TIN: Terapan Informatika Nusantara
Vol 6, No 8, January 2026, page 1261-1269
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i8.8972

Analisis Komparatif Respons Insiden DDoS: Efisiensi MTTR pada Penanganan Manual Versus Otomatis Berbasis SIEM dan SOAR

I Nyoman Darmayoga[1,*], Rodhiyah Mardhiyyah[2]

[1] Department of Informatics, University of Technology Yogyakarta, Yogyakarta, Indonesia
[2] Computer Engineering, University of Technology Yogyakarta, Yogyakarta, Indonesia
Email: [1,*]darmayoga1702@gmail.com, [2]rodhiyah.mardhiyyah@uty.ac.id
Correspondence Author Email: darmayoga1702@gmail.com

Abstrak–Peningkatan penggunaan layanan digital di Indonesia diikuti dengan meningkatnya ancaman keamanan siber, khususnya serangan DDoS yang menargetkan ketersediaan layanan. Salah satu insiden nyata terjadi pada situs berita Suara.com yang mengalami serangan DDoS berskala besar dan ditangani secara manual oleh tim teknis. Penanganan manual pada insiden tersebut menunjukkan keterbatasan pada aspek kecepatan dan keterukuran respons awal, karena tidak seluruh tahapan respons terdokumentasi secara sistematis. Penelitian ini bertujuan untuk membandingkan mekanisme serta kecepatan respons awal antara penanganan manual pada insiden DDoS Suara.com dan respons otomatis menggunakan sistem SYRA. SYRA merupakan sistem keamanan berbasis web yang dikembangkan untuk mendukung deteksi dan respons otomatis terhadap insiden siber melalui integrasi SIEM dan SOAR. Metode penelitian yang digunakan adalah studi komparatif dengan memanfaatkan data publik dari kronologi insiden Suara.com sebagai representasi respons manual, serta data hasil pengujian serangan DDoS pada sistem SYRA yang dilakukan di lingkungan terkontrol sebagai representasi respons otomatis. Parameter utama yang digunakan dalam analisis adalah MTTR sebagai indikator kecepatan respons awal. Hasil penelitian menunjukkan bahwa sistem SYRA mampu menjalankan respons awal secara konsisten dengan nilai MTTR rata-rata sebesar 42,97 detik, sehingga tindakan awal dapat dilakukan dalam waktu kurang dari satu menit setelah serangan terdeteksi. Temuan ini menunjukkan bahwa penerapan respons otomatis memiliki peran penting dalam menjaga keberlangsungan layanan digital, khususnya pada sektor media dan layanan publik yang sangat bergantung pada ketersediaan sistem daring.

Kata Kunci: DDoS; MTTR; SIEM; SOAR; SYRA; Respons Otomatis

Abstract–The increasing use of digital services in Indonesia has been accompanied by a growing number of cybersecurity threats, particularly DDoS attacks that target service availability. One real-world incident occurred on the news website Suara.com, which experienced a large-scale DDoS attack that was handled manually by the technical team. The manual handling of this incident revealed limitations in terms of the speed and measurability of the initial response, as not all response stages were systematically documented. This study aims to compare the mechanisms and speed of initial responses between manual handling of the DDoS incident on Suara.com and automated responses using the SYRA system. SYRA is a web-based security system developed to support automated detection and response to cyber incidents through the integration of SIEM and SOAR. The research method used is a comparative study that utilizes public data from the chronology of the Suara.com incident as a representation of manual response, as well as data from DDoS attack testing on the SYRA system conducted in a controlled environment as a representation of automated response. The main parameter used in the analysis is MTTR as an indicator of initial response speed. The results show that the SYRA system is able to execute initial responses consistently with an average MTTR value of 42.97 seconds, allowing initial mitigation actions to be carried out in less than one minute after the attack is detected. These findings indicate that the implementation of automated response plays an important role in maintaining the continuity of digital services, particularly in the media and public service sectors that are highly dependent on system availability.

Keywords: DDoS; MTTR; SIEM; SOAR; SYRA; Automated Response

1. PENDAHULUAN

Transformasi digital yang berlangsung cepat di Indonesia telah mengubah cara masyarakat mengakses informasi dan berinteraksi dengan layanan berbasis teknologi. Penelitian mengenai digitalisasi di wilayah pedesaan pun menunjukkan bahwa perluasan akses internet tidak hanya memperluas peluang ekonomi (Diana & Sari, 2024), tetapi juga membawa tantangan baru yang berkaitan dengan keamanan dan kesiapan teknologi pada berbagai lapisan masyarakat. Ketergantungan yang semakin tinggi terhadap layanan digital membuat berbagai sektor, termasuk industri media, e-commerce, dan pelayanan publik, semakin bergantung pada sistem daring sebagai tulang punggung operasional (Aska et al., 2025). Namun, peningkatan aktivitas digital juga mendorong munculnya ancaman keamanan siber yang semakin kompleks dan cangih (Hnamte et al., 2024), terutama serangan yang menargetkan layanan berbasis cloud seperti DdoS (Karimi & Yusuf, 2025). DDoS merupakan jenis serangan siber yang bertujuan untuk mengganggu ketersediaan layananan jaringan atau sistem dengan membanjiri target dengan lalu lintas yang sangat besar dari banyak sumber secara simultan (Syaputra et al., 2025), sehingga layanan tidak lagi mampu merespons dengan baik karena permintaan lalu lintas yang melebihi kapasitas normalnya (Rahman & Odja, 2024). Dalam konteks tersebut, kecepatan respons menjadi faktor penting dalam menangani dan meminimalkan gangguan layanan (Zewail et al., 2025).

Dalam beberapa tahun terakhir, Indonesia mengalami peningkatan drastis jumlah insiden DDoS (Karimi & Yusuf, 2025). Peningkatan serangan DDoS tersebut mencapai 92% dan banyak menargetkan platform berita, lembaga pemerintah, dan layanan digital lainnya. Salah satu kejadian yang paling menonjol adalah serangan terhadap Suara.com pada 15 April 2025. Serangan tersebut berlangsung selama sekitar satu setengah jam, dimulai pada pukul 17.50 hingga 19.20 WIB, dan menghasilkan hampir 285 juta permintaan berbahaya yang dikirimkan ke server mereka (Iswinarno, 2025). Berdasarkan penelusuran tim teknis Suara.com, serangan ini berasal dari IP berbagai negara, terutama IP wilayah

Copyright © 2026 the author, Page 1261
This Journal is licensed under a Creative Commons Attribution 4.0 International License


TIN: Terapan Informatika Nusantara
Vol 6, No 8, January 2026, page 1261-1269
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i8.8972

Eropa dan Indonesia. Serangan yang menggunakan pola random path tersebut membuat permintaan tidak dapat difilter oleh mekanisme cache sehingga memberikan tekanan langsung ke origin server. Selain itu, kanal LiKS halaman liputan mendalam yang sering memuat isu-isu sosial dan politik juga menjadi target serangan massif selama 72 jam sebelumnya. Kondisi ini menunjukkan bahwa serangan DDoS tidak hanya berdampak pada aspek teknis (Anugrah et al., 2025), tetapi juga berpotensi berkaitan dengan konteks dan sensitivitas konten yang disajikan.

Penanganan insiden di Suara.com dilakukan secara manual dengan menganalisis pola trafik, mengidentifikasi alamat IP yang mencurigakan (Nisa et al., 2024), dan melakukan pemblokiran melalui konfigurasi sistem keamanan. Proses ini menuntut ketelitian tinggi dan sangat mengandalkan pengalaman operator, terutama ketika serangan berlangsung dalam jumlah besar dan datang dari berbagai sumber. Tantangan tersebut menyebabkan respons manual memerlukan waktu yang relatif panjang untuk mengurangi tekanan serangan. Dalam kajian keamanan siber, durasi yang diperlukan sejak insiden terdeteksi hingga tindakan respons diambil secara umum dikenal sebagai Mean Time to Respond (MTTR), yang sering digunakan sebagai indikator efektivitas proses respons insiden (Khan, 2023). MTTR menggambarkan rata-rata waktu yang dibutuhkan untuk menangani insiden hingga sistem kembali beroperasi secara normal, sehingga semakin singkat nilai MTTR, maka semakin kecil dampak insiden terhadap sistem dan operasional organisasi (Żurawski et al., 2025). Namun, dalam konteks penelitian ini, MTTR tidak dimaknai sebagai waktu hingga layanan sepenuhnya pulih, melainkan difokuskan pada durasi sejak serangan terdeteksi hingga tindakan respons awal atau mitigasi pertama dijalankan. Pendefinisian ini digunakan untuk menekankan fase awal respons insiden, yang dianggap krusial dalam mencegah eskalasi dampak serangan, khususnya pada serangan DDoS yang bersifat volumetrik dan berlangsung cepat.

Seiring meningkatnya kompleksitas ancaman, teknologi keamanan berbasis otomatisasi mulai banyak diterapkan sebagai solusi untuk mempercepat respons terhadap serangan. Integrasi antara Security Information and Event Management (SIEM) dan Security Orchestration, Automation, and Response (SOAR) memungkinkan sistem mendeteksi indikator serangan secara real time dan langsung mengeksekusi tindakan mitigasi tanpa intervensi manual (Anggraini & Widhiantoro, 2025). Dalam konteks ini, SOAR memberikan solusi yang sangat dibutuhkan dengan mengurangi pekerjaan manual dan meningkatkan efisiensi respons (Dwivedi et al., 2025), terutama pada insiden yang menuntut kecepatan dan konsistensi penanganan. SIEM mampu memantau aktivitas domain secara real-time, mendeteksi ancaman, dan mengirimkan log ke server (Fahmi et al., 2025). Kemudian SIEM mampu mengelola log yang dihasilkan dari berbagai sumber data seperti endpoint, perangkat jaringan, maupun firewall sehingga memberikan gambaran menyeluruh terhadap kondisi keamanan sistem (Aditya et al., 2024). Kemampuan pemantauan log secara terpusat ini juga terbukti efektif dalam memangkas waktu deteksi dan respons administrator ketika insiden keamanan terjadi (Heluka & Sulistyo, 2023). Ketika SIEM dikombinasikan dengan SOAR dalam satu sistem terintegrasi, berbagai penelitian menunjukkan bahwa mekanisme tersebut memiliki keandalan dan efektivitas yang lebih baik dalam menjaga keamanan siber, sekaligus mampu mengurangi beban kognitif operator dan meminimalkan kesalahan manusia (Hugo & Proust, 2022). Dalam konteks penelitian ini, efektivitas sistem otomatis dievaluasi berdasarkan kecepatan eksekusi respons awal, bukan pada durasi pemulihan layanan secara menyeluruh, sehingga metrik MTTR digunakan sebagai indikator utama untuk menilai seberapa cepat sistem terintegrasi SIEM dan SOAR dapat merespons serta menanggulangi insiden sejak terdeteksi , sehingga dampak serangan terhadap sistem dan operasional organisasi dapat ditekan seminimal mungkin (Edwards, 2025).

Dalam konteks penerapan otomatisasi respons insiden, penelitian ini menggunakan Secure Your Realm Always (SYRA) sebagai sistem yang merepresentasikan pendekatan respons otomatis. SYRA merupakan aplikasi keamanan berbasis web yang dirancang untuk menyediakan deteksi serangan secara real time, otomatisasi mitigasi, serta dukungan analisis forensik digital dalam satu platform terpadu. Pada implementasinya, SYRA memanfaatkan Wazuh sebagai SIEM yang berfungsi untuk mengumpulkan, menganalisis, dan mengelola log keamanan, sekaligus mendeteksi serangan yang terjadi (Martinez, 2022). Informasi hasil deteksi tersebut selanjutnya diteruskan ke modul SOAR yang diimplementasikan menggunakan n8n, yang bertugas menghubungkan berbagai sistem dan mengotomatisasi proses respons terhadap serangan yang terdeteksi (Nakavisute & Sincharoonsak, 2025). Melalui integrasi ini, tindakan respons awal dapat dieksekusi secara otomatis tanpa bergantung pada intervensi manual (Hafiz & Soewito, 2022). Respons awal yang dimaksud dalam penelitian ini didefinisikan sebagai tindakan mitigasi pertama yang dijalankan sistem, seperti pemblokiran IP penyerang dan pengiriman notifikasi telegram pengguna SYRA bahwa IP penyerang sudah diblokir oleh sistem, sehingga waktu tanggap yang diukur tidak dipengaruhi oleh proses pemulihan layanan secara keseluruhan. Selain itu, SYRA dilengkapi dengan mekanisme pencatatan dan notifikasi yang memastikan setiap kejadian serangan terdokumentasi secara sistematis, memungkinkan pengukuran waktu deteksi dan waktu respons awal dilakukan secara terstruktur. Karakteristik tersebut menjadikan SYRA relevan sebagai objek penelitian untuk mengevaluasi efektivitas respons otomatis, khususnya dalam menurunkan MTTR pada serangan DDoS.

Meskipun manfaat otomatisasi respons insiden telah banyak dibahas dalam berbagai penelitian, masih terbatas kajian yang secara eksplisit membandingkan respons manual pada insiden nyata dengan respons otomatis berbasis SIEM dan SOAR, khususnya dalam konteks serangan DDoS di Indonesia. Sebagian besar penelitian sebelumnya cenderung berfokus pada simulasi atau pengujian teknis sistem dalam lingkungan terkontrol, tanpa mengaitkannya secara langsung dengan kronologi serangan yang benar-benar terjadi pada platform lokal. Padahal, analisis terhadap insiden nyata penting untuk memahami bagaimana mekanisme respons manual bekerja dalam kondisi serangan yang dinamis dan tidak terstruktur, seperti yang dialami oleh Suara.com.

This Journal is licensed under a Creative Commons Attribution 4.0 International License

TIN: Terapan Informatika Nusantara
Vol 6, No 8, January 2026, page 1261-1269
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i8.8972

Berdasarkan latar belakang tersebut, penelitian ini disusun sebagai studi komparatif yang membandingkan dua pendekatan respons awal terhadap serangan DDoS, yaitu penanganan manual pada insiden nyata Suara.com yang dianalisis berdasarkan data publik, dan respons otomatis yang diuji melalui platform SYRA dalam lingkungan terkontrol. Perbandingan dilakukan menggunakan MTTR sebagai metrik utama untuk mengevaluasi kecepatan respons awal, dengan batasan yang jelas bahwa MTTR diukur hingga tindakan mitigasi pertama dijalankan, serta berfokus pada perbedaan mekanisme dan alur kerja respons, bukan pada kesetaraan skala atau volume serangan. Kontribusi penelitian ini terletak pada penyajian analisis berbasis data yang menunjukkan perbedaan karakteristik respons manual dan otomatis, sekaligus memberikan gambaran empiris mengenai keunggulan respons otomatis dalam mempercepat fase awal penanganan serangan DDoS dalam konteks keamanan siber di Indonesia.

2. METODOLOGI PENELITIAN

2.1 Kerangka Dasar Penelitian

Penelitian ini disusun sebagai studi komparatif yang bertujuan membandingkan mekanisme dan kecepatan respons awal terhadap serangan DDoS melalui dua pendekatan yang berbeda, yaitu penanganan manual pada insiden nyata Suara.com dan respons otomatis menggunakan sistem SYRA. Kedua pendekatan tersebut tidak diuji pada situs yang sama, melainkan dianalisis sebagai dua objek penelitian yang merepresentasikan kondisi penanganan insiden yang berbeda.

Objek penelitian pertama adalah insiden serangan DDoS pada situs berita Suara.com, yang ditangani secara manual oleh tim teknis internal. Pada pendekatan ini, penelitian tidak melakukan pengujian langsung terhadap sistem Suara.com, melainkan menggunakan data sekunder berupa kronologi kejadian, laporan publik, dan pemberitaan resmi yang menjelaskan waktu kejadian, dampak serangan, serta mekanisme respons yang dilakukan. Penanganan manual pada penelitian ini diposisikan sebagai studi kasus insiden nyata, yang dianalisis untuk menggambarkan bagaimana respons awal dijalankan ketika proses deteksi dan mitigasi sangat bergantung pada analisis serta pengambilan keputusan manusia.

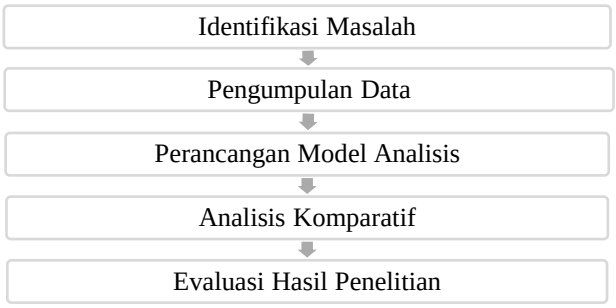
Objek penelitian kedua adalah sistem SYRA, yaitu platform keamanan yang mengintegrasikan SIEM dan SOAR untuk menjalankan respons otomatis terhadap serangan DDoS. Pada pendekatan ini, penelitian melakukan pengujian langsung dengan mensimulasikan serangan DDoS di lingkungan terkontrol. Pengujian dilakukan untuk memperoleh data primer berupa log waktu deteksi serangan dan waktu eksekusi respons awal, sehingga mekanisme dan kecepatan respons otomatis dapat diukur secara kuantitatif.

Dengan dua objek penelitian yang memiliki karakteristik berbeda, penelitian ini tidak bertujuan untuk menyamakan skala atau volume serangan, melainkan untuk membandingkan mekanisme kerja dan kecepatan respons awal yang dihasilkan oleh pendekatan manual dan otomatis. Fokus utama perbandingan diarahkan pada bagaimana masing-masing pendekatan merespons serangan pada fase awal sebelum dampak serangan berkembang lebih jauh.

Parameter utama yang digunakan dalam penelitian ini adalah MTTR, yang didefinisikan sebagai selang waktu sejak indikator serangan terdeteksi hingga tindakan respons awal dijalankan. MTTR dijadikan sebagai variabel dependen, sedangkan jenis mekanisme respons (manual dan otomatis) bertindak sebagai variabel independen. Penelitian ini mengajukan hipotesis bahwa mekanisme respons otomatis akan menghasilkan MTTR yang lebih rendah dibandingkan dengan penanganan manual, karena proses respons tidak dipengaruhi oleh faktor kognitif, koordinasi tim, maupun waktu pengambilan keputusan manusia.

2.2 Tahapan Penelitian

Tahapan penelitian dirancang mengikuti alur kerja dalam studi rekayasa yang umumnya dimulai dari identifikasi masalah hingga evaluasi hasil. Setiap tahap dirancang untuk memperjelas perbedaan proses yang terjadi pada penanganan manual dan respons otomatis. Tahapan penelitian ini dapat dilihat pada Gambar 1 berikut.



Gambar 1. Tahapan Penelitian

Dari Gambar 1, tahap pertama adalah identifikasi masalah, yang dilakukan dengan menelaah insiden serangan DDoS terhadap situs Suara.com sebagai contoh penanganan manual pada kasus nyata. Pada tahap ini, penelitian mengkaji karakteristik serangan, durasi gangguan layanan, serta gambaran umum proses respons yang dilakukan oleh

Copyright © 2026 the author, Page 1263
This Journal is licensed under a Creative Commons Attribution 4.0 International License

TIN: Terapan Informatika Nusantara
Vol 6, No 8, January 2026, page 1261-1269
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i8.8972

tim teknis. Analisis ini bertujuan untuk memahami bagaimana respons awal dijalankan dalam kondisi nyata ketika tidak terdapat sistem otomatis yang langsung mengeksekusi mitigasi.

Tahap kedua adalah pengumpulan data, yang dibedakan berdasarkan pendekatan manual dan otomatis. Pada penanganan manual, data dikumpulkan dari laporan publik dan pemberitaan resmi yang memuat parameter seperti waktu kejadian serangan, durasi gangguan layanan, skala serangan, pola trafik, serta mekanisme respons yang dilakukan oleh tim teknis. Parameter yang diamati pada pendekatan manual meliputi:

1. waktu terjadinya gangguan layanan,
2. durasi serangan,
3. mekanisme deteksi awal berdasarkan pemantauan manusia,
4. tahapan respons sebelum mitigasi dijalankan, dan
5. keterukuran waktu respons awal.

Pada respons otomatis, data diperoleh dari hasil pengujian serangan DDoS pada sistem SYRA di lingkungan terkontrol. Parameter yang diamati pada pendekatan otomatis meliputi:

1. waktu deteksi anomali oleh sistem,
2. waktu eksekusi respons awal oleh sistem otomatis,
3. konsistensi waktu respons antar pengujian, dan
4. nilai MTTR yang dihasilkan berdasarkan log sistem.

Tahap ketiga adalah perancangan model analisis, yang difokuskan pada cara pengukuran dan interpretasi MTTR. Pada pendekatan otomatis, MTTR dihitung secara kuantitatif dari selisih waktu deteksi serangan dan waktu respons awal dijalankan. Pada pendekatan manual, MTTR tidak dihitung secara numerik karena tidak tersedianya pencatatan waktu respons awal secara rinci, sehingga dianalisis secara deskriptif dan relatif berdasarkan kronologi kejadian dan durasi gangguan yang dilaporkan.

Tahap keempat adalah analisis komparatif, yang merupakan tahap inti penelitian. Pada tahap ini, hasil penanganan manual dan respons otomatis dibandingkan secara berdampingan berdasarkan parameter yang telah ditetapkan. Analisis tidak hanya menyoroti perbedaan waktu respons, tetapi juga perbedaan mekanisme kerja, seperti ketergantungan pada analisis manusia pada pendekatan manual dan penggunaan aturan serta alur kerja otomatis pada sistem SYRA.

Tahap terakhir adalah evaluasi hasil penelitian, yang bertujuan menafsirkan temuan secara lebih luas dalam konteks keamanan siber. Evaluasi dilakukan dengan mengaitkan hasil penelitian dengan kebutuhan organisasi dalam menjaga ketersediaan layanan digital. Pada tahap ini juga dibahas keterbatasan penelitian, khususnya terkait penggunaan data manual yang bersifat sekunder, serta peluang pengembangan penelitian selanjutnya dengan data insiden yang lebih terukur atau skenario pengujian otomatis pada skala yang lebih besar.

2.3 Objek Penelitian dan Gambaran Sistem SYRA

Objek penelitian pada pendekatan respons otomatis adalah SYRA, yaitu sistem keamanan berbasis web yang dikembangkan sebagai prototipe penelitian, bukan sistem komersial, dengan tujuan mendukung deteksi dan respons otomatis terhadap insiden siber. SYRA dirancang untuk mengintegrasikan fungsi SIEM dan SOAR dalam satu alur kerja terintegrasi. Pada implementasinya, SYRA memanfaatkan Wazuh sebagai SIEM untuk melakukan pemantauan log keamanan domain secara real time dan mendeteksi anomali trafik. Informasi hasil deteksi kemudian diteruskan ke modul SOAR yang diimplementasikan menggunakan n8n, yang berfungsi menjalankan alur kerja otomatis berupa pemrosesan alert, pemblokiran alamat IP penyerang, serta pengiriman notifikasi kepada pengguna. Integrasi ini memungkinkan tindakan respons awal dijalankan secara otomatis tanpa menunggu analisis manual dari operator. Dalam konteks penelitian ini, SYRA diposisikan sebagai objek uji untuk mengevaluasi kecepatan respons awal sistem otomatis, khususnya pada fase setelah indikator serangan terdeteksi hingga tindakan mitigasi awal dijalankan.

2.4 Lingkungan Pengujian (Testbed) dan Konfigurasi Sistem

Pengujian respons otomatis dilakukan pada lingkungan terkontrol yang disiapkan secara khusus untuk memastikan kestabilan sistem dan keterukuran waktu respons. Lingkungan pengujian ini tidak merepresentasikan sistem produksi berskala besar, melainkan difokuskan pada pengujian mekanisme dan alur kerja respons otomatis. Spesifikasi lingkungan pengujian yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Sistem Operasi Server: Linux (Ubuntu Server)
2. Platform SIEM: Wazuh
3. Platform SOAR: n8n
4. Bahasa Backend: Golang
5. Frontend: React
6. Basis Data: PostgreSQL
7. Manajemen Layanan: Docker Container
8. Media Notifikasi: Telegram Bot

Seluruh komponen dijalankan pada server virtual (VPS) dan dikonfigurasi agar mampu mencatat timestamp kejadian secara konsisten.

Copyright © 2026 the author, Page 1264
This Journal is licensed under a Creative Commons Attribution 4.0 International License

TIN: Terapan Informatika Nusantara
Vol 6, No 8, January 2026, page 1261-1269
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i8.8972

2.5 Skenario Simulasi Serangan DDoS

Simulasi serangan DDoS pada sistem SYRA dilakukan menggunakan skrip berbasis curl yang dijalankan dari sistem penguji. Serangan disimulasikan dalam bentuk controlled low-rate DDoS attack, bukan serangan volumetrik berskala besar. Pada skenario ini, serangan dilakukan dengan mengirimkan total 125 permintaan HTTP ke endpoint target secara berurutan, dengan interval waktu 0,2 detik antar permintaan, sehingga menghasilkan laju sekitar 5 request per detik (RPS) selama ±25 detik. Pendekatan ini dipilih untuk meniru pola serangan random path seperti yang terjadi pada insiden Suara.com, namun dalam skala yang aman dan terkendali untuk lingkungan uji. Skenario ini tidak bertujuan untuk menguji ketahanan bandwidth server, melainkan untuk:

1. Mengamati kemampuan sistem mendeteksi pola trafik tidak normal,
2. Mengukur waktu respons awal sistem otomatis, dan
3. Menilai konsistensi eksekusi mitigasi oleh workflow SOAR.

2.6 Definisi Operasional dan Pengukuran MTTR

Dalam penelitian ini, MTTR didefinisikan secara operasional sebagai selang waktu sejak indikator serangan terdeteksi hingga tindakan respons awal dijalankan, bukan hingga layanan pulih sepenuhnya. Pada pendekatan otomatis, MTTR dihitung berdasarkan:

1. waktu deteksi anomali yang tercatat pada log Wazuh, dan
2. waktu eksekusi tindakan mitigasi awal, yang ditandai dengan pemblokiran IP penyerang dan pengiriman notifikasi melalui Telegram.

Timestamp diambil dari log sistem Linux dan log internal aplikasi SYRA, sehingga waktu respons dapat diukur secara presisi dalam satuan detik.

Pada pendekatan manual, MTTR tidak dihitung secara numerik karena keterbatasan pencatatan waktu respons awal pada data publik. Oleh karena itu, MTTR dianalisis secara deduktif dan deskriptif berdasarkan rentang waktu kejadian dan durasi gangguan layanan yang dilaporkan.

Pengukuran MTTR pada pengujian sistem SYRA dilakukan secara manual menggunakan stopwatch. Penghitungan waktu dimulai sejak serangan DDoS dijalankan pada sistem uji hingga pengguna SYRA menerima notifikasi melalui Telegram yang menginformasikan bahwa alamat IP penyerang telah berhasil diblokir oleh sistem. Rentang waktu tersebut merepresentasikan durasi respons awal sistem, mulai dari deteksi serangan hingga eksekusi tindakan mitigasi otomatis. Metode ini dipilih karena seluruh proses respons berjalan secara end-to-end dalam satu alur kerja terintegrasi, sehingga titik awal dan titik akhir respons dapat diamati secara jelas dan konsisten pada setiap pengujian. Pendekatan pengukuran ini mencerminkan waktu respons yang dirasakan secara operasional oleh pengguna sistem SYRA, sehingga relevan untuk mengevaluasi efektivitas respons awal dari sudut pandang praktis.

2.7 Dasar Logis Perbandingan Manual dan Otomatis

Perbandingan antara respons manual dan otomatis dalam penelitian ini tidak dimaksudkan untuk menyamakan skala atau volume serangan, melainkan untuk membandingkan mekanisme dan kecepatan respons awal. Meskipun serangan pada sistem SYRA disimulasikan dalam skala kecil dan terkontrol, pendekatan ini tetap relevan karena fokus penelitian berada pada fase awal respons. Dengan menggunakan skenario serangan yang terukur dan konsisten, penelitian ini dapat menunjukkan perbedaan mendasar antara respons manual yang bergantung pada analisis manusia dan respons otomatis yang dijalankan berdasarkan aturan sistem. Dengan demikian, hasil perbandingan MTTR mencerminkan perbedaan mekanisme respons, bukan perbedaan kapasitas infrastruktur atau skala serangan.

3. HASIL DAN PEMBAHASAN

Pada bagian ini membahas hasil penelitian yang diperoleh dari analisis terhadap dua pendekatan penanganan serangan DDoS, yaitu penanganan manual pada insiden nyata yang dialami situs berita Suara.com dan respons otomatis menggunakan sistem SYRA. Penyajian hasil dilakukan secara bertahap dan terstruktur, dimulai dari pemaparan proses dan alur kerja sistem SYRA sebagai objek penelitian, kemudian dilanjutkan dengan hasil penanganan manual, hasil respons otomatis, perbandingan kedua pendekatan, serta pembahasan konseptual terhadap temuan penelitian. Fokus utama pembahasan diarahkan pada mekanisme respons awal dan keterukuran waktu respons awal yang direpresentasikan melalui metrik MTTR.

3.1 Proses dan Alur Kerja Sistem SYRA

Sebelum menyajikan hasil pengujian, penting untuk menjelaskan terlebih dahulu alur kerja sistem SYRA agar pembaca memahami bagaimana respons otomatis dijalankan. SYRA merupakan sistem keamanan berbasis web yang mengintegrasikan fungsi SIEM dan SOAR dalam satu alur kerja terintegrasi.

Proses kerja SYRA dimulai ketika domain yang telah terdaftar menerima permintaan HTTP. Seluruh aktivitas permintaan tersebut dicatat dalam log sistem dan dipantau secara real time oleh modul SIEM, yaitu Wazuh. Wazuh melakukan analisis terhadap pola trafik yang masuk dengan membandingkannya terhadap aturan dan ambang batas yang telah ditentukan sebelumnya. Ketika terdeteksi adanya anomali trafik yang mengindikasikan serangan DDoS,

Copyright © 2026 the author, Page 1265
This Journal is licensed under a Creative Commons Attribution 4.0 International License

TIN: Terapan Informatika Nusantara
Vol 6, No 8, January 2026, page 1261-1269
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i8.8972

Wazuh menghasilkan alert yang berisi informasi waktu kejadian, alamat IP penyerang, dan karakteristik serangan. Alert tersebut kemudian diteruskan secara otomatis ke modul SOAR yang diimplementasikan menggunakan n8n. Pada tahap ini, n8n menjalankan workflow respons yang telah dirancang, meliputi validasi alert, pemrosesan data serangan, serta eksekusi tindakan mitigasi awal. Tindakan mitigasi yang dilakukan pada penelitian ini berupa pemblokiran alamat IP penyerang secara otomatis melalui backend SYRA. Setelah pemblokiran berhasil dijalankan, sistem mengirimkan notifikasi kepada pengguna melalui Telegram yang menginformasikan bahwa serangan telah terdeteksi dan alamat IP penyerang telah diblokir.

Alur kerja ini memastikan bahwa proses respons berjalan secara end-to-end tanpa intervensi manual. Dengan memahami tahapan tersebut, pembaca dapat melihat bahwa waktu respons yang diukur dalam penelitian ini mencerminkan keseluruhan proses mulai dari deteksi hingga eksekusi mitigasi awal.

3.2 Hasil Penanganan Manual pada Insiden DDoS Suara.com

Hasil pertama berasal dari penanganan manual pada insiden serangan DDoS yang menimpa situs berita Suara.com pada 15 April 2025. Pada pendekatan ini, penelitian tidak melakukan pengujian langsung, melainkan menganalisis data sekunder berupa kronologi kejadian dan laporan publik yang tersedia secara resmi. Insiden Suara.com diposisikan sebagai studi kasus penanganan manual pada kondisi nyata. Berdasarkan laporan resmi dan kronologi kejadian Suara.com dapat dilihat pada Tabel 1 berikut.

Tabel 1. Data Penanganan Manual pada Insiden DDoS Suara.com

No	Aspek Pengamatan	Deskripsi
1	Objek Insiden	Situs berita Suara.com
2	Jenis Serangan	DDoS
3	Tanggal Kejadian	15 April 2025
4	Waktu Kejadian	Pukul 17.50 – 19.20 WIB
5	Durasi Serangan	± 1.5 jam
6	Volume Serangan	± 285 juta permintaan
7	Skala Insiden	Serangan Siber terbesar yang pernah dialami Suara.com
8	Sumber Serangan	Bot dan IP dari berbagai negara (Eropa, Indonesia, dll)
9	Pola Serangan	Trafik masif dengan metode random path untuk melewati cache
10	Dampak Awal	Situs tidak dapat diakses dalam periode tertentu
11	Mekanisme Deteksi	Penanganan dilakukan berdasarkan analisis tim teknis terhadap kondisi trafik dan sistem.

Berdasarkan data yang dirangkum pada Tabel 1, serangan DDoS berlangsung selama kurang lebih 90 menit dengan volume trafik yang sangat besar. Dampak awal yang dirasakan adalah tidak dapat diaksesnya layanan situs dalam periode tertentu. Proses penanganan dilakukan oleh tim teknis melalui pemantauan trafik, analisis pola serangan, identifikasi sumber IP, serta pengambilan keputusan sebelum tindakan mitigasi dijalankan.

Laporan publik tidak menyediakan pencatatan waktu yang rinci mengenai kapan tindakan mitigasi pertama kali diterapkan. Oleh karena itu, nilai MTTR pada penanganan manual tidak dapat dihitung secara numerik presisi. Namun demikian, sebagai peneliti, dilakukan deduksi logis berdasarkan rentang waktu kejadian. Jika serangan dimulai pada pukul 17.50 WIB dan baru mereda pada pukul 19.20 WIB, maka proses identifikasi hingga mitigasi penuh berlangsung dalam jendela waktu sekitar 90 menit. Hal ini menunjukkan bahwa respons manual memerlukan waktu yang signifikan sebelum dampak serangan dapat dikendalikan secara efektif.

Dengan membandingkan durasi gangguan tersebut terhadap hasil respons otomatis yang mampu dijalankan dalam waktu kurang dari satu menit, dapat disimpulkan bahwa terdapat potensi penghematan waktu respons awal lebih dari 90% apabila mekanisme otomatis diterapkan pada fase awal insiden.

3.3 Hasil Respons Otomatis Menggunakan Sistem SYRA

Hasil kedua diperoleh dari pengujian respons otomatis menggunakan sistem SYRA. Pengujian dilakukan di lingkungan terkontrol dengan mensimulasikan serangan DDoS. Objek penelitian pada bagian ini adalah sistem SYRA, bukan situs Suara.com. Serangan disimulasikan dengan mengirimkan total 125 permintaan HTTP ke endpoint target secara berurutan, dengan interval 0,2 detik antar permintaan. Dengan demikian, intensitas serangan berada pada kisaran ±5 request per detik (RPS) selama ±25 detik. Skenario ini dikategorikan sebagai controlled low-rate DDoS attack yang bertujuan meniru pola serangan random path pada insiden Suara.com, bukan untuk menguji kapasitas bandwidth server.

Waktu respons diukur secara manual menggunakan stopwatch, dimulai sejak serangan selesai dijalankan hingga pengguna menerima notifikasi Telegram yang menginformasikan bahwa alamat IP penyerang telah berhasil diblokir. Ringkasan hasil respons otomatis SYRA disajikan pada Tabel 2 berikut.

Tabel 2. Hasil Pengujian Serangan DDoS pada SYRA

Skenario Pengujian	Uji ke-	Waktu Respons SYRA (detik)
DDoS 125 request	1	41,47
DDoS 125 request	2	40,93
DDoS 125 request	3	40,40

Copyright © 2026 the author, Page 1266
This Journal is licensed under a Creative Commons Attribution 4.0 International License

TIN: Terapan Informatika Nusantara
Vol 6, No 8, January 2026, page 1261-1269
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i8.8972

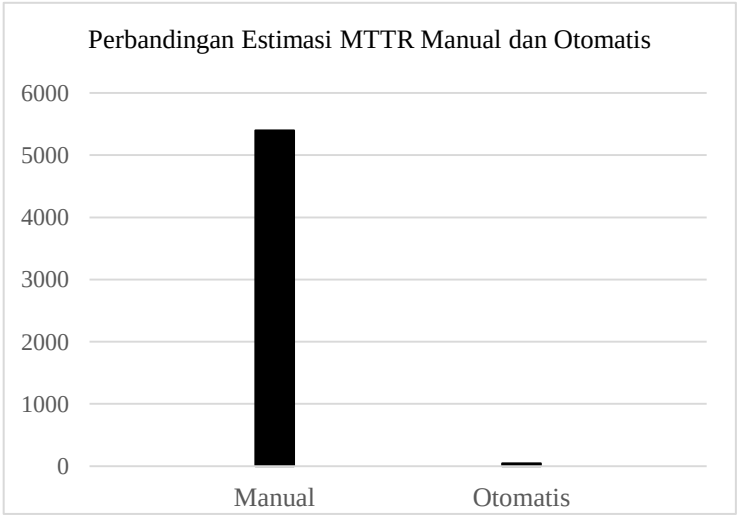
Skenario Pengujian	Uji ke-	Waktu Respons SYRA (detik)
DDoS 125 request	4	42,65
DDoS 125 request	5	45,38
DDoS 125 request	6	42,47
DDoS 125 request	7	41,05
DDoS 125 request	8	42,43
DDoS 125 request	9	48,03
DDoS 125 request	10	44,91
Rata-rata MTTR		42,97

Berdasarkan hasil pengujian Tabel 2, hasil pengujian menunjukkan bahwa waktu respons sistem SYRA berada pada rentang 40,40 hingga 48,03 detik, dengan nilai MTTR rata-rata sebesar 42,97 detik. Variasi waktu antar pengujian relatif kecil, yang menunjukkan bahwa mekanisme respons otomatis berjalan secara stabil dan konsisten. Seluruh pengujian memperlihatkan bahwa respons awal dapat dijalankan dalam waktu kurang dari satu menit setelah serangan terdeteksi.

3.4 Perbandingan Penanganan Manual dan Respons Otomatis

Perbandingan antara penanganan manual dan respons otomatis menunjukkan perbedaan yang sangat signifikan pada aspek kecepatan respons awal. Berdasarkan deduksi logis, penanganan manual pada insiden Suara.com membutuhkan waktu hingga ±90 menit sejak serangan dimulai hingga kondisi layanan kembali terkendali. Sebaliknya, sistem SYRA mampu menjalankan respons awal dalam waktu rata-rata 42,97 detik.

Jika dibandingkan secara proporsional, maka respons otomatis berpotensi menghemat waktu respons lebih dari 90% dibandingkan dengan penanganan manual. Perbedaan ini divisualisasikan dalam bentuk grafik batang yang membandingkan rentang estimasi waktu respons manual dengan waktu respons otomatis seperti yang terlihat pada Gambar 2 berikut.



Gambar 2. Perbandingan Estimasi MTTR Manual dan Otomatis

Berdasarkan Gambar 2, grafik batang tersebut memperlihatkan perbandingan waktu respons awal antara penanganan manual dan respons otomatis menggunakan sistem SYRA dalam satuan detik. Pada grafik tersebut, waktu respons manual divisualisasikan sebagai rentang estimasi yang merepresentasikan durasi respons berdasarkan kronologi insiden DDoS pada Suara.com, yaitu sekitar 5.400 detik (±90 menit) sejak serangan dimulai hingga kondisi layanan kembali terkendali. Rentang ini digunakan karena tidak tersedianya pencatatan waktu respons awal secara presisi pada penanganan manual, sehingga estimasi dilakukan berdasarkan durasi gangguan layanan yang dilaporkan.

Sebaliknya, waktu respons otomatis pada sistem SYRA ditampilkan sebagai satu nilai rata-rata MTTR sebesar 42,97 detik, yang diperoleh dari hasil pengujian langsung di lingkungan terkontrol. Nilai ini merepresentasikan selang waktu sejak serangan DDoS dijalankan hingga pengguna menerima notifikasi Telegram yang menandakan bahwa alamat IP penyerang telah berhasil diblokir oleh sistem.

Perbedaan yang sangat kontras antara kedua nilai pada grafik menunjukkan bahwa mekanisme respons otomatis mampu memangkas waktu respons awal secara signifikan dibandingkan dengan penanganan manual. Jika dibandingkan secara proporsional, respons otomatis berpotensi menghemat waktu lebih dari 90% dari total durasi gangguan pada penanganan manual. Visualisasi ini menegaskan bahwa keunggulan utama sistem SYRA terletak pada kecepatan dan keterukuran respons awal, yang dicapai melalui otomasi penuh tanpa ketergantungan pada analisis dan pengambilan keputusan manusia.

Copyright © 2026 the author, Page 1267
This Journal is licensed under a Creative Commons Attribution 4.0 International License

TIN: Terapan Informatika Nusantara
Vol 6, No 8, January 2026, page 1261-1269
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i8.8972

3.5 Pembahasan

Hasil penelitian ini mendukung hipotesis bahwa mekanisme respons otomatis berbasis SIEM dan SOAR mampu menghasilkan respons awal yang lebih cepat dan lebih terukur dibandingkan dengan penanganan manual. Perbedaan ini dapat dijelaskan melalui konsep *human-in-the-loop* dan *automation* dalam konteks keamanan siber. Pada penanganan manual, seluruh proses respons sangat bergantung pada kemampuan manusia dalam mendeteksi, menganalisis, dan mengambil keputusan. Dalam kondisi serangan DDoS berskala besar, operator menghadapi tekanan waktu yang tinggi, beban kognitif yang besar, serta risiko kesalahan manusia akibat kelelahan dan kompleksitas informasi.

Sebaliknya, sistem otomatis seperti SYRA menghilangkan ketergantungan tersebut dengan menggantikan proses analisis dan pengambilan keputusan awal menggunakan aturan dan alur kerja sistem. Otomatisasi memungkinkan respons dijalankan segera setelah indikator serangan terdeteksi, tanpa menunggu intervensi manusia. Hal ini menjelaskan mengapa MTTR pada sistem otomatis jauh lebih rendah dan lebih konsisten dibandingkan dengan penanganan manual.

Temuan penelitian ini memperkuat hasil penelitian sebelumnya yang menyatakan bahwa integrasi SIEM dan SOAR mampu menurunkan beban kognitif operator, meminimalkan kesalahan manusia, dan meningkatkan kecepatan respons awal. Dengan demikian, otomatisasi respons tidak hanya memberikan keuntungan dari sisi teknis, tetapi juga dari sisi operasional dan manajerial.

Secara ilmiah, penelitian ini memberikan kontribusi empiris dalam membandingkan respons manual pada insiden nyata dengan respons otomatis dalam lingkungan terkontrol. Secara praktis, hasil penelitian menunjukkan bahwa penerapan sistem respons otomatis seperti SYRA dapat membantu organisasi menjaga ketersediaan layanan digital, mengurangi durasi gangguan, serta meningkatkan kesiapan dalam menghadapi serangan DDoS yang bersifat masif dan berulang.

4. KESIMPULAN

Penelitian ini menyimpulkan bahwa mekanisme respons otomatis berbasis integrasi SIEM dan SOAR pada sistem SYRA mampu memberikan respons awal yang secara signifikan lebih cepat, konsisten, dan terukur dibandingkan dengan penanganan manual pada insiden serangan DDoS. Melalui pendekatan studi komparatif dengan menggunakan MTTR sebagai indikator utama respons awal, hasil pengujian menunjukkan bahwa sistem SYRA dapat mengeksekusi tindakan mitigasi awal secara otomatis dengan nilai MTTR rata-rata sebesar 42,97 detik, sehingga respons dapat dilakukan dalam waktu kurang dari satu menit setelah indikator serangan terdeteksi. Sebaliknya, pada penanganan manual seperti yang terjadi pada insiden DDoS Suara.com, waktu respons awal tidak dapat dihitung secara numerik karena keterbatasan data publik, namun berdasarkan analisis kronologi kejadian dapat disimpulkan bahwa proses identifikasi hingga mitigasi penuh memerlukan durasi yang jauh lebih panjang, yaitu hingga sekitar 90 menit sejak serangan dimulai. Perbedaan ini menunjukkan bahwa keunggulan respons otomatis tidak hanya terletak pada aspek kecepatan, tetapi juga pada keterukuran dan konsistensi proses, di mana respons manual sangat bergantung pada analisis, koordinasi, dan pengambilan keputusan manusia, sedangkan respons otomatis dijalankan berdasarkan aturan dan alur kerja sistem yang telah ditetapkan sebelumnya. Dari sisi implikasi praktis, pencapaian MTTR kurang dari satu menit memiliki arti penting bagi industri media seperti Suara.com, karena mampu meminimalkan durasi gangguan layanan, menjaga ketersediaan akses informasi bagi publik, serta mengurangi potensi kerugian reputasi dan kepercayaan pengguna akibat *downtime* berkepanjangan. Keterbatasan penelitian ini terletak pada perbedaan karakteristik dan skala serangan antara data manual dan data otomatis, serta tidak tersedianya pencatatan waktu respons awal yang rinci pada kasus manual, sehingga perbandingan dilakukan secara relatif dan deskriptif. Oleh karena itu, penelitian selanjutnya disarankan untuk menggunakan data insiden manual dengan pencatatan waktu yang lebih lengkap atau melakukan pengujian terkontrol dengan skenario serangan yang setara agar analisis perbandingan dapat dilakukan secara kuantitatif dan lebih komprehensif.

REFERENCES

Aditya, R., Muhyidin, Y., & Singasatia, D. (2024). Implementasi Security Information And Event Management (SIEM) Untuk Monitoring Keamanan Server Menggunakan Wazuh. *Merkurius: Jurnal Riset Sistem Informasi Dan Teknik Informatika*, *2*(5), 137–144. https://doi.org/https://doi.org/10.61132/merkurius.v2i5.289

Anggraini, I., & Widhiantoro, D. (2025). Mengenal SIEM dan SOAR: Pilar Utama Keamanan Informasi Modern. *Prosiding Seminar Nasional Inovasi Vokasi 2025*, 1166–1174. https://prosiding.pnj.ac.id/index.php/sniv/article/view/4170/2279

Anugrah, M. R., Ramadhan, E., & Sutabri, T. (2025). Serangan Siber dan Dampaknya Terhadap Infrastruktur Digital. *Kohesi: Jurnal Multidisiplin Saintek*, *10*(7). https://doi.org/10.8734/Kohesi.v1i2.365

Aska, M. F., Putta, D. pratama, & Sinambela, C. J. M. (2025). Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital. *Journal of Information and Information Security (JIFORTY)*, *5*(2), 187–200. https://doi.org/https://doi.org/10.31599/fzg80847

Diana, B. A., & Sari, J. A. (2024). Dampak Transformasi Digitalisasi terhadap Perubahan Perilaku Masyarakat Pedesaan. *Jurnal Pemerintahan Dan Politik*, *9*(2), 94. https://doi.org/10.36982/jpg.v9i2.3896

Copyright © 2026 the author, Page 1268
This Journal is licensed under a Creative Commons Attribution 4.0 International License

TIN: Terapan Informatika Nusantara
Vol 6, No 8, January 2026, page 1261-1269
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i8.8972

Dwivedi, S., Rajendran, B., Akshay, P. V., Acha, A., Ampatt, P., & Sudarsan, S. D. (2025). IntelliSOAR: Intelligent Alert Enrichment Using Security Orchestration Automation and Response (SOAR). In R. K. Patil, V. T.; Krishnan, R.; Shyamasundar (Ed.), *Lecture Notes in Computer Science (LNCS)* (pp. 453–462). Springer. https://doi.org/https://doi.org/10.1007/978-3-031-80020-7_27

Edwards, J. (2025). *The Cybersecurity Control Playbook: From Fundamentals to Advanced Strategies* (First). John Wiley & Sons Ltd. https://www.google.co.id/books/edition/The_Cybersecurity_Control_Playbook/UVVQEQAAQBAJ?hl=id&gbpv=1&dq=MTTR+(Mean+Time+to+Respond)+in+cybersecurity&pg=PA274&printsec=frontcover

Fahmi, R. N., Hartono, R., & Anwar, D. S. (2025). Intergrasi Wazuh SIEM dengan Modsecurity dan Virus Total Menggunakan NIST Framerwork untuk Mendeteksi Serangan Website. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(4), 6583. https://doi.org/10.36040/jati.v9i4.13804

Hafiz, M., & Soewito, B. (2022). Information Security Systems Design Using SIEM, SOAR, and Honeypot. *Jurnal Pendidikan Tambusai*, *6*(2), 15527–15541. https://doi.org/https://doi.org/10.31004/jptam.v6i2.4850

Heluka, H. D., & Sulistyo, W. (2023). Perancangan dan Implementasi Security Information and Event Management (SIEM) pada Layanan Virtual Server. *Progresif: Jurnal Ilmiah Komputer*, 912–922. https://doi.org/10.35889/progresif.v19i2.1353

Hnamte, V., Najar, A. A., Nhung-Nguyen, H., Hussain, J., & Sugali, M. N. (2024). DDoS attack detection and mitigation using deep neural network in SDN environment. *Computers & Security*, *138*. https://doi.org/https://doi.org/10.1016/j.cose.2023.103661

Hugo, V., & Proust, M. (2022). Integrating Firewalls with SIEM and SOAR Platforms for Automated Threat Response. *International Journal of Trend in Scientific Research and Development (IJTSRD)*, *6*(3), 2315–2323. https://docs.google.com/viewerng/viewer?url=https://www.ijtsrd.com/papers/ijtsrd49651.pdf

Iswinarno, C. (2025). *Situs Suara.com Kena Serangan Siber, Tidak Bisa Diakses Selama 1,5 Jam*. Suara.Com. https://www.suara.com/news/2025/04/15/202213/situs-suaracom-kena-serangan-siber-tidak-bisa-diakses-selama-15-jam

Karimi, B. I., & Yusuf, A. R. (2025). Kebocoran Datadan Distributed Denial of Service(DDoS)dalam Cloud Computing: Systematic Literature Review. *Integrative Perspectives of Social and Science Journal (IPSSJ)*, *2*(3), 3871–3879. https://ipssj.com/index.php/ojs/article/view/502/469

Khan, W. (2023). Improving Incident Response Times Through Efficient Security Operations Center (SOC) Management: Techniques To Reduce The Mean Time To Detect And Respond (MTTD/MTTR). *International Journal of Core Engineering & Management (IJCEM)*, *7*(6), 115–132. https://ijcem.in/wp-content/uploads/Improving-Incident-Response-Times-Through-Efficient-Security-Operations-Center-Soc-Management-Techniques-To-Reduce-The-Mean-Time-To-Detect-And-Respond.pdf

Martinez, R. (2022). *Incident Response with Threat Intelligence* (First Edit). Packt Publishing. https://books.google.co.id/books?hl=id&lr=&id=BK5wEAAAQBAJ&oi=fnd&pg=PP1&dq=SOAR+n8n&ots=Joeb9M8ntf&sig=GDpcmFCtASyXCIpo-pJHiI0fAaI&redir_esc=y#v=onepage&q=SOAR n8n&f=false

Nakavisute, I., & Sincharoonsak, T. (2025). Optimizing the Automation Process With n8n. *TPM*, *32*(S8), 1786–1793. https://tpmap.org/submission/index.php/tpm/article/view/3011/2249

Nisa, A. R., Wijayanto, A. D., Priana, A. P. J., & Setiawan, A. (2024). Analisis Log Server untuk mendeteksi Serang DDoS pada Keamaan Jaringan di Website. *Journal of Internet and Software Engineering*, *1*(3), 1–17. https://doi.org/https://doi.org/10.47134/pjise.v1i3.2612

Rahman, R., & Odja, G. R. . (2024). Analisis dan Pencegahan Serangan DDoS Pada Jaringan Skala Besar. *Technology Sciences Insights Journal*, *1*(2), 37–43. https://journal.midpublisher.com/index.php/tsij/article/view/73

Syaputra, A. E., Kristiawan, H., Nugroho, A. Y., Apriadi, E. A., Martono, Alamin, Z., Aliyah, Arisandi, D., Siswanto, L., Pramana, H. J., Jufri, M. T., Chandra, N. A., Nugroho, P. A., Dahlan, Setiawan, R., Fitri, N. A., Abdulghani, T., Bustomi, Y., Isminarti, & Saptadi, N. T. S. (2025). *Keamanan Jaringan Komputer*. PT Sada Kurnia Pustaka. https://www.google.co.id/books/edition/Keamanan_Jaringan_Komputer/n69jEQAAQBAJ?hl=id&gbpv=1&dq=Perusahaan+swasta,+lembaga+pendidikan,+hingga+individu&pg=PA44&printsec=frontcover

Zewail, A., Abdulghany, Y., & Samy, M. (2025). Reducing Mean Time To Respond Using Large Language Model-Driven Incident Response with the Aid of Reactively Retrieved Threat Intelligence. *Intelligent Methods, Systems, and Applications (IMSA)*, 322–327. https://doi.org/10.1109/IMSA65733.2025.11167573

Żurawski, S., Chrząszcz, A., Ciekanowski, Z., Pauliuchuk, Y., Pietrzyk, S., & Wyrzykowska, B. (2025). Effectiveness of Information Security Incident Management Systems: Identifying Practices, Challenges and Development Perspectives. *European Research Studies Journal*, *XXVIII*(I), 575–588. https://doi.org/10.35808/ersj/3922

Copyright © 2026 the author, Page 1269
This Journal is licensed under a Creative Commons Attribution 4.0 International License