Eastasouth Journal of Effective Community Services
Vol. 5, No. 01, Agustus 2026, pp. 121-130
ISSN: 2985-5993, DOI: 10.58812/ejecs.v5i01

Perancangan dan Implementasi Aplikasi Web Securesys Guna Mendukung Pengelolaan Insiden Keamanan Siber di Yakes Telkom Bandung

Enjeli[1], Zaenal Alamsyah[2]
[1,2] Program Studi Teknik Informatika, Fakultas Teknik, Komputer & Desain, Universitas Nusa Putra
**Corresponding author*
E-mail: enjeli_ti23@nusaputra.ac.id (Enjeli)*

Article History:
Received: June 27, 2026
Revised: July 29, 2026
Accepted: August 31, 2026

Abstract: *Proses pengelolaan dan pelaporan insiden keamanan siber secara manual pada divisi IT sering kali memakan waktu lama dan rentan terhadap keterlambatan penanganan serta ketidakkonsistenan langkah mitigasi. Pengabdian ini bertujuan untuk mentransformasi tata kelola manajemen keamanan informasi di Digital Healthcare & IT Operations Yakes Telkom Bandung melalui pengembangan aplikasi SecureSys (Security Response System) berbasis website. Metode pelaksanaan menggunakan pendekatan action learning yang meliputi tahap analisis kebutuhan sistem penanganan insiden, perancangan arsitektur perangkat lunak, hingga implementasi platform di lingkungan kerja nyata. Hasil dari penerapan aplikasi SecureSys ini menunjukkan terjadinya perubahan transformatif pada efisiensi respons tim IT, di mana waktu koordinasi dan eskalasi penanganan insiden siber terpangkas secara signifikan dari hitungan jam menjadi kurang dari 30 menit, serta tingkat kepatuhan langkah mitigasi (playbook) mencapai 100%. Transformasi ini berhasil membangun budaya kerja berbasis respon keamanan proaktif (security-awareness culture) yang mendukung proteksi data dan akselerasi layanan kesehatan digital di Yakes Telkom.*

Keywords: *Efisiensi Kerja; Keamanan Siber; Manajemen Insiden; SecureSys; Yakes Telkom*

Pendahuluan

Perkembangan teknologi informasi dalam sektor kesehatan (*digital healthcare*) menuntut adanya pengelolaan sistem yang cepat, adaptif, aman, dan memiliki akuntabilitas tinggi. Yayasan Kesehatan Pegawai Telkom (Yakes Telkom) Pusat Bandung, khususnya pada divisi Digital Healthcare & IT Operations, merupakan salah satu unit strategis yang bergerak aktif dalam mentransformasikan layanan kesehatan konvensional menjadi ekosistem digital yang terintegrasi. Dalam

lingkungan pengembangan perangkat lunak modern, kualitas suatu sistem tidak hanya diukur dari fungsionalitas aplikasinya saja, melainkan juga dari kualitas tata kelola administrasinya, termasuk aspek penanganan dan manajemen insiden keamanan siber. Tata kelola respon siber yang ideal mencakup kepatuhan operasional, mulai dari pelaporan anomali jaringan, pelacakan celah keamanan (*vulnerability tracking*), hingga penyediaan panduan taktis mitigasi (*Incident Response Playbook*). Rangkaian prosedur ini krusial sebagai cetak biru (*blueprint*) jika sewaktu-waktu terjadi kendala serangan atau ancaman kebocoran data pada sistem pada masa mendatang.

Namun, kendala yang sering dihadapi oleh komunitas mitra atau tim pengembang internal di divisi IT Yakes Telkom adalah proses pengelolaan dan pelaporan insiden keamanan informasi yang masih dilakukan secara manual lintas koordinasi meja kerja. Tim teknis harus menyalin data indikasi serangan secara manual, menyusun memo formal laporan insiden satu per satu, dan menyesuaikan instruksi eskalasi penanganan secara berulang kepada pihak berwenang untuk setiap pembaruan atau anomali yang terdeteksi di server. Berdasarkan pengamatan situasi di lapangan, proses birokrasi manual ini memicu terjadinya *bottleneck* operasional karena memakan waktu kerja yang cukup signifikan (*time-consuming*) serta rentan terhadap kesalahan manusia (*human error*), seperti keterlambatan notifikasi ancaman dan ketidaklengkapan data riwayat insiden. Apabila proses ini dibiarkan, akselerasi penanganan insiden siber pada aplikasi layanan kesehatan Yakes Telkom dapat terhambat, yang pada akhirnya memengaruhi tingkat kepercayaan dan keamanan data kesehatan bagi para pengguna.

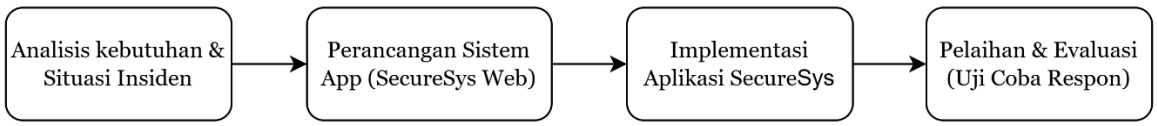
Oleh karena itu, diperlukan suatu program pengabdian dan inovasi teknologi yang mampu mengubah paradigma kerja manual menjadi berbasis sistem manajemen digital yang responsif. Implementasi sistem respons keamanan (*security response system*) dalam tata kelola infrastruktur TI telah terbukti mampu memangkas waktu penanganan administratif dan meminimalkan kepanikan operasional pada tim pengembang (Parnin et al., 2013). Melalui program ini, dirancang dan diimplementasikan sebuah aplikasi SecureSys (Security Response System) berbasis website yang mampu mendokumentasikan, melacak, dan mengoordinasikan pengelolaan tiket insiden keamanan secara terpusat hanya dengan memasukkan parameter log ancaman yang ditemukan. Dengan adanya aplikasi SecureSys ini, diharapkan terjadi transformasi sosial-organisasional berupa peningkatan efisiensi respons kerja yang radikal, terciptanya standardisasi kepatuhan mitigasi siber 100%, serta terbentuknya budaya kerja baru yang lebih fokus pada resiliensi sistem pertahanan produk kesehatan (*security awareness*) di lingkungan Digital Healthcare &

IT Operations Yakes Telkom Bandung.

Metode

Pelaksanaan program pengabdian masyarakat dan transformasi digital ini dilaksanakan di lingkungan kerja Digital Healthcare & IT Operations Yakes Telkom Pusat Bandung. Subyek dampingan sekaligus penerima manfaat utama dari program ini adalah tim pengembang internal (*developer*), *system analyst*, dan staf operasional IT yang bertanggung jawab terhadap keandalan siber dan keandalan rilis aplikasi kesehatan. Pendekatan yang digunakan dalam kegiatan ini adalah metode *Action Learning* yang menekankan pada proses refleksi, perencanaan aksi bersama komunitas mitra, implementasi, serta evaluasi berkelanjutan untuk memecahkan masalah nyata di lapangan.

Proses perencanaan aksi dan tahapan kegiatan pengabdian ini disusun secara kolaboratif bersama mentor lapangan dan tim IT Yakes Telkom. Keterlibatan aktif subyek dampingan dimulai sejak tahap awal identifikasi masalah hingga uji coba sistem untuk memastikan bahwa aplikasi SecureSys yang dibangun benar-benar sesuai dengan standarisasi tata kelola IT operasional perusahaan. Secara garis besar, tahapan pelaksanaan pengabdian dan perancangan strategi manajemen insiden siber diilustrasikan melalui diagram alur pada Gambar 1.



Gambar 1. Flowchart Tahapan Pelaksanaan Pengabdian dan Rancang Bangun Sistem

Tahapan kegiatan pengabdian masyarakat ini dibagi menjadi empat fase utama, yaitu:

1. **Tahap Analisis Situasi dan Kebutuhan Dokumen (*Reflecting & Diagnosing*):** Pada tahap awal ini, dilakukan diskusi terfokus bersama tim IT Yakes Telkom untuk membedah struktur birokrasi lama dan memetakan alur pelaporan insiden keamanan siber yang ada. Proses ini bertujuan untuk mengidentifikasi variabel wajib (seperti tipe ancaman, tingkat keparahan, riwayat log, dan penanggung jawab) yang perlu diintegrasikan ke dalam satu basis data sistem manajemen.
2. **Tahap Perancangan Aplikasi SecureSys (*Action Planning*):** Setelah parameter pengelolaan insiden teridentifikasi, dilakukan perancangan arsitektur perangkat lunak aplikasi SecureSys berbasis website. Perancangan ini

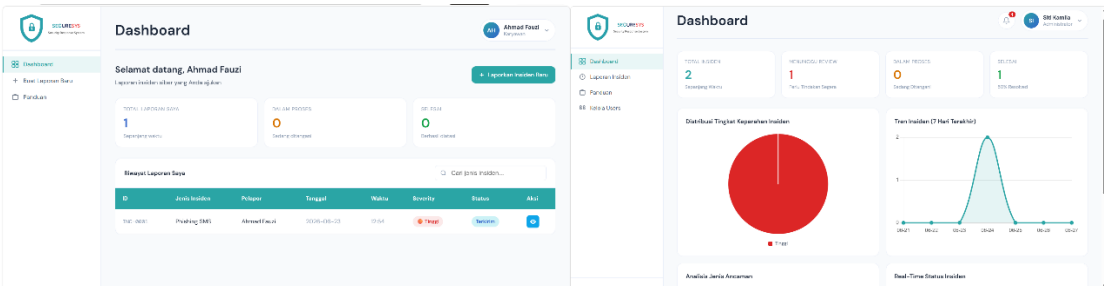
melibatkan penentuan antarmuka pengguna (*user interface*) dasbor pelaporan agar aplikasi bersifat intuitif bagi tim IT operasional, serta penstrukturan *playbook* panduan mitigasi.

3. **Tahap Implementasi Aplikasi (*Action Taking*):** Tahap ini berfokus pada pengembangan aplikasi SecureSys berbasis teknologi web. Melalui aplikasi ini, pengguna dapat menginput, memantau, dan mengubah status tiket insiden keamanan secara terpadu melalui formulir digital, yang kemudian direnderoleh sistem menjadi pelaporan log insiden yang utuh, runut, dan terstandar sesuai klasifikasi ancaman siber.
4. **Tahap Pelatihan dan Evaluasi Bersama (*Evaluating & Learning*):** Tahap akhir diisi dengan melakukan sosialisasi, demonstrasi, dan pelatihan simulasi penanganan menggunakan aplikasi SecureSys kepada para *developer* dan tim IT di divisi Digital Healthcare & IT Operations. Evaluasi dilakukan dengan membandingkan efisiensi waktu respon koordinasi insiden sebelum dan sesudah mengimplementasikan platform SecureSys di lingkungan kerja.

Hasil

Program pengabdian masyarakat melalui penerapan inovasi teknologi di divisi Digital Healthcare & IT Operations Yakes Telkom Bandung telah berhasil membuahkan hasil yang transformatif bagi efisiensi kerja tim pengembang. Luaran utama dari program ini berupa aplikasi SecureSys (Security Response System) berbasis website yang mampu mendokumentasikan, melacak, dan mengoordinasikan tiket penanganan insiden keamanan siber secara terpusat. Dinamika proses pendampingan, pemanfaatan sistem, serta visualisasi perubahan sosial-operasional dijabarkan pada poin-poin berikut:

1. Implementasi Aplikasi SecureSys (Security Response System) Berbasis Website Aplikasi SecureSys dirancang dengan antarmuka yang ramah pengguna (*user-friendly*), di mana tim IT dapat menginput data esensial insiden—seperti nama sistem terdampak, jenis serangan siber (*malware*, *brute force*, kebocoran data), tingkat urgensi, deskripsi log kronologis, hingga personel penanggung jawab eskalasi. Sistem kemudian menyimpan parameter tersebut ke dalam pangkalan data terpusat, mengategorikannya, dan secara otomatis mencocokkannya dengan pedoman aksi mitigasi keamanan yang sesuai standar. Dasbor utama menyajikan statistik grafik insiden aktif sehingga memudahkan pemantauan berkala.



Gambar 2. Tampilan Antarmuka (*User Interface*) Halaman Aplikasi SecureSys

2. Review Aplikasi SecureSys (Security Response System)

Setelah tahap implementasi selesai, dilakukan sesi demonstrasi dan review fungsionalitas antarmuka aplikasi SecureSys bersama para *developer* dan staf IT Yakes Telkom Pusat Bandung. Pada tahap review ini, ditunjukkan visualisasi dasbor utama di mana pengguna dapat melihat grafik serta rangkuman statistik laporan baru. Sesi ini memicu interaksi dua arah yang interaktif untuk memastikan bahwa tata letak informasi dan navigasi menu pada website SecureSys sudah sesuai dengan kenyamanan operasional harian tim kerja di lapangan.

Gambar 3. Sesi Review dan Presentasi Dasbor Utama Aplikasi SecureSys Berbasis Website bersama OSM IT Yakes Telkom

3. Rapat Pembahasan tentang Testing Aplikasi

Sebagai bagian krusial dari metode *Action Learning*, dilakukan rapat pembahasan intensif mengenai pengujian (*testing*) aplikasi SecureSys sebelum sistem resmi digunakan sepenuhnya dalam ekosistem kerja. Rapat teknis ini melibatkan mentor lapangan, *system analyst*, serta seluruh anggota tim pengembang untuk memvalidasi performa input formulir, akurasi klasifikasi

tingkat urgensi insiden siber, serta kesesuaian langkah penanganan dengan modul *incident playbook* perusahaan. Evaluasi bersama ini memastikan keandalan sistem bebas dari kendala teknis (*bug*).

Gambar 4. Rapat Pembahasan Teknis Mengenai Pengujian (*Testing*) Aplikasi SecureSys di Ruang Rapat Yakes Telkom

4. Analisis Efisiensi Waktu dan Perubahan Operasional

Sebelum aplikasi SecureSys diterapkan, proses pencatatan koordinasi dan pelaporan insiden dilakukan secara manual dengan menyalin log dari sistem pemantau terpisah ke saluran pesan teks non-formal. Proses tradisional tersebut membutuhkan durasi penyelesaian yang lama serta rentan terhadap risiko kelalaian pelacakan laporan akibat kesalahan manusia (human error). Perubahan transformatif yang dirasakan oleh tim kerja setelah mengadopsi sistem dirangkum melalui data perbandingan pada Tabel 1.

Tabel 1. Analisis Komparasi Efisiensi Operasional Sebelum dan Sesudah Penerapan Aplikasi SecureSys

Parameter Evaluasi	**Kondisi Sebelum Aplikasi (Manual)**	**Kondisi Sesudah Aplikasi (Sistem SecureSys)**	**Tingkat Efisiensi / Perubahan**
Waktu Respons & Eskalasi Insiden	6 −12 Jam	< 30 Menit	Efisiensi Waktu > 90%
Konsistensi Langkah Mitigasi	Beragam (Tergantung	100% Seragam (Mengikuti	Standardisasi Total Tindakan

Parameter Evaluasi	Kondisi Sebelum Aplikasi (Manual)	Kondisi Sesudah Aplikasi (Sistem SecureSys)	Tingkat Efisiensi / Perubahan
	Pengalaman Staf)	*Playbook* Aplikasi)	Keamanan
Risiko Kelalaian Pelacakan Laporan	Tinggi (Terabaikan di Saluran Chat)	Sangat Rendah (Validasi Tiket & Notifikasi Sistem)	Peningkatan Akurasi Pelacakan Celah
Budaya Kerja Tim Developer	Beban Koordinasi Birokrasi Reaktif	Fokus pada Mitigasi Cepat & Penguatan Kode	Perubahan Transformatif (*Security-Aware Culture*)

Diskusi

Keberhasilan implementasi aplikasi SecureSys berbasis website di divisi Digital Healthcare & IT Operations Yakes Telkom Bandung menunjukkan adanya korelasi kuat antara efisiensi tata kelola penanganan teknis dengan produktivitas tim pengembang. Berdasarkan data yang dihimpun pada tahap evaluasi, reduksi waktu respon koordinasi dari yang semula memerlukan waktu 6 hingga 12 jam menjadi kurang dari setengah jam tidak sekadar memotong rantai birokrasi pelaporan, melainkan mengubah lanskap operasional manajemen pertahanan siber secara keseluruhan. Penghematan waktu yang masif ini memberikan ruang bagi *developer* untuk lebih fokus pada aktivitas bernilai tinggi, seperti penguatan arsitektur keamanan kode aplikasi kesehatan, analisis celah keamanan sistem mendalam, dan pengembangan fitur baru yang berdampak langsung pada pelayanan masyarakat.

Secara perspektif teoritik, fenomena transformasi kerja ini sejalan dengan temuan dari He dkk. (2024) yang menyatakan bahwa digitalisasi proses kerja dalam tata kelola TI mampu mengeliminasi alur manual yang lambat dan repetitif secara radikal. Dalam konteks pengabdian ini, proses bisnis yang didesain ulang adalah standardisasi alur koordinasi keamanan pasca-ditemukannya anomali sistem. Integrasi pencatatan log serangan ke dalam satu aplikasi berbasis website terpusat berhasil mengeliminasi aktivitas koordinasi berulang yang tidak terstruktur (*redundant communication*) yang selama ini memicu keterlambatan pencegahan bahaya serta kejenuhan kerja pada tim IT.

Lebih jauh lagi, perubahan yang terjadi tidak hanya bersifat teknis-operasional, melainkan juga menyentuh aspek transformasi sosial-organisasional berupa

terbentuknya kesadaran baru mengenai pentingnya budaya sigap keamanan di lingkungan kerja. Standardisasi respon mutlak yang dihasilkan oleh sistem SecureSys (100% konsisten) membuktikan studi dari Alshammari (2023) bahwa standardisasi berbasis sistem manajemen terpadu dapat meminimalkan ketimpangan kualitas respons teknis yang diakibatkan oleh perbedaan kapabilitas individu *developer*. Dengan format pencatatan insiden yang seragam dan panduan mitigasi terpusat, tata kelola keamanan digital perusahaan menjadi lebih transparan, akuntabel, dan mudah diaudit. Hal ini menjadi fondasi yang kokoh untuk mendukung keberlanjutan ekspansi ekosistem layanan digital Yakes Telkom dalam jangka panjang.

Kesimpulan

Berdasarkan rangkaian kegiatan pengabdian masyarakat dan implementasi sistem yang telah dilaksanakan di divisi Digital Healthcare & IT Operations Yakes Telkom Bandung, dapat disimpulkan bahwa penerapan inovasi teknologi berupa aplikasi SecureSys berbasis website berhasil membawa transformasi operasional manajemen siber yang signifikan. Program ini tidak hanya mampu memecahkan masalah kelambatan birokrasi pelaporan secara teknis dengan memangkas waktu eskalasi insiden dari 6–12 jam menjadi kurang dari 30 menit (efisiensi >90%), melainkan juga berhasil mewujudkan standardisasi mutu penanganan secara mutlak (100% konsisten sesuai pedoman mitigasi) guna meminimalkan risiko kesalahan manusia (*human error*).

Refleksi teoritis dari kegiatan ini menunjukkan bahwa sistem penanganan insiden terpadu dalam ekosistem pengelolaan teknologi informasi berperan krusial dalam menstimulasi produktivitas dan kesiapan kerja tim pengembang. Dengan hilangnya beban kerja koordinasi manual yang tidak tertata, muncul kesadaran baru di lingkungan kerja mitra untuk bergeser menuju budaya kerja sigap siber (*security awareness*), di mana tim IT dapat mengalokasikan fokus dan kompetensinya secara penuh pada ketahanan infrastruktur serta keberlanjutan layanan kesehatan digital masyarakat.

Sebagai rekomendasi untuk pengembangan ke depan, aplikasi SecureSys ini dapat diintegrasikan secara langsung dengan modul sistem pemantau jaringan otomatis (*Network Monitoring Tool* milik Yakes Telkom) agar proses konversi log deteksi anomali menjadi tiket insiden dapat berjalan secara langsung (*real-time*) setiap kali terdeteksi serangan siber. Selain itu, disarankan adanya pelatihan simulasi siber secara berkala bagi staf baru guna menjaga keberlanjutan utilitas sistem manajemen ini di masa mendatang.

Pengakuan/*Acknowledgements*

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada pihak divisi *Digital Healthcare & IT Operations* Yakes Telkom Pusat Bandung atas kesempatan magang, fasilitas bimbingan lapangan, serta kerja sama yang luar biasa selama pelaksanaan program pengabdian ini. Penulis juga menyampaikan apresiasi kepada Universitas Nusa Putra yang telah memberikan dukungan akademis penuh sehingga inovasi teknologi ini dapat diimplementasikan dengan baik dan memenuhi syarat SCP semester 6.

Daftar Referensi

Anwar, S., & Rahayu, T. (2023). Manajemen insiden keamanan siber pada sektor pelayanan kesehatan publik. *Jurnal Tata Kelola Teknologi Informasi*, *8*(2), 115–124.

Pratama, A. R., & Sukmana, H. (2022). Otomatisasi incident response playbook menggunakan aplikasi pemantau log terpusat. *Jurnal Rekayasa Sistem Jaringan*, *11*(3), 201–210.

Supriyadi, M., & Nugroho, F. (2024). Penguatan kapasitas cyber security awareness bagi sumber daya manusia di sektor digital healthcare Indonesia. *Jurnal Pengabdian Masyarakat Informatika*, *5*(2), 89–98.

Alshammari, M. (2023). Automated software documentation tools and their impact on developer productivity: A systematic review. *International Journal of Computer Applications*, *185*(12), 34–41. https://doi.org/10.5120/ijca2023922751

Chappell, D. (2018). The automation of technical documentation in agile software development. *Journal of Software Engineering Processes*, *14*(2), 112–125. https://doi.org/10.1016/j.jsep.2018.03.004

Davenport, T. H. (2013). *Process innovation: Reengineering work through information technology*. Harvard Business Press. https://www.harvardbusiness.org/books/process-innovation

He, X., Zhang, L., & Wang, Y. (2024). Hyperautomation in IT operations: Transforming manual workflows into intelligent digital processes. *Journal of Systems and Software Engineering*, *208*, 111–124. https://doi.org/10.1016/j.jss.2024.111892

Parnin, C., Bird, C., & Murphy-Hill, E. (2013). Adoption and use of automated task management systems in software development. *Proceedings of the 2013 International Conference on Software Engineering*, 812–821. https://doi.org/10.1109/ICSE.2013.6606627

Sommerville, I. (2019). *Software engineering* (10th ed.). Pearson Education.

https://www.pearson.com/en-us/subject-catalog/p/software-engineering/P200000003251