



**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**



© Hak Cipta milik Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISME

yang bertanda tangan di bawah ini:

: Christian Nataniel Yosua Purba

: 2207421043

Jurusan/Program Studi: 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


10000
METERAN
TEMPER
8666 CANX335253795

(Christian Nataniel Yosua Purba)

NIM. 2207421043

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber ;
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



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

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



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 memungkinkan 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.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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 bermakna 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

**POLITEKNIK
NEGERI
JAKARTA**



© Hak Cipta milik Politeknik Negeri Jakarta

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah

ini

Nama

: Christian Nataniel Yosua Purba

NI

: 2207421043

Jurusan/Program Studi: T. Informatika dan Komputer / T. Multimedia dan Jaringan

Demikian 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



- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



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.

POLITEKNIK
NEGERI
JAKARTA



DAFTAR ISI

LEMBAR PENGESAHAN.....	iii
KATA PENGANTAR.....	iv
ABSTRAK.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	xiv
BAB I	
PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Perumusan Masalah.....	4
1.3 Batasan Masalah.....	4
1.4 Tujuan dan Manfaat.....	5
1.5 Sistematika Penulisan.....	6
BAB II	
TINJAUAN PUSTAKA.....	7
2.1 Security Operations Center (SOC) Proaktif.....	7
2.2 Efisiensi dan Optimalisasi Alur Kerja SOC.....	7
2.3 Security Information and Event Management (SIEM).....	8
2.4 Integrasi SOAR, SIEM dan <i>Firewall</i>	8
2.5 Wazuh.....	9
2.6 Wazuh <i>Agent</i> , Wazuh <i>Manager</i> , dan Wazuh <i>Indexer</i>	9
2.7 Alienvault OTX sebagai <i>Threat Intelligence</i>	11
2.8 Arsitektur OLTP <i>Cache-Database</i>	12
2.9 PostgreSQL.....	13
2.10 Redis.....	13
2.11 Telegram Bot API.....	14
2.12 Pengujian <i>Black Box Testing</i>	14
2.13 Transformasi <i>As-Is</i> dan <i>To-Be</i> untuk Operasional SOC.....	15
2.14 Standar Parameter Waktu Respon dan Kebutuhan Latensi <i>Real-Time</i>	15
2.15 Diagram Sekuensial dengan Fragmen Kombinasi.....	16
2.16 Penelitian Terkait.....	20
BAB III	
METODE PENELITIAN.....	23
3.1 Rancangan Penelitian.....	23
3.2 Tahapan Penelitian.....	23
3.3 Objek Penelitian.....	25
BAB IV	
HASIL DAN PEMBAHASAN.....	27
4.1 Analisis Kebutuhan.....	27



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.1.1 Kebutuhan Fungsional (Functional Requirements).....	27
4.1.2 Analisis Kebutuhan Non-Fungsional.....	29
4.1.3 Analisis Kebutuhan Perangkat Keras (<i>Hardware</i>).....	31
4.1.4 Analisis Kebutuhan Perangkat Lunak (<i>Software</i>).....	32
4.2 Perancangan Sistem.....	34
4.2.1 Arsitektur Perangkat Lunak dan Aliran Data.....	34
4.2.2 Rancangan Optimalisasi Alur Kerja Operasional (<i>As-Is</i> dan <i>To-Be</i>)	36
4.2.3 Perancangan Penyimpanan Data (<i>Cache-Database Architecture</i>)....	57
4.3 Implementasi Sistem.....	63
4.3.1 Implementasi Lingkungan Operasional (Orkestrasi Kontainer).....	63
4.3.2 Implementasi Hub Manajemen Konfigurasi Multi-Wazuh.....	68
4.3.3 Implementasi Hub Agregasi Multi-Agen Wazuh.....	85
4.3.4 Implementasi Pengayaan Intelijen Ancaman (<i>Threat Intelligence</i>)..	95
4.3.5 Implementasi Pemantauan Proaktif dan Notifikasi <i>Real-Time</i> (Telegram).....	108
4.3.6 Implementasi Hak Akses Berbasis Peran (<i>Role-Based Access Control</i>)...	124
4.4 Pengujian.....	126
4.4.1 Deskripsi Pengujian.....	126
4.4.2 Prosedur Pengujian.....	127
A. Prosedur Pengujian Fungsional (<i>Black Box Testing</i>).....	128
B. Prosedur Pengujian Non-Fungsional.....	136
C. Prosedur Pengujian Efisiensi Operasional.....	140
4.4.3 Data Hasil Pengujian.....	149
A. Data Hasil Pengujian Fungsional (<i>Black Box Testing</i>).....	150
B. Data Hasil Pengujian Non-Fungsional.....	155
C. Data Hasil Pengujian Efisiensi Operasional.....	160
4.4.4 Analisis Data / Evaluasi Pengujian.....	162
A. Analisis Pengujian Fungsional (<i>Black Box Testing</i>).....	163
B. Analisis Pengujian Non-Fungsional.....	164
C. Analisis dan Evaluasi Efisiensi Operasional.....	168
BAB V	
PENUTUP.....	176
5.1. Simpulan.....	176
5.2. Saran.....	177
DAFTAR RIWAYAT HIDUP PENULIS.....	178
DAFTAR PUSTAKA.....	179
LAMPIRAN.....	180



DAFTAR GAMBAR

Gambar 2.1 Ilustrasi Data Multi-Sumber pada Data <i>Aggregation Module</i>	8
Gambar 2.2 Ilustrasi berbagai Kapabilitas SOAR.....	9
Gambar 2.3 Topologi Arsitektural Komponen Wazuh.....	10
Gambar 2.4 Fungsi-Fungsi Komponen Wazuh.....	10
Gambar 2.5 Struktur Model Data Alienvault OTX.....	12
Gambar 2.6 Diagram Mekanisme Implementasi <i>Cache-Database</i>	13
Gambar 2.8 Contoh Fragment Gabungan <i>Break</i> dan <i>Loop</i> dalam Satu <i>Sequential</i> ..	17
Gambar 2.9 Contoh Diagram Sekuensial dengan Alternatives.....	18
Gambar 2.10 Contoh Diagram Sekuensial dengan Operator Parallel.....	19
Gambar 2.11 Contoh Diagram Sekuensial dengan Operator <i>Loop</i>	19
Gambar 3.1 Diagram Tahapan Penelitian.....	23
Gambar 3.2 Diagram Arsitektur Objek Penelitian.....	26
Gambar 4.1 Diagram Arsitektur Hub Manajemen Keamanan Terpusat.....	34
Gambar 4.2 Diagram Alur Komparasi Aktivitas Inventarisasi Komponen Baru Metode Manual (Existing) dan Metode Usulan (<i>Proposed</i>).....	39
Gambar 4.3 Diagram Alur Komparasi Aktivitas Pemeliharaan Kredensial (Perubahan <i>Password</i>) Metode Manual (Kiri) dan Metode Usulan (Kanan).....	41
Gambar 4.4 Diagram Alur Komparasi Aktivitas Pemantauan Kesehatan Multi-Komponen Metode Manual (Kiri) dan Metode Usulan (Kanan).....	43
Gambar 4.5 Diagram Alur Komparasi Aktivitas Inventarisasi Daftar Agen (<i>Agent List</i>) Metode Manual (Kiri) dan Metode Usulan (Kanan).....	45
Gambar 4.6 Diagram Alur Komparasi Aktivitas Investigasi On-Demand Metode Manual (Kiri) dan Metode Usulan (Kanan).....	47
Gambar 4.7 Diagram Alur Komparasi Aktivitas Investigasi Alert (<i>Click-to-Investigate</i>) Metode Manual (Kiri) dan Metode Usulan (Kanan).....	49
Gambar 4.8 Diagram Alur Komparasi Aktivitas Konfigurasi API <i>Threat Intelligence</i> Metode Manual (Kiri) dan Metode Usulan (Kanan).....	51
Gambar 4.9 Diagram Alur Komparasi Aktivitas Konfigurasi Notifikasi Metode Manual (Kiri) dan Metode Usulan (Kanan).....	53
Gambar 4.10 Diagram Alur Komparasi Aktivitas Uji Coba Integrasi (<i>Connectivity Test</i>) Metode Manual (Kiri) dan Metode Usulan (Kanan).....	55
Gambar 4.11 Diagram Alur Komparasi Aktivitas Pemantauan Status Komponen Metode Manual (Kiri) dan Metode Usulan (Kanan).....	57
Gambar 4.12 Diagram Ilustrasi Orkestrasi Kontainer dalam Docker.....	63
Gambar 4.13 Potongan Konfigurasi Bagian PostgreSQL docker-compose.yaml.....	65
Gambar 4.14 Potongan Konfigurasi Bagian Redis docker-compose.yaml.....	66
Gambar 4.15 Potongan Konfigurasi Bagian Hub docker-compose.yaml.....	67
Gambar 4.16 Potongan Konfigurasi <i>Background Scheduler</i> docker-compose.yaml.....	67



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.17 Konfigurasi Bagian Volume <i>Global</i> docker-compose.yaml.....	68
Gambar 4.18 Diagram Alur Sekuensial Penambahan Komponen Berhasil.....	70
Gambar 4.19 Diagram Alur Sekuensial Penambahan Komponen Gagal.....	71
Gambar 4.20 Antarmuka Manajemen Komponen Infrastruktur (Wazuh <i>Indexer</i>)...	72
Gambar 4.21 Antarmuka Manajemen Komponen Infrastruktur (Wazuh <i>Manager</i>)	72
Gambar 4.22 Raw Response <i>Unauthorized</i> untuk Wazuh <i>Manager</i> dan <i>Indexer</i>	73
Gambar 4.23 Raw Response Generasi <i>Token</i> JWT pada Wazuh <i>Manager</i> via CLI.	73
Gambar 4.24 Raw Response Data Log dari Wazuh <i>Indexer</i> via CLI.....	74
Gambar 4.25 Potongan Kode Konektor Wazuh <i>Indexer</i> (HTTP Basic <i>Authentication</i>).....	75
Gambar 4.26 Potongan Konektor Wazuh <i>Manager</i> (JWT & <i>Caching</i>).....	77
Gambar 4.27 Potongan Kode Model Data <i>WazuhManager</i>	78
Gambar 4.28 Tampilan Table <i>wazuh_indexers</i>	78
Gambar 4.29 Tampilan Table <i>wazuh_managers</i>	78
Gambar 4.30 Potongan Kode <i>Controller</i> Hub Multi-Wazuh.....	79
Gambar 4.31 Potongan Kode Logika Edit dan <i>Delete</i> Hub Multi-Wazuh.....	81
Gambar 4.32 Tampilan Notifikasi <i>Toast</i> saat Mengedit Komponen.....	81
Gambar 4.33 Tampilan Notifikasi <i>Toast</i> saat Update Komponen Berhasil.....	82
Gambar 4.34 Tampilan <i>Modal</i> untuk Konfirmasi Penghapusan Komponen.....	82
Gambar 4.35 Tampilan <i>Toast</i> Notifikasi Saat Berhasil Menghapus Komponen..	82
Gambar 4.36 Potongan Kode Logika Frontend <i>Refresh</i>	83
Gambar 4.37 Tampilan Notifikasi <i>Toast</i> saat <i>Refresh</i> dari <i>Cache</i>	84
Gambar 4.38 Tampilan Notifikasi <i>Toast</i> saat <i>Refresh Live Status</i>	84
Gambar 4.39 Tampilan Status Indikator saat Komponen Tersambung.....	84
Gambar 4.40 Tampilan Status Indikator saat Komponen Terputus.....	85
Gambar 4.41 Proses Manual Penarikan Data Agen Wazuh via CLI (Sistem Lama <i>As-Is</i>).....	86
Gambar 4.42 Diagram Alur Sekuensial Sistem Penarikan Data Multi-Agen secara Paralel (Sistem <i>Proposed</i>).....	87
Gambar 4.43 Potongan Fungsi Kode Agregasi Paralel.....	89
Gambar 4.44 Potongan Kode Fungsi Pengayaan Data di dalam <i>Thread</i>	89
Gambar 4.45 <i>Field Manager</i> Name yang diambil dari enrichment.....	90
Gambar 4.46 Diagram Abstraksi Mekanisme <i>Caching</i> Operasional.....	91
Gambar 4.47 Potongan Kode Logika Redis <i>Caching</i>	92
Gambar 4.48 Tampilan UI Wazuh <i>Agents</i>	92
Gambar 4.49 Tampilan Pencarian dan Filtering <i>Agent</i>	93
Gambar 4.50 Potongan Kode JS Logika URL <i>State Management</i>	94
Gambar 4.51 Tautan Interaktif Agen menuju <i>Dashboard</i> Analisis.....	94



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.52 Panel Interaktif <i>Connected Agents</i> di Dashboard.....	95
Gambar 4.53 Antarmuka Web AlienVault OTX untuk Mencari Satu IP.....	96
Gambar 4.54 Antarmuka Tab Analysis di Web AlienVault OTX.....	96
Gambar 4.55 Antarmuka Tab Pulses di Web AlienVault OTX.....	97
Gambar 4.56 Respons Mentah (Raw JSON) dari API AlienVault OTX via Terminal.....	97
Gambar 4.57 Diagram Alur Sekuensial Investigasi Asinkron (<i>Threat Intelligence</i>).....	99
Gambar 4.58 Potongan Kode Fungsi Konektor dan Penarikan Data OTX.....	101
Gambar 4.59 Potongan Model Penyimpanan <i>Threat Intelligence</i>	103
Gambar 4.60 Bentuk <i>Ciphertext</i> dari <i>encrypted_api_key</i>	103
Gambar 4.61 Bagian Tab <i>Intelligence</i> di Dashboard.....	104
Gambar 4.62 Hasil <i>Threat Intelligence</i> di Modul untuk Pencarian IoC IPv4....	104
Gambar 4.63 Hasil <i>Threat Intelligence</i> di Modul untuk Pencarian IoC domain	105
Gambar 4.64 Tampilan Related Threat Pulses.....	106
Gambar 4.65 Komponen Interaktif JSON <i>Document Explorer</i>	107
Gambar 4.66 Tombol Lookup untuk <i>Shortcut Intelligence</i> pada Dashboard....	108
Gambar 4.67 Diagram Alur Sekuensial Pemantauan Latar Belakang (Sentinel)....	109
Gambar 4.68 Potongan Kode Fungsi Utama Pemantauan.....	111
Gambar 4.69 Potongan Kode Fungsi Evaluasi Status <i>UP DOWN</i> Komponen..	113
Gambar 4.70 Diagram Alur Sekuensial Pengiriman Pesan Asinkron (Pub/Sub)....	114
Gambar 4.71 Potongan Kode Konektor API Telegram.....	115
Gambar 4.72 Tampilan Pembuatan Bot Telegram dengan BotFather.....	116
Gambar 4.73 Tampilan Grup Telegram.....	117
Gambar 4.74 Tampilan URL untuk Mendapatkan Chat ID Grup Telegram.....	117
Gambar 4.75 Tampilan <i>Field Configuration</i> untuk Input Bot Token dan Chat IDs.	118
Gambar 4.76 Tampilan <i>Toast</i> Sukses dan Keseluruhan Page Telegram Integration	118
Gambar 4.77 Tampilan Notifikasi <i>Test Message</i>	119
Gambar 4.78 Potongan Kode Fungsi Pemformatan Teks Telegram.....	120
Gambar 4.79 Perintah CLI untuk Mensimulasikan Skenario B (Pemadaman Server Target).....	121
Gambar 4.80 Umpan Balik Peringatan Kritis dan Pemulihan pada Telegram...	122
Gambar 4.81 Peringatan Berkala (Reminder) pada Insiden Pemadaman Jangka Panjang.....	123
Gambar 4.82 Banner Peringatan Kegagalan Proses Pemantauan Latar Belakang...	123
Gambar 4.83 Halaman Login Sistem Hub Manajemen Terpusat.....	124



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.84 Tampilan Antarmuka Manajemen Pengguna Khusus Administrator.	125
Gambar 4.85 Adaptasi Dinamis Menu Navigasi Peran <i>Executor</i>	125
Gambar 4.86 Adaptasi Dinamis Menu Navigasi Peran <i>Viewer</i>	126
Gambar 4.87 Grafik Komparasi Waktu Muat Antarmuka.....	164
Gambar 4.88 Grafik Komparasi Waktu Eksekusi Asinkron dan Timeout.....	165
Gambar 4.89 Grafik Komparasi Waktu Latensi Notifikasi.....	166
Gambar 4.86 Grafik Komparasi Langkah per Aksi Operasional Eksisting & Usulan.....	171
Gambar 4.87 Grafik Komparasi detik per Operasional Eksisting & Usulan.....	172





DAFTAR TABEL

Tabel 2.1. Perbandingan Karakteristik Komponen Arsitektur Wazuh.....	11
Tabel 2.2. Perbandingan Penelitian Terkait.....	20
Tabel 4.1. Daftar Kebutuhan Perangkat Keras (<i>Hardware</i>).....	31
Tabel 4.2. Daftar Kebutuhan Perangkat Lunak (<i>Software</i>).....	32
Tabel 4.3. Perbandingan Alur Kerja Inventarisasi Komponen Baru.....	38
Tabel 4.4. Perbandingan Alur Kerja Pemeliharaan Kredensial.....	40
Tabel 4.5. Perbandingan Alur Kerja Pemantauan Kesehatan Multi-Komponen...	42
Tabel 4.6. Perbandingan Alur Kerja Inventarisasi Daftar Agen.....	44
Tabel 4.7. Perbandingan Alur Kerja Investigasi <i>On-Demand</i>	46
Tabel 4.8. Perbandingan Alur Kerja Investigasi <i>Alert (Click-to-Investigate)</i>	48
Tabel 4.9. Perbandingan Alur Kerja Konfigurasi API <i>Threat Intelligence</i>	50
Tabel 4.10. Perbandingan Alur Kerja Konfigurasi Notifikasi Telegram.....	52
Tabel 4.11. Perbandingan Alur Kerja Uji Coba Integrasi (<i>Connectivity Test</i>).....	54
Tabel 4.12. Perbandingan Alur Kerja Identifikasi Insiden <i>Down</i>	56
Tabel 4.13. Penjelasan Peran Redis dalam Sistem.....	58
Tabel 4.14. Penjelasan Spesifikasi <i>Key</i> Redis per Modul.....	60
Tabel 4.15. Penjelasan Spesifikasi <i>Key</i> Redis per Modul.....	62
Tabel 4.16. Spesifikasi Kontainer dan Alokasi Layanan.....	64
Tabel 4.17. Tabel Daftar Skenario dan Keadaan <i>State Machine</i>	112
Tabel 4.18. Skenario Pengujian Modul Sentralisasi Multi-Wazuh.....	128
Tabel 4.19. Skenario Pengujian Modul Integrasi <i>Threat Intelligence</i>	132
Tabel 4.20. Skenario Pengujian Modul Notifikasi Status Sistem.....	134
Tabel 4.21. Skenario Pengujian Waktu Respons (<i>Response Time</i>).....	137
Tabel 4.22. Skenario Pengujian Keamanan Data (<i>Security</i>).....	138
Tabel 4.23. Skenario Pengujian Keandalan (<i>Reliability & Fault Tolerance</i>).....	139
Tabel 4.24. Prosedur Pengujian Efisiensi Aksi 1 (Inventarisasi Komponen Baru)....	140
Tabel 4.25. Prosedur Pengujian Efisiensi Aksi 2 (Pemeliharaan Kredensial).....	141
Tabel 4.26. Prosedur Pengujian Efisiensi Aksi 3 (Pemantauan Kesehatan Multi-Komponen).....	142
Tabel 4.27. Prosedur Pengujian Efisiensi Aksi 4 (Inventarisasi Daftar Agen).....	143
Tabel 4.28. Prosedur Pengujian Efisiensi Aksi 5 (Investigasi <i>On-Demand</i>).....	144
Tabel 4.29. Prosedur Pengujian Efisiensi Aksi 6 (Investigasi <i>Alert</i>).....	145
Tabel 4.30. Prosedur Pengujian Efisiensi Aksi 7 (Konfigurasi API Intelijen).....	146
Tabel 4.31. Prosedur Pengujian Efisiensi Aksi 8 (Konfigurasi Notifikasi).....	146
Tabel 4.32. Prosedur Pengujian Efisiensi Aksi 9 (Uji Coba Integrasi).....	147
Tabel 4.33. Prosedur Pengujian Efisiensi Aksi 10 (Pemantauan Status).....	148
Tabel 4.34. Hasil Pengujian Modul Sentralisasi Multi-Wazuh.....	150

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tabel 4.35 Hasil Pengujian Modul Sentralisasi <i>Threat Intelligence</i>	152
Tabel 4.36 Hasil Pengujian Modul Telegram Notifikasi Status Sistem.....	153
Tabel 4.37 Hasil Pengujian Waktu Muat Antarmuka (NF.1.1).....	155
Tabel 4.38 Hasil Pengujian Eksekusi Asinkron & <i>Timeout</i> (NF.1.2).....	156
Tabel 4.39 Hasil Pengujian Latensi Notifikasi (NF.1.3).....	157
Tabel 4.40 Hasil Pengujian Keamanan Data (NF.2).....	158
Tabel 4.41 Hasil Pengujian Keandalan (<i>Reliability</i>).....	159
Tabel 4.42 Rekapitulasi Data Waktu Penyelesaian (<i>Time on Task</i>).....	160
Tabel 4.43 Rekapitulasi Data Jumlah Langkah Interaksi (<i>Step Count</i>).....	161
Tabel 4.44 Tingkat Efisiensi (<i>Reduction Rate</i>) per Aksi Operasional.....	169





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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*. Baruwat 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



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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*.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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/>.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- 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-Keyboards 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/>.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- 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). <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].



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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/ijrem43432>.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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., Fadhilahman, 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/ijssrm/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>.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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.

Shafiyah, A., Nama, G.F. dan Pradipta, R.A. 2024. "Implementasi Wazuh Menggunakan Metode PPDIIO 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>.

**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- 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>.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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>.

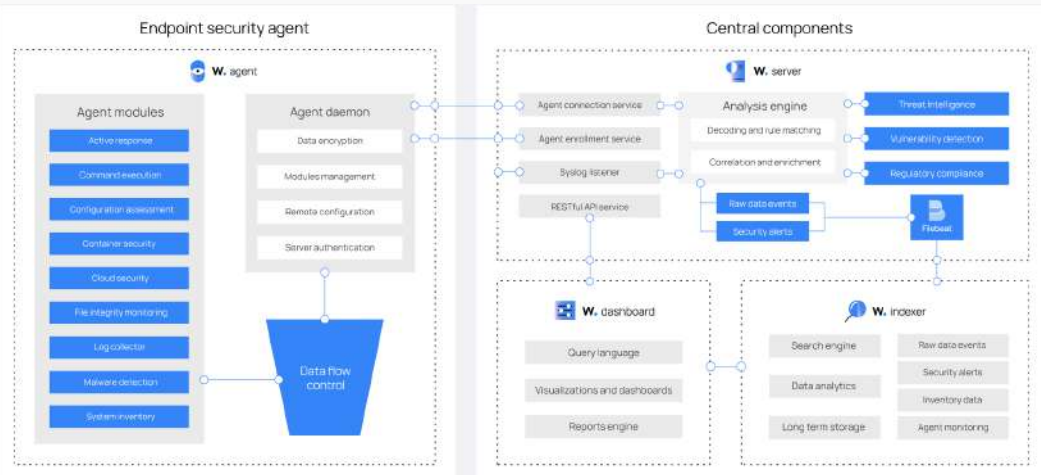
World Economic Forum. 2025. *Global Cybersecurity Outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf#page=4.02.

**POLITEKNIK
NEGERI
JAKARTA**

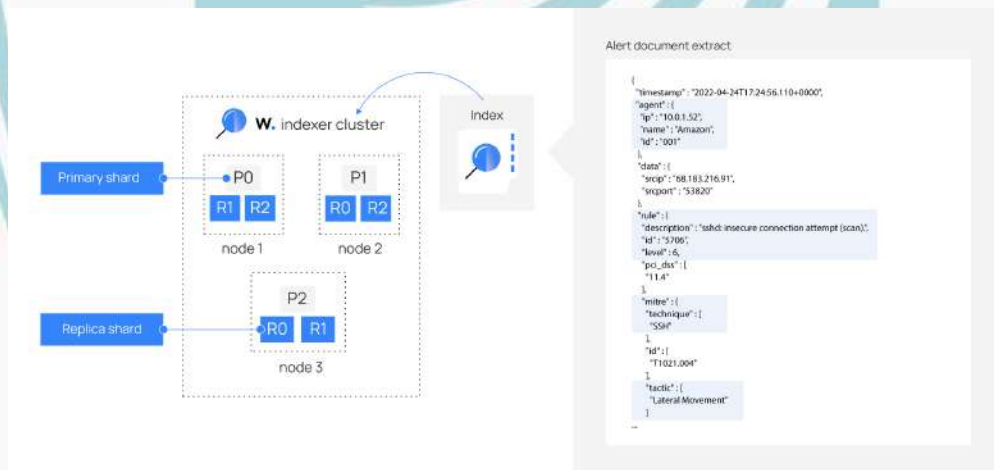


LAMPIRAN

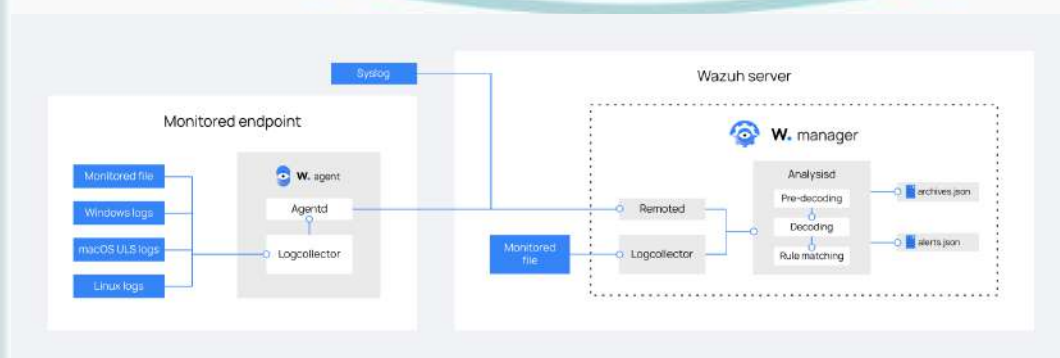
Lampiran 1 Diagram Arsitektur Wazuh



Lampiran 2 Diagram Arsitektur Komponen Wazuh Indexer



Lampiran 3 Diagram Arsitektur Komponen Wazuh Manager



Hak Cipta :

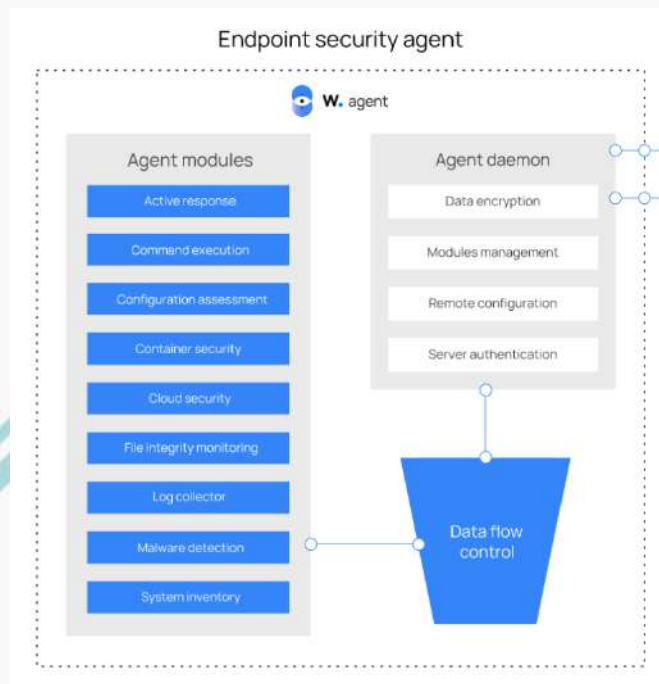
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 4 Diagram Arsitektur Komponen Wazuh Agent



POLITEKNIK
NEGERI
JAKARTA



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	

Hak Cipta :

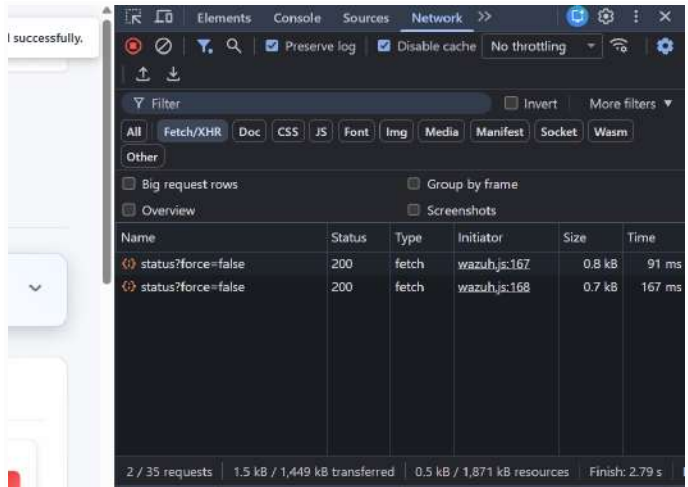
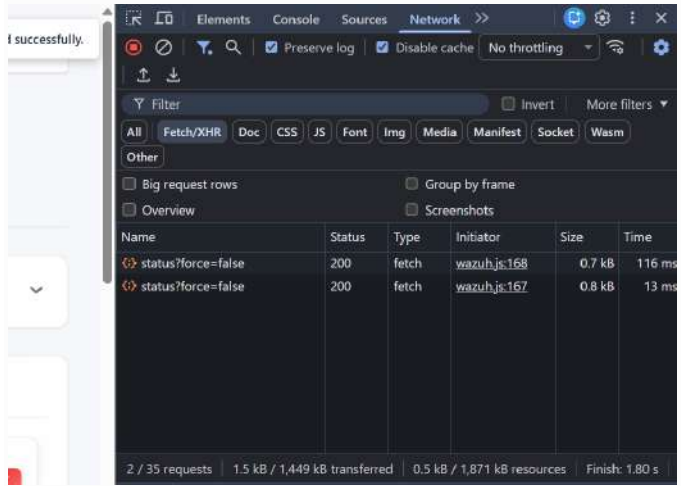
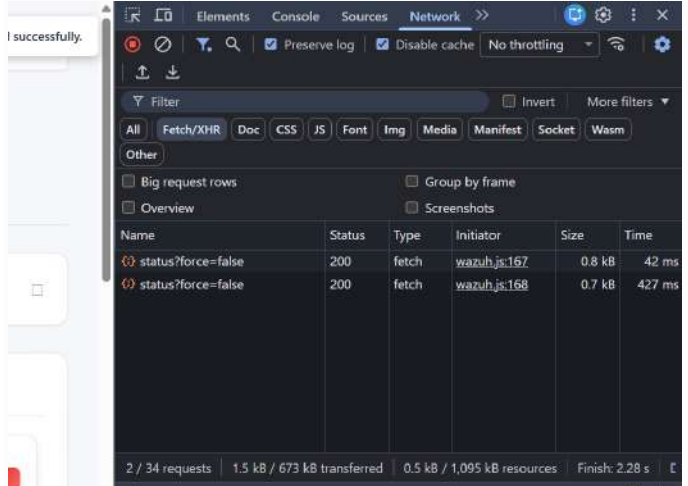
- Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
- Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

(lanjutan)

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



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

(lanjutan)

- Iterasi 1	6,23 s	1 successfully. 2 / 35 requests 1.5 kB / 1,449 kB transferred 0.5 kB / 1,871 kB resources Finish: 6.23 s
- Iterasi 2	9,78 s	1 successfully. 2 / 35 requests 1.5 kB / 1,449 kB transferred 0.5 kB / 1,871 kB resources Finish: 9.78 s
- Iterasi 3	4,87 s	successfully. 2 / 35 requests 1.5 kB / 1,449 kB transferred 0.5 kB / 1,871 kB resources Finish: 4.87 s



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

(lanjutan)

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



(lanjutan)

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

(lanjutan)

- Iterasi 5	30,55 s	The screenshot shows the Chrome DevTools Network tab with two requests: 'status?force=false' and 'status?force=false'. Both requests have a status of 200 and a type of 'fetch'. The initiator for both is 'wazuh.js:167' and 'wazuh.js:168' respectively. The sizes are 0.8 kB and 0.7 kB, and the times are 2.13 s and 2.16 s. The bottom status bar shows '2 / 35 requests', '1.5 kB / 593 kB transferred', '0.5 kB / 1,016 kB resources', 'Finish: 30.55 s', and 'DOM'.
-------------	---------	--

POLITEKNIK
NEGERI
JAKARTA



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

Threat Intelligence Search
Enter an Indicator of Compromise (e.g., IP, Domain, Hash) to analyze.
Data is provided by AlienVault OTX.

Q 44d88612fea8a6f36de82e1276abb02f **ANALYZE**

Example indicators:
192.168.1.1 malicious-site.com 44d88612fea8a6f36de82e1276abb02f

Analysis Failed for: 44d88612fea8a6f36de82e1276abb02f
Failed to retrieve analysis result

Name	Status	Type	Initiator	Size	Time
alerts?page=1&per_page=1	(failed) ne...	fetch	api.js:149	0.0 kB	1 ms
alerts?page=1&per_page=1	(failed) ne...	fetch	api.js:149	0.0 kB	1 ms
alerts?page=1&per_page=1	(failed) ne...	fetch	api.js:149	0.0 kB	1 ms
analyze	(failed) ne...	fetch	intelligence.js:81	0.0 kB	6 ms
alerts?page=1&per_page=1	(failed) ne...	fetch	api.js:149	0.0 kB	1 ms
analyze	202	fetch	intelligence.js:81	0.6 kB	311 ms
alerts?page=1&per_page=1	200	fetch	api.js:149	2.1 kB	174 ms
status	(failed) ne...	fetch	api.js:182	0.0 kB	1 ms
status	(failed) ne...	fetch	api.js:183	0.0 kB	1 ms
d54b9244-b52c-459d-8a28-0224e0f5...	(failed) ne...	fetch	intelligence.js:113	0.0 kB	2 ms
alerts?page=1&per_page=1	(failed) ne...	fetch	api.js:149	0.0 kB	1 ms

83 / 176 requests 266 kB / 3,483 kB transferred 248 kB / 4,906 kB resources Finish 3.8 min DOMContentLoaded

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

Configured Indexers

- Chris Indexer
https://192.168.111.6:9200
- Honeypot

```

RX errors 0 dropped 0 overruns 0 frame 0
TX packets 14113617 bytes 4749317261 (4.7 GB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

chris@lst-thread-intel-risk:~$ ls
lamis-docker ldap-auto opencti wazuh-agent_4.12.0-1_amd64.deb wazuh-docker
chris@lst-thread-intel-risk:~$ cd wazuh-docker/
chris@lst-thread-intel-risk:~/wazuh-docker$ cd single-node/
chris@lst-thread-intel-risk:~/wazuh-docker/single-node$ date; docker compose pause
Wed May 26 11:05:24 AM WIB 2026
WARN[0000] /home/chris/wazuh-docker/single-node/docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Pausing 2/2
✓ Container single-node-wazuh.manager-1 Paused 0.0s
✓ Container single-node-wazuh.indexer-1 Paused 0.0s
  
```

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

SOAR Alerting
CRITICAL HEALTH ALERT

Component Offline:
Wazuh Indexer - Wazuh Server C

Failure Details:
Connection timed out. The server is unreachable or slow.

Detected At: 2026-05-20 11:05:49 WIB

```

RX errors 0 dropped 0 overruns 0 frame 0
TX packets 14113617 bytes 4749317261 (4.7 GB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

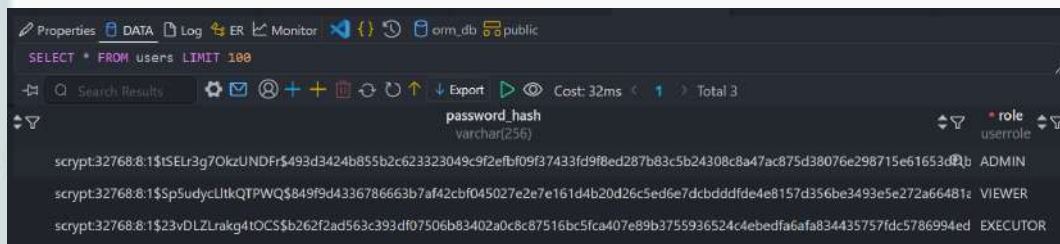
chris@lst-thread-intel-risk:~$ ls
lamis-docker ldap-auto opencti wazuh-agent_4.12.0-1_amd64.deb wazuh-docker
chris@lst-thread-intel-risk:~$ cd wazuh-docker/
chris@lst-thread-intel-risk:~/wazuh-docker$ cd single-node/
chris@lst-thread-intel-risk:~/wazuh-docker/single-node$ date; docker compose pause
Wed May 26 11:05:24 AM WIB 2026
WARN[0000] /home/chris/wazuh-docker/single-node/docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Pausing 2/2
✓ Container single-node-wazuh.manager-1 Paused
✓ Container single-node-wazuh.indexer-1 Paused
chris@lst-thread-intel-risk:~/wazuh-docker/single-node$
  
```

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

id	name	url	username	encrypted_password	is_active
2	Ubuntu 2	https://192.168.111.7:9200	admin	gAAAAABo9ddT1dAX10ZbtayicgDTTea-FNTa0SmA3	true
5	Tama Wazuh	https://192.168.111.5:9200	admin	gAAAAABpIWY_7z5gcZNI6UvABow4yXPDVVOjQi	true
6	Chris Indexer	https://192.168.111.6:9200	admin	gAAAAABpoQ0fk-tu4RK0cNaCl69zk1UK5Ce0cnvK	true
1	Honeypot	https://192.168.111.2:9200	admin	gAAAAABo9bRpaBRASKL40cPZBhcW79zeReavenf	true

Hak Cipta :

- Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
- Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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


Properties DATA Log ER Monitor orm_db public

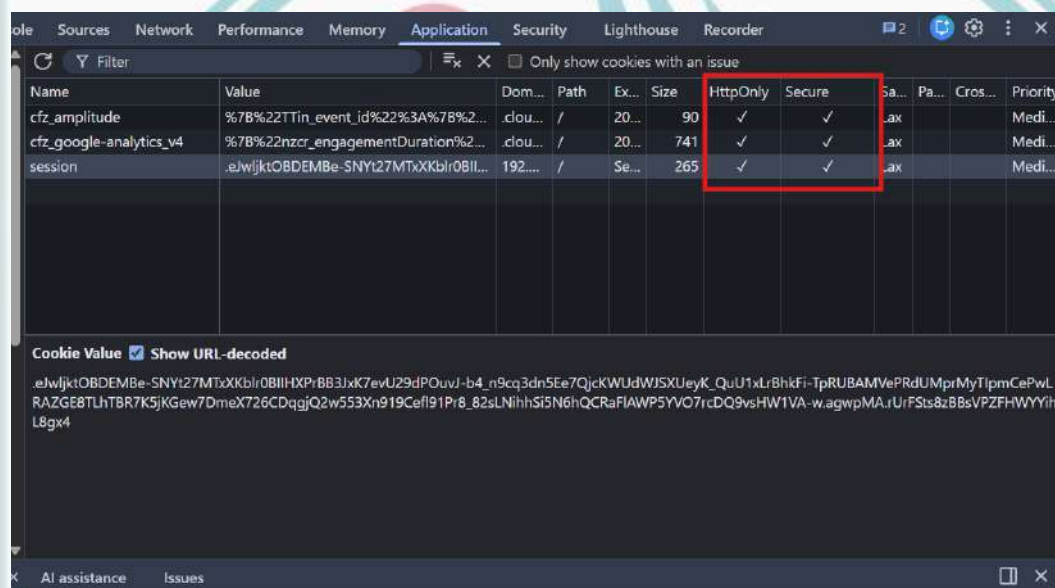
SELECT * FROM users LIMIT 100

Search Results

password_hash varchar(256)

Cost: 32ms 1 Total 3

sCrypt:32768:8:1\$tSElr3g7OkzUNDFr\$493d3424b855b2c623323049c9f2efbf09f37433fd9f8ed287b83c5b24308c8a47ac875d38076e298715e61653d0b	ADMIN
sCrypt:32768:8:1\$SpSudyclUlkQTPWQ\$849f9d4336786663b7af42cbf045027e2e7e161d4b20d26c5ed6e7dcbdddfde4e8157d356be3493e5e272a66481a	VIEWER
sCrypt:32768:8:1\$23vDLZLrakg4tOCS\$b262f2ad563c393df07506b83402a0c8c87516bc5fca407e89b3755936524c4ebdfaf6af834435757fde5786994ed	EXECUTOR

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


ole Sources Network Performance Memory Application Security Lighthouse Recorder

Filter Only show cookies with an issue

Name	Value	Dom...	Path	Ex...	Size	HttpOnly	Secure	sa...	Pa...	Cros...	Priority
cfz_amplitude	%7B%22Ttin_event_id%22%3A%7B%2...	.clou...	/	20...	90	✓	✓	.ax			Medi...
cfz_google-analytics_v4	%7B%22nzc_engagementDuration%2...	.clou...	/	20...	741	✓	✓	.ax			Medi...
session	.ejwljktOBDEMBE-SNYt27MTxXKblr0BIL...	192...	/	Se...	265	✓	✓	.ax			Medi...

Cookie Value Show URL-decoded

.ejwljktOBDEMBE-SNYt27MTxXKblr0BILHXPrBB3jxK7evU29dPOUwJ-b4_n9cq3dn5Ee7QjcKWUdWJSXUeyK_QuU1xLrBhkFi-TpRUBAMVePRdUMprMyTpmCePwLRAZGE8TLhTBR7K5JKGew7DmeX726CDqgjQ2w553Xn919Cefl91Pr8_82sLNihhS15N6hQCRaFlAWP5YVO71rcDQ9vsHW1VA-w.agwpMA.iUrFSst8zBBsVPZFHWYYihL8gx4

AI assistance Issues



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

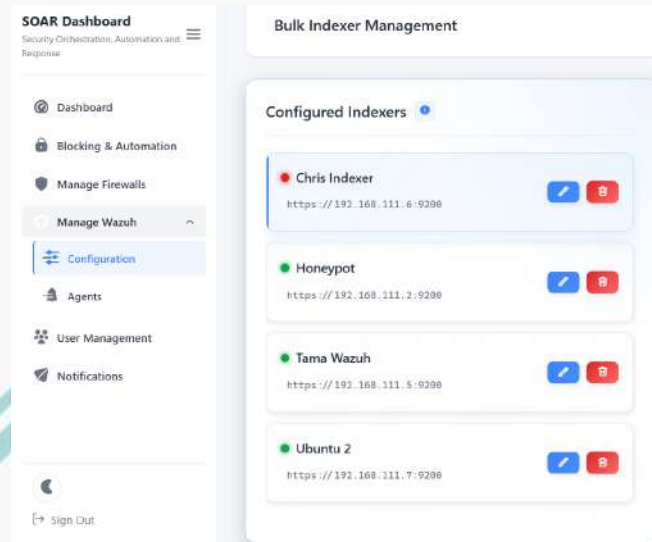
NEGERI
JAKARTA



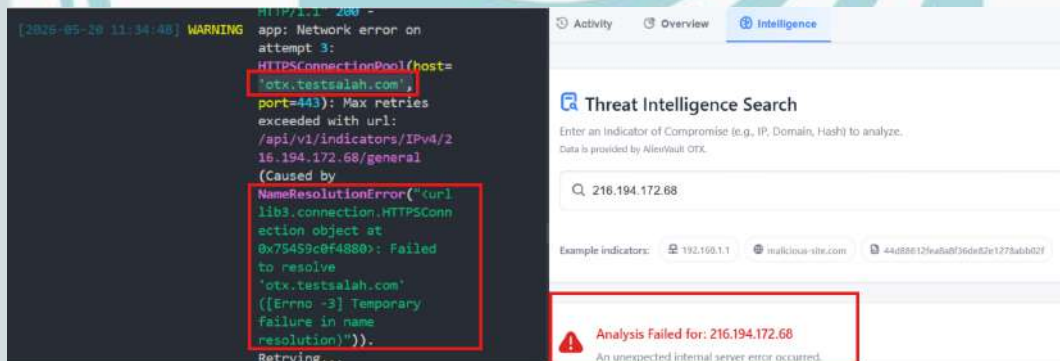
Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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



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





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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)

```

2026-05-20 11:54:06] ERROR HTTP/1.1" 200 -
app: HTTP Error sending to
-4933498946, 404 -
{"ok":false,"error_code":404,"description":"Not Found"}
INFO werkzeug: 127.0.0.1 - - [20/May/2026 11:54:06]
"[35m[1mPOST
/notifications/telegram/test HTTP/1.1[2m" 500 -
2026-05-20 11:54:07] ERROR app: Network error during
INFO app: Background task finished.
INFO app: Successfully cached summary stats for 58985 alerts.
INFO app: Successfully recalculated and cached overview statistics.
INFO app: Autoblocking is globally disabled. Skipping processing.

```

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

ID Aksi	Metode Eksisting (Manual)			Metode Sistem Usulan (Hub Terpusat)		
	Waktu Mulai (<i>Start</i>)	Waktu Selesai (<i>End</i>)	Total Waktu	Waktu Mulai (<i>Start</i>)	Waktu Selesai (<i>End</i>)	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



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

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