sudo
Jurnal Teknik Informatika
https://jurnal.ilmubersama.com/index.php/sudo

Artikel Penelitian

# Otomatisasi Respons pada Sistem Keamanan Siber Terintegrasi *Threat Intelligence* pada Pusat Data Pemerintah Kota Tangerang dengan Metode *PPDIOO*

*Muhammad Ridwan Na'im* [*], *Yudi Kurniawan*

*Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia*

INFORMASI ARTIKEL

Diterima Redaksi: 15 Mei 2026
Revisi Akhir: 02 Juni 2026
Diterbitkan *Online*: 20 Juni 2026

KATA KUNCI

Sistem Keamanan Siber
Wazuh *SIEM*
*Threat Intelligence*
Shuffle *SOAR*
*PPDIOO*

KORESPONDENSI (*)

E-mail: muhammadridwannaim@gmail.com

**A B S T R A K**

Pemerintah Kota Tangerang memiliki ratusan aplikasi layanan publik dan manajemen pemerintahan yang memiliki risiko tinggi terhadap serangan siber. Aplikasi-aplikasi tersebut di-*hosting* pada pusat data yang dikelola oleh Dinas Komunikasi dan Informatika Kota Tangerang. Keterbatasan jumlah personel keamanan informasi menjadi tantangan dalam melakukan pengawasan serta mitigasi ancaman siber. Selain itu, tim keamanan masih mengalami kesulitan dalam menentukan indikator yang memengaruhi tingkat ancaman, sehingga berdampak pada ketepatan pengambilan keputusan. Oleh karena itu, diperlukan suatu sistem keamanan siber yang terintegrasi dan terotomatisasi. Penelitian ini bertujuan untuk mengintegrasikan Wazuh sebagai *Security Information and Event Management* (*SIEM*) dengan platform otomasi Shuffle dalam melakukan respons otomatis terhadap serangan siber. Selain itu, pemanfaatan *Threat Intelligence* digunakan untuk meningkatkan akurasi dalam penentuan indikator ancaman. Mempertimbangkan kompleksitas sistem pada pusat data, penerapan solusi ini dilakukan menggunakan metode *PPDIOO* (*Prepare, Plan, Design, Implement, Operate, Optimize*) sebagai kerangka kerja implementasi dan evaluasi. Hasil penelitian menunjukkan bahwa Wazuh mampu mendeteksi berbagai pola serangan dan mengintegrasikannya dengan Shuffle serta *Threat Intelligence* untuk menghasilkan respons otomatis, seperti notifikasi dan pemblokiran pada *firewall*, dalam waktu yang relatif singkat.

## PENDAHULUAN

Kemajuan teknologi informasi mendorong berbagai instansi pemerintah di Indonesia berlomba melakukan digitalisasi layanan publik maupun manajemen pemerintahan. Salah satunya adalah Pemerintah Kota Tangerang yang menjadi pemerintah daerah paling banyak memiliki sistem elektronik di Indonesia. Tercatat sebanyak 222 sistem elektronik baik layanan publik maupun manajemen pemerintahan dikelola dan ditunjang dengan infrastruktur TI yang cukup kompleks pada pusat data Pemerintah Kota Tangerang [1]. Infrastruktur tersebut tentu berisiko tinggi terhadap ancaman siber. Salah satu upaya Pemerintah Kota Tangerang dalam melakukan perlindungan terhadap sistem tersebut yaitu bekerjasama dengan Badan Siber dan Sandi Nasional dalam membentuk TangerangKota-CSIRT [2]. Tim tersebut bertugas untuk melakukan pemantauan, menerima laporan, menganalisa, dan merespons insiden keamanan siber. Selain itu pemanfaatan *firewall* pada pusat data juga dilakukan untuk memperkuat keamanan sistem.

Keterbatasan personel keamanan informasi menjadi tantangan dalam melakukan pengawasan dan respons terhadap serangan siber. Selain itu, tim keamanan juga menghadapi kesulitan dalam menentukan indikator yang relevan untuk mengukur tingkat ancaman. Kondisi tersebut berdampak pada menurunnya akurasi analisis dan keterlambatan pengambilan keputusan. Akibatnya, proses deteksi dan respons insiden masih bersifat reaktif dan membutuhkan waktu yang relatif lama.

https://doi.org/10.56211/sudo.v5i2.1742 

Maka dari itu, diperlukan suatu pendekatan yang mampu mengintegrasikan proses monitoring, analisis, dan respons keamanan secara otomatis. Salah satu solusi yang dapat diterapkan adalah penggunaan *Security Information and Event Management* (*SIEM*) yang dikombinasikan dengan platform *Security Orchestration, Automation, and Response* (*SOAR*). Penelitian ini menggunakan Wazuh sebagai *Security Information and Event Management* (*SIEM*) untuk melakukan pengumpulan dan analisis *log* dari berbagai sumber, sedangkan Shuffle dimanfaatkan sebagai platform *SOAR* untuk menjalankan respons terhadap insiden secara otomatis. Selain itu, integrasi dengan *Threat Intelligence* dilakukan untuk memperkaya informasi ancaman dan meningkatkan akurasi dalam proses deteksi dan pengambilan keputusan.

Mengingat kompleksitas sistem yang berjalan pada pusat data, penerapan solusi keamanan memerlukan kerangka kerja yang sistematis untuk menghindari gangguan pada layanan. Oleh karena itu, penelitian ini menggunakan metode *PPDIOO* (*Prepare, Plan, Design, Implement, Operate, Optimize*) sebagai panduan dalam merancang, mengimplementasikan, serta mengevaluasi sistem keamanan siber yang diusulkan.

Penelitian terdahulu oleh Fahrudi dan Suartana [3], Wazuh berhasil mendeteksi serangan *SQL Injection, Cross-Site Scripting* (*XSS*), dan *brute force* serta mengirimkan notifikasi ke Telegram. Namun, penelitian tersebut masih mengalami keterlambatan pengiriman notifikasi akibat keterbatasan sumber daya perangkat yang digunakan. Penelitian yang dilakukan oleh Shafiyyah [4] menunjukkan bahwa sistem mampu meningkatkan kemampuan monitoring dan respons keamanan jaringan, meskipun masih terdapat keterbatasan dalam mendeteksi serangan DoS dengan intensitas tertentu. Habibie [5] mengimplementasikan platform Shuffle sebagai *SOAR* dan menunjukkan bahwa otomatisasi orkestrasi keamanan mampu meningkatkan efisiensi serta efektivitas respons terhadap insiden keamanan siber. Sementara Hidayat [6] mengintegrasikan Wazuh dengan *MISP* dan *DFIR-IRIS* sehingga mampu meningkatkan presisi deteksi ancaman hingga 96,3% serta mendukung respons insiden secara *real-time*.

Namun, sebagian besar penelitian terdahulu masih berfokus pada implementasi Wazuh sebagai *SIEM*, pemanfaatan Telegram sebagai media notifikasi, atau implementasi *SOAR* secara terpisah. Penelitian yang mengintegrasikan *SIEM, SOAR*, dan *Threat Intelligence* dalam satu arsitektur keamanan dengan evaluasi yang komprehensif masih relatif terbatas, khususnya pada lingkungan pusat data pemerintahan.

Tabel 1 Tabel Komparasi Penelitian

| Penelitian | *SIEM* | *SOAR* | *Threat Intelligence* | Otomatisasi Respons | Evaluasi |
|---|---|---|---|---|---|
| Fahrudi & Suartana (2023) | ✓ | ✗ | ✗ | Notifikasi | Tidak |
| Shafiyyah (2024) | ✓ | ✗ | ✗ | Sebagian | Tidak |
| Habibie (2024) | ✗ | ✓ | ✗ | ✓ | Tidak |
| Hidayat dkk. (2025) | ✓ | ✗ | ✓ | Sebagian | *Confusion Matrix* |
| Penelitian ini | ✓ | ✓ | ✓ | ✓ | *Confusion Matrix* + *Response Time* |

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk membangun dan mengimplementasikan sistem keamanan siber yang terintegrasi dan terotomatisasi dengan memanfaatkan Wazuh, Shuffle, dan *Threat Intelligence*. Kontribusi utama dari penelitian ini adalah (1) integrasi *SIEM* dan *SOAR* dalam satu arsitektur keamanan yang terpadu, (2) penerapan otomatisasi respons terhadap ancaman siber, serta (3) penggunaan *Threat Intelligence* untuk meningkatkan akurasi deteksi dan efektivitas pengambilan keputusan. Diharapkan hasil penelitian ini dapat membantu meningkatkan kemampuan deteksi dan respons terhadap ancaman siber, khususnya pada lingkungan pusat data pemerintahan.

## TINJAUAN PUSTAKA

### *Sistem Keamanan Siber*

Keamanan siber merupakan tindakan yang diambil untuk melindungi komputer atau sistem komputer (seperti di Internet) terhadap akses atau serangan yang tidak sah [7]. Salah satu manfaat utama keamanan siber adalah melindungi data pribadi dan informasi sensitif dari akses yang tidak sah atau pencurian, menjaga integritas data agar tidak terpengaruh oleh manipulasi yang tidak sah, serta memastikan ketersediaan sistem dan layanan bagi pengguna yang berhak [8]. Pendapat ini

menyebutkan tiga fungsi utama yang merupakan bagian dari triad *CIA* (*Confidentiality, Integrity, Availability*). Triad *CIA* adalah model terkenal untuk pengembangan kebijakan keamanan, digunakan untuk mengidentifikasi masalah dan solusi yang diperlukan untuk keamanan dan sistem informasi [9]. Penulis dalam hal ini menafsirkan bahwa istilah keamanan siber dalam kutipan tersebut dimaknai sebagai sistem keamanan siber—yakni serangkaian komponen yang terdiri dari teknologi, manusia, prosedur, dan kebijakan yang saling berkaitan untuk menjamin keamanan sistem informasi secara menyeluruh.

### *Security Information and Event Management*

*Security Information and Event Management* (*SIEM*) adalah sistem monitoring yang dapat mendeteksi *log* dari berbagai peristiwa yang berasal dari sumber data secara *real-time* [10]. *Log* adalah catatan yang berisi aktivitas pada sistem seperti peristiwa keamanan, deteksi kesalahan, pola penggunaan, dan lain-lain. Kemampuan *SIEM* meliputi koleksi, pemantauan, analisis, penyimpanan, dan pelaporan. *SIEM* membutuhkan *log collector* yang dipasang pada sistem yang ingin dipantau aktivitasnya, kemudian *collector* tersebut akan mengirimkannya ke *SIEM*. *Log* yang berhasil dikumpulkan nantinya bisa disajikan dalam bentuk grafis atau tabel sehingga lebih mudah dipahami. Teknologi *SIEM* dapat melakukan teknik korelasi yang terintegrasi dengan berbagai sumber data sehingga data dapat diproses menjadi informasi yang bermanfaat [11].

### *Security Orchestration, Automation, and Response*

*Security Orchestration, Automation, and Response* (*SOAR*) adalah kerangka kerja otomatisasi keamanan yang menyederhanakan dan mengotomatiskan proses respons terhadap insiden keamanan [12]. Berdasarkan penelitian yang dilakukan oleh Wiratama, *SIEM* yang terintegrasi dengan *SOAR* dapat digunakan untuk mengumpulkan, menganalisis, dan merespons data keamanan secara *real-time* sehingga membantu dalam mendeteksi ancaman lebih awal dan merespons secara otomatis [13].

### *Threat Intelligence*

*Threat Intelligence* adalah sistem perangkat lunak khusus yang menerapkan proses pengumpulan, pemrosesan, analisis, produksi, penyebaran, dan integrasi intelijen ancaman internal dan eksternal [14]. Sedangkan McMillan berpendapat bahwa *Threat Intelligence* adalah pengetahuan berbasis bukti, termasuk konteks, mekanisme, indikator, implikasi, dan saran berorientasi tindakan tentang ancaman atau bahaya yang ada atau yang muncul terhadap aset [15]. Terdapat banyak sekali *Threat Intelligence* yang bisa digunakan seperti VirusTotal, Crowdsec, AbuseIP DB, AllienVault, dan lain-lain. Platform tersebut menyediakan *API* gratis dengan kuota permintaan yang dibatasi. Selain itu kita juga bisa menggunakan platform yang bersifat *open source* seperti OpenCTI dan YETI (*Your Everyday Threat Intelligence*).

### *Metode PPDIOO*

Metode *Prepare, Plan, Design, Implement, Operate, Optimize* (*PPDIOO*) adalah kerangka kerja manajemen jaringan yang sistematis untuk memastikan perencanaan, penerapan, dan pemeliharaan jaringan yang efektif [16]. Menurut Shafiyyah, *PPDIOO* Cisco merupakan metodologi dari Cisco yang mendefinisikan siklus layanan berkelanjutan yang dibutuhkan oleh jaringan komputer yang dirancang untuk mendukung pengembangan jaringan [4]. Keunggulan dari metode ini adalah pengurangan *Total Cost of Ownership* (*TCO*) [17]. Kesimpulannya, metode *PPDIOO* Cisco adalah sebuah metode yang dirancang untuk mendukung pengembangan jaringan mulai dari persiapan hingga optimasi dengan keunggulan pengurangan *Total Cost of Ownership*.

## METODOLOGI

### *Metode Wawancara*

Wawancara dilakukan dengan dua narasumber yaitu Katim Keamanan Informasi dan Persandian serta Tenaga Ahli Keamanan Informasi. Metode ini digunakan untuk mendapatkan gambaran awal infrastruktur TI pada pusat data Pemerintah Kota Tangerang, mengetahui kendala operasional yang dihadapi, dan konsultasi mengenai sistem keamanan yang diusulkan.

 https://doi.org/10.56211/sudo.v5i2.1742

### *Metode Implementasi*

*Prepare (Persiapan)*

Pada tahap ini, dilakukan observasi terhadap kebutuhan sistem keamanan siber yang akan diimplementasikan. Observasi meliputi analisa pendalaman terhadap arsitektur sistem dan integrasi aplikasi, topologi jaringan, identifikasi sistem kritis, dan identifikasi kebutuhan yang meliputi kebutuhan fungsional dan non fungsional.

*Plan (Perencanaan)*

Data observasi yang dihimpun pada tahap persiapan dijadikan acuan dalam proses perencanaan. Tahap perencanaan mencakup strategi implementasi dengan mempertimbangkan integrasi sistem dan topologi jaringan yang kompleks untuk meminimalisir gangguan pada sistem yang sedang berjalan. Berdasarkan tahap persiapan, dilakukan juga perencanaan kebutuhan perangkat keras dan perangkat lunak. Hal ini dilakukan untuk memastikan sistem yang dibangun dapat memenuhi tujuan deteksi dan respons ancaman secara otomatis serta mampu beradaptasi dengan infrastruktur yang ada.

*Design (Perancangan)*

Pada tahapan ini, dilakukan perancangan terhadap arsitektur keamanan siber yang akan diimplementasikan seperti integrasi Wazuh dengan sistem otomasi Shuffle, serta *Threat Intelligence*. Desain yang terdokumentasi akan memudahkan dalam melakukan evaluasi, *troubleshooting* dan pengembangan sistem di kemudian hari.

*Implementation (Implementasi)*

Tahap ini merupakan tahapan dimana proses instalasi dan konfigurasi sistem keamanan siber beserta integrasinya dilakukan. Tahapan implementasi dimulai dari instalasi dan konfigurasi *Server* Wazuh, instalasi *Agent* Wazuh pada *server-server* kritis yang akan dipantau, dilanjutkan dengan implementasi sistem otomasi Shuffle, integrasi dengan *Threat Intelligence* dan integrasi dengan perangkat *firewall*.

*Operate (Operasional)*

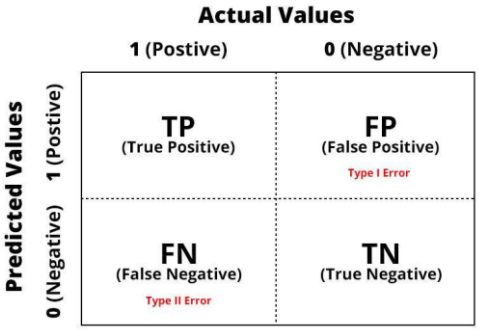
Tahap ini mencakup pengoperasian sistem secara penuh dengan pengawasan ketat terhadap keakuratan sistem dalam deteksi ancaman serta kemampuan sistem otomatisasi dalam merespons serangan.

*Optimize (Optimasi)*

Tahapan optimasi merupakan tahapan evaluasi sistem berdasarkan data operasional untuk mengukur akurasi sistem dalam mendeteksi ancaman. Selain itu, pengukuran waktu respons sistem otomasi Shuffle dari mulai serangan hingga proses notifikasi dan pemblokiran juga dilakukan.

### *Metode Analisis Data*

Pada tahapan operasional, dilakukan pengumpulan data *alert* yang terdeteksi oleh Wazuh. Selain itu akan dilakukan juga uji deteksi dengan percobaan serangan dengan teknik yang beragam. Data-data tersebut kemudian akan dianalisa menggunakan *confusion matrix*. Metode ini akan mengklasifikasikan hasil deteksi Wazuh menjadi empat kategori yaitu: *true positive* (ancaman terdeteksi sebagai ancaman), *true negative* (bukan ancaman, terdeteksi bukan ancaman), *false positive* (bukan ancaman, terdeteksi sebagai ancaman), *false negative* (ancaman, terdeteksi bukan ancaman/tidak terdeteksi) [4].




Gambar 1. Diagram *Confusion Matrix*

## HASIL DAN PEMBAHASAN

Berdasarkan hasil wawancara dengan *stakeholder* terkait dan observasi terhadap pusat data Pemerintah Kota Tangerang, didapatkan hasil mulai dari jumlah *endpoint* yang akan dipantau yaitu berjumlah 290 yang terdiri dari *virtual machine* maupun *bare metal*. Data tersebut digunakan sebagai acuan untuk menentukan spesifikasi *Server* Wazuh dan Shuffle. Berdasarkan dokumentasi resmi Wazuh, spesifikasi *server* yang direkomendasikan untuk 50-100 *endpoint* adalah 8 *Core CPU,* dengan *memory* 8 GB, dan penyimpanan 200 GB untuk 90 hari [18].

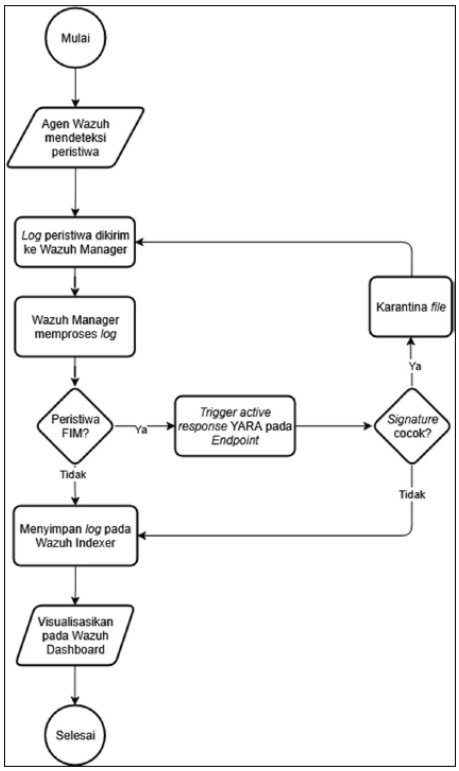
Tabel 2. Spesifikasi *Server* Wazuh

| | | |
|---|---|---|
| **Perhitungan kebutuhan *CPU*:** | | |
| *CPU* | : | Jumlah *endpoint* x 0,08 = 290 x 0,08 = 23,2 Core ~ 23 Core |
| **Perhitungan kebutuhan *memory*:** | | |
| *Memory* | : | Jumlah *endpoint* x 0,08 = 290 x 0,08 = 23,2 GB ~ 23 GB |
| **Perhitungan kebutuhan penyimpanan:** | | |
| *Storage* | : | Jumlah *endpoint* x 0,5 GB = 290 x 0,5 = 145 GB<br>Untuk menyimpan *log* selama 1 tahun = 145 GB x 4 = 580 GB ~ 600 GB |

Tabel 3. Spesifikasi *Server* Shuffle dan *Threat Intelligence* (Docker)

| | | |
|---|---|---|
| ***CPU*** | : | *8 Core* |
| ***Memory*** | : | 16 GB |
| ***Storage*** | : | 250 GB |

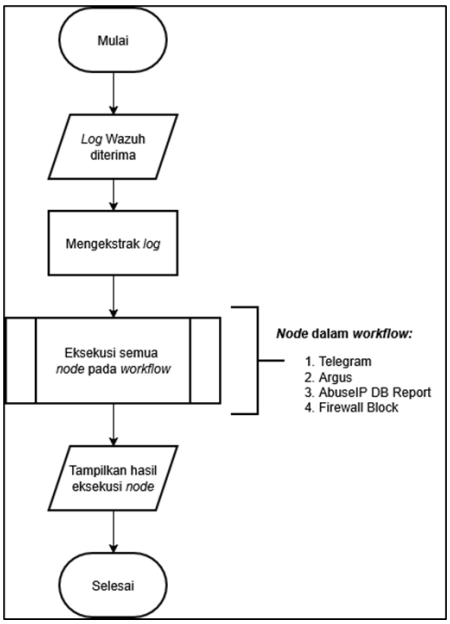
Selain itu, dilakukan juga penyesuaikan konfigurasi *log* pada *server* yang akan dipantau agar data yang dapat diekstrasi lebih banyak dan dapat digunakan untuk menentukan apakah *log* tersebut merupakan tanda ancaman atau bukan. Adapun alur kerja dari Wazuh sebagaimana gambar di bawah ini:




Gambar 2. Alur Kerja Wazuh

 https://doi.org/10.56211/sudo.v5i2.1742

*Server* yang akan dipantau akan dipasang Agen Wazuh yang bertugas mengirimkan *log* dan informasi aktivitas ke *Server* Wazuh sedangkan YARA akan menjadi *active response* dengan memanfaatkan fitur *File Integrity Monitoring* dari Wazuh. Melalui fitur tersebut, Wazuh mampu deteksi terhadap penambahan, modifikasi, dan penghapusan *file*. Jika jenis *log* adalah penambahan atau perubahan, maka *executable* YARA akan dijalankan. Jika *file* yang ditambahkan atau dimodifikasi memiliki kecocokan dengan *rule* YARA, maka *file* tersebut akan dikarantina secara otomatis.




Gambar 3. Alur Otomasi Shuffle

*Event* yang terdeteksi oleh Wazuh akan diteruskan ke Shuffle. Namun, *event* yang diteruskan pada penelitian ini hanyalah yang mengandung *observable* berupa alamat IP (IP penyerang) dan *hash file* (untuk *event File Integrity Monitoring*). *Observable* tersebut nantinya akan diekstrak dari *log* dan diteruskan ke *Threat Intelligence* untuk dianalisa.

Pada penelitian ini, peneliti menggunakan beberapa *Threat Intelligence* eksternal yang semuanya terhubung pada alat bernama Argus-*OSINT*. Argus bertugas melakukan agregasi data dari semua *Threat Intelligence* yang digunakan kemudian melakukan penilaian yang akan dijadikan acuan untuk pengambilan keputusan otomatis.


Gambar 4. Alur Kerja Argus-*OSINT*

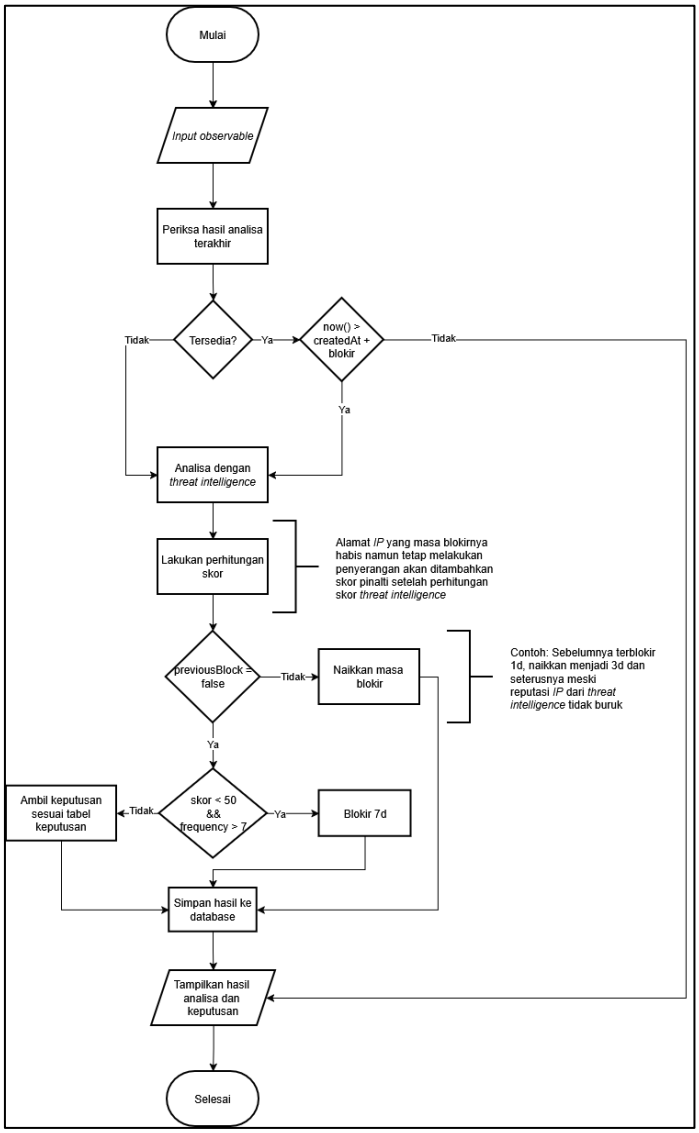
Argus menerima *observable* berupa alamat *IP* atau *hash file* yang didukung yaitu MD5, SHA1, dan SHA256. Jika *observable* adalah *hash,* maka periksa analisa terakhir *hash* pada *database.* Jika *hash* pernah dianalisa dalam rentang waktu kurang dari 90 hari, maka tidak perlu melakukan analisa ulang. Jika *hash* belum pernah dianalisa atau hasil analisa terakhir adalah 90 hari yang lalu atau lebih, Argus akan melakukan analisa ulang dengan *threat intelligence* yang terkonfigurasi. Adapun *threat intelligence* yang digunakan pada Argus beserta bobotnya adalah sebagai berikut:

Tabel 4. Daftar *threat intelligence* yang digunakan

| ***IP Analyzer* (*tip*)** | **Bobot ($\omega$)** |
|---|---|
| VirusTotal (*tip_1*) | 0,1 |
| Crowdsec (*tip_2*) | 0,15 |
| AbuseIP DB (*tip_3*) | 0,3 |
| CriminalIP (*tip_4*) | 0,05 |
| FireHOL *blocklist* (*tip_5*) | 0,3 |
| Threatbook.io (*tip_6*) | 0,1 |
| ***Hash Analyzer* (*tip*)** | **Bobot ($\omega$)** |
| VirusTotal (*tip_1*) | 0,35 |
| Malware Bazaar (*tip_2*) | 0,2 |
| YARAify (*tip_3*) | 0,15 |
| Malprobe (*tip_4*) | 0,30 |

Jika *observable* merupakan alamat *IP*, Argus akan memeriksa terlebih dahulu apakah alamat *IP* tersebut sedang dalam masa pemblokiran dengan memeriksa hasil analisa dan keputusan terakhir. Jika *IP* dalam masa blokir, maka tidak perlu melakukan analisa dengan *threat intelligence*. Sedangkan jika alamat *IP* tidak dalam masa blokir atau belum pernah dianalisa, maka analisa dengan *threat intelligence* akan dilakukan. Alamat *IP* yang pernah terblokir dan kembali melakukan penyerangan, akan ditambahkan penalti pada skor keseluruhan dan ditambah masa pemblokirannya sebagaimana diagram alur berikut:

 https://doi.org/10.56211/sudo.v5i2.1742




Gambar 5. Alur Argus-*OSINT* untuk *Observable IP*

Rumus agregasi dan pengambilan keputusan pada Argus-*OSINT* adalah sebagai berikut:

$$S = \sum_{i=1}^{n}(\omega_i \cdot tip_i) \quad (1)$$

Jika objek adalah *IP* dan kembali melakukan penyerangan, berlaku:

$$S_{final} = min(1,\ S + (p \cdot h)) \quad (2)$$

Sedangkan pengambilan keputusan pemblokiran alamat *IP* didasarkan pada tabel berikut:

Tabel 5. Tabel Keputusan Pemblokiran

| **Keputusan ($A$)** | **Skor ($S_{overall}$)** |
|---|---|
| Tidak diblokir (*no_action*) | < 0,15 |
| Blokir 1 Hari (1d) | 0,15 – 0,29 |
| Blokir 3 Hari (3d) | 0,3 – 0,49 |
| Blokir 7 Hari (7d) | 0,5 – 0,69 atau alamat *IP* memicu *alert* Wazuh |

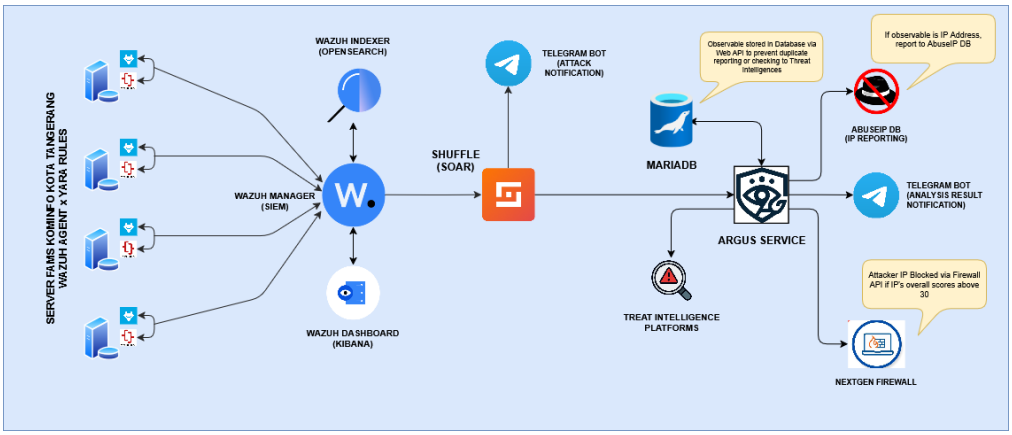
| | |
|---|---|
| | (*frequency*) ≥ 8 kali |
| Blokir Permanen (*permanent*) | ≥ 0,7 |

Nilai skor akhir dibatasi pada rentang 0–1 menggunakan fungsi minimum untuk menjaga konsistensi terhadap rentang skor agregasi dan mekanisme pengambilan keputusan pada Tabel 5. Misalnya sebuah IP memperoleh skor agregasi awal sebesar 0,65 dan telah terdeteksi melakukan serangan sebanyak empat kali sebelumnya, maka:

$$S_{\text{final}} = min(1, 0{,}65 + (0{,}1 \cdot 4)) = 1$$

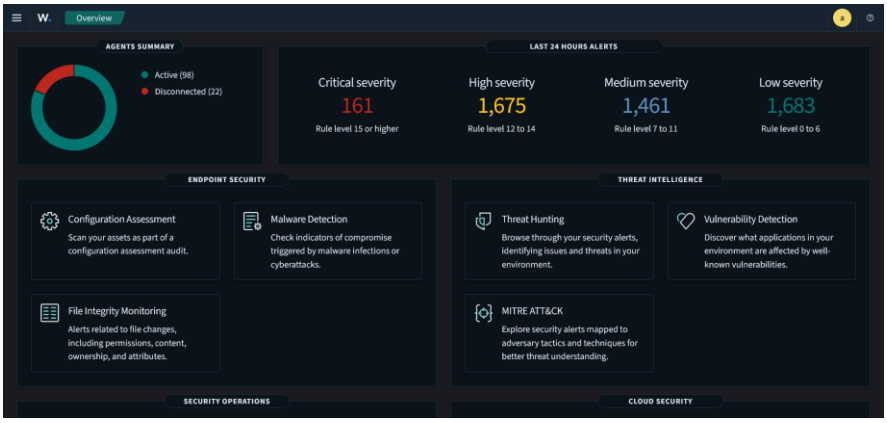
Berdasarkan Tabel 5, *IP* tersebut akan dikenakan pemblokiran permanen.

Secara keseluruhan desain arsitektur sistem keamanan siber yang diterapkan sebagaimana gambar di bawah ini:




Gambar 6. Arsitektur Sistem Keseluruhan

Wazuh menyediakan *dashboard* dan memungkinkan operator keamanan informasi melakukan pemantauan serangan dan kondisi *agent*.




Gambar 7. Halaman Utama Dashboard Wazuh

Operator juga dapat membuat *dashboard* kustom yang menyesuaikan dengan kebutuhan operasional dan monitoring. Berikut ini adalah *dashboard* kustom yang berhasil diterapkan.

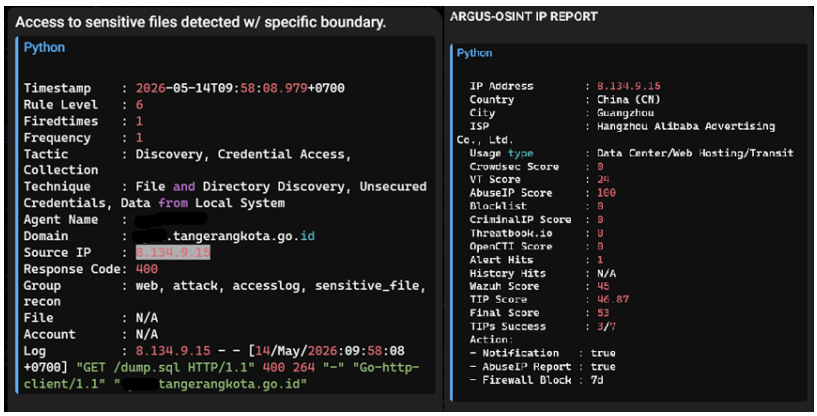
 https://doi.org/10.56211/sudo.v5i2.1742


Gambar 8. Dashboard Kustom

Kemudian, dilanjutkan dengan implementasi dan integrasi *server* Wazuh dengan Shuffle. Berikut ini adalah *workflow* yang dibuat pada Shuffle untuk proses otomatisasi respons ancaman.

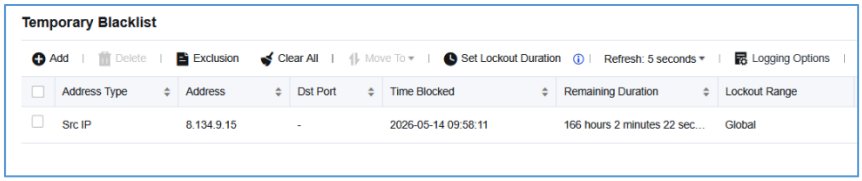

Gambar 9. Konfigurasi *Workflow* Shuffle

Proses otomatisasi ancaman berhasil berjalan dengan baik. *Log* serangan dan hasil analisa *Threat Intelligence* dapat diteruskan ke *channel* Telegram sebagaimana gambar berikut ini:




Gambar 10. Notifikasi Telegram

Shuffle juga berhasil meneruskan alamat *IP* penyerang untuk dilakukan pemblokiran pada perangkat *firewall* sebagaimana pada gambar berikut:




Gambar 11. Alamat *IP* yang Terblokir

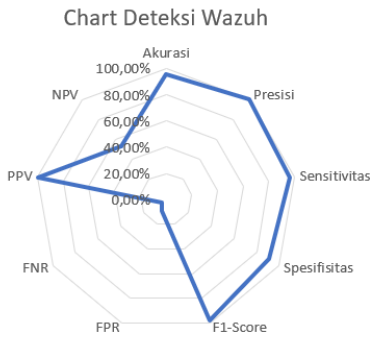
Berdasarkan data *timestamp* pada *alert* Telegram (Gambar 10) diketahui bahwa serangan terjadi pada 14 Mei 2026 pukul 09:58:08 WIB dan terblokir pada *firewall* melalui Shuffle pada 14 Mei 2026 pukul 09:58:11 WIB. Berdasarkan data tersebut, kinerja sistem sudah sangat baik yaitu hanya selisih 3 detik dari deteksi ke respons.

Kemampuan deteksi Wazuh juga dievaluasi menggunakan 10.000 sampel operasional untuk dianalisa. Berdasarkan hasil tersebut, didapati sebanyak 19 *log* adalah *false positive*, dan 9.981 *log* adalah *true positive* atau terkonfirmasi merupakan percobaan serangan. Selain sampel operasional, sampel *log* dari simulasi beberapa teknik serangan juga ditambahkan dan berikut ini adalah tabel hasil sebelum optimasi:

Tabel 6. Tabel Hasil Uji Sebelum Optimasi

| | | **Serangan** | **Bukan Serangan** | **Total** |
|---|---|---|---|---|
| ***GROUND TRUTH*** | **Serangan** | 10579 | 446 | **11025** |
| | **Bukan Serangan** | 52 | 509 | **561** |
| | **Total** | **10631** | **955** | **11586** |

Sehingga didapatkan hasil dari perhitungan metode *confusion matrix* sebagaimana grafik berikut:



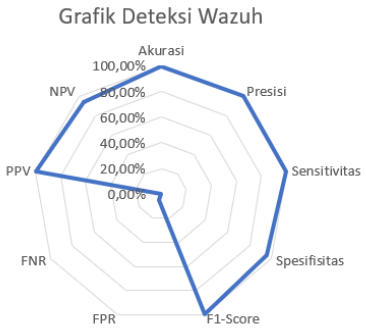

Gambar 12. Grafik Hasil Uji sebelum Optimasi

Sebagaimana terlihat pada Gambar 12, *rule* Wazuh yang diterapkan sebenarnya sudah cukup akurat dalam mengklasifikasikan apakah sebuah *event* merupakan serangan atau bukan. Meskipun masih terdapat *false positive* maupun *false negative.* Maka dari itu, peneliti melakukan evaluasi dan optimasi terhadap *rule* Wazuh dan didapatkan hasil sebagai berikut:

Tabel 7. Tabel Hasil Uji Setelah Optimasi

| | | **Serangan** | **Bukan Serangan** | **Total** |
|---|---|---|---|---|
| ***GROUND TRUTH*** | **Serangan** | 11011 | 33 | **11044** |
| | **Bukan Serangan** | 26 | 520 | **546** |
| | **Total** | **11037** | **553** | **11590** |

 https://doi.org/10.56211/sudo.v5i2.1742




Gambar 13. Grafik Deteksi Wazuh setelah Optimasi

Adapun detail dari perhitungan sebelum dan sesudah optimasi dalam dilihat pada tabel berikut:

Tabel 8. Tabel Perhitungan Confusion Matrix

| Perhitungan | Sebelum Optimasi | Sesudah Optimasi | Peningkatan |
|---|---|---|---|
| **Akurasi** = *(TP + TN) / (TP + TN + FP + FN)* | 95,70% | 99,49% | 3,79% |
| **Presisi** = *TP / (TP + FP)* | 99,51% | 99,76% | 0,25% |
| **Sensitivitas** = *TP / (TP + FN)* | 95,95% | 99,70% | 3,75% |
| **Spesifisitas** = *TN / (TN + FP)* | 90,73% | 95,24% | 4,51% |
| **F1-*Score*** = 2 × (Presisi × Sensitivitas) / (Presisi + Sensitivitas) | 97,70% | 99,73% | 2,03% |
| ***MCC*** = *(TP×TN - FP×FN) / √[(TP+FP)(TP+FN)(TN+FP)(TN+FN)]* | 0,667 | 0,944 | 0,267 |
| ***FPR* (*False Positive Rate*)** = *FP / (FP + TN)* | 9,27% | 4,76% | -4,51% |
| ***FNR* (*False Negative Rate*)** = *FN / (TP + FN)* | 4,05% | 0,30% | -3,75% |
| ***PPV* (*Positive Predictive Value*)** = *TP / (TP + FP)* | 99,51% | 99,76% | 0,25% |
| ***NPV* (*Negative Predictive Value*)** = *TN / (TN + FN)* | 53,30% | 94,03% | 40,75% |

Hasil penelitian ini menunjukkan akurasi deteksi sebesar 99,49% setelah optimasi *rule* Wazuh. Nilai tersebut lebih tinggi dibandingkan beberapa implementasi *SIEM* konvensional yang umumnya masih menghadapi tantangan *false positive* dalam *volume log* yang tinggi. Selain itu, integrasi Wazuh, Shuffle, dan *Threat Intelligence* (Argus-*OSINT*) memungkinkan respons otomatis dalam waktu sekitar tiga detik sejak deteksi awal. Temuan ini menunjukkan bahwa pendekatan *SIEM-SOAR* yang diperkaya *Threat Intelligence* dapat meningkatkan efektivitas operasional keamanan siber pada lingkungan pusat data pemerintahan.

## KESIMPULAN DAN SARAN

Sebagaimana telah dipaparkan pada bab hasil dan pembahasan, komponen sistem keamanan siber yang dirancang telah terintegrasi dan berfungsi secara optimal baik dalam hal deteksi, notifikasi, maupun pemblokiran *IP*. Optimasi yang dilakukan pada *rule* Wazuh juga menunjukkan hasil yang sangat signifikan. Berdasarkan hasil optimasi, akurasi deteksi Wazuh meningkat dari 95,7% menjadi 99,49%, menunjukkan peningkatan kemampuan klasifikasi sebesar 3,79%. Hal ini mengindikasikan bahwa metode optimasi yang diterapkan efektif dalam meningkatkan performa keseluruhan sistem. Konsistensi peningkatan pada seluruh metrik evaluasi yang digunakan (akurasi, presisi, sensitivitas, spesifisitas, F1-*Score*, *FPR, FNR, PPV*, dan *NPV*) memvalidasi bahwa metodologi optimasi *rule* Wazuh yang diterapkan dalam penelitian ini sangat efektif.

Adapun untuk penelitian selanjutnya disarankan melakukan penerapan terdistribusi dengan klasterisasi *multi-node* untuk penyeimbangan beban (*load balancing*) dan ketersediaan tinggi (*high availability*). Saran lainnya yaitu implementasi *machine learning* untuk deteksi anomali berbasis perilaku menggunakan algoritma *supervised learning*. Model ini dapat dilatih menggunakan dataset historis yang telah dilabeli untuk mengenali pola serangan yang kompleks dan sulit dideteksi melalui *rule-based system*.

## DAFTAR PUSTAKA


[1] DISKOMINFO Kota Tangerang, "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.

[2] Pemerintah Kota Tangerang, "Jaga Keamanan Lembaga, Diskominfo Launching Kota Tangerang CSIRT," https://www.tangerangkota.go.id/berita/detail/29867/jaga-keamanan-lembaga-diskominfo-launching-kota-tangerang-csirt.

[3] M. A. Fahrudi and I. M. Suartana, "Integrasi End-point Security Berbasis Agent dan Bot Messenger untuk Deteksi dan Monitoring Serangan pada Web Server secara Real-time," *Journal of Informatics and Computer Science*, vol. 04, 2023.

[4] A. Shafiyyah, G. F. Nama, and R. A. Pradipta, "IMPLEMENTASI WAZUH MENGGUNAKAN METODE PPDIOO DI SISTEM KEAMANAN JARINGAN PSDKU UNIVERSITAS LAMPUNG WAYKANAN SEBAGAI DETEKSI DAN RESPON SERANGAN SIBER," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 2, Apr. 2024, doi: 10.23960/jitet.v12i2.4074.

[5] M. N. H. Muhammad Nayyul Habibie, "IMPLEMENTASI SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR) SISTEM MENGGUNAKAN SHUFFLE DI POLITEKNIK CALTEX RIAU," Politeknik Caltex Riau, 2024.

[6] M. R. T. Hidayat, N. Widiyasono, and R. Gunawan, "OPTIMASI DETEKSI MALWARE PADA SIEM WAZUH MELALUI INTEGRASI CYBER THREAT INTELLIGENCE DENGAN MISP DAN DFIR-IRIS," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 13, no. 1, Jan. 2025, doi: 10.23960/jitet.v13i1.5686.

[7] M. G. Cains, L. Flora, D. Taber, Z. King, and D. S. Henshel, "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation," *Risk Analysis*, vol. 42, no. 8, pp. 1643–1669, Aug. 2022, doi: 10.1111/risa.13687.

[8] J. T. Santoso, "Teknologi Keamanan Siber (Cyber Security)," Nov. 2023.

[9] A. H. H. Harahap, C. D. Andani, A. Christie, D. Nurhaliza, and A. Fauzi, "Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder," *Jurnal Manajemen dan Pemasaran Digital*, vol. 1, no. 2, pp. 73–83, Apr. 2023, doi: 10.38035/jmpd.v1i2.34.

[10] M. Rijal Kamal and M. Andri Setiawan, "Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII."

[11] H. Khotimah, F. Bimantoro, and R. S. Kabanga, "Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat," *Jurnal Begawe Teknologi Informasi (JBegaTI)*, vol. 3, no. 2, Sep. 2022, doi: 10.29303/jbegati.v3i2.752.

[12] V. Gustina DM and A. Ananda, "Kecerdasan Buatan untuk Security Orchestration, Automation and Response: Tinjauan Cakupan," *Jurnal Komputer Terapan*, vol. 10, no. 1, pp. 36–47, Jun. 2024, doi: 10.35143/jkt.v10i1.6247.

[13] A. D. Wiratama, "Cyber Security In 2023: The Latest Challenges And Solutions," *Jurnal Komputer Indonesia*, vol. 2, no. 1, pp. 47–54, Jun. 2023, doi: 10.37676/jki.v2i1.569.

[14] A. de Melo e Silva, J. J. Costa Gondim, R. de Oliveira Albuquerque, and L. J. García Villalba, "A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence," *Future Internet*, vol. 12, no. 6, p. 108, Jun. 2020, doi: 10.3390/fi12060108.

[15] D. P. F. Möller, "Threats and Threat Intelligence," 2023, pp. 71–129. doi: 10.1007/978-3-031-26845-8_2.

[16] A. P. Arini, M. R. R. Isworo, and others, "Desain Dan Manajemen Jaringan Pada Sma Negeri 15 Surabaya Menggunakan Cisco Packet Tracer Dengan Metode PPDIOO," in *Prosiding Seminar Nasional Informatika Bela Negara*, 2024, pp. 26–32.

[17] P. I. O. Br Sipayung, V. Purba, and A. Agussalim, "Analisis, Perancangan, dan Simulasi Jaringan VLAN Menggunakan Metode PPDIOO (Studi Kasus: SMAS Santo Yusup Surabaya)," *TeknoIS : Jurnal Ilmiah Teknologi Informasi dan Sains*, vol. 14, no. 1, pp. 110–118, Jan. 2024, doi: 10.36350/jbs.v14i1.237.

[18] Wazuh.com, "Overwiev | Wazuh," https://wazuh.com/platform/overview/

## NOMENKLATUR

| | | |
|---|---|---|
| S | : | Skor agregasi *observable* |
| $\omega_i$ | : | Bobot *threat intelligence* ke-*i* |
| $tip_i$ | : | Hasil analisis *threat intelligence* ke-*i* |
| n | : | Jumlah sumber *threat intelligence* |
| p | : | Penalti per *hit* (0,1) |
| h | : | Jumlah kemunculan *IP* pada riwayat analisis |
| $S_{final}$ | : | Skor akhir setelah penambahan dari riwayat analisis |