnerabilities/upload/, ModSecurity langsung menolak akses tersebut, yang rekam jejaknya juga terdeteksi secara paralel oleh lalu lintas HTTP Suricata.

Selanjutnya, ketangguhan sistem diuji terhadap serangan yang mengancam ketersediaan dan autentikasi. Pada simulasi ancaman volumetrik berupa *Denial of Service* (DoS), Dasbor Wazuh mencatat lonjakan lalu lintas ekstrem hingga 1.092 ketukan (*hits*). ModSecurity merespons anomali ini secara akurat dengan menolak kueri secara massal, di mana log mengidentifikasi bahwa alamat IP penyerang yang sama telah memicu lima kali pemblokiran dalam rentang waktu sepuluh menit. Di sisi lain, serangan autentikasi *brute-force* yang disimulasikan menggunakan perangkat lunak Hydra (dengan menguji ratusan ribu kombinasi kata sandi terhadap *host* target 136.66.102.115) berhasil dikenali pola persistennya oleh SIEM. Sebagai respons, Wazuh secara otomatis memicu fitur *Active Response* dan mengeksekusi perintah *firewall-drop*. Eksekusi ini langsung memblokir alamat IP penyerang (36.69.81.173), sehingga seluruh akses peretas ke dalam infrastruktur terputus seketika (*real-time*).

Ringkasan keberhasilan deteksi dan mitigasi terhadap kelima vektor serangan tersebut dapat dilihat pada Tabel 2 berikut.

Tabel 2. Hasil Analisis Pengujian

No	Jenis Serangan	Sensor Deteksi	Aksi Mitigasi (*Blocking*)	Status Pengujian
1	*SQL Injection*	Suricata, Wazuh	Diblokir oleh ModSecurity	Berhasil

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

			(HTTP 403 *Access Denied*)	
2	*Cross-Site Scripting* (XSS)	Suricata, Wazuh	Diblokir oleh ModSecurity (HTTP 403 *Access Denied*)	Berhasil
3	*Denial of Service* (DoS)	Suricata, Wazuh	Diblokir oleh ModSecurity (Penolakan kueri otomatis)	Berhasil
4	*Brute-force Attack*	Wazuh	Diblokir oleh Wazuh (*Active Response* / *firewall-drop*)	Berhasil
5	*File Upload Vulnerability*	Suricata, Wazuh	Diblokir oleh ModSecurity (HTTP 403 *Access Denied*)	Berhasil

4.3. Perbandingan dengan Studi Terdahulu

Keberhasilan arsitektur keamanan terintegrasi pada penelitian ini sejalan dengan temuan sejumlah studi terdahulu yang mengevaluasi efektivitas SIEM dan *Web Application Firewall* (WAF). Sebagai contoh, penelitian Zaidan M [34] mengonfirmasi bahwa integrasi kolaboratif agen Wazuh dan ModSecurity sangat andal dalam memitigasi *SQL Injection*—khususnya varian *Time-Based* dan *Error-Based*—jika dibandingkan dengan WAF NAXSI. Kapabilitas respons instan ini juga diperkuat oleh riset Younus Z [35], yang membuktikan efektivitas metode berbasis SIEM (penggabungan Wazuh, fungsionalitas IDS, dan *File Integrity Monitoring*) dalam menangkal serangan DoS dan modifikasi berkas tanpa jeda waktu.

Sebagai perbandingan terhadap pengembangan teknologi di masa depan, penelitian Dawadi B [36] mengusulkan arsitektur WAF berlapis menggunakan pemodelan *Deep Learning* (LSTM) yang mampu mendeteksi serangan DDoS dengan akurasi 97,57%, serta XSS dan SQLi dengan akurasi 89,34%. Meskipun pendekatan *machine learning* tersebut menawarkan pengukuran metrik akurasi yang spesifik, arsitektur *Defense in Depth* deterministik yang diusulkan dalam penelitian ini terbukti telah mampu secara independen memberikan tingkat pemblokiran instan yang memadai dan komprehensif terhadap vektor-vektor ancaman serupa di lingkungan produksi.

5. KESIMPULAN DAN SARAN

Penerapan arsitektur yang mengintegrasikan Wazuh SIEM, Suricata, dan ModSecurity telah terbukti berhasil membangun ekosistem keamanan *Defense in Depth* yang tangguh dan adaptif. Sistem ini secara konsisten mampu mengidentifikasi aktivitas anomali pada multi-lapisan (jaringan dan aplikasi), serta secara langsung mengonversi temuan tersebut menjadi tindakan mitigasi berupa pemblokiran otomatis tanpa memerlukan intervensi manual dari administrator keamanan.

Meskipun pengujian menunjukkan tingkat efektivitas yang sangat tinggi dalam mendeteksi dan mencegah serangan terhadap infrastruktur web publik, sistem keamanan ini masih memiliki keterbatasan dalam menghadapi ancaman *zero-day exploit* maupun kerentanan *Common Vulnerabilities and Exposures* (CVE) yang baru dipublikasikan. Sebagai saran pengembangan, penelitian di masa mendatang dapat memperluas cakupan sistem dengan mengintegrasikan umpan *Threat Intelligence* guna mengenali indikator serangan mutakhir secara proaktif. Selain itu, penambahan modul peringatan dini terintegrasi melalui *email* atau platform komunikasi lainnya sangat direkomendasikan agar administrator keamanan dapat menerima notifikasi eskalasi insiden secara *real-time*.

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

REFERENSI

[1] Ismail Setiawan, R. Surya Kusuma, T. Muhammad Fadhil, dan I. Nafisah Miftahul Jannah, "PENINGKATAN KAPASITAS MAHASISWA DALAM BIDANG AI DAN KEAMANAN SIBER UNTUK MENCEGAH ANCAMAN DI DUNIA DIGITAL," *Empowerment Journal*, vol. 5, no. 2, hlm. 101–108, Sep 2025, doi: 10.30787/empowerment.v5i2.2121.

[2] K. M. Rajasekharaiah, C. S. Dule, dan E. Sudarshan, "Cyber Security Challenges and its Emerging Trends on Latest Technologies," dalam *IOP Conference Series: Materials Science and Engineering*, IOP Publishing Ltd, 2020. doi: 10.1088/1757-899X/981/2/022062.

[3] Z. Imaddudin, "RANCANG BANGUN APLIKASI HTTP OBSERVATORY DAN WEB VULNERABILITY SCANNER UNTUK ANALISIS KEAMANAN WEBSITE," Universitas Mercu Buana-Menteng, 2025.

[4] F. P. E. Putra, U. Ubaidi, A. Hamzah, W. A. Pramadi, dan A. Nuraini, "Systematic Literature Review: Security Gap Detection On Websites Using Owasp Zap," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, hlm. 348–355, Jul 2024, doi: 10.47709/brilliance.v4i1.4227.

[5] F. H. Harahap, J. A. Sutanto, W. Abraham, P. Adrianus, dan D. A. Junaidi, "ANALISIS CELAH KEAMANAN APLIKASI E-COMMERCE XYZ MENGGUNAKAN METODE PENETRATION TESTING," 2025. [Daring]. Tersedia pada: https://owasp.org/www-project-top-ten/.

[6] M. Amin, M. Hasbi, B. Widada, dan B. W. Yudanto, "IMPLEMENTASI MONITORING JARINGAN INTERNET PADA MIKROTIK MENGGUNAKAN NOTIFIKASI BOT TELEGRAM DI SMK," *Jurnal Teknologi Informasi dan Komunikasi (TIKomSiN)*, vol. 13, no. 1, hlm. 67, Agu 2025, doi: 10.30646/tikomsin.v13i1.997.

[7] M. Yusuf Fardiansyah, dan Aryo Nugroho, S. Informasi, F. Ilmu Komputer, dan U. Narotama Jl Arief Rahman Hakim No, "OPTIMASI JARINGAN INTERNET MENGGUNAKAN KOMBINASI LOAD BALANCING DAN QUEUE PADA ROUTER MIKROTIK", doi: 10.26623/elektrika.

[8] A. Rahma, F. Indriyani, T. Alfian, dan A. Sandi, "Perancangan Dan Implementasi Monitoring Perangkat Server Menggunakan Zabbix Pada PT. Rizki Tujuh Belas Kelola," *Jurnal INSAN (Journal of Information Systems Management Innovation*, vol. 3, no. 2, 2023, [Daring]. Tersedia pada: http://jurnal.bsi.ac.id/index.php/jinsan

[9] O. Rivaldi dan N. L. Marpaung, "Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata," vol. 8, no. 1, hlm. 2023.

[10] M. R. Alim, R. N. Sarbini, dan I. Kurniasari, "Implementasi Intrusion Prevention System Suricata sebagai Pengamanan dari Serangan DoS dan DDoS," *Portal Riset dan Inovasi Sistem Perangkat Lunak*, vol. 2, no. 2, hlm. 91–96, Apr 2024, doi: 10.59696/prinsip.v2i2.113.

[11] M. Surakarta, J. A. Yani, dan J. Tengah, "DETEKSI AKTIVITAS MALWARE AKIBAT SOFTWARE PIRACY DENGAN MENGGUNAKAN SURICATA BERBASIS NETWORK BASED INTRUSION PREVENTION SYSTEM 'Azizil'an Sarina Putra[1] , Bana Handaga[2]."

[12] Nikhil, "Real-Time Threat Detection: Suricata Log Analysis and Visualization for Network MSc Research Project Master of Science in Cyber Security Nikhil Nikhil," Agu 2024.

[13] Juhari, Nuralamsah Zulkarnaim, Muh Rafli Rasyid, dan Andi M. Yusuf, "Random Forest Implementation for Suricata-Based Real-Time DDoS Attack Detection," *Journal of Embedded*

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

Systems, Security and Intelligent Systems, hlm. 119–132, Jun 2025, doi: 10.59562/jessi.v6i2.8339.

[14] N. Hidayasari, Mansur, Kasmawi, dan Z. Efendi, "Implementasi Prototipe SIEM Berbasis Wazuh pada Website dengan Pengujian FIM dan Threat Hunting," *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 4, hlm. 372–382, Des 2025, doi: 10.62527/jitsi.6.4.523.

[15] S. ardy Nuswantoro, M. Ziaurrahman, M. Miftahurrizqi, M. Achiril Haq, dan R. A. Rashid, "Implementasi Wazuh-ELK-Suricata untuk Deteksi Privilege Escalation di Ubuntu Server," *Jurnal SAINTEKOM*, vol. 15, no. 2, hlm. 153–164, Sep 2025, doi: 10.33020/saintekom.v15i2.941.

[16] A. Z. A. Adrian, R. A. Megantara, dan F. Al Zami, "Hybrid Multilayer Architecture Integrating Suricata, Wazuh, and Cyber Threat Intelligence for Drive-by-Download Malvertising Detection," *sinkron*, vol. 10, no. 1, hlm. 161–168, Jan 2026, doi: 10.33395/sinkron.v10i1.15616.

[17] Suryayusra, "Integrasi Wazuh File Integrity Monitoring Dan Suricata Dengan Notifikasi Telegram Untuk Keamanan Jaringan," *Jurnal Ilmiah MATRIK*, Mei 2026.

[18] M. Dehan Pratama, F. Nova, dan D. Prayama, "Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos." [Daring]. Tersedia pada: http://jurnal-itsi.org

[19] G. Munn, K. C. Nwosu, dan M. Abdulgader, "Design and Integration of Intelligent Agents for Automated Threat Intelligence in Suricata-Based Intrusion Detection Systems," dalam *2025 International Conference on Computer and Applications (ICCA)*, 2025, hlm. 1–11. doi: 10.1109/ICCA66035.2025.11430927.

[20] Juhari, Nuralamsah Zulkarnaim, Muh Rafli Rasyid, dan Andi M. Yusuf, "Random Forest Implementation for Suricata-Based Real-Time DDoS Attack Detection," *Journal of Embedded Systems, Security and Intelligent Systems*, hlm. 119–132, Jun 2025, doi: 10.59562/jessi.v6i2.8339.

[21] A. Bonifasius Simbolon, D. Kiswanto, D. Siregar, dan A. Shaleh Lbn Gaol, "RANCANG BANGUN SISTEM ANALISIS LOG JARINGAN BERBASIS WEB UNTUK DETEKSI REAL-TIME ANCAMAN CANGGIH DAN GERAKAN LATERAL," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 14, no. 1, Jan 2026, doi: 10.23960/jitet.v14i1.8219.

[22] S. Kumar Jangam dan P. Sarathi Reddy Pedda Muntala, "Comprehensive Defense-in-Depth Strategy for Enterprise Application Security," *Golden Sun-Rise International Journal of Multidisciplinary on Science and Management*, vol. 1, hlm. 3048–5037, doi: 10.71141/30485037/V1I3P106.

[23] R. Abdullah dan F. Fachri, "Mitigasi Keamanan Webserver Sistem Informasi Akademik terhadap Serangan Brute Force Menggunakan Penetration Testing," *remik*, vol. 9, no. 3, hlm. 885–896, Agu 2025, doi: 10.33395/remik.v9i3.15104.

[24] A. P. Paramaputra, G. M. Suranegara, dan E. Setyowati, "MITIGATION OF MULTI TARGET DENIAL OF SERVICE (DOS) ATTACKS USING WAZUH ACTIVE RESPONSE," *Journal of Computer Networks, Architecture and High Performance Computing*, vol. 7, no. 2, hlm. 483–493, Apr 2025, doi: 10.47709/cnahpc.v7i2.5755.

[25] A. Al Siam, M. M. Hassan, A. K. M. Masum, dan T. Bhuiyan, "Automating Malware Detection and Response via Real-Time Threat Feed Integration with Wazuh SIEM," dalam

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS), 2025, hlm. 1–6. doi: 10.1109/COMPAS67506.2025.11381876.

[26] E. Nurelasari dan D. G. Al Farabi, "Analisis Keamanan Sistem Website Menggunakan Metode Open Web Application Security Project (Owasp) Pada Simantep. Id," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 3, hlm. 3049–3054, 2024.

[27] H. A. Damanik, M. Anggraeni, dan others, "Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Active Response (XDR) Wazuh dan Suricata," *Jurnal Pekommas*, vol. 9, no. 2, hlm. 309–322, 2024.

[28] J. R. Nandaputra, P. Sukarno, dan A. A. Wardana, "Detection and prevention system on computer network to handle distributed denial-of-service (ddos) attack in realtime and multi-agent," dalam *Proceedings of the 2024 10th International Conference on Computer Technology Applications*, 2024, hlm. 237–241.

[29] M. R. Alim, R. N. Sarbini, dan I. Kurniasari, "Implementasi Intrusion Prevention System Suricata sebagai Pengamanan dari Serangan DoS dan DDoS: Studi Kasus pada Jaringan Laboratorium SMK PGRI Kras," *Portal Riset dan Inovasi Sistem Perangkat Lunak*, vol. 2, no. 2, hlm. 91–96, 2024.

[30] F. V Niskov, E. A. Kutovoy, dan S. F. Kurmangaleev, "Enhanced s2e for analysis of multi-thread software," *Programming and Computer Software*, vol. 49, no. Suppl 1, hlm. S39–S44, 2023.

[31] D. I. Pratama dan others, "TINDAKAN PENCEGAHAN ANCAMAN WEB MELALUI PENDEKATAN TEKNIK WEB APPLICATION FIREWALL MENGGUNAKAN MODSECURITY," 2024.

[32] C. Scano *dkk.*, "Modsec-learn: Boosting modsecurity with machine learning," dalam *International Symposium on Distributed Computing and Artificial Intelligence*, 2024, hlm. 23–33.

[33] N. A. Widiyono dan U. Y. Oktiawati, "Implementasi Web Application Firewall (WAF) pada Aplikasi Fishku Berbasis Google Cloud Armor," *Journal of Internet and Software Engineering*, vol. 5, no. 2, 2024.

[34] M. N. Zaidan, P. Sukarno, dan A. A. Wardana, "Collaborative Detection of SQL Injection Attacks using SIEM, Multi-Wazuh Agents, and Diverse Web Application Firewalls," dalam *2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*, 2024, hlm. 1–6. doi: 10.1109/CIEES62939.2024.10811420.

[35] Z. S. Younus dan M. Alanezi, "Detect and Mitigate Cyberattacks Using SIEM," dalam *2023 16th International Conference on Developments in eSystems Engineering (DeSE)*, 2023, hlm. 510–515. doi: 10.1109/DeSE60595.2023.10469387.

[36] B. R. Dawadi, B. Adhikari, dan D. K. Srivastava, "Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks †," *Sensors*, vol. 23, no. 4, Feb 2023, doi: 10.3390/s23042073.