OPTIMALISASI PROSES KEAMANAN PROAKTIF MELALUI HUB MANAJEMEN MULTI-WAZUH TERINTEGRASI *THREAT INTELLIGENCE* DAN NOTIFIKASI *REAL-TIME*

SKRIPSI

CHRISTIAN NATANIEL YOSUA PURBA
NIM 2207421043

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
TAHUN 2026

OPTIMALISASI PROSES KEAMANAN PROAKTIF MELALUI HUB MANAJEMEN MULTI-WAZUH TERINTEGRASI *THREAT INTELLIGENCE* DAN NOTIFIKASI *REAL-TIME*

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

CHRISTIAN NATANIEL YOSUA PURBA
NIM 2207421043

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
TAHUN 2026

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Christian Nataniel Yosua Purba

NIM : 2207421043

Jurusan/ProgramStudi : T.Informatika dan Komputer / T. Multimedia dan Jaringan

Judul skripsi : OPTIMALISASI PROSES KEAMANAN PROAKTIF MELALUI HUB MANAJEMEN MULTI-WAZUH TERINTEGRASI THREAT INTELLIGENCE DAN NOTIFIKASI REAL-TIME

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 8 Juni, 2026

Yang membuat pernyataan

(Christian Nataniel Yosua Purba)

NIM. 2207421043

LEMBAR PENGESAHAN

Skripsi diajukan oleh :
Nama : Christian Nataniel Yosua Purba
NIM : 2207421043
Program Studi : TMJ
Judul Skripsi : OPTIMALISASI PROSES KEAMANAN PROAKTIF MELALUI HUB MANAJEMEN MULTI-WAZUH TERINTEGRASI *THREAT INTELLIGENCE* DAN NOTIFIKASI *REAL-TIME*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Senin Tanggal 22 Bulan Juni Tahun 2026 dan dinyatakan **LULUS**.

Disahkan oleh:

Pembimbing I : Ayu Rosyida Zain, S.ST., M.T ( )

Penguji I : Dr. Defiana Arnaldy, S.Tp., M.Si. ( )

Penguji II : Iik Muhamad Malik Matin, S.Kom., M.T. ( )

Penguji III : Andika Riyadi Jasril, S.Pd., M.Pd.T ( )

Mengetahui:
Jurusan Teknik Informatika dan Komputer
Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003

KATA PENGANTAR

Puji syukur kepada Tuhan Yesus Kristus karena hanya oleh anugerah dan kasih sayang-Nya penulis dapat melaksanakan perkuliahan dengan baik dan sampai kepada penyelesaian penulisan Skripsi yang berjudul "Optimalisasi Proses Keamanan Proaktif melalui Hub Manajemen Multi-Wazuh Terintegrasi *Threat Intelligence* dan Notifikasi *Real-Time*". Skripsi ini disusun sebagai salah satu syarat untuk meraih gelar Sarjana Terapan pada Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta.

Penulis menyadari bahwa perjalanan panjang dalam menyusun penelitian ini bukanlah jalan yang mudah untuk dilalui sendiri. Terdapat banyak doa, bimbingan, pengorbanan, dan dukungan tanpa henti dari berbagai pihak yang memampukan penulis untuk tiba di titik ini. Oleh karena itu, dengan kerendahan hati penulis ingin menyampaikan rasa terima kasih yang mendalam kepada:

1. Almh. Ibunda tercinta, sosok luar biasa yang telah membentuk karakter penulis, dan yang kasih sayangnya terus mengalir menjadi kekuatan yang mengiringi langkah penulis hingga akhir hayat.
2. Keluarga besar penulis, secara khusus Opung, Tante, dan Tulang serta Bapak yang senantiasa mendoakan dan memberikan dukungan yang luar biasa, sehingga memungkinkan penulis untuk memiliki kesempatan menempuh pendidikan hingga di bangku perkuliahan ini.
3. Ibu Ayu Rosyida Zain, S.ST., M.T., selaku dosen pembimbing yang telah mendedikasikan waktu, tenaga, serta kesabarannya untuk memberikan arahan dan masukan yang sangat berharga selama proses penyusunan skripsi ini.
4. Rekan seperjuangan kuliah, kerja dan skripsi, Pratama dan Abian. Terima kasih untuk segala suka dan duka, serta momen ramai maupun sepi yang kita lewati bersama demi menyelesaikan sistem dan penelitian ini hingga tuntas.

5. Rekan-rekan PBL Group lainnya, yaitu Azzuri, Ayu, Caca, Izza, dan Rei karena tanpa kehadiran dan kebersamaan kalian, perjalanan perkuliahan penulis tidak akan seberwarna dan sebermakna ini.
6. Teman-teman seiman dalam Connect Group, POSA PNJ, dan PBI Kartini, yang tidak dapat disebutkan satu per satu, atas setiap doa, penguatan rohani, dan kehangatan persaudaraan yang terus menguatkan penulis.
7. Seluruh teman-teman seperjuangan Teknik Multimedia dan Jaringan angkatan 2022 (TMJ 22), atas kebersamaan dan kenangan indah selama menempuh pendidikan di Politeknik Negeri Jakarta.

Penulis menyadari bahwa Skripsi ini masih memiliki kekurangan dan jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi penyempurnaan ke depannya. Akhir kata, semoga penelitian ini dapat memberikan manfaat nyata bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan siber.

Depok, 8 Juni 2026

Christian Nataniel Yosua Purba

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini

Nama : Christian Nataniel Yosua Purba

NIM : 2207421043

Jurusan/ProgramStudi : T.Informatika dan Komputer / T. Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan , menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul :

OPTIMALISASI PROSES KEAMANAN PROAKTIF MELALUI HUB MANAJEMEN MULTI-WAZUH TERINTEGRASI THREAT INTELLIGENCE DAN NOTIFIKASI REAL-TIME

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 08 Juni 2026

Yang menyatakan

Christian Nataniel Yosua Purba

OPTIMALISASI PROSES KEAMANAN PROAKTIF MELALUI HUB MANAJEMEN MULTI-WAZUH TERINTEGRASI *THREAT INTELLIGENCE* DAN NOTIFIKASI *REAL-TIME*

ABSTRAK

Security Operations Center (SOC) menghadapi tantangan penyempitan breakout time akibat fragmentasi infrastruktur keamanan dan tingginya beban kognitif analis dari perpindahan konteks (context-switching) saat investigasi manual. Penelitian ini bertujuan untuk mengoptimalkan proses keamanan proaktif melalui rancang bangun Hub Manajemen Terpusat berbasis arsitektur cache-database (PostgreSQL dan Redis). Sistem ini mengintegrasikan komponen multi-Wazuh sebagai Single Source of Truth (SSOT), layanan Threat Intelligence (AlienVault OTX) secara asinkron, dan modul background scheduler (Sentinel) untuk notifikasi real-time via Telegram. Metode penelitian menggunakan System Engineering dengan pendekatan eksperimental kuantitatif. Pengujian fungsional Black Box dan non-fungsional memastikan sistem tangguh dalam menangani anomali jaringan dan mengamankan kredensial dengan enkripsi AES. Hasil pengujian efisiensi operasional membuktikan bahwa sistem usulan mampu mentransformasi pemantauan pasif menjadi proaktif. Evaluasi komparatif menunjukkan bahwa Hub Manajemen ini berhasil memangkas rata-rata waktu operasional sebesar 58,33% dan mereduksi beban interaksi analis sebesar 52,0%. Kesimpulannya, sistem ini sukses mengeliminasi redundansi kerja manual dan mengakselerasi respons investigasi SOC secara signifikan.

Kata kunci: AlienVault, cache-database, notifikasi real-time, Redis, SOAR, threat intelligence, Wazuh.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan digital yang memperluas konektivitas secara bersamaan juga memperlebar ruang serang siber. Sebagaimana ditegaskan oleh World Economic Forum (2025), "*As our digital footprints widen, so does the potential attack surface for nefarious actors.*" Di Indonesia, urgensi ini tercermin dalam lanskap keamanan siber yang mencatat total trafik anomali selama tahun 2024 mencapai 330.527.636 anomali (BSSN, 2024). Tren ini belum menunjukkan tanda-tanda penurunan di tahun 2025, di mana semester pertama saja telah mencatat lebih dari 133 juta serangan digital (AwanPintar.id, 2025).

Di tengah permasalahan ini, kecepatan respons insiden menjadi faktor yang sangat penting dalam meminimalkan dampak serangan. Hal ini berkaitan erat dengan konsep *breakout time*, yakni waktu yang dibutuhkan penyerang untuk bergerak secara lateral dari satu sistem yang terbobol ke bagian lain. Berdasarkan laporan CrowdStrike (2023), rata-rata *breakout time* berada pada angka 79 menit, kemudian menyusut drastis menjadi 62 menit pada 2024 dan terus menurun hingga tersisa 48 menit pada 2025 (CrowdStrike, 2024; 2025). Dari data ini jelas bahwa organisasi kini berpacu dalam hitungan menit untuk mencegah kerusakan sistemik.

Guna menghadapi jendela waktu yang semakin sempit tersebut, organisasi mengandalkan *Security Operations Center* (SOC) yang mengintegrasikan proses, teknologi, dan sumber daya manusia. Struktur SOC yang mumpuni sangat krusial dalam menciptakan *situational awareness*, memitigasi risiko yang terpapar (*exposed risks*), serta membantu organisasi memenuhi persyaratan regulasi yang berlaku (Vielberth et al., 2020). Namun, pendekatan reaktif tradisional yang hanya berfokus pada penanganan insiden setelah serangan terjadi terbukti tidak lagi memadai. Menurut Ofoegbu et al. (2024), terdapat kebutuhan mendesak untuk bergeser menuju strategi keamanan siber proaktif yang menekankan pada antisipasi dan mitigasi ancaman sebelum dampak serangan meluas ke operasional organisasi. Paradigma ini menuntut kemampuan deteksi proaktif yang berfokus

pada prediksi dan pencegahan melalui pemanfaatan teknik canggih serta integrasi teknologi yang berkelanjutan (Abiade, 2024).

Dengan banyaknya tugas yang ingin dicapai dalam waktu cepat, muncul sebuah pertanyaan kritis: apakah penambahan alat berbanding lurus dengan peningkatan kualitas pertahanan? Studi IBM dan Ponemon (2020) mengindikasikan bahwa perusahaan rata-rata menggunakan 45 perangkat keamanan yang berbeda. Ironisnya, studi yang sama mencatat organisasi yang dengan lebih dari 50 perangkat keamanan justru melaporkan tingkat kepercayaan yang lebih rendah dalam kemampuan deteksi dan respons mereka.

Kondisi banyaknya perangkat yang tidak terintegrasi ini memaksa analis melakukan korelasi informasi secara manual lintas sistem, sebuah proses yang memicu beban kognitif tinggi secara terus-menerus yang disebut dengan *context-switching*. Baruwal Chhetri et al. (2024) menegaskan bahwa volume peringatan yang membanjir tanpa korelasi dan konteks memadai menghambat proses pengambilan keputusan yang efektif saat terjadi serangan. Dampak dari fragmentasi ini divalidasi oleh penelitian Arif et al. (2025) yang menyimpulkan bahwa arsitektur yang terpecah-pecah berkontribusi langsung pada inefisiensi operasional dan eskalasi risiko keamanan. Penelitian tersebut secara eksplisit menyatakan urgensi pengembangan solusi yang terkonsolidasi dan berpusat pada pengguna (*user-centric*) guna mengatasi permasalahan ini.

Tantangan industri tersebut tercermin secara empiris di perusahaan yang dalam penelitian ini selanjutnya dianonimkan sebagai PT. XYZ, di mana eskalasi infrastruktur *data center* memunculkan rantai hambatan operasional bagi tim SOC meskipun telah mengadopsi Wazuh. Kompleksitas ini memicu empat masalah krusial: (1) fragmentasi operasional akibat arsitektur terdistribusi yang memaksa administrator melakukan navigasi manual berulang ke berbagai *dashboard* untuk memantau ratusan agen; (2) inefisiensi tata kelola kredensial karena ketiadaan *Single Source of Truth* (SSOT) yang menyebabkan data kredensial tidak terpusat dan perubahannya tak terlacak (*untracked*); (3) kesenjangan kontekstual (*contextual gap*) akibat absennya integrasi *Cyber Threat Intelligence* (CTI), sehingga analis harus melakukan *context-switching* untuk verifikasi manual; serta (4) visibilitas pasif tanpa notifikasi *real-time* yang menciptakan *blind spot* saat

sistem mengalami *downtime*. Rangkaian kendala ini mengakibatkan alur kerja pertahanan berjalan dalam kondisi suboptimal, di mana sumber daya analis terkuras untuk proses administratif manual alih-alih berfokus pada analisis strategis, yang secara langsung menurunkan kecepatan respon terhadap ancaman.

Menjawab tantangan di PT. XYZ, penelitian ini berfokus pada pembangunan arsitektur dasar bagi ekosistem SOAR (*Security Orchestration*, *Automation*, and *Response*) di PT. XYZ. Dengan mengembangkan modul manajemen Wazuh terpusat, sistem notifikasi *real-time*, dan integrasi *Threat Intelligence*, sistem ini berfungsi sebagai "saraf pusat" yang mengintegrasikan langkah-langkah manual ke dalam satu alur kerja terpadu. Infrastruktur ini menjadi elemen fundamental yang melandasi penelitian lanjutan dalam kelompok riset, termasuk pengembangan dasbor *filtering* log terpusat dan modul otomasi respons (*autoblocking*) pada sistem multi-*firewall*.

Untuk menjamin operasional dengan integritas dan performa tinggi, sistem ini dirancang dengan standar *Online Transaction Processing* (OLTP). Arsitektur ini mengandalkan pola *cache-database* menggunakan PostgreSQL sebagai SSOT untuk menjamin *system of record* yang aman melalui fitur kontrol akses dan enkripsi (Singh, 2015), serta Redis sebagai lapisan *cache in-memory* untuk memastikan responsivitas sistem dalam menangani aliran kueri CTI dari *AlienVault* OTX dan notifikasi Telegram secara instan.

Berdasarkan pendekatan tersebut, penelitian ini mengangkat judul "Optimalisasi Proses Keamanan Proaktif melalui Hub Manajemen Terpusat Multi-Wazuh Terintegrasi *Threat Intelligence* dan *Notifikasi Real-Time*" Implementasi ini diharapkan dapat mentransformasi postur pemantauan keamanan PT. XYZ dari yang bersifat tersebar, pasif, dan manual menjadi terpusat, kontekstual, dan proaktif dengan mengeliminasi langkah-langkah manual yang redundan sehingga lebih optimal.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang sudah dijabarkan di atas, maka rumusan masalah yang dijadikan fokus pada penelitian ini adalah:

1. Bagaimana merancang bangun Hub Manajemen terpusat sebagai *Single Source of Truth* (SSOT) untuk komponen multi-Wazuh guna mengatasi fragmentasi operasional dan risiko tata kelola kredensial?
2. Bagaimana mengimplementasikan *Threat Intelligence* dan sistem notifikasi *real-time* untuk menutup celah visibilitas (*blind spot*)?
3. Bagaimana mengintegrasikan hub manajemen terpusat dan *threat intelligence* dalam satu platform terpadu guna mengurangi langkah manual dan mengoptimalkan proses pemantauan keamanan proaktif?

1.3 Batasan Masalah

Agar penelitian ini tetap fokus dan terarah pada tujuan yang ingin dicapai, maka penulis menetapkan batasan-batasan masalah sebagai berikut:

1. Pengembangan sistem difokuskan pada manajemen inventaris dan pemantauan status komponen multi-Wazuh (*Manager* & *Indexer*) secara terpusat beserta informasi Wazuh *Agent*. Penelitian ini tidak mencakup analisis mendalam isi log, *filtering alert*, atau modifikasi komponen.
2. Integrasi komponen dilakukan dengan memanfaatkan *Application* Programming *Interface* (API) yang disediakan oleh Wazuh, Telegram dan *AlienVault*.
3. Mekanisme notifikasi *real-time* diimplementasikan menggunakan platform Telegram secara satu-arah dan dibatasi pada penyampaian peringatan kondisi operasional sistem.
4. Pengayaan informasi (*enrichment*) menggunakan sumber *open source*, yang secara spesifik dibatasi pada penggunaan *AlienVault* OTX.
5. Evaluasi sistem berfokus pada pengukuran efisiensi operasional (reduksi jumlah langkah kerja dan percepatan waktu akses informasi). Penelitian ini tidak mencakup pengukuran akurasi aturan deteksi (*detection rate*) atau analisis tingkat *false positive*.

6. Sistem dirancang sebagai aplikasi berbasis web yang berfungsi sebagai antarmuka manajemen administratif (*administrative hub*), bukan sebagai pengganti penuh dasbor visualisasi data historis untuk analisis forensik mendalam.

1.4 Tujuan dan Manfaat

Adapun tujuan yang hendak dicapai melalui penelitian ini meliputi:

1. Merancang bangun sistem manajemen komponen multi-Wazuh terpusat berbasis OLTP dengan arsitektur *cache-database* menggunakan PostgreSQL dan Redis.
2. Mengimplementasikan modul pengayaan informasi melalui integrasi API *Threat Intelligence* (*AlienVault* OTX) serta notifikasi *real-time* berbasis Telegram sebagai mekanisme peringatan dini guna menutup celah visibilitas (*blind spot*) sistem.
3. Mereduksi jumlah langkah operasional yang dibutuhkan dan mempercepat proses dalam workflow tim keamanan.

Berdasarkan tujuan yang telah dirumuskan, penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Memangkas waktu yang dibutuhkan tim keamanan dalam mendeteksi dan memvalidasi insiden dengan mengeliminasi langkah-langkah manual (*context-switching*) yang berulang, sehingga membantu organisasi mengejar target waktu respon (*breakout time*) yang optimal.
2. Memberikan referensi akademik mengenai penerapan pola arsitektur *cache-database* (menggunakan PostgreSQL dan Redis) dalam membangun sistem manajemen keamanan siber berkinerja tinggi (*High-Performance Security Management*).
3. Memberikan visibilitas menyeluruh dan konteks ancaman secara instan kepada analis, sehingga meningkatkan kesadaran situasi (*situational awareness*) tanpa perlu melakukan korelasi data manual.

4. Memitigasi risiko keamanan internal melalui sentralisasi manajemen kredensial (*Single Source of Truth*), memastikan setiap komponen keamanan terdata dan terkontrol dengan baik.
5. Menyediakan infrastruktur dasar yang stabil dan terintegrasi bagi pengembangan fitur keamanan lanjutan, seperti otomasi respons (*autoblocking*) dan analisis log terpusat dalam peta jalan pengembangan SOAR perusahaan.

1.5 Sistematika Penulisan

Berikut adalah sistematika penulisan yang digunakan dalam penyusunan penelitian ini

1. BAB I PENDAHULUAN

   Bab ini memaparkan latar belakang yang mendasari penelitian, rumusan masalah, serta batasan masalah agar pembahasan tetap terfokus. Selain itu, dijelaskan pula tujuan dan manfaat yang diharapkan dari penelitian ini.
2. BAB II TINJAUAN PUSTAKA

   Bab ini menyajikan landasan teori dan konsep-konsep yang digunakan untuk menganalisis masalah. Di dalamnya juga termuat kajian terhadap penelitian-penelitian terdahulu yang relevan sebagai referensi pendukung.
3. BAB III METODE PENELITIAN

   Bab ini merincikan metodologi yang diterapkan, mencakup desain dan tahapan penelitian, objek serta model yang digunakan, teknik pengumpulan dan analisis data, hingga jadwal pelaksanaan penelitian.
4. BAB IV HASIL DAN PEMBAHASAN

   Bab ini menguraikan hasil penelitian secara teknis, mulai dari analisis kebutuhan, perancangan dan implementasi sistem, pengujian sistem, hingga analisis terhadap efektivitas sistem yang dibangun.
5. BAB V PENUTUP

   Bab terakhir ini berisi kesimpulan yang diperoleh dari seluruh rangkaian penelitian serta saran-saran konstruktif untuk pengembangan penelitian selanjutnya.

BAB V
PENUTUP

5.1. Simpulan

Penelitian ini menghasilkan sebuah Hub Manajemen Terpusat yang mengintegrasikan pengelolaan infrastruktur multi-Wazuh, pengayaan *Threat Intelligence*, dan notifikasi status sistem ke dalam satu platform. Untuk mendukung pengelolaan data, sistem memanfaatkan PostgreSQL sebagai pusat penyimpanan konfigurasi (*Single Source of Truth*) dengan mekanisme enkripsi AES untuk melindungi kredensial, sedangkan Redis digunakan sebagai penyimpanan sementara untuk mendukung proses *caching* dan pemantauan status sistem secara *real-time*. Berdasarkan hasil pengujian yang dilakukan, seluruh skenario fungsional yang dirancang berhasil dijalankan sesuai dengan keluaran yang diharapkan. Selain itu, pengujian non-fungsional menunjukkan bahwa sistem mampu mempertahankan waktu respons, menangani gangguan layanan eksternal melalui mekanisme yang sesuai, serta menjaga keamanan data sensitif selama proses operasional. Integrasi dengan AlienVault OTX juga memungkinkan proses pencarian *Indicator of Compromise* (IoC) dilakukan secara asinkron, sementara modul Sentinel secara otomatis memantau kondisi infrastruktur dan mengirimkan notifikasi ke Telegram ketika terdeteksi perubahan status layanan.

Menjawab tujuan utamanya, sistem yang diusulkan mampu menyederhanakan proses kerja sekaligus mengurangi waktu yang diperlukan untuk menyelesaikan berbagai aktivitas administrasi dan pemantauan. Hasil pengujian menunjukkan rata-rata durasi penyelesaian tugas berkurang sebesar 58,33%, sedangkan jumlah langkah interaksi pengguna berkurang sebesar 52,0%. Pengurangan tersebut dicapai melalui penyatuan berbagai fungsi ke dalam satu antarmuka sehingga kebutuhan berpindah aplikasi, melakukan autentikasi berulang, serta menyalin data secara manual dapat diminimalkan. Dengan demikian, Hub Manajemen Terpusat yang dikembangkan pada penelitian ini memberikan pendekatan yang lebih sederhana, terintegrasi, dan proaktif dalam mendukung operasional *Security Operations Center* (SOC), sehingga administrator dan analis dapat memperoleh informasi yang dibutuhkan dengan

lebih cepat untuk mendukung proses pengambilan keputusan selama penanganan insiden.

5.2. Saran

Penelitian ini menghasilkan sebuah arsitektur yang dapat menjadi fondasi bagi pengembangan sistem pada penelitian selanjutnya. Meskipun fungsi utama yang dirancang telah diimplementasikan dan dievaluasi, masih terdapat sejumlah peluang untuk memperluas cakupan sistem sesuai kebutuhan operasional *Security Operations Center* (SOC). Salah satunya adalah memperluas mekanisme pemantauan otomatis yang saat ini diterapkan pada komponen Wazuh agar juga mencakup perangkat infrastruktur lain, seperti *firewall*, *load balancer*, maupun layanan jaringan yang bersifat kritis. Selain itu, pola integrasi API asinkron yang digunakan pada sistem dirancang secara modular sehingga memungkinkan penambahan sumber *Threat Intelligence* lain, seperti VirusTotal, MISP, atau IBM X-Force, tanpa memerlukan perubahan yang signifikan pada arsitektur yang telah dibangun. Integrasi beberapa sumber tersebut diharapkan dapat memperkaya informasi pendukung yang tersedia selama proses investigasi insiden.

Pengembangan berikutnya juga dapat difokuskan pada peningkatan mekanisme notifikasi. Pada penelitian ini, notifikasi Telegram digunakan untuk menyampaikan perubahan status kesehatan infrastruktur secara *real-time*. Ke depan, mekanisme yang sama dapat diperluas untuk mendistribusikan peringatan ancaman siber yang berasal dari hasil analisis log maupun *Threat Intelligence*. Apabila volume peringatan meningkat, penerapan algoritma *Machine Learning* dapat dipertimbangkan untuk membantu mengelompokkan, memprioritaskan, dan menyaring notifikasi berdasarkan tingkat risiko. Pendekatan ini berpotensi mengurangi jumlah peringatan yang kurang relevan (*alert fatigue*), sehingga analis dapat lebih memfokuskan perhatian pada insiden yang memiliki prioritas penanganan lebih tinggi.

DAFTAR RIWAYAT HIDUP PENULIS

Christian Nataniel Yosua Purba menempuh pendidikan menengah di SMA Swasta Methodist dengan peminatan Ilmu Pengetahuan Alam (IPA). Setelah menyelesaikan pendidikan tersebut, penulis melanjutkan studi pada Program Studi Sarjana Terapan Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta (PNJ). Selama masa perkuliahan, penulis aktif mengembangkan kompetensi akademik maupun non-akademik melalui berbagai organisasi, kepanitiaan, dan kegiatan pengembangan diri. Selama perkuliahan penulis menjadi bagian 2 organisasi yakni KSM Computer Student Club (CSC) divisi Cyber Security serta menjadi Mentor divisi Speech di Polytechnic English Club (PEC). Selain itu, penulis berkesempatan menjadi panitia pada ajang nasional Kompetisi Mahasiswa Bidang Informatika Politeknik (KMIPN VI) dan konferensi International Conference on Computing, Communication, and Information Engineering (IC2IE), serta mengikuti Program Studi Independen Bersertifikat Kampus Merdeka di bidang Digital Forensik. Selain berbagai pengalaman tersebut, penulis meraih Juara I Nasional pada kompetisi Dashboard Analysis Competition oleh GELAR RASA UPNV Jatim.

DAFTAR PUSTAKA

Aare, C.R. 2025. "Scalable SIEM Architectures for Global Enterprises: Engineering Real-Time Visibility with Splunk". *Zenodo (CERN European Organization for Nuclear Research)*, 4(8). https://doi.org/10.5281/zenodo.16786607.

Abiade, O. 2024. *Enhancing Cybersecurity Through Predictive Threat Intelligence and Automated Incident Handling*. EasyChair Preprint 14890. https://easychair.org/publications/preprint/FqhD.

Adrian, A.Z.A., Megantara, R.A. dan Al Zami, F. 2026. "Hybrid Multilayer Architecture Integrating Suricata, Wazuh, and Cyber Threat Intelligence for Drive-by-Download Malvertising Detection". *Sinkron*, 10(1), 161–168. https://doi.org/10.33395/sinkron.v10i1.15616.

Allegretta, M., Siracusano, G., Gonzalez, R. dan Gramaglia, M. 2023. "Are Crowd-Sourced CTI Datasets Ready for Supporting Anti-Cybercrime Intelligence?". *Computer Networks*, 234, 109920. https://doi.org/10.1016/j.comnet.2023.109920.

Amami, R., Charfeddine, M. dan Masmoudi, S. 2024. "Exploration of Open Source SIEM Tools and Deployment of an Appropriate Wazuh-Based Solution for Strengthening Cyberdefense". *2024 10th International Conference on Control, Decision and Information Technologies (CoDIT)*, 8, 1–7. https://doi.org/10.1109/codit62066.2024.10708476.

Andali, D.A.S. dan Susetyo, Y.A. 2025. "Performance Analysis of NoSQL Databases: MongoDB Document Store and Redis Key-Value Store in Microservices-Based Applications Using Flask". *International Journal Software Engineering and Computer Science (IJSECS)*, 5(2), 691–705. https://doi.org/10.35870/ijsecs.v5i2.4206.

Arif, I., Tariq, A. dan Barchuk, B. 2025. "The Cost of Fragmentation: Measuring Time, Spend and Risk in Personal Cybersecurity Tool Stacks". *World Journal of Advanced Engineering Technology and Sciences*, 16(3), 334–363. https://doi.org/10.30574/wjaets.2025.16.3.1350.

AwanPintar.id. 2025. *Laporan Ancaman Digital di Indonesia Semester 1 Tahun 2025*. PT PROSPERITA SISTEM INDONESIA. https://www.awanpintar.id/publikasi/.

Badan Siber dan Sandi Negara (BSSN). 2024. *Lanskap Keamanan Siber Indonesia 2024*. Jakarta Selatan: Id-SIRTII /CC – BSSN. https://www.bssn.go.id/monitoring-keamanan-siber/. [9 Januari 2026].

Barman, U. dan Joshi, K. 2025. "Polyglot Persistence - Usage and Challenges". *Journal of Artificial Intelligence, Machine Learning and Data Science*, 3(4), 3079–3089. https://doi.org/10.51219/jaimld/utpal-barma/633.

Baruwal Chhetri, M., Tariq, S., Singh, R., Jalalvand, F., Paris, C. dan Nepal, S. 2024. "Towards Human-AI Teaming to Mitigate Alert Fatigue in Security Operations Centres". *ACM Transactions on Internet Technology*, 24(3). https://doi.org/10.1145/3670009.

Bell, D. 2023. *Explore the UML Sequence Diagram*. IBM Developer. https://developer.ibm.com/articles/the-sequence-diagram/.

Burke, G. 2025. *SIEM SERIES WAZUH*. Objectfirst.com. https://objectfirst.com/blog/siem-series-wazuh/.

Chaitanya, A.K., Jignyasa, G., Keerthi, S. dan Reddy, G.H. 2025. "Fortifying Cyber Defenses: Empowering Web Application Firewalls Through Threat Intelligence". *International Journal of Information Technology and Computer Engineering*, 13(1), 242–249. https://ijitce.org/index.php/ijitce/article/view/881. [18 Januari 2026].

CrowdStrike. 2023. *CrowdStrike 2023 Threat Hunting Report Reveals Identity-Based Attacks and Hands-on-Keyboard Activity on the Rise as Adversaries Look to Bypass Defenses*. Crowdstrike.com. https://www.crowdstrike.com/en-us/press-releases/crowdstrike-releases-2023-threat-hunting-report/.

CrowdStrike. 2024. *2024 CrowdStrike Global Threat Report: From Breakout to Breach in Under Three Minutes; Cloud Infrastructure Under Attack*. Crowdstrike.com. https://www.crowdstrike.com/en-us/press-releases/2024-crowdstrike-global-threat-report-release/.

CrowdStrike. 2025. *CrowdStrike Releases 2025 Global Threat Report: Cyber Threats Reach New Highs*. Crowdstrike.com. https://www.crowdstrike.com/en-us/press-releases/crowdstrike-releases-2025-global-threat-report/.

Dharma, B.S. dan Muslikh, A.R. 2025. "Implementasi Rate Limiting dan Bot Telegram untuk Mitigasi Serangan HTTP GET Flood". *Journal of Information System and Application Development*, 3(1). https://doi.org/10.26905/jisad.v3i1.15398.

Domo, Inc. 2026. *What Is Real-Time Data? Definition, Benefits, and Best Practices for 2026*. www.domo.com. https://www.domo.com/glossary/what-is-real-time-data.

Gault, J. 2025. *Understanding Real-Time Analytics*. dbt Labs. https://www.getdbt.com/discover/understanding-real-time-analytics.

Grobler, M., Gaire, R. dan Nepal, S. 2021. "User, Usage and Usability: Redefining Human Centric Cyber Security". *Frontiers in Big Data*, 4. https://doi.org/10.3389/fdata.2021.583723.

Hardika, B., Kurniawan, M.D., Adzka, M., Prastowiyono, D., Banyubasa, A., Wicaksono, A. dan Nasir, M. 2024. "Pengujian Blackbox Testing Website Garuda Farm Menggunakan Teknik Equivalence Partitioning". *Jurnal Kridatama Sains dan Teknologi*, 6(2), 740–753. https://doi.org/10.53863/kst.v6i02.1420.

Hegde, R.C. 2020. "Low Latency Message Brokers". *International Research Journal of Engineering and Technology (IRJET)*. https://www.semanticscholar.org/paper/Low-Latency-Message-Brokers-Hegde/522190ca1b32b734d98ac731feacfe6ff2763f9c.

Hugo, V. dan 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://www.ijtsrd.com/papers/ijtsrd49651.pdf.

Hyun, G., Oak, J., Kim, D. dan Kim, K. 2024. "The Impact of an Automation System Built with Jenkins on the Efficiency of Container-Based System Deployment". *Sensors*, 24(18), 6002. https://doi.org/10.3390/s24186002.

IBM Security dan Ponemon Institute. 2020. *IBM Study: Security Response Planning on the Rise, But Containing Attacks Remains an Issue*. IBM News Room. https://newsroom.ibm.com/2020-06-30-IBM-Study-Security-Response-Planning-on-the-Rise-But-Containing-Attacks-Remains-an-Issue. [17 Juli 2021].

Islam, M.R. dan Rafique, R. 2024. "Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries". *International Journal of Engineering Materials and Manufacture*, 9(4), 136–144. https://doi.org/10.26776/ijemm.09.04.2024.02.

Ismail, Kurnia, R., Brata, Z.A., Nelistiani, G.A., Heo, S., Kim, H. dan Kim, H. 2025. "Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic Artificial Intelligence". *Information*, 16(5), 365. https://doi.org/10.3390/info16050365.

ISO. 2018. *Ergonomics of Human-System Interaction — Part 11: Usability: Definitions and Concepts*. Iso.org. https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en.

Izzatillah, T.I., Fania, F. dan Zulfata, Z. 2024. "The Effectiveness of Snort in DDoS Attack Scenarios". *IC-ITECHS*, 5(1), 603–612. https://doi.org/10.32664/ic-itechs.v5i1.1588.

Jovanović, M. 2024. *Caching in ASP.NET Core: Improving Application Performance*. Milanjovanovic.tech. https://www.milanjovanovic.tech/blog/caching-in-aspnetcore-improving-application-performance. [26 Maret 2026].

Kaptsov, L. 2025. "Using Redis for Caching Optimization in High-Traffic Web Applications". *International Journal of Advanced Multidisciplinary Research and Studies*, 5(4), 1714–1722. https://doi.org/10.62225/2583049x.2025.5.4.4839.

Kelton, C., Ryoo, J., Balasubramanian, A. dan Das, S. 2017. "Improving User Perceived Page Load Time Using Gaze". *Proceedings of the 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI '17)*, Boston, MA, USA. https://www.usenix.org/system/files/conference/nsdi17/nsdi17-kelton.pdf.

Kumar, K.S. 2025. "Next-Generation Security Operations: Leveraging Automation for Proactive Threat Mitigation". *International Journal of Scientific Research in Engineering and Management*, 9(4), 1–9. https://doi.org/10.55041/ijsrem43432.

Kummarapurugu, C.S. 2024. "Architectural Framework for Threat Intelligence Integration with SIEM and SOAR in Hybrid Cloud Security Environments". *International Journal of Innovative Research and Creative Technology (IJIRCT)*, 10(2), 1–9. https://www.ijirct.org/viewPaper.php?paperId=2411031.

Kurniawan, A., Aufar, T.Q. dan Agustin, M. 2024. "Configuration Management dengan Ansible dan Telegram untuk Automasi Laboratorium Komputer". *Multinetics*, 10(1), 50–59. https://doi.org/10.32722/multinetics.v10i1.6360.

Lucidchart. 2018. *The Basics of Documenting and Analyzing Your As-Is Process*. www.lucidchart.com. https://www.lucidchart.com/blog/as-is-process-analysis.

Matin, M., Fadhilrahman, Kurniawan, A., Zain, A.R. dan Agustin, M. 2025. "Sistem Monitoring Keamanan pada Data Center Berbasis Security Information and Event Management (SIEM) dengan Wazuh dan IDS". *Journal of Innovative and Creativity*, 5(1), 530–539. https://doi.org/10.31004/joecy.v5i1.1761.

Muhammad, R., Ismail, S.A. dan Hassan, N.H. 2024. "Botnet Detection and Incident Response in Security Operation Center (SOC): A Proposed Framework". *International Journal of Advanced Computer Science and Applications*, 15(3). https://doi.org/10.14569/ijacsa.2024.0150389.

Nagar, G. 2018. "The Evolution of Security Operations Centers (SOCs): Shifting from Reactive to Proactive Cybersecurity Strategies". *International Journal of Scientific Research and Management (IJSRM)*, 6(9), 100–115. https://doi.org/10.18535/ijsrm/v6i9.ec03.

Neumann, F. dan Weber, C. 2021. "Automated Security Operations: Scaling Threat Response with SOAR and AI-Driven Playbooks". *International Journal of Trend in Scientific Research and Development (IJTSRD)*, 5(2), 1317–1323. www.ijtsrd.com/papers/ijtsrd38541.pdf.

Nova, F., Pratama, M.D. dan Prayama, D. 2022. "Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan DoS". *JITSI: Jurnal Ilmiah Teknologi Sistem Informasi*, 3(1), 1–7. https://doi.org/10.62527/jitsi.3.1.59.

Object Management Group. 2017. *An OMG Unified Modeling Language Publication (OMG UML)*. https://www.omg.org/spec/UML/2.5.1/PDF.

Ofoegbu, K.D.O., Osundare, O.S., Ike, C.S., Fakeyede, O.G. dan Ige, A.B. 2024. "Proactive Cyber Threat Mitigation: Integrating Data-Driven Insights with User-Centric Security Protocols". *Computer Science & IT Research Journal*, 5(8), 2083–2106. https://doi.org/10.51594/csitrj.v5i8.1493.

Pressman, R.S. dan Maxim, B.R. 2014. *Software Engineering: A Practitioner's Approach*. New York: Mcgraw-Hill Education.

Pulyala, S.R., Desetty, A.G. dan Jangampet, V.D. 2019. "The Impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) Efficiency: A Comprehensive Analysis". *Turkish Journal of Computer and Mathematics Education*, 10(3), 1545–1549. https://doi.org/10.61841/turcomat.v10i3.14323.

Radview. 2026. *Benchmark Testing: How to Measure & Compare Performance*. Radview. https://www.radview.com/blog/benchmark-testing/. [26 Mei 2026].

Salunke, S.V. dan Ouda, A. 2024. "A Performance Benchmark for the PostgreSQL and MySQL Databases". *Future Internet*, 16(10), 382. https://doi.org/10.3390/fi16100382.

Seidl, M., Scholz, M., Huemer, C. dan Kappel, G. 2015. *UML @ Classroom*. Undergraduate Topics in Computer Science. Cham: Springer International Publishing.

Shafiyyah, A., Nama, G.F. dan Pradipta, R.A. 2024. "Implementasi Wazuh Menggunakan Metode PPDIOO di Sistem Keamanan Jaringan PSDKU Universitas Lampung Waykanan Sebagai Deteksi dan Respon Serangan Siber". *Jurnal Informatika dan Teknik Elektro Terapan*, 12(2). https://doi.org/10.23960/jitet.v12i2.4074.

Shavaf, M., Nair, M., Fayas, M., Rasheed, N. dan Babu, A. 2025. "Optimising Security Threats with Open-Source Threat Intelligence". *IJRTI*, 10(5), 679. https://www.ijrti.org/papers/IJRTI2505081.pdf. [18 Januari 2026].

Sheeraz, M., Paracha, M.A., Ulhaq, M., Durad, H. dan Mosavi, A. 2023. "Effective Security Monitoring Using Efficient SIEM Architecture". *Human-Centric Computing and Information Sciences*, 13(23). https://doi.org/10.22967/HCIS.2023.13.023.

Shevchenko, V. 2025. "Strategies for Database Performance Optimization in High-Load Systems: A Review of PostgreSQL and Redis Use Cases". *International Journal of Computer (IJC)*, 56(1), 279–289. https://ijcjournal.org/InternationalJournalOfComputer/article/view/2476.

Siam, A.A., Alazab, M., Awajan, A., Hasan, M.R., Obeidat, A. dan Faruqui, N. 2025. "IP SafeGuard–An AI-Driven Malicious IP Detection Framework". *IEEE Access*, 13, 90249–90261. https://doi.org/10.1109/access.2025.3569289.

Sijabat, D.R. dan Evo, S. 2023. "Perancangan Security Information and Event Management (SIEM) untuk Mendeteksi Insiden pada Situs Web". *J-Intech: Journal of Information and Technology*, 11(1), 10–17. https://doi.org/10.32664/j-intech.v11i1.860.

Singh, B. 2015. "Ensuring Data Integrity and Availability with Robust Database Security Protocols". *International Journal of Research in Electronics and Computer Engineering (IJRECE)*, 3(1). https://www.researchgate.net/publication/394294551_Ensuring_Data_Integrity_and_Availability_with_Robust_Database_Security_Protocols.

StreamNative. 2025. *Latency Numbers Every Data Streaming Engineer Should Know*. Streamnative.io. https://streamnative.io/blog/latency-numbers-every-data-streaming-engineer-should-know. [6 Februari 2026].

Sundaramurthy, S.C., Bardas, A.G., Case, J., Ou, X., Wesch, M., McHugh, J. dan Rajagopalan, S.R. 2015. "A Human Capital Model for Mitigating Security Analyst Burnout". *Symposium on Usable Privacy and Security (SOUPS)*, 347–359.

Sutanto, A. dan Rakhman, A. 2025. "Experimental Evaluation of Wazuh-Grafana Integration for Real-Time Cyber Threat Detection in Resource-Constrained Environments". *Journal of Applied Informatics and Computing*, 9(5), 2783–2790. https://doi.org/10.30871/jaic.v9i5.10404.

Thakker, A., More, A. dan Kumar, K. 2025. "Automated Defense Against Application-Layer Attacks on Windows Systems Using Wazuh and Shuffle". *International Journal of Education Science Technology and Engineering (IJESTE)*, 8(1), 45–57. https://doi.org/10.36079/lamintang.ijeste-0801.842.

Velamoo, G. dan Samanta, A. 2024. *Adaptive Timeout Strategies for Microservice Application*. MIT PRIMES 2024. https://math.mit.edu/research/highschool/primes/materials/2024/Velamoor-Samanta.pdf.

Vielberth, M., Bohm, F., Fichtinger, I. dan Pernul, G. 2020. "Security Operations Center: A Systematic Study and Open Challenges". *IEEE Access*, 8, 227756–227779. https://doi.org/10.1109/access.2020.3045514.

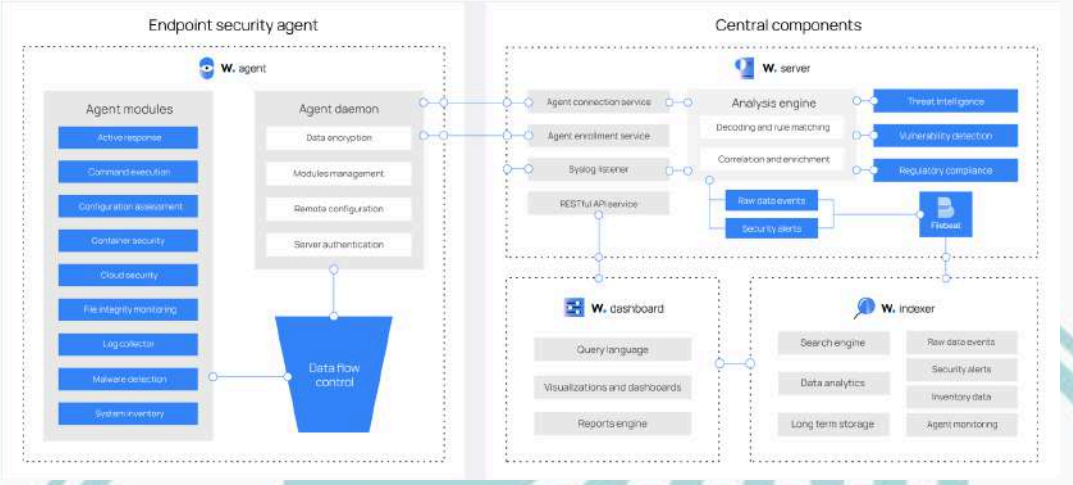
Visual Paradigm. 2016. *How to Develop As-Is and To-Be Business Process?*. Visual-paradigm.com. https://www.visual-paradigm.com/tutorials/as-is-to-be-business-process.jsp.

Wazuh. n.d. *Architecture - Getting Started with Wazuh · Wazuh Documentation*. documentation.wazuh.com. https://documentation.wazuh.com/current/getting-started/architecture.html.

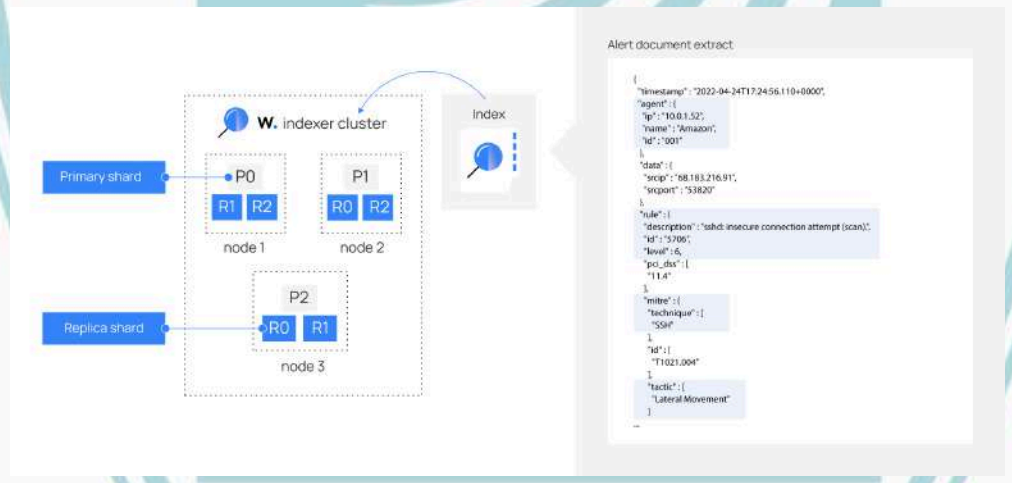
World Economic Forum. 2025. *Global Cybersecurity Outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf#page=4.02.

LAMPIRAN

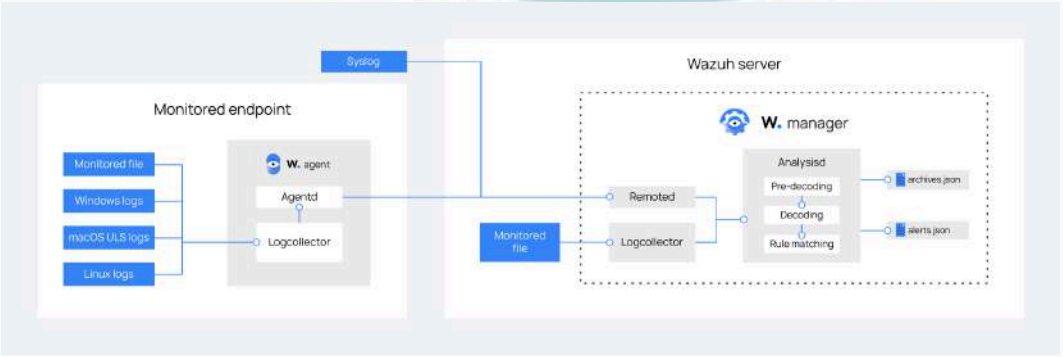
Lampiran 1 Diagram Arsitektur Wazuh



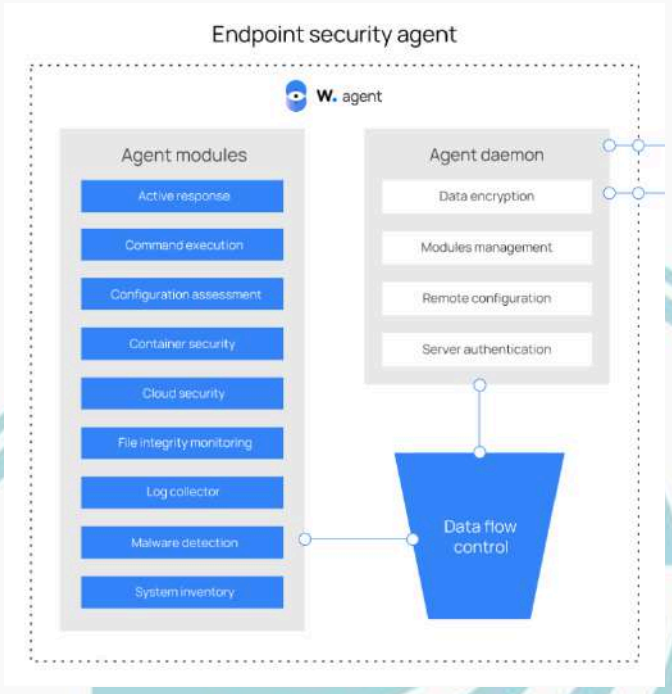
Lampiran 2 Diagram Arsitektur Komponen Wazuh *Indexer*



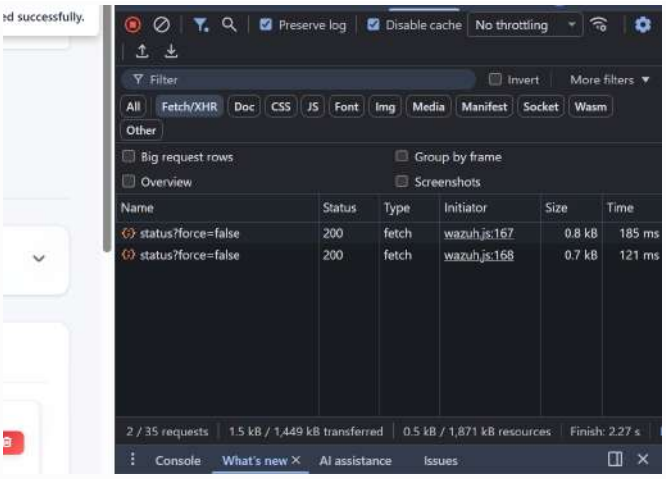
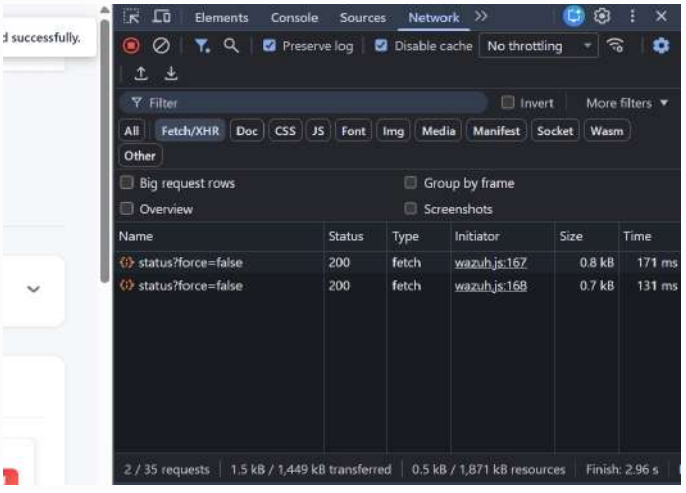
Lampiran 3 Diagram Arsitektur Komponen Wazuh *Manager*



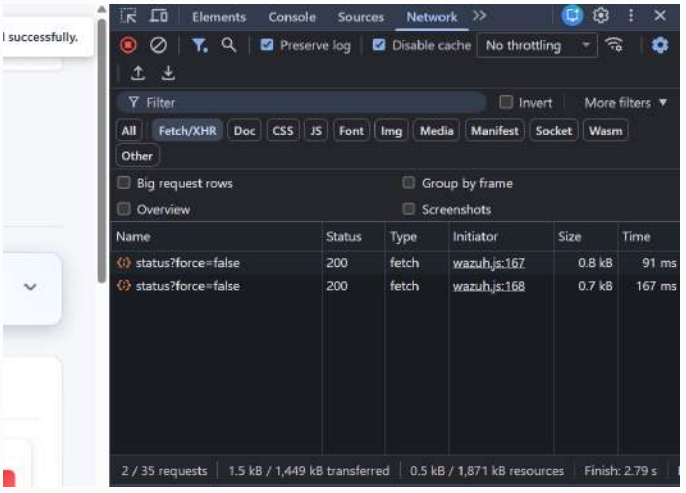
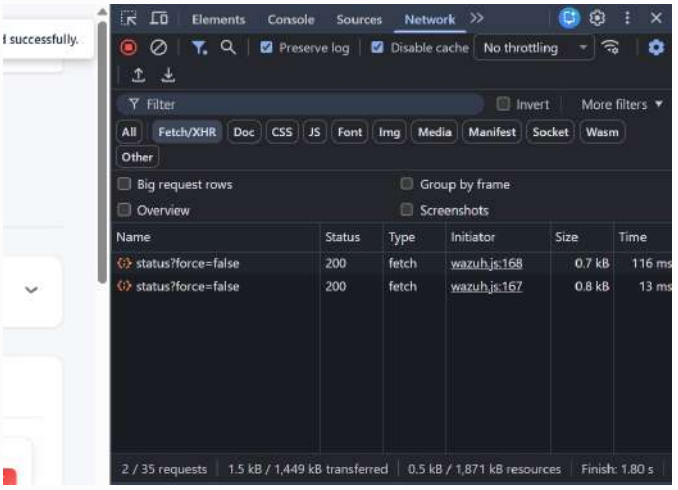
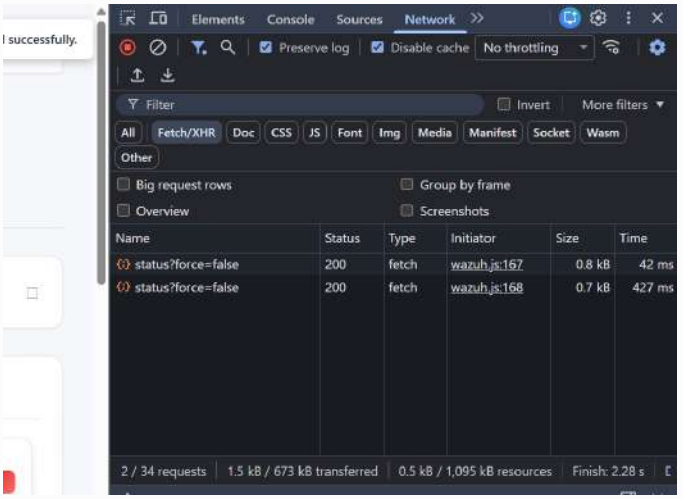
Lampiran 4 Diagram Arsitektur Komponen Wazuh *Agent*



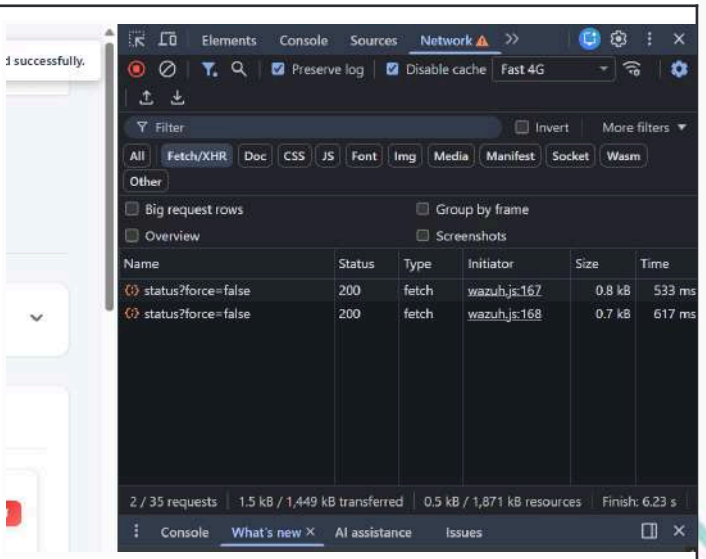
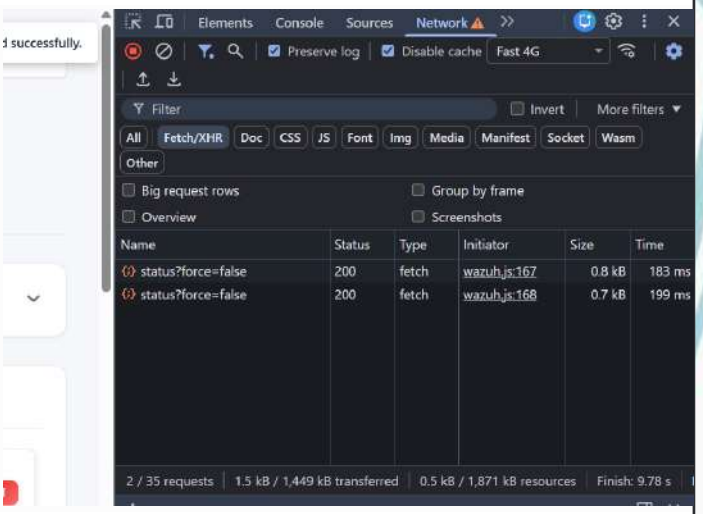
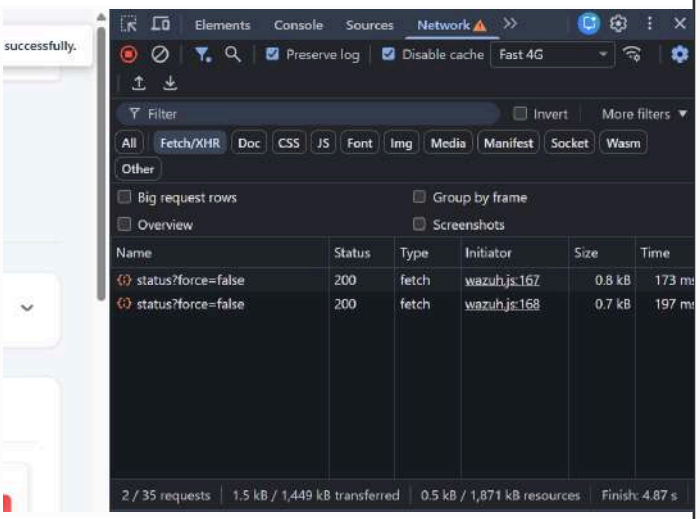
Lampiran 5 Tabel Hasil Pengujian dan Rujukan Bukti Waktu Muat Antarmuka (NF.1.1)

Kondisi Jaringan / Iterasi	**Waktu Muat (s)**	**Screenshot Bukti**
Kondisi *Ideal* (*No Throttling*)		
- Iterasi 1	2,27 s	
- Iterasi 2	2,96 s	

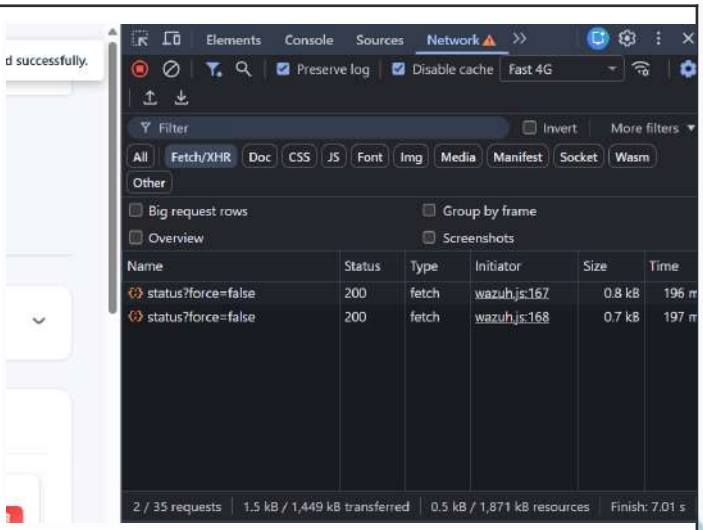
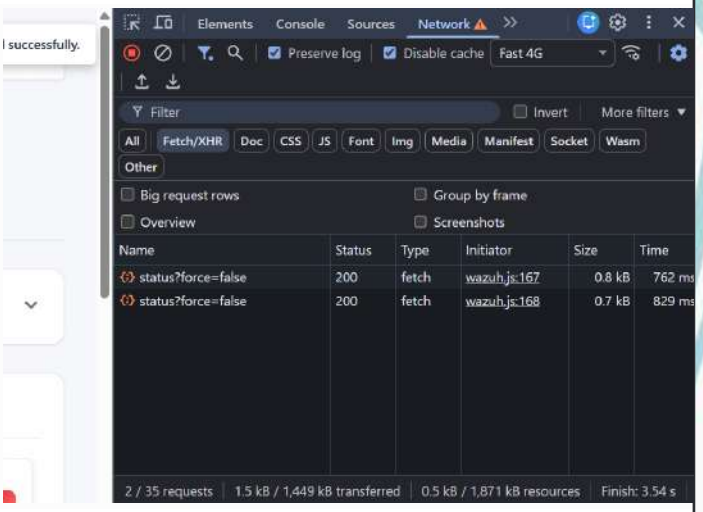
(lanjutan)

- Iterasi 3	2,79 s	
- Iterasi 4	1,80 s	
- Iterasi 5	2,28 s	
Kondisi Moderat (*Fast 4G*)		

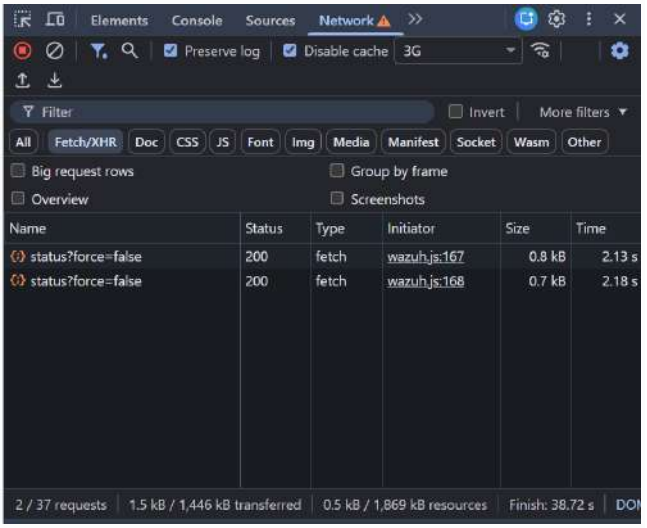
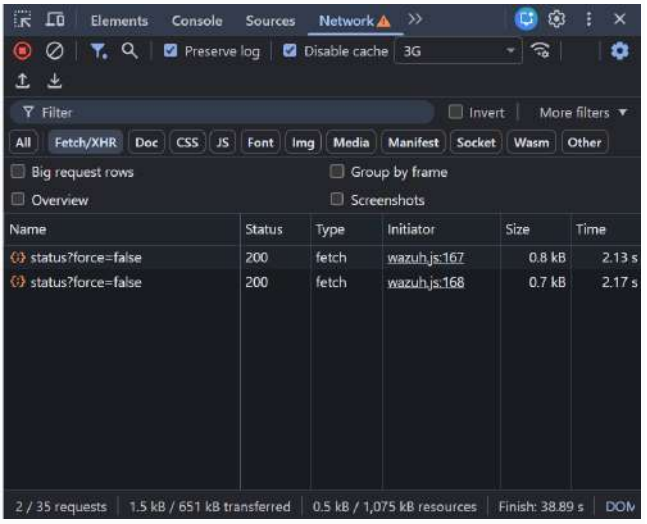
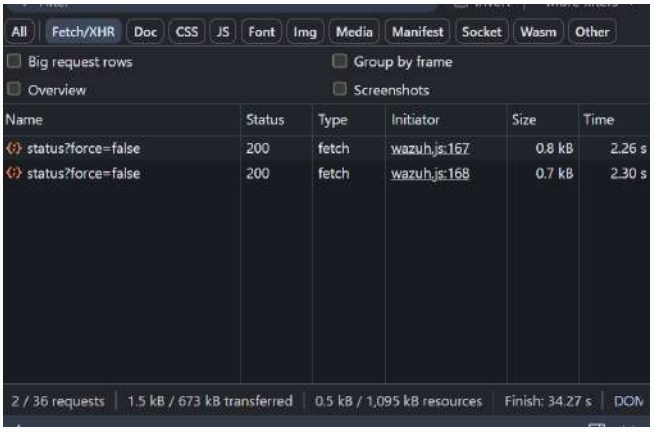
(lanjutan)

- Iterasi 1	6,23 s	
- Iterasi 2	9,78 s	
- Iterasi 3	4,87 s	

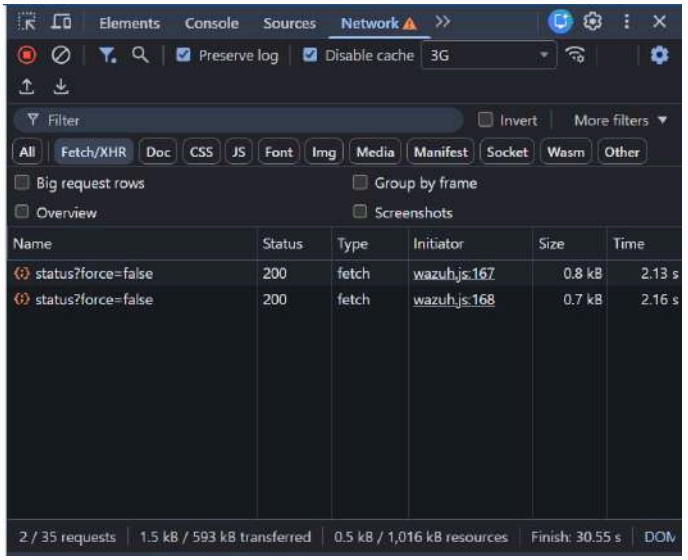
(lanjutan)

- Iterasi 4	7,01 s	
- Iterasi 5	3,54 s	
Kondisi Buruk (*3G*)		
- Iterasi 1	40,36 s	

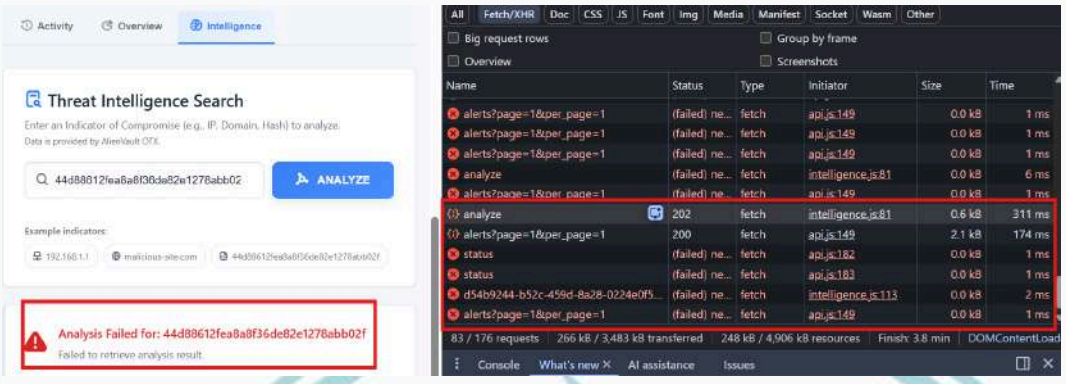
(lanjutan)

- Iterasi 2	38,72 s	
- Iterasi 3	38,89 s	
- Iterasi 4	34,27 s	

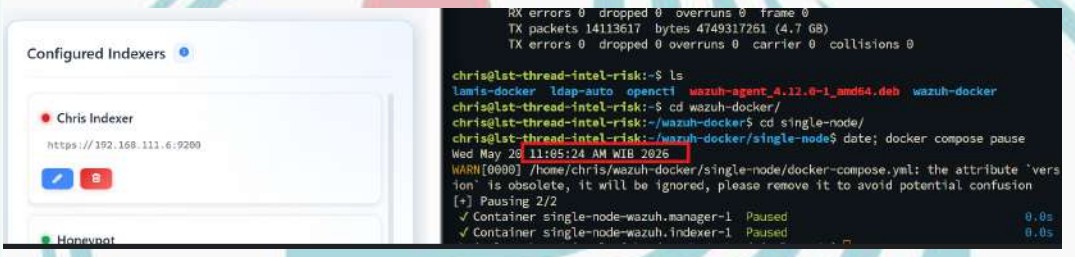
(lanjutan)

- Iterasi 5	30,55 s	

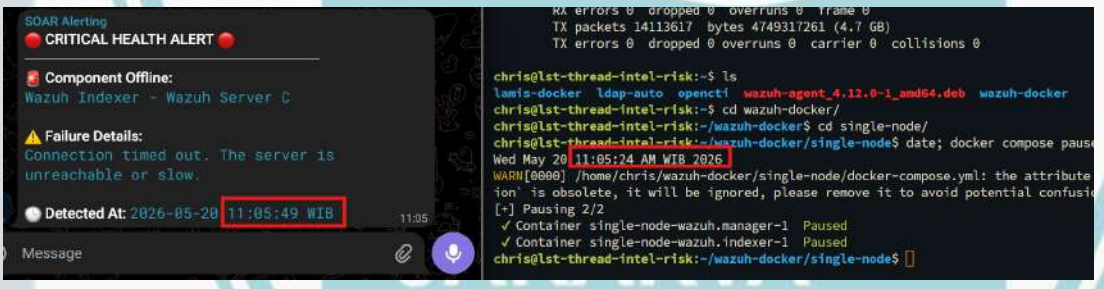
Lampiran 6 Simulasi Gagal Fetch untuk Analyze *Threat Intelligence* (NF.1.2)



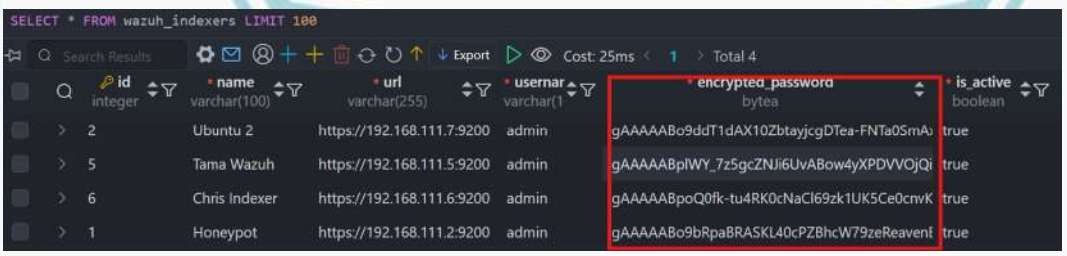
Lampiran 7 Status Down Ketika Compose Wazuh Paused (NF.1.3.)



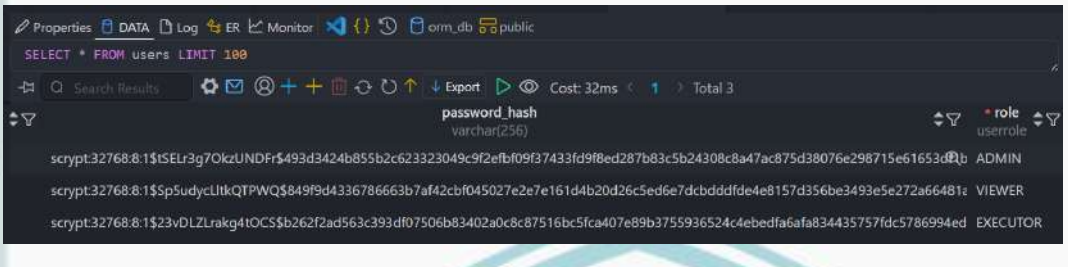
Lampiran 8 Notifikasi Wazuh *Sentinel* Muncul 25 Detik Setelah Paused (11:05:24 ~ 11:05:49 WIB) (NF.1.3.)



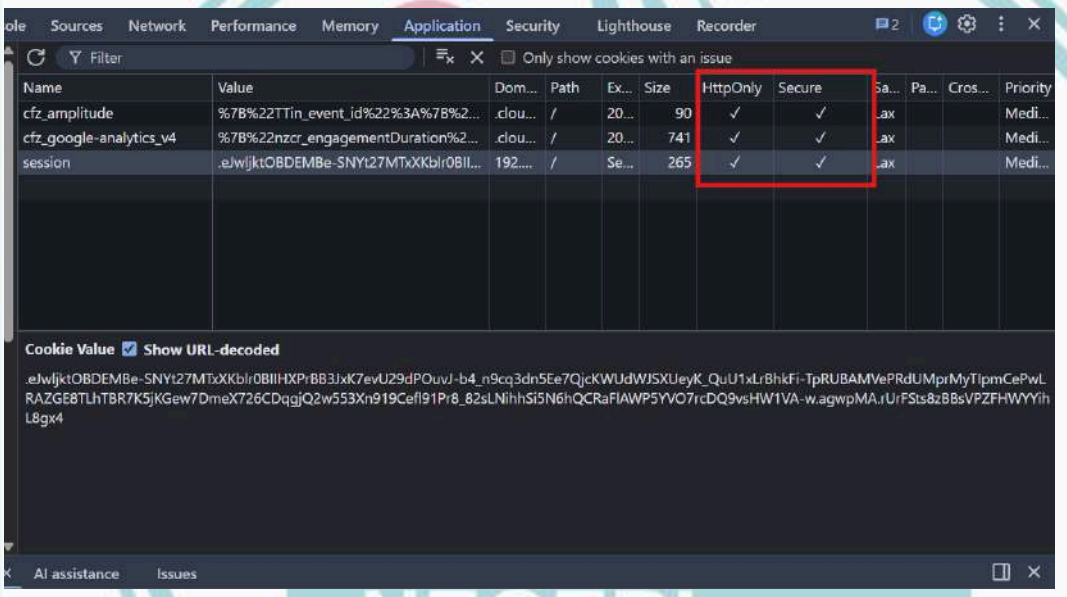
Lampiran 9 *Field Password* Terenkripsi AES dan Berbentuk *Ciphertext* (NF.2.1)



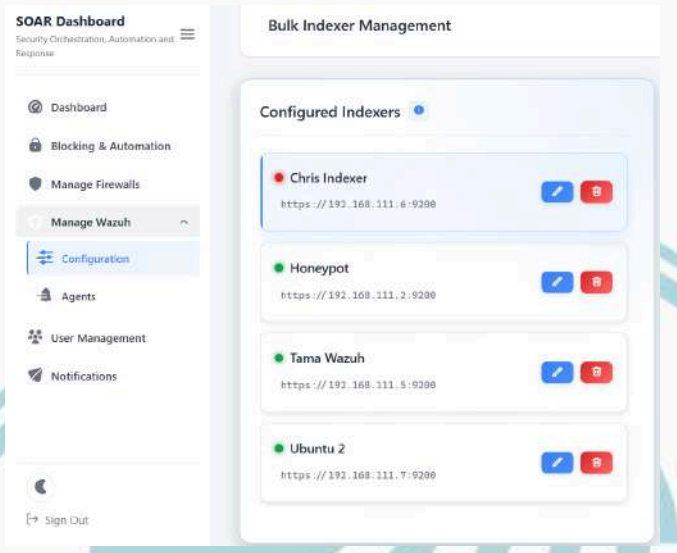
Lampiran 10 *Password Field* untuk User Telah Dihash (NF.2.2)



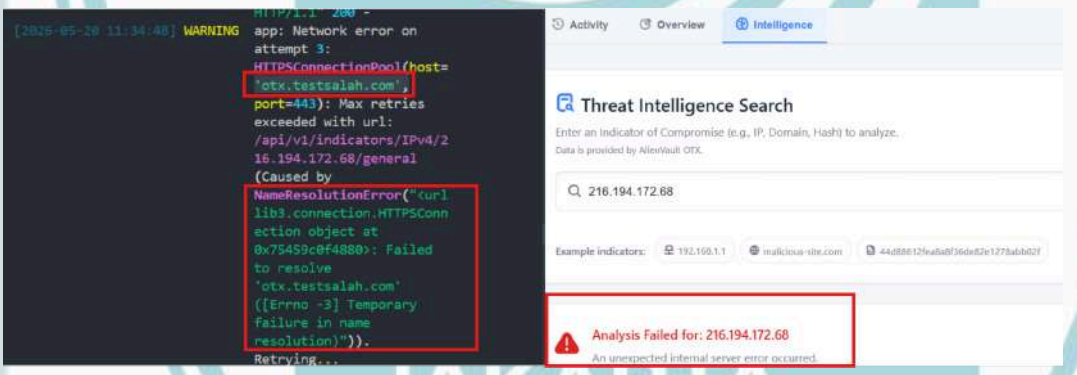
Lampiran 11 Bukti Pengujian Cookies HTTP Sudah *HttpOnly* dan Secure (NF.2.3)



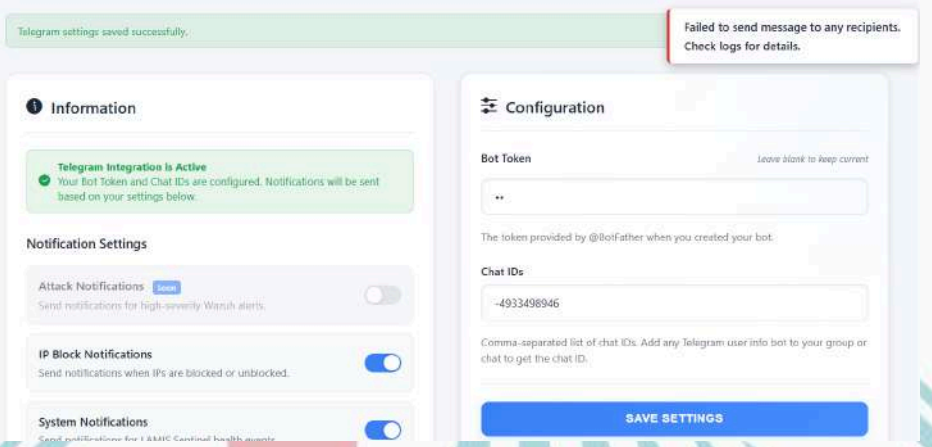
Lampiran 12 Kegagalan Salah Satu *Node* Wazuh Membuat Sistem Masih Berjalan (NF.3.1)



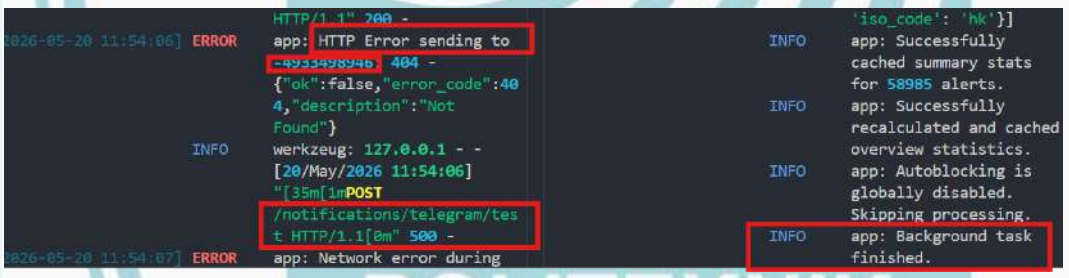
Lampiran 13 Isolasi *Error* API *Alienvault* (NF.3.2)



Lampiran 14 Tampilan UI es Resiliensi *Scheduler* dengan Menyalahkan *Token* Bot (NF.3.3)



Lampiran 15 Tampilan Log Tes Resiliensi *Scheduler* dengan Menyalahkan *Token* Bot (NF.3.3)



Lampiran 16 Data *Raw Timestamp* Pengukuran Waktu Penyelesaian (*Time on Task*)

ID Aksi	**Metode Eksisting (Manual)**			**Metode Sistem Usulan (Hub Terpusat)**		
	Waktu Mulai (*Start*)	**Waktu Selesai (*End*)**	**Total Waktu**	**Waktu Mulai (*Start*)**	**Waktu Selesai (*End*)**	**Total Waktu**
1	12:06:44	12:07:47	**63 detik**	11:57:47	11:58:24	**37 detik**
2	10:53:19	10:54:33	**74 detik**	10:58:43	10:59:08	**25 detik**
3	11:11:48	11:12:46	**58 detik**	11:15:10	11:15:30	**20 detik**

4	11:24:54	11:25:36	**42 detik**	11:29:44	11:29:56	**12 detik**
5	11:40:32	11:40:57	**25 detik**	11:41:09	11:41:26	**17 detik**
6	12:01:08	12:01:46	**38 detik**	12:03:40	12:04:00	**20 detik**
7	15:02:01	15:02:40	**39 detik**	15:08:22	15:08:36	**14 detik**
8	15:35:41	15:36:47	**66 detik**	11:38:33	11:38:52	**19 detik**
9	15:56:58	15:57:42	**44 detik**	16:01:30	16:01:55	**25 detik**
10	16:17:51	16:18:58	**67 detik**	16:26:16	16:26:42	**26 detik**

Lampiran 17 Data Video Recording yang Tersedia untuk Verifikasi Uji Efisiensi Operasional

Name	Date	Type	Size	Length
AKSI 1 - MANUAL.mkv	01/06/2026 12:07	MKV File	3.030 KB	00:01:06
AKSI 1 - USULAN.mkv	01/06/2026 11:58	MKV File	2.752 KB	00:00:44
AKSI 2 - MANUAL.mkv	02/06/2026 10:54	MKV File	2.520 KB	00:01:18
AKSI 2 - USULAN.mkv	02/06/2026 10:59	MKV File	1.601 KB	00:00:29
AKSI 3 - MANUAL.mkv	02/06/2026 11:12	MKV File	1.921 KB	00:00:43
AKSI 3 - USULAN.mkv	02/06/2026 11:15	MKV File	1.650 KB	00:00:23
AKSI 4 - MANUAL.mkv	02/06/2026 11:25	MKV File	4.736 KB	00:00:46
AKSI 4 - USULAN.mkv	02/06/2026 11:29	MKV File	1.508 KB	00:00:17
AKSI 5 - MANUAL.mkv	02/06/2026 11:40	MKV File	4.375 KB	00:00:28
AKSI 5 - USULAN.mkv	02/06/2026 11:41	MKV File	3.972 KB	00:00:20
AKSI 6 - MANUAL.mkv	02/06/2026 12:01	MKV File	3.470 KB	00:00:43
AKSI 6 - USULAN.mkv	02/06/2026 12:04	MKV File	3.536 KB	00:00:27
AKSI 7 - MANUAL.mkv	02/06/2026 15:02	MKV File	1.316 KB	00:00:47
AKSI 7 - USULAN.mkv	02/06/2026 15:08	MKV File	1.861 KB	00:00:18
AKSI 8 - MANUAL.mkv	02/06/2026 15:36	MKV File	5.169 KB	00:01:15
AKSI 8 - USULAN.mkv	02/06/2026 15:38	MKV File	2.030 KB	00:00:22
AKSI 9 - MANUAL.mkv	02/06/2026 15:57	MKV File	1.926 KB	00:00:51
AKSI 9 - USULAN.mkv	02/06/2026 16:01	MKV File	3.376 KB	00:00:29
AKSI 10 - MANUAL.mkv	02/06/2026 16:18	MKV File	1.662 KB	00:01:14
AKSI 10 - USULAN.mkv	02/06/2026 16:26	MKV File	4.617 KB	00:00:42