JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 4, September 2025
ISSN 3025-0919 (media online)
Hal 938-940

Perancangan Aplikasi Auto Mitigasi Berbasis Website untuk Meningkatkan Ketahanan Keamanan Siber

Muhamad Ilham Irvian[1], Riski Ferlianta[2], Sonasa Rinusantoro[3]

[1,2,3]Ilmu Komputer, Teknik Informatika, Universitas Pamulang. Jl. Raya Puspitek, Buaran, Kec. Pamulang, Kota Tangerang Selatan, Banten 15310, (021) 7412566
E-mail: [1]rizkifirly2109@gmail.com, [2]teknikinformatika313@gmail.com

Abstrak− Dalam era digital yang penuh ancaman siber, kebutuhan akan sistem mitigasi risiko yang tanggap dan otomatis menjadi sangat krusial. Penelitian ini bertujuan untuk merancang aplikasi berbasis web yang mampu mendeteksi, memvalidasi, dan merespons ancaman siber secara otomatis. Aplikasi dikembangkan dengan integrasi teknologi seperti Suricata IDS, parser Python, dan auto-patching script. Metodologi yang digunakan adalah SDLC dengan pendekatan simulasi sistem dalam lingkungan uji (sandbox). Hasil pengujian menunjukkan bahwa sistem mampu mengurangi waktu respons insiden dan meningkatkan efisiensi pemantauan insiden secara real-time. Temuan ini diharapkan dapat menjadi solusi strategis dalam meningkatkan ketahanan keamanan digital perusahaan.

Kata Kunci: Mitigasi Otomatis, Keamanan Siber, Suricata, Auto Patch, Web-Based Security

Abstract− *Cybersecurity threats are becoming increasingly complex and demand responsive and adaptive mitigation strategies. This study presents the design and implementation of a web-based auto mitigation application developed to enhance incident response efficiency. The system integrates Suricata IDS for real-time threat detection, Python-based log parsing, and an automated patching engine to handle vulnerabilities. Utilizing a simulation environment, the system was tested using black-box methods and successfully detected and mitigated various attack scenarios. Results indicate that the application can significantly reduce response time, minimize human error, and improve documentation and incident tracking through a centralized dashboard. This solution provides a scalable foundation for enhancing digital resilience within enterprise-level IT infrastructure.*

Keywords*: Cybersecurity, Auto Mitigation, Suricata IDS, Log Analysis, Automated Patching, Web-Based Application*

1. PENDAHULUAN

Revolusi digital telah memperluas lanskap ancaman siber, menjadikan deteksi dan respons cepat terhadap insiden keamanan sebagai kebutuhan mendesak dalam organisasi. PT Sigma Cipta Caraka, yang bergerak dalam bidang layanan TI, memiliki tantangan tersendiri dalam proses mitigasi yang masih manual. Masalah utama yang diidentifikasi antara lain lambatnya waktu tanggap, ketergantungan terhadap personel teknis, serta kurangnya sistem dokumentasi dan pelaporan yang real-time.

Untuk menjawab permasalahan tersebut, perancangan aplikasi auto mitigasi berbasis website dilakukan sebagai solusi yang mampu mengotomatisasi berbagai tahap penanganan insiden. Dengan integrasi sistem deteksi (Suricata IDS), proses validasi signature, serta auto patching berbasis template, diharapkan sistem ini dapat meningkatkan ketahanan digital perusahaan secara keseluruhan.

2. TINJAUAN LITERATUR

Yani *et al.* (2025) merancang model *ICyMI* yang menggabungkan teknologi *AI*, *machine learning*, dan *SIEM* untuk mitigasi otomatis. Sementara Ashidiq *et al.* (2025) menekankan pentingnya sistem keamanan berbasis ISO dan PCI DSS untuk sektor finansial. Tamarell Vimy *et al.* (2022) menyoroti ancaman terhadap keamanan nasional yang timbul akibat lemahnya sistem deteksi siber. Penelitian-penelitian ini menunjukkan bahwa sistem mitigasi berbasis web yang terintegrasi dan responsif dapat menjadi jawaban terhadap tantangan keamanan modern.

Dalam konteks teknologi, penggunaan *Suricata* sebagai *IDS* real-time terbukti mampu menangani berbagai jenis ancaman jaringan. Suricata menghasilkan log *eve.json* yang berisi metadata serangan, yang kemudian dapat diproses menggunakan *Python* untuk menentukan tindakan mitigasi lanjutan.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 4, September 2025
ISSN 3025-0919 (media online)
Hal 938-940

3. METODOLOGI

Penelitian ini mengadopsi metode pengembangan perangkat lunak SDLC (Software Development Life Cycle) dengan tahapan berikut:

1. Observasi dan Analisis Kebutuhan: Dilakukan melalui wawancara dan pemantauan langsung terhadap alur mitigasi.
2. Perancangan Sistem: Melibatkan pembuatan flowchart, use case diagram, dan desain UI/UX.
3. Implementasi: Sistem dikembangkan menggunakan Python (untuk parsing log dan patching otomatis), HTML, CSS, JavaScript (untuk dashboard), serta Suricata sebagai IDS.
4. Pengujian: Menggunakan metode black box terhadap tiap fitur dan skenario ancaman siber.
5. Evaluasi: Menilai efektivitas sistem dalam mendeteksi dan merespons ancaman.

4. HASIL DAN PEMBAHASAN

Aplikasi auto mitigasi berhasil mengintegrasikan beberapa komponen utama, yaitu monitoring log Suricata, validasi signature, auto patching, logging, dan pelaporan. Dalam pengujian simulasi serangan menggunakan bWAPP, sistem mampu:

a. Menangkap ancaman SQL Injection dan XSS dari log eve.json.
b. Memvalidasi pola signature secara lokal.
c. Melakukan patch terhadap file HTML/JS yang terinfeksi.
d. Menampilkan notifikasi insiden dalam dashboard web secara real-time.

4.1. Fitur Utama

Dashboard dirancang agar user-friendly dengan fitur filter, pencarian log, dan klasifikasi insiden berdasarkan tingkat bahaya. Semua aktivitas mitigasi tercatat secara otomatis, lengkap dengan timestamp dan status mitigasi. Uji black box menunjukkan semua modul berfungsi sesuai ekspektasi dengan tingkat error < 5%.

Fitur pelengkap yang turut dikembangkan meliputi:

1. Manajemen aturan (rule management)
2. Laporan serangan (exportable)
3. Statistik ancaman per waktu
4. Logging terintegrasi dan sistem pencatatan historis insiden
5. Simulasi patch ulang terhadap serangan serupa

4.2. Pengujian Sistem

Pengujian dilakukan terhadap empat fitur utama menggunakan metode black box:

1. Login dan Otentikasi: Sistem berhasil membedakan hak akses user dan admin serta mencegah akses tidak sah.
2. Pemantauan Log: Log dari Suricata berhasil dibaca dan dikategorikan dalam berbagai jenis serangan.
3. Mitigasi Ancaman: Serangan yang tervalidasi diproses otomatis dan dilakukan patch sesuai prosedur yang ditetapkan.
4. Pelaporan dan Dokumentasi: Semua kegiatan dicatat dalam sistem log dan dapat diunduh sebagai laporan.

Selain pengujian fungsional, dilakukan juga pengujian performa terhadap sistem. Aplikasi dapat memproses log dengan volume sedang tanpa penurunan performa yang signifikan. Proses auto patch diselesaikan rata-rata dalam waktu 3–4 detik.

Simulasi juga dilakukan terhadap skenario multi-user untuk menguji integritas data saat diakses bersamaan. Hasilnya sistem tetap stabil tanpa konflik akses atau kesalahan pengambilan data.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 4, September 2025
ISSN 3025-0919 (media online)
Hal 938-940

4.3. Relevansi terhadap Lingkungan Industri

Dengan konfigurasi berbasis web dan pengelolaan insiden real-time, sistem ini mampu mendukung proses kerja SOC (Security Operation Center) modern. Fleksibilitas dan skalabilitas sistem juga memungkinkan integrasi dengan sistem SIEM atau database kerentanan nasional seperti CVE/NVD. Dengan dokumentasi otomatis dan fitur pelaporan visual, sistem ini sesuai dengan kebutuhan audit dan compliance industri teknologi.

5. KESIMPULAN

Sistem auto mitigasi berbasis website yang dirancang mampu menjawab permasalahan manualitas dan keterlambatan dalam mitigasi risiko siber di PT Sigma Cipta Caraka. Sistem ini tidak hanya mampu bekerja secara otomatis dan efisien, tetapi juga memberikan transparansi dalam proses mitigasi melalui dashboard yang informatif. Ke depannya, sistem dapat dikembangkan lebih lanjut dengan fitur AI untuk analisis perilaku ancaman dan integrasi dengan sistem keamanan eksternal.

UCAPAN TERIMA KASIH

Kami ucapkan terima kasih juga kepada:

1. Dr. Eng. Ahmad Musyafa, S.Kom., M.Kom. Selaku Kaprodi Teknik Informatika Universitas pamulang
2. SONASA RINUSANTORO S.Kom.,M.A. Selaku Dosen Pembimbing Teknik Informatika Universitas pamulang
3. Deni Purwanto selaku Head of Cyber Security Operation
4. Bagian Prodi Teknik Informatika Universitas Pamulang
5. Semua anggota dan para professional perusahaan PT.Sigma Cipta Caraka (Telkom Sigma)
6. Semua anggota dan para profesional yang terlibat dalam penyusunan laporan kegiatan KP.

REFERENCES

Anisya Caty Praniffa, Syahri, A., & Sandes, F. (2023). Pengujian Blackbox Sistem Informasi. Jurnal TISI

Ashidiq, A. R., Kurniawan, L. D., & Ronaldi. (2025). Kajian Kriminologi: Mitigasi Cyber Security. Jurnal ISO.

Stephani, E., Nova, F., & Asri, E. (2020). Implementasi IDS Suricata. Jurnal Ilmiah TSI.

Tamarell Vimy, Wiranto, S., & Suwarno, P. (2022). Ancaman Serangan Siber pada Keamanan Nasional. Jurnal Kewarganegaraan

Yani, A., Ruseno, N., Irfansyah, D., & Santoso, G. (2025). Strategi Mitigasi Serangan Siber, Data Science, dan Database. Jurnal PASTI.