Jurnal Riset Informatika dan Teknologi Informasi (JRITI)
Jejaring Penelitian dan Pengabdian Masyarakat (JPPM)
Vol. 4, No. 1, Agustus – November 2026, Hal. 399 - 406
Web : https://ejurnal.jejaringppm.org/index.php/jriti

ISSN (Print) : 3024-8167
e-ISSN : 3109-8959

Mitigasi Ancaman Siber pada Aplikasi Web Melalui SIEM: Tinjauan Literatur Sistematis

Muhammad Nabel[1], Felix Enrique[2], Ahmad Muhammad Taqy[3], Yehezkiel Nesta[4], dan Arief Afriandi[5]

Universitas Negeri Semarang[1,2,3,4,5]
Email : muhammadnabel70@students.unnes.ac.id, felixenrique@students.unnes.ac.id, amta02@students.unnes.ac.id, yehezkieln85@students.unnes.ac.id, arfriandi@mail.unnes.ac.id

ABSTRAK

Aplikasi web telah menjadi tulang punggung ekosistem digital modern, namun keterbukaannya menjadikan platform ini target utama serangan siber yang sering kali gagal dideteksi oleh mekanisme pertahanan konvensional. Artikel ini menyajikan tinjauan literatur sistematis (*Systematic Literature Review*) terhadap 13 publikasi terpilih dari database Scopus periode 2020-2025 untuk menganalisis efektivitas *Security Information and Event Management* (SIEM) dalam memitigasi ancaman pada aplikasi web. Hasil kajian mengidentifikasi kategori serangan dominan yang meliputi *SQL Injection* (SQLi), *Cross-Site Scripting* (XSS), dan serangan *Denial of Service* (DoS) lapisan aplikasi. Penelitian menunjukkan bahwa pendekatan hibrida yang mengintegrasikan SIEM dengan *Web Application Firewall* (WAF) serta penerapan algoritma *Machine Learning* terbukti mampu mendeteksi anomali serangan *zero-day* dengan tingkat akurasi mencapai 97% hingga 100%. Selain itu, penggunaan platform *open-source* seperti Wazuh dan ELK Stack memungkinkan pemantauan visibilitas keamanan secara terpusat dan pengurangan waktu respons insiden secara signifikan. Artikel ini merekomendasikan adopsi arsitektur keamanan terintegrasi yang menggabungkan analisis log berbasis aturan dan perilaku untuk meminimalkan tingkat peringatan palsu dan membangun pertahanan web yang adaptif.

Kata Kunci: *Keamanan Siber, , SIEM, Deteksi Anomali, Tinjauan Literatur*

ABSTRACT

Web applications have become the backbone of the modern digital ecosystem, yet their openness makes them primary targets for cyberattacks that conventional defense mechanisms often fail to detect. This article presents a systematic literature review of 13 selected publications from the Scopus database from the 2020-2025 period to analyze the effectiveness of Security Information and Event Management (SIEM) in mitigating threats to web applications. The review identifies dominant attack categories including SQL Injection (SQLi), Cross-Site Scripting (XSS), and application-layer Denial of Service (DoS) attacks. Research demonstrates that a hybrid approach integrating SIEM with Web Application Firewalls (WAF) and the application of Machine Learning algorithms is proven to detect zero-day attack anomalies with accuracy rates reaching 97% to 100%. Furthermore, the use of open-source platforms such as Wazuh and ELK Stack enables centralized security visibility monitoring and significant reduction in incident response times. This article recommends the adoption of an integrated security architecture combining rule-based and behavioral log analysis to minimize false positive rates and build robust, adaptive web defenses.

Keywords: *Cybersecurity, Web Application, SIEM, Anomaly Detection, Systematic Literature Review.*

Penulis Korespondensi
Muhammad Nabel

Tanggal Submit : 12/12/2025
Tanggal Diterima : 05/11/2026
Tanggal Terbit : 10/11/2026

This is an open access article under the CC–BY-NC-SA license

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 (CC BY-NC-SA 4.0) International License (https://creativecommons.org/licenses/by-nc-sa/4.0/).

Publisher's Note: JPPM stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

I. PENDAHULUAN

Dalam era transformasi digital saat ini, aplikasi web telah menjadi infrastruktur kritikal bagi operasional bisnis dan layanan publik. Namun, aksesibilitas yang luas menjadikan aplikasi web sebagai entitas yang paling sering ditargetkan dalam ekosistem siber. Laporan keamanan global menunjukkan bahwa serangan terhadap lapisan aplikasi (*Application Layer*) terus meningkat, baik dari segi frekuensi maupun kecanggihan teknik yang digunakan. Organisasi modern kini dihadapkan pada tantangan untuk menjaga ketersediaan layanan di tengah ancaman yang dinamis, di mana metode pertahanan konvensional sering kali tidak lagi memadai untuk membendung serangan yang terkoordinasi [1].

Mekanisme pertahanan tradisional yang mengandalkan *firewall* jaringan dan sistem deteksi intrusi berbasis tanda tangan (*signature-based*) memiliki keterbatasan fundamental dalam melindungi lingkungan web. Perangkat keamanan ini sering kali bekerja secara terisolasi (*siloed*), sehingga gagal memberikan konteks yang utuh mengenai sebuah insiden. Akibatnya, tim keamanan sering mengalami kesulitan dalam membedakan antara lalu lintas pengguna yang sah dengan aktivitas berbahaya yang menyamar, seperti serangan *Distributed Denial of Service* (DDoS) pada lapisan aplikasi yang dirancang untuk melumpuhkan logika bisnis tanpa memicu peringatan pada pemantauan volume jaringan biasa [2]. Selain itu, tingginya volume peringatan palsu (*false positive*) yang dihasilkan oleh alat deteksi konvensional sering menyebabkan kelelahan pada analis keamanan (*alert fatigue*), yang berdampak pada lambatnya respons terhadap insiden nyata [3].

Untuk mengatasi fragmentasi visibilitas keamanan ini, teknologi *Security Information and Event Management* (SIEM) diadopsi sebagai pusat komando operasi keamanan (*Security Operations Center*). SIEM memungkinkan organisasi untuk mengumpulkan, menormalisasi, dan mengkorelasikan log peristiwa dari berbagai sumber data, seperti *Web Application Firewall* (WAF), server web, dan basis data, ke dalam satu platform terpusat. Pendekatan ini memungkinkan deteksi ancaman yang lebih akurat melalui korelasi silang, di mana indikator serangan yang tersebar di berbagai lapisan infrastruktur dapat dihubungkan untuk memetakan rantai serangan (*kill chain*) secara komprehensif [4].

Implementasi SIEM yang efektif juga mulai bergeser dari ketergantungan pada aturan statis menuju pemanfaatan teknologi cerdas. Integrasi algoritma *Machine Learning* ke dalam platform SIEM terbukti mampu meningkatkan kemampuan deteksi terhadap ancaman yang tidak dikenal (*zero-day*) dengan mempelajari pola perilaku normal sistem dan mengidentifikasi anomali secara *real-time* [5]. Studi terbaru menunjukkan bahwa kombinasi antara *Proxy-WAF* dan SIEM dapat memberikan perlindungan yang jauh lebih kuat terhadap kerentanan standar industri seperti OWASP Top 10 dibandingkan penggunaan alat keamanan secara terpisah [6].

Meskipun urgensi penerapan SIEM pada keamanan web sangat tinggi, literatur yang secara sistematis membahas efektivitas integrasi ini masih terbatas. Penelitian ini bertujuan untuk melakukan Tinjauan Literatur Sistematis (*Systematic Literature Review*) terhadap publikasi terkini periode 2020-2025. Kajian ini akan fokus mengidentifikasi jenis ancaman web dominan yang dapat dimitigasi oleh SIEM, menganalisis metode integrasi teknologi yang paling efektif, serta mengevaluasi tantangan yang dihadapi dalam implementasinya.

II. PENELITIAN YANG TERKAIT

Penelitian mengenai keamanan siber pada infrastruktur web terus berkembang seiring dengan meningkatnya kompleksitas serangan yang menargetkan lapisan aplikasi. Studi terdahulu menunjukkan bahwa meskipun teknologi pertahanan telah maju, ancaman klasik seperti serangan injeksi (*SQL Injection*) masih menjadi risiko persisten yang berdampak fatal terhadap kerahasiaan, integritas, dan ketersediaan data, terutama pada sistem basis data yang rentan terhadap manipulasi *payload* [7]. Tantangan ini semakin diperberat dengan migrasi infrastruktur organisasi ke lingkungan komputasi awan (*cloud computing*). Arsitektur keamanan tradisional sering kali gagal memantau lalu lintas terdistribusi di lingkungan ini secara efektif, sehingga memerlukan pendekatan pemantauan ancaman yang lebih proaktif berbasis SIEM untuk mendeteksi intrusi yang menargetkan sumber daya virtual dan melindungi aset data sensitif di *cloud* [8].

Sejalan dengan kebutuhan mitigasi tersebut, metode analisis log juga mengalami pergeseran signifikan dari teknik manual menuju otomatisasi cerdas guna menangani volume data yang masif. Penelitian yang dilakukan oleh [9] mengusulkan pendekatan *Online Log Analysis* (OLA) yang memanfaatkan tumpukan teknologi modern untuk memproses aktivitas pengguna secara *real-time*, yang terbukti mampu mendeteksi sesi pengguna berbahaya (*malicious user sessions*) sebelum eskalasi insiden terjadi. Lebih lanjut, pentingnya kerangka kerja pertahanan yang terstruktur juga ditekankan dalam studi [10], yang mengklasifikasikan kejadian keamanan (*security events*) dan permukaan serangan secara sistematis. Pendekatan ini dirancang untuk membantu administrator SIEM dan analis keamanan dalam membuat keputusan yang tepat serta merespons insiden dengan lebih terstruktur dan presisi. Kajian-kajian ini secara kolektif menegaskan urgensi integrasi alat deteksi canggih ke dalam ekosistem SIEM untuk mengatasi keterbatasan visibilitas pada mekanisme pertahanan terdahulu.

III. METODE PENELITIAN

Artikel *review* ini menggunakan pendekatan Tinjauan Literatur Sistematis (*Systematic Literature Review*/SLR). Pendekatan sistematis ini bertujuan untuk menelusuri serta mengidentifikasi seluruh bukti empiris yang memenuhi kriteria inklusi yang telah ditetapkan sebelumnya guna menjawab pertanyaan penelitian yang dirumuskan oleh peneliti. Proses tinjauan dilakukan dengan mengikuti protokol PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) yang mencakup tahapan perencanaan, pelaksanaan, dan pelaporan tinjauan.

A. *Perencanaan dan Pertanyaan Penelitian*

Tahap perencanaan dimulai dengan penetapan protokol pencarian menggunakan prosedur PICOC (*Population, Intervention, Comparison, Outcome, dan Context*). Prosedur ini digunakan untuk mendefinisikan objek kajian menjadi kata kunci pencarian yang spesifik. Elemen PICOC yang digunakan dalam penelitian ini dirinci pada Tabel 1.

Tabel 1. PICOC

Elemen	Deskripsi
Population	Aplikasi Web (*Web Applications*) dan Infrastruktur Server Web.
Intervention	Implementasi *Security Information and Event Management* (SIEM).
Comparison	Metode keamanan konvensional (firewall standar) atau tanpa korelasi log otomatis.
Outcome	Deteksi ancaman yang efektif, mitigasi serangan, dan visibilitas keamanan.
Context	Keamanan Siber (*Cybersecurity*) pada lingkungan TI perusahaan atau *cloud*.

Berdasarkan elemen tersebut, penelitian ini merumuskan tiga Pertanyaan Penelitian (*Research Questions*/RQ) sebagai berikut:

1. RQ1: Apa saja jenis ancaman siber pada aplikasi web yang paling efektif dideteksi dan dimitigasi oleh SIEM?
2. RQ2: Bagaimana metode integrasi dan teknologi SIEM yang diterapkan dalam studi terkini?
3. RQ3: Apa temuan utama terkait efektivitas implementasi SIEM dalam skenario serangan nyata?

B. *Strategi Pencarian*

Sumber informasi yang digunakan pada penelitian ini adalah database Scopus. Database ini dipilih karena merupakan salah satu indeks bibliografi terbesar dan paling bereputasi yang mencakup berbagai disiplin ilmu, termasuk ilmu komputer dan keamanan siber. Pencarian dilakukan menggunakan fitur *Advanced Search* dengan *string* pencarian yang menggabungkan kata kunci menggunakan operator Boolean (AND/OR) sesuai standar PICOC.

String pencarian yang diterapkan adalah: TITLE-ABS-KEY (("SIEM" OR "Security Information and Event Management") AND ("Web Application" OR "Web Security") AND ("Mitigation" OR "Detection"))

C. *Kriteria Kelayakan*

Kriteria kelayakan digunakan untuk menentukan artikel yang diinklusi dan dikecualikan dalam proses tinjauan. Kriteria inklusi dan eksklusi ditetapkan untuk menjaga relevansi dan kualitas data, sebagaimana terlihat pada Tabel 2.

Tabel 2. Kriteria Inklusi dan Eksklusi

Kriteria	Inklusi
Periode	2020 – 2025
Bahasa	Bahasa Inggris
Tipe Dokumen	Artikel Jurnal (*Article*) dan Prosiding (*Conference Paper*) | Buku, *Review Article*, Editorial.
Topik	Fokus teknis pada SIEM dan Keamanan Web | Fokus pada IoT, *Smart Grid*, atau aspek hukum/manajemen murni.
Akses	Akses Terbuka

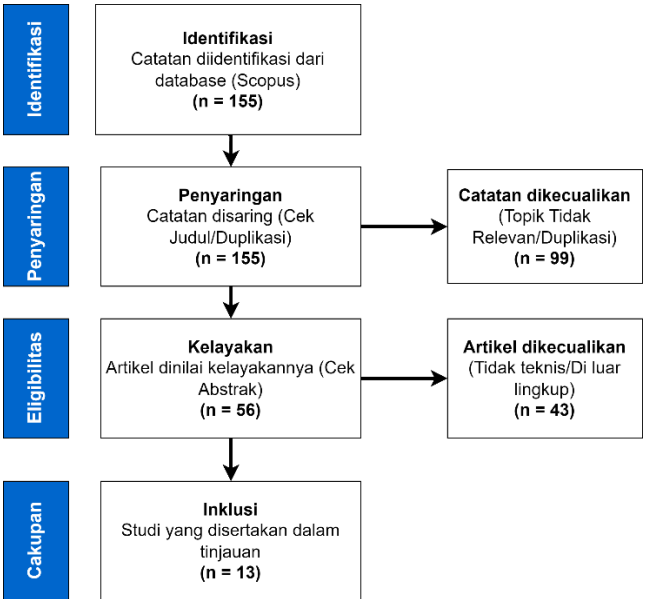
D. *Pengumpulan Data*

Proses seleksi literatur dalam penelitian ini mengikuti diagram alir PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) untuk memastikan transparansi dan reproduktifitas. Proses ini terdiri dari empat tahapan utama: identifikasi, penyaringan (*screening*), penilaian kelayakan (*eligibility*), dan inklusi.

1. Tahap Identifikasi: Proses dimulai dengan pencarian literatur pada database Scopus menggunakan *string* pencarian yang telah ditentukan. Pada tahap awal ini, ditemukan sebanyak 155 artikel yang memuat kata kunci terkait SIEM dan keamanan web.
2. Tahap Penyaringan: Terhadap 155 artikel tersebut, dilakukan penyaringan awal dengan menerapkan kriteria inklusi dan eksklusi (seperti batasan tahun 2020-2025, dokumen berbahasa Inggris, dan jenis artikel jurnal/prosiding). Selain itu, pemeriksaan judul dilakukan untuk membuang artikel yang terindikasi duplikasi atau topik yang jelas tidak relevan (misalnya membahas keamanan fisik). Dari proses ini, sebanyak 99 artikel dieksklusi, sehingga menyisakan 56 artikel untuk diproses lebih lanjut.
3. Tahap Penilaian: Sebanyak 56 artikel yang tersisa dievaluasi lebih mendalam melalui pembacaan abstrak. Fokus evaluasi adalah untuk memastikan artikel membahas implementasi teknis SIEM secara spesifik pada domain aplikasi web, bukan pada domain lain seperti IoT (*Internet of Things*) atau manajemen kebijakan semata. Pada tahap ini, sebanyak 43 artikel dinyatakan tidak memenuhi syarat karena kurangnya kedalaman teknis atau fokus

pembahasan yang melebar. Akibatnya, tersisa 13 artikel yang dianggap potensial.

4. Tahap Inklusi: Sebanyak 13 artikel yang lolos seleksi abstrak kemudian diverifikasi ketersediaan teks lengkapnya (*full text*) dan kesesuaiannya untuk menjawab pertanyaan penelitian. Seluruh 13 artikel tersebut dinyatakan valid dan dimasukkan sebagai data primer (*included studies*) untuk dilakukan ekstraksi data dan sintesis kualitatif pada bab pembahasan.



Gambar. 1 Diagram Alir PRISMA

IV. HASIL DAN PEMBAHASAN

Berdasarkan ekstraksi data dari 13 artikel terpilih yang diterbitkan dalam periode 2020-2025, bagian ini menyajikan analisis mendalam untuk menjawab pertanyaan penelitian mengenai jenis ancaman, metode integrasi, dan efektivitas implementasi SIEM pada keamanan web. Berikut adalah ringkasan ekstraksi data dari 13 artikel terpilih yang menjadi basis analisis dalam penelitian ini, sebagaimana disajikan pada Tabel 3.

Tabel 3. Ringkasan Studi Utama

Ref	Metode	Fokus/Topik	Temuan Utama/Hasil Implementasi
[8]	Integrasi Wazuh SIEM + Multi-WAF (ModSecurity, NAXSI)	SQL Injection	Integrasi kolaboratif meningkatkan deteksi varian SQLi dan memberikan visibilitas serangan terpusat.
[9]	Wazuh SIEM + Metode Deteksi OSCAR	Reconnaissance (Port 80 Attacks)	Sistem mampu mendeteksi aktivitas pemindaian pada server web dengan rata-rata penundaan hanya 1,402 detik
[10]	Analisis Korelasi SIEM	Web Application Attacks (Umum)	Mengembangkan pendekatan sistematis untuk klasifikasi *event* keamanan guna mempercepat perlindungan aplikasi web.
[11]	Akuisisi Data SIEM + Machine Learning	Intrusi Jaringan & Web	Penerapan prinsip ML pada akuisisi data SIEM meningkatkan efisiensi analisis ancaman siber yang kompleks.
[12]	Machine Learning (*Isolation Forest*) + Integrasi SIEM	Anomali Trafik HTTP	Mampu mendeteksi pola lalu lintas abnormal (*unknown attacks*) pada log HTTP tanpa memerlukan data latih berlabel
[13]	AI Log Analysis + Blockchain	Analisis Log Aman	Mengusulkan kerangka kerja berbasis *blockchain* untuk menjamin integritas log selama proses analisis AI
[14]	Proxy WAF + Integrasi SIEM	OWASP Top 10	Tingkat akurasi deteksi mencapai 100% untuk serangan XSS dan 97% untuk serangan SQL Injection.
[15]	Model Prediksi SIEM	SQL Injection Payload	Model mampu memprediksi dampak serangan terhadap aspek Kerahasiaan, Integritas, dan Ketersediaan (CIA)
[16]	Cloud-Based SIEM	Keamanan Cloud	Menawarkan pendekatan proaktif untuk pemantauan ancaman pada infrastruktur *cloud* menggunakan arsitektur SIEM
[17]	Monitoring SIEM (Cloud)	Cookie Bomb Attack (DoS)	Berhasil mendeteksi serangan *Cookie Bomb* dengan memantau ambang batas ukuran *cookie* pada lingkungan komputasi awan.
[18]	Online Log Analysis (OLA)	Malicious User Activities	Kerangka kerja analisis log *real-time* untuk mengidentifikasi aktivitas pengguna berbahaya secara instan.
[19]	Platform AKER (IDS + SIEM)	Lalu Lintas Terenkripsi	Platform *open-source* yang mengintegrasikan fungsi IDS dan

			SIEM untuk menganalisis ancaman pada lalu lintas terenkripsi.
[20]	Analisis Log Akses *Real-Time*	DDoS (Application Layer)	Mencegah serangan DDoS dengan menganalisis log akses secara waktu nyata untuk mengidentifikasi lonjakan permintaan abnormal.

A. Analisis Jenis Ancaman Siber pada Aplikasi Web (RQ1)

Hasil tinjauan menunjukkan bahwa SIEM tidak hanya berfungsi sebagai pengumpul log pasif, tetapi berperan aktif dalam memitigasi spektrum serangan yang luas pada lapisan aplikasi (*Layer 7*).

1. Serangan Injeksi dan Kerentanan Standar (OWASP Top 10): Ancaman yang paling dominan dibahas dalam literatur adalah *SQL Injection* (SQLi). Studi [8] dan [15] secara spesifik mengevaluasi kemampuan SIEM dalam mendeteksi varian SQLi (*Time-based, Error-based, Union*) dengan menganalisis pola *payload* berbahaya yang lolos dari validasi input standar. Selain itu, penelitian [14] menyoroti efektivitas SIEM dalam mendeteksi ancaman OWASP lainnya, seperti *Cross-Site Scripting* (XSS) dan *Local File Inclusion* (LFI), yang sering digunakan penyerang untuk mencuri sesi pengguna atau mengambil alih server.
2. Serangan Penolakan Layanan (DoS) Lapisan Aplikasi: Berbeda dengan serangan DDoS volumetrik pada lapisan jaringan, serangan pada lapisan aplikasi lebih sulit dideteksi karena menyerupai lalu lintas pengguna yang sah. Studi [20] membahas deteksi serangan HTTP Flooding menggunakan analisis log akses waktu nyata. Temuan menarik lainnya terdapat pada studi [17], yang membahas mitigasi serangan spesifik bernama "Cookie Bomb", di mana penyerang memanipulasi ukuran cookie browser untuk membebani pemrosesan server hingga menolak layanan bagi pengguna lain.
3. Anomali Perilaku dan Serangan Zero-Day: Keterbatasan deteksi berbasis tanda tangan diatasi dalam studi [12] dan [19], yang berfokus pada deteksi aktivitas bot berbahaya dan serangan zero-day. SIEM digunakan untuk memantau penyimpangan perilaku, seperti frekuensi permintaan yang tidak wajar atau pola navigasi situs yang anomali, yang mengindikasikan adanya upaya pengintaian (reconnaissance) atau serangan otomatis [9].

B. Metode dan Teknologi SIEM Terkini (RQ2)

Tinjauan literatur memperlihatkan pergeseran paradigma dari implementasi SIEM standalone (berdiri sendiri) menuju arsitektur terintegrasi dan cerdas.

1. Pendekatan Hybrid (SIEM dan WAF): Mayoritas penelitian merekomendasikan integrasi erat antara SIEM dan Web Application Firewall (WAF). Studi [8] dan [14] menunjukkan bahwa penggunaan agen SIEM (seperti Wazuh) yang dikombinasikan dengan WAF (seperti ModSecurity) menciptakan mekanisme pertahanan berlapis. WAF bertindak sebagai sensor depan yang memblokir serangan umum, sementara SIEM mengkorelasikan log WAF dengan log sistem operasi untuk mendeteksi serangan yang lebih kompleks atau lolos dari perimeter.
2. Integrasi Machine Learning (ML) dan Blockchain: Untuk mengatasi tingginya tingkat false positive pada SIEM tradisional, peneliti mengintegrasikan algoritma Machine Learning. Studi [12] mengusulkan penggunaan algoritma Isolation Forest pada log HTTP untuk mendeteksi anomali tanpa memerlukan data latih berlabel (unsupervised learning). Studi [18] menerapkan prinsip ML untuk akuisisi data yang lebih cerdas guna mengurangi noise. Bahkan, inovasi terbaru dalam studi [13] mengusulkan penggunaan teknologi blockchain untuk menjamin integritas log (tamper-proof) selama proses analisis berbasis AI, memastikan bukti forensik tetap valid.
3. Platform Cloud-Native dan Open Source: Seiring dengan adopsi komputasi awan, studi [16] menunjukkan efektivitas penggunaan platform SIEM berbasis cloud (seperti Microsoft Sentinel) untuk memantau infrastruktur web terdistribusi. Di sisi lain, solusi open-source seperti Wazuh dan ELK Stack (Elasticsearch, Logstash, Kibana) mendominasi penelitian akademis [8], [19] karena fleksibilitasnya untuk dikustomisasi sesuai kebutuhan deteksi spesifik tanpa biaya lisensi yang tinggi.

C. Efektivitas Implementasi (RQ3)

Implementasi strategi SIEM yang tepat terbukti memberikan dampak positif yang terukur terhadap postur keamanan organisasi.

1. Peningkatan Akurasi Deteksi: Integrasi WAF berbasis proxy dengan SIEM terbukti meningkatkan akurasi deteksi secara signifikan. Studi [14] melaporkan tingkat keberhasilan deteksi mencapai 100% untuk serangan XSS dan 97% untuk SQL Injection, jauh melampaui kemampuan deteksi log server standar.
2. Respons Waktu Nyata (Real-time): Kecepatan deteksi adalah kunci dalam mitigasi. Studi [9] mencatat bahwa sistem berbasis Wazuh dengan metode deteksi OSCAR mampu mengidentifikasi aktivitas pemindaian (*port scanning*) pada server web dengan rata-rata penundaan hanya 1,402 detik.

Respons cepat ini memungkinkan pemblokiran IP penyerang secara otomatis sebelum mereka menemukan kerentanan.

3. Visibilitas Terpusat: Studi [10] dan [16] menekankan bahwa kontribusi utama SIEM adalah memberikan "pandangan tunggal" (*single pane of glass*). Kemampuan untuk mengklasifikasikan kejadian keamanan dan memprediksi dampak serangan terhadap aspek kerahasiaan, integritas, dan ketersediaan (CIA Triad) [15] memungkinkan tim keamanan memprioritaskan penanganan insiden berdasarkan tingkat risikonya.

V. KESIMPULAN

Berdasarkan tinjauan sistematis terhadap 13 artikel terpilih yang diterbitkan dalam periode 2020-2025, penelitian ini menyimpulkan bahwa teknologi Security Information and Event Management (SIEM) memegang peranan yang semakin imperatif dalam arsitektur pertahanan aplikasi web modern. SIEM terbukti tidak lagi sekadar berfungsi sebagai alat kepatuhan (compliance) untuk penyimpanan log pasif, melainkan telah berevolusi menjadi pusat komando aktif yang efektif memitigasi spektrum ancaman lapisan aplikasi yang luas. Temuan penelitian menegaskan bahwa SIEM sangat andal dalam mendeteksi dan merespons serangan kritis seperti SQL Injection, Cross-Site Scripting (XSS), dan serangan Denial of Service (DoS) spesifik (seperti Cookie Bomb dan HTTP Flooding), yang sering kali gagal diidentifikasi oleh perangkat keamanan jaringan konvensional karena kemampuannya menyamar sebagai lalu lintas pengguna yang sah.

Tinjauan ini juga menyoroti pergeseran paradigma teknologi yang signifikan dari pendekatan berbasis aturan statis (rule-based) menuju model pertahanan hibrida yang cerdas. SIEM tradisional yang bekerja sendiri (standalone) dinilai memiliki keterbatasan dalam menghadapi dinamika serangan siber modern. Sebaliknya, integrasi strategis antara SIEM dengan Web Application Firewall (WAF) sebagai sensor garda depan terbukti menciptakan sinergi pertahanan yang kuat, di mana korelasi data lintas platform mampu meningkatkan akurasi deteksi hingga mencapai rentang 97% hingga 100% pada skenario serangan injeksi. Lebih jauh lagi, inkorporasi algoritma Machine Learning dan teknik Unsupervised Learning ke dalam platform SIEM telah berhasil mengatasi kelemahan utama sistem lama, yaitu tingginya tingkat peringatan palsu (false positive) dan ketidakmampuan mendeteksi serangan baru (zero-day) yang belum memiliki tanda tangan serangan.

Dari sisi implementasi operasional, solusi berbasis open-source seperti Wazuh dan ELK Stack (Elasticsearch, Logstash, Kibana) mendominasi lanskap penelitian sebagai alternatif yang fleksibel dan efisien biaya dibandingkan solusi komersial tertutup. Platform-platform ini terbukti mampu memberikan visibilitas keamanan terpusat (single pane of glass) yang memungkinkan tim keamanan memantau postur risiko secara real-time. Kemampuan sistem untuk memproses dan mengkorelasikan log dengan latensi rendah (rata-rata di bawah 2 detik) menjadi faktor kunci yang memungkinkan pemblokiran serangan secara otomatis sebelum kerusakan fatal terjadi pada basis data atau integritas sistem.

Meskipun demikian, implementasi SIEM pada lingkungan web bukan tanpa tantangan. Kompleksitas konfigurasi aturan korelasi dan tingginya kebutuhan sumber daya komputasi untuk memproses volume log HTTP yang masif masih menjadi hambatan utama, terutama pada infrastruktur dengan lalu lintas tinggi. Oleh karena itu, penelitian ini merekomendasikan arah pengembangan masa depan yang berfokus pada integrasi Security Orchestration, Automation, and Response (SOAR) untuk mengurangi beban kerja analis melalui respons insiden otomatis. Selain itu, eksplorasi teknik analisis lalu lintas terenkripsi yang efisien dan pengembangan model federated learning untuk menjaga privasi data juga menjadi area riset yang mendesak guna memastikan keberlanjutan dan ketangguhan sistem keamanan web di masa depan.

VI. KETERBATASAN DAN SARAN

Pelaksanaan tinjauan literatur sistematis ini memiliki beberapa batasan metodologis yang dapat memengaruhi generalisasi temuan. Kendala utama terletak pada pembatasan sumber data yang hanya berfokus pada pangkalan data Scopus. Meskipun Scopus memiliki reputasi tinggi, pendekatan *single-source* ini berpotensi mengabaikan studi teknis relevan yang mungkin hanya terindeks di repositori spesifik bidang teknik seperti IEEE Xplore atau ACM Digital Library. Fokus penelitian yang dibatasi pada rentang tahun 2020 hingga 2025 juga berarti bahwa konsep dasar arsitektur SIEM lawas yang mungkin masih menjadi fondasi sistem saat ini tidak tercakup dalam analisis.

Merujuk pada temuan dan kendala tersebut, terdapat sejumlah rekomendasi konstruktif untuk pengembangan penelitian dan implementasi praktis di masa depan. Bagi peneliti selanjutnya, sangat disarankan untuk melakukan analisis perbandingan lintas *database* dan mengupayakan akses teks penuh guna membedah metrik performa sistem (seperti latensi dan *throughput*) secara lebih granular. Dari sisi topik riset, celah penelitian (*research gap*) yang mendesak untuk digali adalah efektivitas SIEM dalam menganalisis lalu lintas terenkripsi (HTTPS/TLS 1.3) tanpa dekripsi, serta integrasi konsep *Explainable AI* (XAI) untuk mengatasi masalah transparansi pada deteksi berbasis anomali. Sementara itu, bagi organisasi yang hendak mengadopsi teknologi ini, disarankan untuk beralih dari penggunaan SIEM pasif menuju

ekosistem pertahanan aktif yang mengintegrasikan *Web Application Firewall* (WAF) dan orkestrasi respons otomatis (SOAR), guna meminimalkan waktu tunggu antara deteksi ancaman dan eksekusi mitigasi.

DAFTAR PUSTAKA

[1] S. A. Chamkar, Y. Maleh, and N. Gherabi, "Security Operations Centers: Use Case Best Practices, Coverage, and Gap Analysis Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge," *Journal of Cybersecurity and Privacy*, vol. 4, no. 4, pp. 777–793, 2024, doi: 10.3390/jcp4040036.

[2] I. Nugraha, "A Review on the Role of Modern SOC in Cybersecurity Operations," *International Journal of Current Science Research and Review*, vol. 4, 2021, doi: 10.47191/ijcsrr/V4-i5-.

[3] A. Reeves and D. Ashenden, "Understanding decision making in security operations centres: building the case for cyber deception technology," *Frontiers in Psychology*, vol. 14, 2023, doi: 10.3389/fpsyg.2023.1165705.

[4] "Human–AI Collaboration in Security Operations: Measuring Alert Trust, Automation Bias, and Analyst Upskilling in AI-Augmented SOC Environments," *IJCTEC*, vol. 8, no. 5, pp. 11375–11380, Oct. 2025, doi: 10.15680/IJCTECE.2025.0805011.

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

[6] M. A. Sapura, D. Stiawan, and R. Budiarto, "Machine learning model approach in cyber attack threat detection in security operation center," *Computer Science and Information Technology*, vol. 6, no. 1, pp. 80–90, Mar. 2025.

[7] R. Bhavsar and V. Thakar, "Design and Implementation of an Open-Source Security Operations Center for Effective Cyber Threat Detection and Response," 2025, doi: 10.21203/rs.3.rs-5795888/v1.

[8] M. N. Zaidan, P. Sukarno, and A. A. Wardana, "Collaborative Detection of SQL Injection Attacks using SIEM, Multi-Wazuh Agents, and Diverse Web Application Firewalls,"in Proc. CIEES 2024 – IEEE International Conference on Communications, Information, Electronic and Energy Systems, IEEE, 2024, doi: 10.1109/CIEES62939.2024.10811420.

[9] T. Suryantoro, B. D. P. Purnomosidi, and W. Andriyani, "The Analysis of Attacks Against Port 80 Webserver with SIEM Wazuh Using Detection and OSCAR Methods," in *Proc. 2022 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2022, pp. 1–6.

[10] A. Yushko et al., "Shielding Web Application against Cyber-Attacks using SIEM," *Proc. International Conference on Advanced Computer Information Technologies (ACIT)*, pp. 393–396, 2023.

[11] N. Tendikov et al., "Security Information Event Management data acquisition and analysis methods with machine learning principles," *Results in Engineering*, vol. 22, 2024.

[12] W. Ahmad and M. F. Amjad, "Anomaly Detection in HTTP Logs: Leveraging Machine Learning for Uncovering Anomalous Traffic Patterns with SIEM Integration,"in Proc. 2024 21st International Bhurban Conference on Applied Sciences and Technology (IBCAST 2024), IEEE, 2024, pp. 622–629, doi: 10.1109/IBCAST61650.2024.10877256.

[13] R. U. Rahman, P. Kumar, G. P. Kachare, M. M. Gawde, T. Tsundue, and D. S. Tomar, "A novel machine learning-based artificial intelligence approach for log analysis using blockchain technology," *Sigma Journal of Engineering and Natural Sciences*, vol. 42, no. 5, pp. 1391–1409, 2024.

[14] T. Rahmawati, R. W. Shiddiq, M. R. Sumpena, S. Setiawan, N. Karna, and S. N. Hertiana, "Web Application Firewall Using Proxy and Security Information and Event Management (SIEM) for OWASP Cyber Attack Detection,"in Proc. 2023 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS 2023), IEEE, 2023, pp. 280–285, doi: 10.1109/IoTaIS60147.2023.10346051.

[15] Y. Muliono, M. Y. Darus, C. R. Pardomuan, M. A. M. Ariffin, and A. Kurniawan, "Predicting Confidentiality, Integrity, and Availability from SQL Injection Payload,"in Proc. 2022 International Conference on Information Management and Technology (ICIMTech 2022), IEEE, 2022, pp. 600–605, doi: 10.1109/ICIMTech55957.2022.9915227.

[16] E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas, and A. Rekeraho, "Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach," *Applied Sciences (Switzerland)*, vol. 13, no. 22, 2023.

[17] R. Kaneko and T. Saito, "Detection of Cookie Bomb Attacks in Cloud Computing Environment Monitored by SIEM," *Journal of Advances in Information Technology*, vol. 14, no. 2, pp. 193–203, 2023.

[18] P. Muse, S. M. Shalinie, and H. Stanly, "Online Log Analysis (OLA) for Malicious User Activities,"in Proc. 2023 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing (PCEMS 2023), IEEE, 2023, doi: 10.1109/PCEMS58491.2023.10136101.

[19] A. Esseghir, F. Kamoun, and O. Hraiech, “AKER: An open-source security platform integrating IDS and SIEM functions with encrypted traffic analytic capability,” *Journal of Cyber Security Technology*, vol. 6, no. 1–2, pp. 27–64, 2022.
[20] H.-P. Nguyen, T.-N. Luong, T.-H. Dao, and N.-T. Truong, “An Approach to Prevent DDoS Attack Using Real-Time Access Logs Analysis,” *Communications in Computer and Information Science*, vol. 1863, pp. 92–105, 2023.