Router : Jurnal Teknik Informatika dan Terapan
Volume. 3 Nomor. 4 Desember 2025
e-ISSN : 3032-3312; p-ISSN : 3026-3611, Hal. 120-134
DOI: https://doi.org/10.62951/router.v3i4.752
Tersedia: https://journal.aptii.or.id/index.php/Router

Implementasi dan Evaluasi Sistem Keamanan Siber Berbasis Wazuh, Shuffle, dan Yara di Pusat Data Diskominfo Kota Tangerang dengan Metode PPDIOO

Muhammad Ridwan Na'im[1], Yudi Kurniawan[2]*
[1-2]Program Studi Teknik Informatika, Universitas Pamulang, Indonesia
Penulis Korespondensi: dosen00298@unpam.ac.id

Abstract. *Tangerang City has the most applications in Indonesia, with 222 applications. All of these applications are supported by more than 100 servers located in the data center of the Tangerang City Communication and Information Agency. The large number of servers and applications that are managed brings up new problems in the midst of increasing complex cyber threats, especially in government data centers. One of them is how to monitor and respond quickly when there is an attack on the existing system. The implementation of a cyber security system based on Wazuh, Shuffle, and YARA is able to monitor threats in realtime and automate responses against attacks. Wazuh acts as a log-based monitoring and detection platform and behavior analysis, Shuffle is used to automate incident response through integrated workflow, and YARA is applied for signature-based malware identification. The PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) method used in this research is used as a framework in designing and evaluating the system. From the research conducted, it is expected that Wazuh successfully monitors anomalies that occur on the server which will then be forwarded to Shuffle to automate the next steps to be taken. YARA integrated with Wazuh also successfully detects and quarantines malicious files that enter the server automatically based on the available signature list.*

Keywords: *Information Security; PPDIOO; Shuffle; Wazuh; YARA.*

Abstrak. Kota Tangerang adalah daerah yang memiliki aplikasi terbanyak di Indonesia, yaitu 222 aplikasi. Semua aplikasi tersebut didukung lebih dari 100 server yang berada pada pusat data Dinas Komunikasi dan Informatika Kota Tangerang. Banyaknya server dan aplikasi yang dikelola memunculkan masalah baru di tengah peningkatan ancaman siber yang kompleks, khususnya di pusat data pemerintahan. Salah satunya adalah, bagaimana cara melakukan monitoring dan respons cepat ketika terjadi serangan terhadap sistem yang ada. Implementasi sistem keamanan siber berbasis Wazuh, Shuffle, dan YARA mampu memonitoring ancaman secara realtime dan mampu mengautomasi respons terhadap serangan. Wazuh berperan sebagai platform monitoring dan deteksi berbasis log serta analisis perilaku, Shuffle dimanfaatkan untuk mengautomasi respons insiden melalui workflow terintegrasi, dan YARA diterapkan untuk identifikasi malware berbasis signature. Metode PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) yang digunakan dalam penelitian ini digunakan sebagai framework dalam merancang dan mengevaluasi sistem. Dari penelitian yang dilakukan, diharapkan Wazuh berhasil memonitoring anomali yang terjadi pada server yang kemudian log tersebut akan diteruskan ke Shuffle untuk automasi langkah yang akan diambil selanjutnya. YARA yang terintegrasi dengan Wazuh juga diharapkan mampu mendeteksi dan mengkarantina malicious file yang masuk ke server secara otomatis berdasarkan daftar signature yang tersedia.

Kata kunci: Keamanan Informasi; PPDIOO; Shuffle; Wazuh; YARA.

1. LATAR BELAKANG

Era digital telah mendorong institusi pemerintah untuk meningkatkan layanan publik dan manajemen pemerintahan melalui aplikasi dan sistem informasi yang terintegrasi. Pemerintah Kota Tangerang, yang menjadi pelopor dalam adopsi teknologi informasi, telah mengembangkan ekosistem digital yang luas dengan 222 aplikasi dan lebih dari 100 *server* di pusat data Dinas Komunikasi dan Informatika Kota Tangerang (DISKOMINFO Kota Tangerang, 2023). Infrastruktur TI yang dimiliki cukup kompleks dan rentan terhadap berbagai ancaman, termasuk ancaman siber. Ancaman siber bisa menyebabkan gangguan layanan elektronik dan membahayakan data sensitif yang dipegang pemerintah. Untuk mengatasi

Naskah Masuk: 18 Oktober 2025; Revisi: 17 November 2025; Diterima: 29 Desember 2025; Terbit: 31 Desember 2025

tantangan ini, Pemerintah Kota Tangerang telah membentuk TangerangKota-CSIRT (*Computer Security Incident Response Team*) melalui kerja sama dengan Badan Siber dan Sandi Negara (BSSN) (Pemerintah Kota Tangerang, 2022). Tujuan tim ini adalah untuk memantau, menerima laporan, meninjau, dan merespons insiden keamanan siber.

Upaya keamanan yang sebelumnya diterapkan, seperti penilaian keamanan aplikasi dan pemasangan *firewall*, merupakan langkah positif tetapi belum cukup untuk menghadapi kompleksitas ancaman modern. Penelitian sebelumnya menunjukkan bahwa menggabungkan berbagai alat keamanan seperti *Security Information and Event Management* (*SIEM*), *Security Orchestration Automation and Response* (*SOAR*), dan perangkat deteksi *malware* dapat meningkatkan efektivitas deteksi dan respons insiden. Penelitian yang dilakukan oleh Saputra et al. (2024), membuktikan bahwa Wazuh, sebagai solusi *SIEM open-source*, dapat mendeteksi berbagai jenis serangan, termasuk *brute force* dan *SQL injection*, dengan notifikasi *real-time*. Sementara itu, penelitian oleh Muhammad Nayyul Habibie (2024) menunjukkan bahwa mengintegrasikan Wazuh dengan *SOAR* menggunakan Shuffle dapat meningkatkan efisiensi respons insiden secara signifikan melalui otomatisasi alur kerja.

Kedua penelitian tersebut sudah cukup baik, namun belum menerapkan YARA sebagai alat deteksi *malware* berbasis *signature*. Selain itu, penelitian sebelumnya belum menerapkan Wazuh beserta integrasinya dalam konteks pusat data pemerintah daerah dengan infrastruktur TI yang kompleks. Selain memiliki infrastruktur TI yang kompleks, keterbatasan personel keamanan informasi di TangerangKota-CSIRT menjadi tantangan tersendiri sehingga sistem yang diimplementasikan harus memiliki kemampuan otomatisasi proses. Proses ini tidak hanya perlu efektif dalam mendeteksi ancaman tetapi juga mampu memberikan respons otomatis untuk mengurangi beban kerja operasional.

Penelitian ini penting karena akan memberikan model implementasi praktis yang dapat diterapkan pada konteks serupa di institusi pemerintah lainnya. Penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi sistem keamanan siber yang terintegrasi. Sistem ini harus memiliki kemampuan deteksi *ancaman real-time*, respons otomatis terhadap insiden, dan deteksi *malware* berbasis *signature* di pusat data Dinas Komunikasi dan Informatika Kota Tangerang. Metode yang digunakan dalam penelitian ini adalah *PPDIOO* (*Prepare, Plan, Design, Implement, Operate, Optimize*). Sistem ini diharapkan dapat menciptakan layanan publik dan pemerintahan yang lebih aman dan optimal.

2. KAJIAN TEORITIS

Sistem Keamanan Siber dan Komponen *SOC*

Sistem adalah sekumpulan komponen yang saling berinteraksi untuk mencapai tujuan tertentu (Nafisah & Handayani Ujianti, 2024). Sedangkan Meriam-Webster mendefinisikan keamanan siber adalah suatu tindakan yang dilakukan untuk melindungi komputer atau sistem komputer terhadap serangan dan akses tidak sah (Cains et al., 2022). Maka sistem keamanan siber dapat diartikan sebagai sekumpulan komponen yang saling berinteraksi untuk melindungi sistem komputer dari serangan dan akses tidak sah. Sistem ini biasa dioperasikan dalam ekositem *Security Operation Center* (*SOC*). *SOC* adalah komponen penting dalam infrastruktur keamanan informasi. Van tony & Setiadi Yazid (2024) mendefinisikan *SOC* sebagai pusat operasi keamanan yang bertanggungjawab untuk memantau, mendeteksi, dan merespons insiden keamanan siber melalui tim analis, operator, dan pakar.

SOC dibentuk berdasarkan *framework People, Process, and Technology* (*PPT*). Aspek teknologi berarti mengharuskan *SOC* memiliki alat baik perangkat keras maupun perangkat lunak untuk mencapai tujuan deteksi dan respons. Salah satu perangkat lunak yang ada dalam ekosistem *SOC* adalah *Security Information and Event Management* (*SIEM*). *SIEM* berfungsi sebagai tulang punggung *SOC* dengan kemampuan mengumpulkan *log* dari berbagai sumber, melakukan analisis *event*, dan menyajikan informasi keamanan dalam format yang dapat dipahami oleh analis keamanan. Menurut Rijal Kamal & Andri Setiawan (n.d.), *SIEM* dapat mendeteksi *log* berbagai *event* yang berasal dari sumber data secara *real-time* dengan kemampuan koleksi, pemantauan, analisis, penyimpanan, dan pelaporan yang menyeluruh.

Perangkat lunak lainnya yang biasa digunakan dalam ekosistem *SOC* adalah *Security Orchestration, Automation, and Response* (*SOAR*). *SOAR* memberikan kemampuan otomatisasi dalam merespons insiden keamanan. Menurut Gustina DM & Ananda (2024), *SOAR* adalah alat otomasi keamanan yang menyederhanakan dan mengotomatiskan respons terhadap insiden keamanan. Integrasi *SIEM* dengan *SOAR* memungkinkan peringatan dari *SIEM* direspons secara otomatis tanpa memerlukan intervensi manual sehingga mengurangi waktu respons dan meminimalkan dampak insiden.

Wazuh *SIEM*

Menurut Shafiyyah et al. (2024), Wazuh adalah perangkat lunak *open-source* yang berfungsi sebagai sistem deteksi berbasis *host* (*endpoint*) yang menyatukan kemampuan *External Data Representation* dan *Security Information and Event Management* (*SIEM*). Arsitektur Wazuh terdiri dari tiga komponen utama yaitu *Wazuh Indexer* yang bertanggung jawab menyimpan dan mengindeks data *log*, *Wazuh Server* yang melakukan pemrosesan dan

analisis *log*, serta *Wazuh Dashboard* yang menyediakan antarmuka visualisasi untuk analisis dan monitoring.

Penelitian sebelumnya menunjukkan efektivitas Wazuh dalam berbagai skenario deteksi ancaman. Saputra et al. (2024) melaporkan bahwa Wazuh berhasil mendeteksi serangan *brute force, SQL injection*, dan *denial of service* melalui *log* Suricata *IDS* yang terintegrasi dan mampu mengirimkan notifikasi *real-time* ke Telegram. Lebih lanjut, Shafiyyah et al. (2024) mendemonstrasikan bahwa integrasi Wazuh dengan *active response* berbasis Fail2ban dapat mencegah serangan *brute force* secara otomatis, meskipun terdapat keterbatasan dalam mendeteksi serangan *denial of service* dengan skala tinggi di bawah 4000 koneksi HTTP rata-rata.

Shuffle *SOAR*

Shuffle adalah perangkat lunak *Security Orchestration, Automation, and Response* (*SOAR*). Menurut Ødegårdstuen (2020), Shuffle merupakan interpretasi *open-source* dari *SOAR* dengan tujuan menghadirkan semua kemampuan yang diperlukan untuk mentransfer data ke seluruh perusahaan dengan aplikasi *plug-and-play*, sehingga otomatisasi dapat diakses oleh semua orang. Penelitian yang dilakukan Muhammad Nayyul Habibie (2024) menyatakan bahwa integrasi Wazuh dengan *SOAR* (Shuffle), *Incident Management* (TheHive), analisis ancaman (Cortex), dan *Firewall Fortigate* mampu meningkatkan efisiensi dan efektivitas respons terhadap insiden keamanan siber. Shuffle memiliki kemampuan mengorkestrasi alat-alat keamanan, memungkinkan respons yang lebih cepat, dan konsisten terhadap berbagai jenis ancaman.

YARA untuk Deteksi *Malware* Berbasis *Signature*

YARA adalah alat yang ditujukan untuk (tetapi tidak terbatas pada) membantu peneliti malware untuk mengidentifikasi dan mengklasifikasikan sampel malware (VirusTotal, 2024). Penulisan YARA *rules* mirip dengan bahasa pemrograman yang memungkinkan definisi variabel untuk mewakili pola yang diidentifikasi dalam *malware*. Menurut Patel et al. (2023), YARA *rules* seperti bahasa pemrograman yang beroperasi dengan menentukan variabel yang menunjukkan pola yang diidentifikasi dalam *malware*, tergantung pada aturannya. Jika satu atau semua kondisi terpenuhi, aturan tersebut dapat digunakan untuk mengidentifikasi *malware*.

Confusion Matrix

Evaluasi sistem keamanan siber memerlukan metodologi yang *robust* untuk mengukur akurasi deteksi dan mengidentifikasi area yang perlu ditingkatkan. *Confusion matrix* adalah metode evaluasi performa sistem yang membandingkan hasil prediksi sistem dengan kondisi

sesungguhnya di lapangan. Matriks ini mengklasifikasikan hasil dalam empat kategori utama: *true positive* (*TP*) di mana prediksi dan nilai aktual sama-sama benar, *true negative* (*TN*) di mana keduanya salah, *false positive* (*FP*) di mana prediksi benar tetapi nilai aktual salah, dan *false negative* (*FN*) di mana prediksi salah tetapi nilai aktual benar (Suci Amaliah et al., 2022).

Dari *confusion matrix* ini dapat diturunkan beberapa metrik evaluasi yang penting. Akurasi mengukur seberapa kuat sistem dapat mengklasifikasikan dengan benar, presisi mengukur akurasi antara data yang diperlukan dengan hasil prediksi dari sistem (dengan nilai presisi besar menunjukkan rendahnya *false positive*), *recall* mengukur seberapa baik sistem dalam menemukan semua data positif, dan *F1-Score* merupakan harmonik rata-rata dari presisi dan *recall* yang cocok digunakan pada data yang tidak seimbang. Penggunaan metrik-metrik ini sangat penting dalam konteks keamanan siber karena sistem yang terlalu ketat akan meningkatkan false positive sementara sistem yang terlalu longgar akan meningkatkan *false negative*.

Metode *PPDIOO* Cisco

Metode *PPDIOO* (*Prepare, Plan, Design, Implement, Operate, Optimize*) adalah metode yang dikembangkan oleh Cisco untuk mendukung pengembangan dan pemeliharaan infrastruktur jaringan secara berkelanjutan. Menurut Arini et al. (2024), metode *PPDIOO* adalah kerangka kerja manajemen jaringan yang sistematis untuk memastikan perencanaan, penerapan, dan pemeliharaan jaringan yang efektif. Metode ini telah terbukti efektif dalam berbagai konteks implementasi sistem keamanan, khususnya ketika menangani infrastruktur yang kompleks. Penerapan metode ini dalam membangun sistem keamanan siber telah menunjukkan keberhasilan dalam menghasilkan sistem yang stabil dan optimal sebagaimana penelitian Widyantono & Sulistyo (2023) dan Shafiyyah et al. (2024).

3. METODE PENELITIAN

Penelitian yang dilakukan menggunakan metode kualitatif dan kuantitatif. Metode kualitatif dilakukan dengan observasi terhadap infrastruktur yang ada serta wawancara dengan *stakeholder* terkait. Sedangkan aspek kuantitatif ditunjukkan dengan pengumpulan data *log* keamanan dan evaluasi sistem menggunakan *confusion matrix* untuk mengukur akurasi, presisi, *recall*, dan *F1-score* dari sistem yang telah diterapkan.

Objek Penelitian

Objek penelitian adalah Pusat Data Dinas Komunikasi dan Informatika Kota Tangerang yang berlokasi di Gedung Pusat Pemerintahan Kota Tangerang Lantai 4, Jalan Satria, RT

02/RW 01, Kelurahan Sukaasih, Kecamatan Tangerang, Kota Tangerang. Penelitian dilaksanakan dari tahap persiapan hingga optimasi dalam periode enam bulan.

Populasi dan Sampel Penelitian

Populasi penelitian mencakup seluruh infrastruktur TI yang ada di pusat data Dinas Komunikasi dan Informatika Kota Tangerang. Sampel penelitian yaitu *server-server* kritis yang dipilih berdasarkan kriteria pentingnya layanan aplikasi yang dijalankan dan sensitivitas data yang dikelola.

Teknik dan Instrumen Pengumpulan Data

Pengumpulan data dilakukan melalui metode berikut:

1) Wawancara (*interview*) dilakukan dengan *stakeholder* terkait termasuk ketua tim Keamanan Informasi dan Persandian, teknisi sistem, dan analis keamanan informasi untuk mendapatkan pemahaman menyeluruh tentang infrastruktur TI, kebutuhan keamanan siber, tantangan operasional yang dihadapi, dan ekspektasi dari implementasi sistem keamanan yang akan dilakukan.
2) Observasi langsung dilakukan terhadap arsitektur dan topologi pusat data, konfigurasi *network*, penempatan *server*, sistem monitoring yang ada, dan proses operasional yang sedang berjalan.
3) Studi literatur, yaitu mengumpulkan referensi mengenai *SIEM* Wazuh, *SOAR* Shuffle, deteksi *malware* dengan YARA, metodologi *PPDIOO*, *threat intelligence*, dan *best practices* dalam implementasi *Security Operation Center*. Literatur dikumpulkan dari jurnal penelitian, publikasi resmi perangkat lunak yang digunakan, dan dokumentasi teknis yang relevan.

Variabel Penelitian dan Definisi Operasional

Variabel independen penelitian mencakup tiga komponen teknologi utama: (1) Wazuh sebagai *SIEM* untuk fungsi *log collection*, monitoring, dan *event correlation*; (2) Shuffle sebagai *SOAR* untuk fungsi *workflow automation* dan *orchestration*; (3) YARA sebagai *detection engine* untuk identifikasi *malware* berbasis *signature*. Sedangkan variabel dependen adalah kapabilitas sistem keamanan dalam hal deteksi ancaman (*threat detection*) dan respons ancaman (*threat response*), serta efisiensi operasional yang dicapai melalui otomatisasi.

Deteksi ancaman didefinisikan sebagai kemampuan sistem untuk mengidentifikasi aktivitas mencurigakan atau ancaman keamanan terhadap infrastruktur yang dipantau. Respons ancaman didefinisikan sebagai kemampuan sistem untuk melakukan tindakan *automated* terhadap insiden yang terdeteksi, termasuk *blocking*, karantina, atau notifikasi. Efisiensi

operasional diukur dari pengurangan waktu respons terhadap insiden dan pengurangan beban kerja manual pada petugas keamanan informasi.

Metode Implementasi Sistem *PPDIOO*

Implementasi sistem keamanan siber dalam penelitian ini menggunakan metodologi *PPDIOO* yang terdiri dari enam fase sebagai berikut:

1) Fase *Prepare* (Persiapan): Pada fase ini dilakukan observasi mendalam terhadap topologi jaringan pusat data, identifikasi *server-server* kritis dan aplikasi-aplikasi penting.
2) Fase *Plan* (Perencanaan): Fase ini mencakup perencanaan strategis implementasi sistem dengan mempertimbangkan topologi jaringan yang kompleks untuk meminimalkan disrupsi terhadap operasional yang sedang berjalan.
3) Fase *Design* (Desain): Pada fase ini dilakukan perancangan arsitektur sistem keamanan siber yang komprehensif, khususnya desain integrasi antara Wazuh, Shuffle, dan YARA.
4) Fase *Implement* (Implementasi): Fase implementasi mencakup instalasi dan konfigurasi setiap komponen sistem (*Wazuh Indexer, Wazuh Server, Wazuh Dashboard*, Shuffle), penyiapan *agents* dan YARA pada *server* yang akan dipantau, serta konfigurasi lainnya yang diperlukan.
5) Fase *Operate* (Operasi): Fase operasional mencakup pengoperasian sistem secara penuh dengan monitoring terus-menerus terhadap kinerja sistem dan akurasi deteksi.
6) Fase *Optimize* (Optimasi): Melakukan optimasi terhadap berbagai aspek sistem berdasarkan fase operasi, khususnya optimasi *rules* untuk mengurangi *false positive* dengan tetap mempertahankan kemampuan deteksi terhadap ancaman sebenarnya.

Metode Analisis Data

Analisis data sistem deteksi ancaman menggunakan pendekatan *confusion matrix* yang mengklasifikasikan hasil deteksi sistem ke dalam empat kategori: *true positive* (insiden yang terdeteksi dan benar-benar merupakan ancaman), *true negative* (insiden normal yang diidentifikasi dengan benar sebagai bukan ancaman), *false positive* (insiden normal yang salah diidentifikasi sebagai ancaman), dan *false negative* (insiden yang merupakan ancaman tetapi tidak terdeteksi sistem).

Berdasarkan klasifikasi *confusion matrix* tersebut, dihitung metrik-metrik evaluasi sebagai berikut:

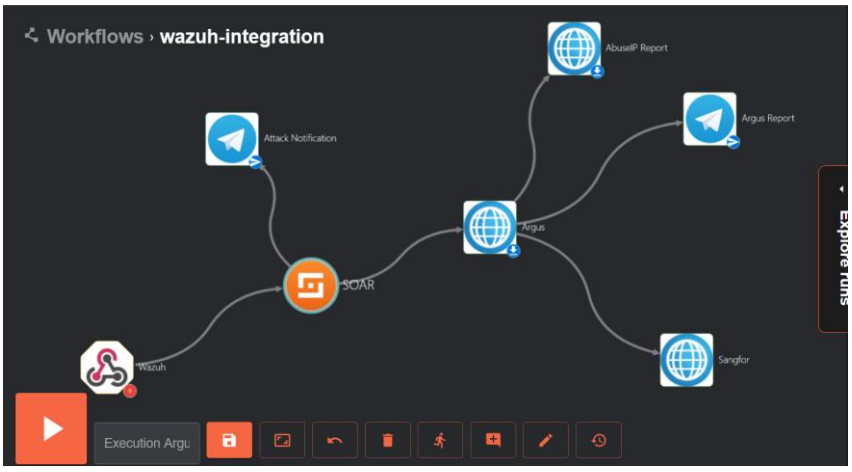
1) Akurasi = *(TP + TN) / (TP + TN + FP + FN)*, mengukur seberapa kuat sistem dapat mengklasifikasikan dengan benar secara keseluruhan.
2) Presisi = *TP / (TP + FP)*, mengukur proporsi *alert* positif yang benar-benar merupakan ancaman sebenarnya, dengan nilai tinggi menunjukkan rendahnya *false positive*.
3) *Recall* = *TP / (TP + FN)*, mengukur proporsi ancaman sebenarnya yang berhasil terdeteksi sistem, dengan nilai tinggi menunjukkan rendahnya *false negative*.
4) F1-*Score* = 2 × (Presisi × *Recall*) / (Presisi + *Recall*), merupakan harmonik rata-rata presisi dan *recall* yang cocok digunakan ketika data tidak seimbang.

Analisis kualitatif dilakukan melalui observasi terhadap efektivitas alur kerja otomatisasi yang diimplementasikan menggunakan Shuffle, evaluasi terhadap waktu respons sistem dalam merespons insiden, serta analisis terhadap dokumentasi insiden untuk mengidentifikasi pola ancaman dan efektivitas respons yang dilakukan.

4. HASIL DAN PEMBAHASAN

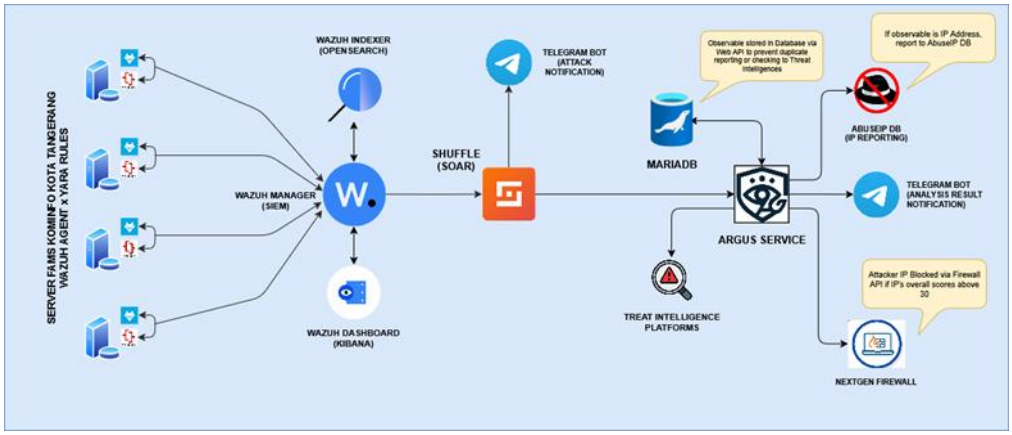
Hasil Implementasi Sistem

Implementasi sistem keamanan siber berbasis Wazuh, Shuffle, dan YARA pada pusat data Pemerintah Kota Tangerang berhasil dilakukan dengan metode *PPDIOO*. Wazuh mengumpulkan *log* dari 70 *endpoint* melalui *agent* yang terpasang, melakukan analisis berdasarkan *rules* yang dibuat, dan mengirimkan *alert* yang memenuhi kriteria ke *webhook* Shuffle.



Gambar 1. Workflow Shuffle.

Selanjutnya dilakukan ekstraksi data, *filtering*, dan orkestrasi *workflow* oleh Shuffle untuk mengirimkan notifikasi ke Telegram, melakukan analisis *observable* (*IP* atau *hash*) melalui Argus-*OSINT* yang terintegrasi dengan *Threat Intelligence Platforms*, dan melakukan pemblokiran *IP* otomatis pada *firewall* berdasarkan hasil analisis.



Gambar 2. Arsitektur sistem yang diimplementasikan.

Hasil implementasi menunjukkan bahwa sistem mampu mendeteksi berbagai jenis serangan termasuk *file inclusion, SQL injection, cross-site scripting, webshell scanning, SEO cloaking attempts, dan sensitive file scanning*. Selain itu, Wazuh mampu mendeteksi *outgoing connection* mencurigakan dan eksekusi perintah melalui pengguna tidak sah. Selain itu, pengujian terhadap kemampuan deteksi YARA membuktikan bahwa sistem berhasil mengidentifikasi dan melakukan karantina terhadap *webshell* yang diunggah ke *server* melalui modul *File Integrity Monitoring*.

Hasil Evaluasi Deteksi Wazuh

Evaluasi deteksi Wazuh dilakukan dengan menganalisa 10.919 sampel *event* yang terdiri dari 10.000 *event* dari *log* operasional dan 919 *event* dari simulasi serangan. Data yang dikumpulkan mencakup berbagai teknik serangan seperti *file inclusion, SQL injection, cross-site scripting, webshell scanning, SEO cloaking attempts, sensitive file scanning*, dan trafik normal. Hasil evaluasi Wazuh sebelum optimasi menunjukkan nilai *confusion matrix* dengan hasil sebagai berikut:

Tabel 1. Tabel *confussion matrix* deteksi Wazuh.

		Wazuh Detection		
		Malicious	***Benign***	**Total**
Ground Truth	***Malicious***	10220	138	10358
	Benign	52	509	561
	Total	10272	647	10919

Setelah dilakukan evaluasi dan optimasi melalui penambahan dan perbaikan *rules* Wazuh, terjadi peningkatan kemampuan deteksi Wazuh dengan hasil sebagai berikut:

Tabel 2. Tabel *confussion matrix* deteksi Wazuh setelah optimasi.

		Wazuh Detection		
		Malicious	***Benign***	***Total***
Ground Truth	***Malicious***	11011	33	11044
	Benign	26	520	546
	Total	11037	553	11590

Berdasarkan tabel di atas, didapatkan metrik evaluasi sebagai berikut:

Tabel 3. Tabel metrik evaluasi Wazuh.

Perhitungan	**Sebelum Optimasi**	**Sesudah Optimasi**	**Peningkatan**
Accuracy (Akurasi)	98,26%	99,49%	1,23%
Precision (Presisi)	99,49%	99,76%	0,27%
Recall/Sensitivity (Sensitivitas)	98,67%	99,70%	1,03%
Specificity (Spesifisitas)	90,73%	95,24%	4,51%
F1-Score	99,08%	99,73%	0,65%
False Positive Rate (FPR)	9,27%	4,76%	-4,51%
False Negative Rate (FNR)	1,33%	0,30%	-1,03%
Positive Predictive Value (PPV)	99,49%	99,76%	0,27%
Negative Predictive Value (NPV)	78,67%	94,03%	15,36%

Pengurangan *false positive rate* dari 9,27% menjadi 4,76% dan *false negative rate* dari 1,33% menjadi 0,30% menunjukkan bahwa optimasi berhasil menurunkan *alert fatigue* dan meningkatkan kemampuan menangkap serangan aktual. Nilai *negative predictive value* yang meningkat dari 78,67% menjadi 94,03% mengindikasikan peningkatan signifikan dalam tingkat kepercayaan prediksi negatif sistem.

Hasil Evaluasi Deteksi YARA

Evaluasi deteksi YARA dilakukan dengan melakukan pemindaian terhadap 2.663 sampel *file* yang terdiri dari 165 *malware* (termasuk *webshell*, *binary malware*, dan *malicious file* lainnya) dan 2.498 *benign files*. Pengujian dilakukan dalam lingkungan *sandbox* yang terpisah dari *production* untuk menjamin keamanan.

Hasil evaluasi YARA sebelum optimasi menunjukkan nilai *confusion matrix* sebagai berikut:

Tabel 4. Tabel *confusion matrix* deteksi YARA.

		YARA *Detection*		
		Malicious	***Benign***	**Total**
Ground Truth	***Malicious***	92	73	165
	Benign	4	2494	2498
	Total	96	2567	2663

Setelah dilakukan perbaikan terhadap *rules* YARA yang menimbulkan *false positive*, penambahan *magic bytes checking*, dan pembuatan *rules* baru untuk mendeteksi varian *malware* yang sebelumnya tidak terdeteksi, terdapat peningkatan yang sangat signifikan dengan nilai *confusion matrix* sebagaimana pada tabel berikut:

Tabel 5. Tabel *confusion matrix* YARA setelah optimasi.

		YARA *Detection*		
		Malicious	***Benign***	***Total***
Ground Truth	***Malicious***	164	1	165
	Benign	1	2497	2498
	Total	165	2498	2663

Berdasarkan tabel di atas, didapatkan metrik evaluasi sebagai berikut:

Tabel 6. Tabel metrik evaluasi YARA.

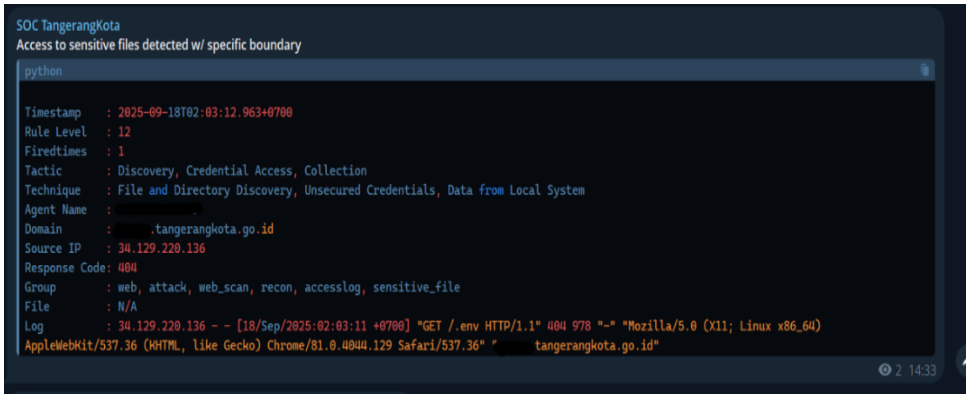
Perhitungan	Sebelum Optimasi	Sesudah Optimasi	Peningkatan
Accuracy (Akurasi)	97,11%	99,92%	2,82%
Precision (Presisi)	95,83%	99,40%	3,56%
Recall/Sensitivity (Sensitivitas)	55,76%	99,40%	43,64%
Specificity (Spesifisitas)	99,84%	99,96%	0,12%
F1-Score	70,50%	99,40%	28,90%
False Positive Rate (FPR)	0,16%	0,04%	-0,12%
False Negative Rate (FNR)	44,24%	0,60%	-43,64%
Positive Predictive Value (PPV)	95,83%	99,40%	3,56%
Negative Predictive Value (NPV)	99,84%	99,96%	0,12%

Pengurangan *false negative rate* dari 44,24% menjadi 0,60% merupakan pencapaian yang sangat signifikan, menunjukkan bahwa sistem berhasil menangkap hampir semua *malware* aktual dengan *false positive rate* 0,04%.

Integrasi dan Otomatisasi Respons

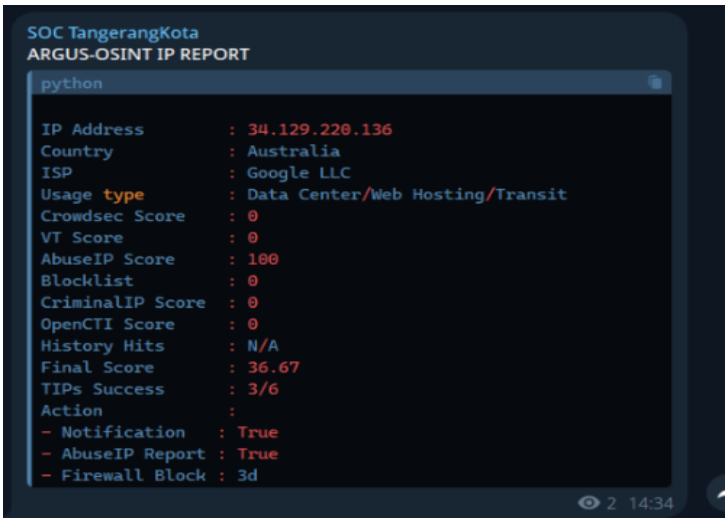
Integrasi antara Wazuh dan Shuffle melalui *webhook* berhasil menghasilkan alur otomatisasi ke berbagai sistem tujuan (Telegram, Argus-*OSINT*, AbuseIPDB, dan *Firewall*).

Hasil pengujian integrasi menunjukkan bahwa notifikasi Telegram berhasil dikirimkan dengan informasi yang terstruktur dan informatif, mencakup *timestamp* serangan, *rule level*, taktik dan teknik MITRE yang digunakan, nama *endpoint*, domain target, *IP source*, *response code*, grup *rule*, dan *raw log*.



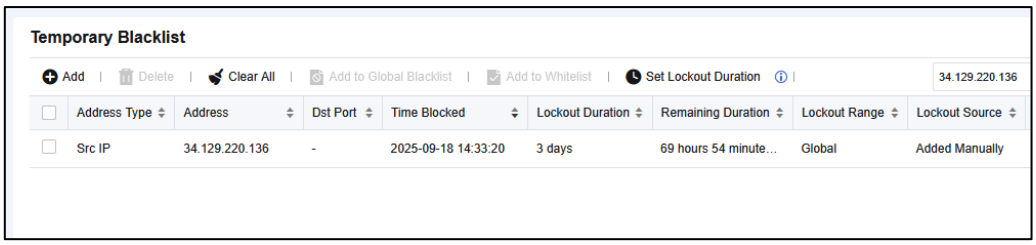
Gambar 3. Notifikasi telegram.

Untuk *observable* berupa *IP address*, Argus-*OSINT* berhasil melakukan analisis menggunakan lima *Threat Intelligence Platform* (VirusTotal, CrowdSec, AbuseIPDB, CriminalIP, dan FireHOL *Blocklist*) dengan performa *aggregation API calls* yang paralel, menghasilkan skor keseluruhan yang akurat dan keputusan pemblokiran yang moderat.



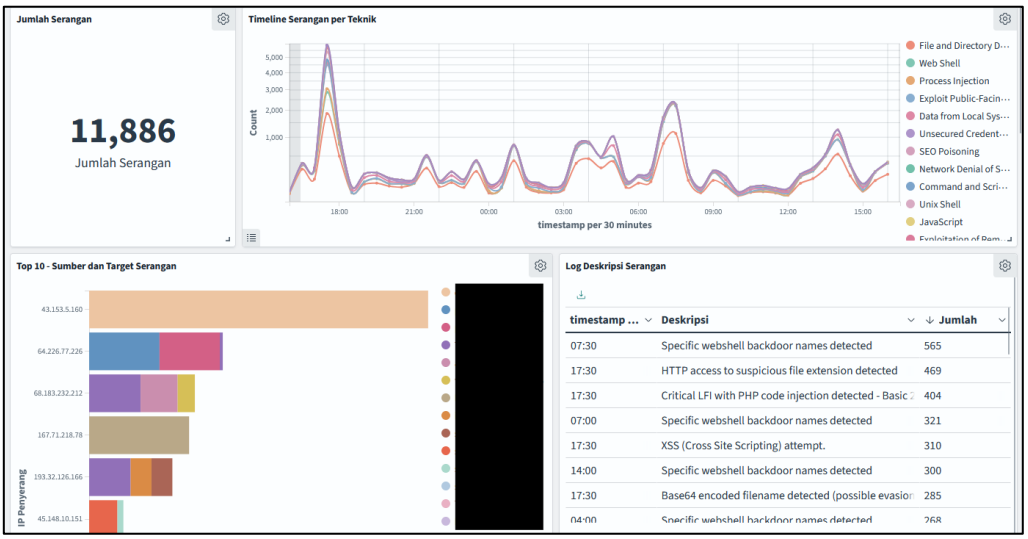
Gambar 4. Notifikasi hasil analisa Argus-*OSINT*.

Pemblokiran otomatis *IP* pada *firewall* berhasil dilakukan dengan skor ancaman ≥ 30, dengan durasi pemblokiran yang bervariasi tergantung skor: 1 hari untuk skor 15-29, 3 hari untuk skor 30-49, 7 hari untuk skor 50-69, dan permanen untuk skor ≥ 70.



Gambar 5. *IP* penyerang terblokir pada *firewall.*

Implementasi sistem menghasilkan efisiensi operasional tim keamanan informasi TangerangKota-CSIRT. Sebanyak 70 *endpoint* yang dipantau secara *real-time* melalui Wazuh, sistem mampu mengumpulkan, menganalisis, dan memproses ribuan *event* per hari tanpa memerlukan intervensi manual untuk setiap *event*. Repons otomatis yang dijalankan melalui Shuffle mengurangi waktu respons dari hitungan jam (ketika memerlukan permintaan manual ke operator jaringan) menjadi detik, meningkatkan *Mean Time To Response* (*MTTR*) sistem secara dramatis. Pengurangan *false positives* dari 9,27% menjadi 4,76% berarti mengurangi *alert fatigue* pada tim *SOC* dan memungkinkan mereka fokus pada investigasi *alert* yang benar-benar merupakan ancaman.



Gambar 6. Dasbor kustom Wazuh.

Selain itu, dibuatkan juga dasbor khusus pada Wazuh yang menyediakan visualisasi data seperti tren serangan, *top attacker IPs*, *country distribution*, *attack techniques*, sehingga memfasilitasi *threat hunting* dan *strategic security planning*. *Log retention policy* yang dikonfigurasi menggunakan *Index State Management* dengan *state transitions* (*hot* → *warm* → *cold* → *delete*) mengoptimalkan *storage efficiency* dengan mempertahankan akses cepat ke data untuk investigasi dalam 30 hari terakhir.

5. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang dilakukan mulai dari tahap persiapan hingga optimasi, semua komponen yang terintegrasi telah berfungsi secara optimal baik dalam hal deteksi, notifikasi, maupun respons seperti pemblokiran *IP*. Proses optimasi yang dilakukan terhadap *rule* Wazuh maupun YARA juga berhasil meningkatkan kemampuan deteksi dan meminimalisir *false positive*. Penelitian selanjutnya disarankan untuk menerapkan Wazuh dalam mode *multi-node* untuk penyeimbangan beban dan *high availability* dalam penerapan skala besar. Pola serangan dan *malware* yang terus berkembang mengharuskan *rule* Wazuh dan YARA diperbarui secara berkala. Maka selain menerapkan sistem monitoring, diperlukan aktivitas *threat hunting* untuk memperoleh tren serangan terkini.

DAFTAR REFERENSI

Arini, A. P., Isworo, M. R. R., & others. (2024). Desain dan manajemen jaringan pada SMA Negeri 15 Surabaya menggunakan Cisco Packet Tracer dengan metode PPDIOO. Prosiding Seminar Nasional Informatika Bela Negara, 4, 26–32.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643–1669. https://doi.org/10.1111/risa.13687

DISKOMINFO Kota Tangerang. (2023, December 15). Sukses terapkan smart city, Kota Tangerang miliki 222 aplikasi hingga diburu 47 daerah. https://diskominfo.tangerangkota.go.id/berita/sukses-terapkan-smart-city-kota-tangerang-miliki-222-aplikasi-hingga-diburu-47-daerah

Gustina, D. M. V., & Ananda, A. (2024). Kecerdasan buatan untuk security orchestration, automation and response: Tinjauan cakupan. Jurnal Komputer Terapan, 10(1), 36–47. https://doi.org/10.35143/jkt.v10i1.6247

Habibie, M. N. (2024). Implementasi security orchestration, automation and response (SOAR) sistem menggunakan Shuffle di Politeknik Caltex Riau (Tesis/Skripsi). Politeknik Caltex Riau.

Nafisah, N., & Ujianti Handayani, M. (2024). Perancangan sistem informasi akademik pengolahan data nilai siswa pada SD Negeri Mangunsaren 02 berbasis website. JATI (Jurnal Mahasiswa Teknik Informatika), 9(1), 138–144. https://doi.org/10.36040/jati.v9i1.12231

Ødegårdstuen, F. S. (2020, May 20). Introducing Shuffle—An open source SOAR platform (Part 1). Medium. https://medium.com/shuffle-automation/introducing-shuffle-an-open-source-soar-platform-part-1-58a529de7d12

Patel, P. S., Kunwar, R. S., & Thakar, A. (2023). Malware detection using YARA rules in SIEM. In Advances in cybersecurity analytics (pp. 313–330). IGI Global. https://doi.org/10.4018/978-1-6684-8666-5.ch014

Pemerintah Kota Tangerang. (2022, February 21). Jaga keamanan lembaga, Diskominfo launching Kota Tangerang CSIRT. https://www.tangerangkota.go.id/berita/detail/29867/jaga-keamanan-lembaga-diskominfo-launching-kota-tangerang-csirt

Rijal Kamal, M., & Setiawan, A. (n.d.). Deteksi anomali dengan security information and event management (SIEM) Splunk pada jaringan UII.

Saputra, F. A., Dharmawan, T. R., & Rustianto, A. (2024). Implementasi Wazuh SIEM untuk manajemen log event di Pesantren Teknologi Informasi dan Komunikasi Jombang. Jurnal Informatika Terpadu, 10(2), 146–155. https://doi.org/10.54914/jit.v10i2.1435

Shafiyyah, A., Nama, G. F., & Pradipta, R. A. (2024). Implementasi Wazuh menggunakan metode PPDIOO di sistem keamanan jaringan PSDKU Universitas Lampung Way Kanan sebagai deteksi dan respons serangan siber. Jurnal Informatika dan Teknik Elektro Terapan, 12(2). https://doi.org/10.23960/jitet.v12i2.4074

Suci Amaliah, N., Nusrang, M., & Aswi, A. (2022). Penerapan metode random forest untuk klasifikasi varian minuman kopi di Kedai Kopi Konijiwa Bantaeng. VARIANSI: Journal of Statistics and Its Application on Teaching and Research, 4(3), 121–127. https://doi.org/10.35580/variansiunm31

Van Tony, F., & Yazid, S. (2024). Perancangan tim security operation center di perusahaan sektor finansial: Studi kasus dan analisis. Cyber Security dan Forensik Digital, 7(2), 95–110. https://doi.org/10.14421/csecurity.2024.7.2.4895

VirusTotal. (2024, December 13). YARA in a nutshell. https://virustotal.github.io/yara/

Widyantono, D. P., & Sulistyo, W. (2023). Pemodelan intrusion prevention system untuk pendeteksi dan pencegahan penyebaran malware menggunakan Wazuh. Journal of Information Technology Ampera, 4(1), 113–127.