RANCANG BANGUN SISTEM OTOMASI PADA WAZUH MENGGUNAKAN VALIDASI MULTI-SOURCE CTI UNTUK MITIGASI MALWARE

SUB JUDUL

Rancang Bangun Sistem Pengambilan Keputusan Berbasis Multi-Source Cyber Threat Intelligence Pada Wazuh SIEM

SKRIPSI

MUHAMMAD ILHAM SUTAMA **2207421028**

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2026

RANCANG BANGUN SISTEM PENGAMBILAN KEPUTUSAN BERBASIS MULTI-SOURCE CYBER THREAT INTELLIGENCE PADA WAZUH SIEM

SKRIPSI

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

MUHAMMAD ILHAM SUTAMA

2207421028

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2026

SURAT PERNYATAAN BEBAS PLAGIARISME

saya yang bertanda tangan di bawah ini:

Nama : Muhammad Ilham Sutama

NIM : 2207421028

Jurusan/ProgramStudi : Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Judul skripsi : Rancang Bangun Sistem Pengambilan Keputusan Berbasis Multi-Source Cyber Threat Intelligence Pada Wazuh SIEM

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya seni 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, 09 Juni 2026

yang membuat pernyataan

Muhammad Ilham Sutama

NIM. 2207421028

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama	: Muhammad Ilham Sutama
NIM	: 2207421028
Program Studi	: Teknik Multimedia dan Jaringan
Judul Skripsi	: Rancang Bangun Sistem Pengambilan Keputusan Berbasis Multi-Source Cyber Threat Intelligence Pada Wazuh SIEM

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 17, Bulan Juni, Tahun 2026 dan dinyatakan **LULUS**.

Disahkan oleh:

Pembimbing I	Asep Kurniawan S,Pd., M.Kom	( )
Penguji I	Ayu Rosyida Zain, S.ST, M.T.	( )
Penguji II	Dr. Defiana Arnaldy, S.T.P., M.Si.	( )
Penguji III	Andika Riyadi Jasril, M.Pd.T.	( )

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

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

KATA PENGANTAR

Puji serta syukur penulis panjatkan kepada Allah *subhanallahu wa ta'ala* yang atas berkat rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini yang berjudul "Rancang Bangun Sistem Pengambilan Keputusan Berbasis *Multi-Source Cyber Threat Intelligence* Pada Wazuh SIEM".

Penulisan skripsi ini menjadi tahapan dalam rangka memenuhi salah satu syarat untuk memperoleh gelar Diploma Empat Politeknik. Penulis menyadari bahwa kontribusi dan dukungan dari seluruh pihak sejauh inilah yang membantu penulis dalam menyelesaikan tugas skripsi ini. Oleh karena itu penulis mengucapkan terimakasih kepada:

1. Bapak Asep Kurniawan, S.Pd., M.Kom, selaku dosen pembimbing yang telah banyak membantu, memberi masukan dan mendukung sepenuh hati dalam proses pengerjaan skripsi ini hingga selesai.
2. Ibu, ayah dan adik yang telah memberikan dukungan baik dalam segi material dan moral serta terus memotivasi penulis dalam taraf yang tidak bisa diukur.
3. Bayu Dwi Setianto selaku rekan yang telah mengerahkan seluruh tenaga dan upaya hingga dapat menyelesaikan skripsi ini, serta kepada Raden Muhammad Fadil Azhar, Stephanie Meissya Permata Asri Tarigan, dan Harsdyka Wibisono selaku rekan dan sahabat, serta umumnya kepada seluruh rekan seperjuangan dari kelas TMJ A dan TMJ B yang membantu penulis dalam perkuliahan.

Penulis menyadari bahwa skripsi ini jauh dari kata sempurna dan memiliki kesalahan serta kekurangan di dalamnya, oleh karena itu penulis meminta maaf yang sebesar–besarnya atas kesalahan dan segala kekurangan yang ada. Penulis juga mengucapkan terima kasih kepada seluruh pihak dan semoga ilmu yang didapatkan selama masa perkuliahan ini dapat terus mengalir sehingga menumbuhkan manfaat kepada lingkungan sekitar.

Depok, 09 Juni 2026

Muhammad Ilham Sutama
NIM. 2207421028

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan di bawah ini : Nama : Muhammad Ilham Sutama

NIM : 2207421028

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

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

Rancang Bangun Sistem Pengambilan Keputusan Berbasis Multi-Source Cyber Threat Intelligence pada Wazuh SIEM

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 membuat pernyataan,

Muhammad Ilham Sutama
NIM. 2207421028

RANCANG BANGUN SISTEM PENGAMBILAN KEPUTUSAN BERBASIS MULTI-SOURCE CYBER THREAT INTELLIGENCE PADA WAZUH SIEM

ABSTRAK

Proses validasi alert yang masih dilakukan secara manual oleh tim analis Security Operations Center (SOC) di PT. XYZ membuka peluang optimasi alur kerja dalam tim, validasi alert yang umumnya dilakukan dengan mengakses berbagai platform Cyber Threat Intelligence (CTI) secara terpisah memerlukan waktu yang relatif lama dan berpotensi menambah beban kerja berlebih serta menghasilkan keputusan yang kurang konsisten. Penelitian ini bertujuan untuk merancang dan mengimplementasikan Multi-Source Cyber Threat Intelligence untuk pengambilan keputusan pada Wazuh SIEM di lingkungan PT. XYZ. Penelitian ini menggunakan metode eksperimental dengan mensimulasikan proses pengunduhan file malware pada lingkungan Wazuh agent parameter yang diukur berupa F1-score dari hasil verdict sistem pengambilan keputusan dan waktu percepatan yang didapatkan melalui proses otomatisasi didapatkan dari speedup test. Berdasarkan hasil evaluasi pengujian terhadap 188 sampel malware file unik dan 240 sampel file normal didapati sistem memiliki nilai precision sebesar 98,41%, recall sebesar 98,94% dan F1-score sebesar 98,67%. Pengujian waktu respon menunjukan sistem usulan yang digunakan mampu menangani proses validasi dalam waktu rata-rata 3 detik, lebih cepat dibandingkan proses manual yang membutuhkan waktu rata-rata 42,2 detik sehingga menghasilkan percepatan 14 kali lebih cepat. Penelitian ini menunjukan sistem pengambilan keputusan pada Wazuh SIEM mampu memberikan hasil validasi ancaman dengan nilai F1-score sebesar 98,67%, mempercepat respons insiden, sehingga berpotensi pada berkurangnya beban kerja analis SOC.

Kata kunci: *Multi-Source Cyber Threat Intelligence,* Wazuh *SIEM, Security Operations Center, Decision Fusion.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era dimana perkembangan teknologi berjalan sangat cepat dan masif, membuat keamanan siber menjadi aspek yang sangat penting dalam menjaga integritas, kerahasiaan dan ketersediaan data (Hidayat et al., 2025). Berbagai upaya dilakukan dalam menghalau serangan siber yang terjadi, salah satunya adalah dengan mengimplementasikan *Security Information and Event Manager* (SIEM) dalam ekosistem jaringan komputer (Hidayat et al., 2025).

Dalam implementasi SIEM terkait erat dengan pemanfaatan *tools* pengumpulan informasi keamanan siber seperti *Cyber Threat Intelligence* (CTI) untuk mendeteksi serangan. SIEM berfungsi sebagai pusat kendali yang bertugas mengumpulkan log dari berbagai *tools* keamanan secara *real-time*. Sedangkan CTI berperan dalam memberikan informasi mengenai indikator serangan yang sudah pernah dilaporkan pada platform komunitas siber.

Meskipun SIEM memiliki peran krusial dalam memusatkan pemantauan keamanan, tingginya volume alert yang dihasilkan setiap harinya sering kali tidak sebanding dengan kapasitas analitik manusia. Kondisi ini memicu fenomena yang dikenal sebagai alert fatigue, di mana analis Security Operations Center (SOC) mengalami beban kognitif berlebih akibat keharusan memverifikasi ribuan notifikasi yang mayoritas merupakan false positive. Akibatnya, *alert* krusial yang menandakan ancaman *real* sering kali terabaikan.

Dalam hal ini, PT.XYZ telah mengimplementasikan SIEM sebagai alat pemantauan berbagai aktivitas keamanan yang terjadi pada *endpoint*. Namun berdasarkan proses operasional yang berjalan pada lingkungan SOC PT.XYZ ditemukan permasalahan pada proses validasi ancaman yang saat ini masih dilakukan secara manual, di mana ketika SIEM menghasilkan *alert* yang berisi indikator berupa hash dan IP. Analis harus mengakses berbagai

platform CTI seperti VirusTotal, CTX.IO, OTX Alienvault, dan Abuse IPDB secara manual dengan membuka satu persatu platform untuk memperoleh informasi terkait indikator yang ditemukan.

Proses tersebut berjalan repetitif dan memakan waktu karena analis perlu mencari dan membandingkan informasi dari berbagai sumber CTI. Kondisi ini sesuai dengan tantangan operasional SOC yang dikemukakan oleh (Khayat et al., 2025), di antaranya tingginya beban kerja analis, tidak adanya otomatisasi, serta kebutuhan untuk meningkatkan efektivitas proses validasi dan respons insiden.

Selain itu menurut (santos et.al 2025), ketergantugan pada satu sumber CTI memiliki keterbatasan karena hanya merepresentasikan sebagian sudut pandang terhadap ancaman yang diamati. Meskipun demikian, sumber - sumber CTI ini memiliki karakteristik dan tingkat keandalan yang berbeda dalam mengidentifikasi ancaman sehingga diperlukan sistem yang mampu merepresentasikan tingkat keandalan yang sesuai antara satu platform CTI dengan platfrom lainnya.

Untuk menghadapi permasalahan tersebut, dibutuhkan suatu sistem yang mampu mengintegrasikan SIEM Wazuh dengan berbagai sumber CTI yang digunakan pada lingkungan perusahaan. Salah satu pendekatan yang dapat diterapkan pada kasus ini adalah *Decision Level Fusion*, metode ini menggabungkan hasil penilaian dari berbagai sumber untuk menghasilkan sebuah verdict atau keputusan akhir. Pendekatan ini mengadaptasi kerangka kerja *Multimodal Data Fusion* yang telah digunakan untuk meningkatkan kualitas pengambilan keputusan dari lingkungan yang membutuhkan banyak sumber informasi (Dong et al., 2025).

Berdasarkan hal tersebut, penelitian ini mengusulkan rancang bangun mekanisme pengambilan keputusan berbasis *Multi-Source Cyber Threat Intelligence* (Multi CTI) dengan Wazuh SIEM. Dengan mengintegrasikan berbagai sumber pengayaan informasi melalui platform CTI VirusTotal, CTX.io, OTX Alienvault, dan Abuse IPDB terkait indikator yang diawasi, proses validasi ancaman diharapkan dapat dilakukan secara lebih efisien serta

mendukung pengambilan keputusan dalam operasional harian SOC PT TirtaNawasena Teknologi.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana cara merancang dan mengimplementasikan Multi-Source *Cyber Threat Intelligence* untuk pengambilan keputusan pada Wazuh SIEM?
2. Bagaimana menganalisis kinerja deteksi ancaman pada SIEM Wazuh dengan penggunaan Multi-Source CTI?
3. Bagaimana cara mengotomatisasi proses *Cyber Threat Intelligence* pada log SIEM Wazuh?

1.3 Batasan Masalah

Fokus penelitian ini adalah sebagai berikut:

1. Integrasi CTI yang digunakan terbatas pada CTI dengan layanan API gratis dari platform: CTX.io, Virus Total, OTX, dan Abuse IPDB.
2. Indikator IOC yang digunakan terbatas pada IP dan hash (SHA 256).
3. Agent yang dimonitoring terbatas pada sistem operasi ubuntu desktop.
4. Penelitian dilakukan menggunakan lingkungan lokal pada *virtual machine*.
5. Evaluasi kinerja difokuskan pada metrik *F-1 Score*, *precision*, dan *recall*.
6. *File* yang dapat dideteksi berbasis exe, dll, msi, js / javascript, ps1 / powershell, py / python, vba, xls, rtf, txt, zip, rar, html, asp, crx (Ekstensi Browser Chrome), mp3 / *file* audio.

1.4 Tujuan dan Manfaat

Adapun tujuan dari penelitian ini antara lain:

1. Merancang dan mengimplementasikan Multi-Source *Cyber Threat Intelligence* untuk pengambilan keputusan pada Wazuh SIEM.
2. Menganalisis kinerja sistem yang diusulkan dalam mengotomatisasi proses pengambilan keputusan (verdict) *alert*.

3. Mengotomatisasi proses investigasi manual melalui *Cyber Threat Intelligence (CTI)* pada log SIEM Wazuh.

Beberapa manfaat yang diharapkan dari penelitian ini antara lain:

1. Menurunkan beban kerja tim SOC L1 pada proses *data enrichment* log *alert*.
2. Meningkatkan kualitas pendeteksian pada SIEM Wazuh yang optimal antara penurunan *false positive* dan kemampuan mendeteksi serangan.
3. Menyediakan hasil analisis data mengenai spesialisasi dan tingkat akurasi setiap vendor CTI, memungkinkan identifikasi sumber yang paling andal untuk mendeteksi jenis serangan dan dapat menjadi dasar dalam pengembangan sistem selanjutnya.

1.5 Sistematika Penulisan

Berikut adalah sistematika penulisan dari skripsi ini:

A. BAB I PENDAHULUAN

Bab I berisikan penjelasan mengenai urgensi dari penelitian yang dilakukan. Bagian ini meliputi latar belakang masalah, perumusan masalah, batasan masalah, serta tujuan dan manfaat dari rancang bangun mekanisme pengambilan keputusan berbasis *Multi-Source* CTI pada SIEM Wazuh.

B. BAB II TINJAUAN PUSTAKA

Bab II berisikan penjelasan mengenai landasan teori serta tinjauan dari penelitian terdahulu yang relevan dengan penelitian yang dilakukan saat ini.

C. BAB III METODOLOGI PENELITIAN

Bab III menjelaskan mengenai rancangan penelitian, implementasi integrasi yang menjadi tahapan penelitian, dan objek penelitian.

D. BAB IV HASIL DAN PEMBAHASAN

Bab IV menjelaskan mengenai hasil dan pembahasan penelitian yang dilakukan meliputi, analisis kebutuhan, perancangan sistem, implementasi, pengujian serta hasil analisis pengujian.

E. BAB V PENUTUP

Bab V Berisi penjelasan mengenai kesimpulan dan saran secara singkat dari hasil penelitian terhadap pembahasan yang telah diuraikan pada bagian isi.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat diambil kesimpulan sebagai berikut:

1. Rancang bangun sistem pengambilan keputusan berbasis Multi-Source *cyber threat intelligence* pada wazuh SIEM berhasil dirancang dan diimplementasikan sebagai *middleware* berbasis Python yang mengintegrasikan empat platform CTI yaitu VirusTotal, CTX.io, OTX alienvault, dan Abuse IPDB kedalam Wazuh SIEM. dan hasil keputusan telah terintegrasi dengan (SOAR) active respon.
2. Pengujian sistem terhadap 428 sampel yang terdiri dari 188 sampel *malicious* dan 240 sampel normal menghasilkan nilai *precision* sebesar 0,984, *recall* sebesar 0,9894, dan F1-Score sebesar 0,9867. Pengujian ini menunjukan sistem dapat mengenali 98% malware dari data sampel yang diuji selain itu, hasil dari tiga skenario pengujian *Balance ccuracy* menghasilkan nilai *balance accuracy* sebesar 0.9884, 0.9890, dan 0.9879 menunjukan F1-*score* yang digunakan merepresentasikan nilai yang valid terhadap kinerja sistem secara keseluruhan.
3. Otomatisasi proses validasi CTI berhasil dilakukan dan terbukti meningkatkan kecepatan pemrosesan validasi ancaman. Metode otomatis menggunakan sistem usulan memiliki nilai speedup yang diperoleh 14.07 ini berarti proses validasi dapat berjalan 14 kali lebih cepat dalam kondisi normal. selain itu, sistem berhasil menerapan mekanisme rate limiting, rotasi API key, caching melalui SQL lite,dan visualisasi log melalui dashboard *OpenSearch* pada Wazuh *Dashboard* untuk mendukung aktivitas operasional harian tim analis SOC.

5.2 Saran

Berdasarkan temuan yang terjadi pada saat dilakukannya penelitian, berikut saran yang dapat diimplementasikan pada penelitian lebih lanjut :

1. Pada penelitian ini terdapat keterbatasan pada penggunaan CTI yang digunakan dikarenakan dua jenis CTI yang digunakan (OTX alienvault dan abuse IPDB) memilki keterbatasan pemrosesan request hash pada tier API gratis dan ketidak cocokan pada jenis request. Sangat disarankan untuk menambahkan platform CTI dari sumber lain pada penelitian selanjutnya. Penulis mereomendasikan beberapa opsi untuk menggantikan fungsi OTX seperti malware bazar API dan Wazuh CTI API
2. Melakukan pengujian dengan volume alert yang lebih tinggi untuk memvalidasi skalabilitas dan keandalan sistem secara lebih baik. Serta dilakukan perhitungan F-1 score ulang dengan dataset untuk menentukan bobot awal dalam skala produksi yang lebih besar.
3. Mengotomatisasi perhitungan bobot awal secara dinamis. Karena nilai awal saat ini ditetapkan secara statis pada 0,10. Penelitian selanjutnya dapat mengeksplorasi mekanisme penyesuaian threshold secara adaptif sesuai kebijakan operasional yang berjalan terkait IOC.
4. Melakukan pengujian lebih lanjut terkait jumlah CTI optimal serta pengujian dengan API tier Premium (berbayar) sehingga diketahui *cost per incident* yang dibutuhkan untuk melakukan validasi secara otomatis.
5. Mengaplikasikan *whitelist* pada sistem pengambilan keputusan.

DAFTAR PUSTAKA

Abdullah R.A , 2025. Analisis Kinerja SIEM Wazuh Dengan Fim, Yara, Dan Virustotal Dalam Mendeteksi Malware Pada Ubuntu Server.

About-AbuseIPDB.(2026).Abuseipdb.Com. https://www.abuseipdb.com/about

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers and Security, 132. https://doi.org/10.1016/j.cose.2023.103352

Aktar, M. N., Sakib, M. N., Hossain, A., Ullah, A., Robin, K. H., Rahman, K. M., Reza, M. T., Ameen, A., Hossain, M. R., & Kundu, D. (2024). Enhancing False positive Alert Detection in Security Information and Event Management System Using Recurrent Neural Network. 2024 27th International Conference on Computer and Information Technology, ICCIT 2024 - Proceedings, 2794–2799. https://doi.org/10.1109/ICCIT64611.2024.11022066

Cohen, D., Te'eni, D., Yahav, I., Zagalsky, A., Schwartz, D., Silverman, G., Mann, Y., Elalouf, A., & Makowski, J. (2025). Human–AI Enhancement of Cyber Threat Intelligence. International Journal of Information Security, 24(2). https://doi.org/10.1007/s10207-025-01004-4

Dong, J., Hao, M., Ding, F., Chen, S., Wu, J., Zhuo, J., & Jiang, D. (2025). A Novel Multimodal Data Fusion Framework: Enhancing Prediction and Understanding of Inter-State Cyberattacks. Big Data and Cognitive Computing, 9(3). https://doi.org/10.3390/bdcc9030063

Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (2023). A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms. IEEE Access, 11, 121118–121141. https://doi.org/10.1109/ACCESS.2023.332835

Hidayat, M. R. T., Widiyasono, N., & Gunawan, R. (2025). OPTIMASI DETEKSI MALWARE PADA SIEM WAZUH MELALUI INTEGRASI CYBER THREAT INTELLIGENCE DENGAN MISP DAN DFIR-IRIS. Jurnal Informatika Dan Teknik Elektro Terapan, 13(1). https://doi.org/10.23960/jitet.v13i1.5686

Hiruta, S., Umemura, Y., Kubo, M., Kanaya, N., & Kasama, T. (2025). Post-Exploitation Unveiled: Analyzing RAT Behaviors in a Realistically Simulated Enterprise Network. 1–8. https://doi.org/10.1109/dsc65356.2025.11260867

Hong Jun Choi, H. L. J.-Y. C. 2021. 2021 23rd International Conference on Advanced Communication Technology Is a False positive really False positive? IEEE.

How it works. (2025). VirusTotal. https://docs.virustotal.com/docs/how-it-works

Jang, H. S., Alawami, M. A., & Park, K. W. (2025). AV-Teller: Browser Fingerprinting for Client-Side Security Software Identification. Applied Sciences (Switzerland), 15(9). https://doi.org/10.3390/app15095059

Khayat, M., Barka, E., Adel Serhani, M., Sallabi, F., Shuaib, K., & Khater, H. M. (2025). Empowering Security Operation Center with Artificial Intelligence and Machine Learning - A Systematic Literature Review. IEEE Access, 13, 19162–19197. https://doi.org/10.1109/ACCESS.2025.3532951

Lab, S. (2026). CTX | Cyber Threat Intelligence Platform. CTX | Cyber Threat Intelligence Platform. https://www.ctx.io/about/ctx

Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. PLOS ONE, 19(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

Olabanji, S. O. (2023). Advancing Cloud Technology Security: Leveraging High-Level Coding Languages like Python and SQL for Strengthening Security Systems and Automating Top Control Processes. Journal of Scientific Research and Reports, 29(9), 42–54. https://doi.org/10.9734/jsrr/2023/v29i91783

Pekar, A., & Jozsa, R. (2024). Evaluating ML-based anomaly detection across datasets of varied integrity: A case study. Computer Networks, 251. https://doi.org/10.1016/j.comnet.2024.110617

Rafsanjani, A. S., Kamaruddin, N. B., Behjati, M., Aslam, S., Sarfaraz, A., & Amphawan, A. (2024). Enhancing Malicious URL Detection: A Novel Framework Leveraging Priority Coefficient and Feature Evaluation. IEEE Access, 12, 85001–85026. https://doi.org/10.1109/ACCESS.2024.3412331

Santos, P., Abreu, R., Reis, M. J. C. S., Serôdio, C., & Branco, F. (2025). A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats. In Sensors (Vol. 25, Number 14). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s25144272

Schryen, G. (2024). Speedup and efficiency of computational parallelization: A unifying approach and asymptotic analysis. Journal of Parallel and Distributed Computing, 187. https://doi.org/10.1016/j.jpdc.2023.104835

Silva, P., Baye, G., Broggi, A., Bastian, N. D., Kul, G., & Fiondella, L. (2024). Predicting F1-Scores of Classifiers in Network Intrusion Detection Systems. Proceedings - International Conference on Computer Communications and Networks, ICCCN. https://doi.org/10.1109/ICCCN61486.2024.10637544

Soumik, S., Kh Said Al Mamun, Omim, S., Khan, H. A., & Sarkar, M. (2024). Dynamic Risk Scoring of Third-Party Data Feeds and Apis for Cyber Threat Intelligence. https://doi.org/10.32996/jcsts

Threat, O. (2026). LevelBlue - Open Threat Exchange. LevelBlue Open Threat Exchange. https://otx.alienvault.com/api

Zhao, Y. 2022. Information Fusion Method for Building Grassroots Teaching Organization Based on Intelligent Optimization. Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022/8902762

DAFTAR RIWAYAT HIDUP

Muhammad Ilham Sutama

Lahir di salah satu kota di Jawa Barat pada tahun 2004 dari pasangan bapak Hendra Sutama S.Pd dan ibu Ratna Sari Dewi S.Pd. Saat ini penulis berdomisili di daerah Depok. Penulis menuntaskan jenjang sekolah dasar di Madrasah Ibtidaiyah (MI) Alhidayah Arco pada tahun 2016, lalu melanjutkan Pendidikan pada jenjang sekolah menengah pertama di Madrasah Tsanawiyah (MTs) Negeri 1 Bogor pada tahun 2019, selanjutnya penulis melanjutkan sekolah pada jenjang sekolah menengah atas di SMA Negeri 5 Depok dengan jurusan Ilmu Pengetahuan Alam (IPA) dan lulus pada tahun 2022. Penulis menyelesaikan Pendidikan Diploma Empat (D4) di Politeknik Negeri Jakarta dengan Program Studi Teknik Multi Media dan Jaringan pada tahun 2026.

Penulis memiliki dedikasi yang kuat pada riset akademis dan cybersecurity engineering, didukung oleh pengalaman sebagai asisten dosen dan partisipasi aktif dalam pengabdian masyarakat di Sekolah Alam Indonesia. Perjalanan akademis penulis ditandai dengan publikasi paper ilmiah di IEEE dan berkesempatan mempresentasikan secara langsung pada konferensi IC2IE 2024, serta pengerjaan skripsi yang berfokus pada evaluasi akurasi sistem deteksi malware dengan menerapkan metodologi validitas statistik.

LAMPIRAN

Lampiran 1 Dokumen F4

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
POLITEKNIK NEGERI JAKARTA
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
Jl. Prof.DR.G.A. Siwabesy, Kampus UI, Depok 16425
Telp. (021) 91274097, Fax (021) 7863531
Laman : http://www.pnj.ac.id, e-mail:tik@pnj.ac.id

F4

LEMBAR PERSETUJUAN PEMBIMBING MENGIKUTI SIDANG SKRIPSI

Yang bertanda tangan di bawah ini adalah Pembimbing skripsi :

Nama Mahasiswa	: Muhammad Ilham Sutama
NIM	: 2207421028
Program Studi	: TMJ
Judul Skripsi	: Rancang Bangun Sistem Pengambilan Keputusan Berbasis Multi Source Cyber Threat Intelligence Pada Wazuh SIEM

Sesuai dengan persyaratan yang diatur dalam Pedoman Skripsi Jurusan Teknik informatika dan Komputer, maka dengan ini menyetujui mahasiswa tersebut di atas untuk mengikuti sidang skripsi Tahun Akademik 2025 / 2026

Depok, 07 Juni 2026
Pembimbing,

(Asep Kurniawan, S.Pd., M.Kom.)
NIP.199109262019031012

Lampiran 2 Surat Izin Observasi

TIRTA NAWASENA TEKNOLOGI

SURAT PERSETUJUAN IZIN OBSERVASI

Nomor : 01/TNT/HR-B/VI/2026
Lampiran : -

Kepada Yth.
Ibu Dr. Anita Hidayati, S.Kom., M.Kom.
Ketua Jurusan
Politeknik Negeri Jakarta

Dengan hormat,

Sehubungan dengan surat permohonan izin observasi Nomor 793/DST/PL.312/B/KM.07.00/2026 yang kami terima pada tanggal 29 Juni 2026, perihal permohonan izin pelaksanaan kegiatan observasi bagi mahasiswa semester 8 (delapan) Jurusan Teknik Multimedia dan Jaringan dari Politeknik Negeri Jakarta.

Melalui surat ini, kami sampaikan bahwa pihak manajemen PT. Tirta Nawasena Teknologi **MENERIMA / MENYETUJUI** permohonan izin observasi tersebut untuk mahasiswa yang bersangkutan :

No.	Nama	NIM
1	Muhammad Ilham Sutama	2207421028
2	Bayu Dwi Setianto	2207421008

Kegiatan observasi dilaksanakan dengan ketentuan yang berjalan selama periode magang. Sejak dimulai hingga berakhirnya periode magang dan observasi ini, para mahasiswa yang bersangkutan telah mematuhi seluruh praturan, menjaga kerahasiaan data internal, serta mematuhi tata tertib yang berlaku di lingkungan PT. Tirta Nawasena Teknologi.

Demikian surat balasan ini kami sampaikan. Atas perhatian dan kerja samanya, kami ucapkan terima kasih.

Tangerang Selatan, 30 Juni 2026
PT. Tirta Nawasena Teknologi

Camelia fatimah
Human Resource & GA

Email. info@tirtanawasena.com
Ph. (+62) 888 1772 211

Vila Dago Tol Blok. C14 No. 1 RT. 009 RW. 019
Serua, Ciputat, Kota Tangerang Selatan, Banten

Lampiran 3 Dataset Pembobotan 200 IOC (100 Malicious dan 100 Normal)

No	SHA-256	Ground Truth	VirusTotal	Abusel PDB	CTX.io	OTX	Skor VT	Skor CTX	Final Score
1	1e621fd2a755f05c20670d2f4cb546baff6478d4979ff5f80e4d7e583e6bc401	MALICIOUS	26/71.	N/A%	Malicious	0	0,3662	1,0000	0,6861
2	c91183175ce77360006f964841eb4048cf37cb82103f2573e262927be4c7607f	MALICIOUS	37/61.	N/A%	Malicious	0	0,6066	1,0000	0,8052
3	8c1dc9732884c6078b23953b78314a8d0d8b8d9fe42e5f97a7cd09b8ace943a9	MALICIOUS	55/72.	N/A%	Malicious	0	0,7639	1,0000	0,8831
4	52b6fb40e7efb09c2bebe8550178e7e30009600bdedd1acae085d753761b7598	MALICIOUS	47/72.	N/A%	Malicious	0	0,6528	1,0000	0,8281
5	40c2e559992a7f595c593b419930a3f216516c3042ad86fb985348d53b6e01b9	MALICIOUS	46/72.	N/A%	Malicious	0	0,6389	1,0000	0,8212
6	9f4672c1374034ac4556264f0d4bf96ee242c0b5a9edaa4715b5e61fe8d55cc8	MALICIOUS	29/62.	N/A%	Malicious	0	0,4677	1,0000	0,7364
7	5a17cfaea0cc3a82242fdd11b53140c0b56256d769b07c33757d61e0a0a6ec02	MALICIOUS	36/61.	N/A%	Malicious	0	0,5902	1,0000	0,7970
8	b2ba51b4491da8604ff9410d6e004971e3cd9a321390d0258e294ac42010b546	MALICIOUS	38/61.	N/A%	Malicious	0	0,6230	1,0000	0,8133
9	fd3f13db41cd5b442fa26ba8bc0e9703ed243b3516374e3ef89be71cbf07436b	MALICIOUS	37/61.	N/A%	Malicious	0	0,6066	1,0000	0,8052
10	969d2776df0674a1cca0f74c2fccbc43802b4f2b62ecccecc26ed538e9565eae	MALICIOUS	38/61.	N/A%	Malicious	0	0,6230	1,0000	0,8133
11	425b2f283b71237276f84d941d9c2982c7f61a9aff12ece10e15065b73b7165e	MALICIOUS	54/71.	N/A%	Malicious	0	0,7606	1,0000	0,8814
12	b211537ea626fae4ad2ef5ee2652633dc68aaf20da6eb953a44f266c4106b367	MALICIOUS	54/70.	N/A%	Malicious	0	0,7714	1,0000	0,8868
13	324eabc27a25f524c94bb62573986b3335ab5181ddc6825d959d16aaaccdc7aa	MALICIOUS	49/67.	N/A%	Malicious	0	0,7313	1,0000	0,8670
14	618070d597dd73c43ba5d4bde2baa93a4f6038e3279de3bafe688caa5c409a58	MALICIOUS	55/68.	N/A%	Malicious	0	0,8088	1,0000	0,9053
15	fafb6c5e12dfeefaba5ac8982d5bb13dd206cfcd328b9d36aa87257f762ee24a	MALICIOUS	49/72.	N/A%	Malicious	0	0,6806	1,0000	0,8418
16	7a311b584497e8133cd85950fec6132904dd5b02388a9feed3f5e057fb891d09	MALICIOUS	52/70.	N/A%	Malicious	0	0,7429	1,0000	0,8727
17	4c82fbafef9bab484a2fbe23e4ec8aac06e8e296d6c9e496f4a589f97fd4ab71	MALICIOUS	32/72.	N/A%	Malicious	0	0,4444	1,0000	0,7249
18	3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235	MALICIOUS	54/71.	N/A%	Malicious	0	0,7606	1,0000	0,8814
19	51b9f246d6da85631131fcd1fabf0a67937d4bdde33625a44f7ee6a3a7baebd2	MALICIOUS	52/72.	N/A%	Malicious	0	0,7222	1,0000	0,8624
20	788ba200f776a188c248d6c2029f00b5d34be45d4444f7cb89ffe838c39b8b19	MALICIOUS	22/64.	N/A%	Malicious	0	0,3438	1,0000	0,6750
21	79d64863f197cd5e962212b06610e33dc9f8b34205bc6c74b8e06b0ed8eae4bd	MALICIOUS	61/73.	N/A%	Malicious	0	0,8356	1,0000	0,9186
22	860a6177b055a2f5aa61470d17ec3c69da24f1cdf0a782237055cba431158923	MALICIOUS	51/71.	N/A%	Malicious	0	0,7183	1,0000	0,8605
23	efaf8e7422ffd09c7f03f1a5b4e5c2cc32b05334c18d1ccb9673667f8f43108f	MALICIOUS	51/71.	N/A%	Malicious	0	0,7183	1,0000	0,8605
24	66713bed042b05671e7979cd7533587eca35f10228a879a9bfa015c9c4b850b9	MALICIOUS	9/62.	N/A%	Malicious	0	0,1452	1,0000	0,5767
25	73b6b7b19f154d96dbf420044fe43b3cde406c404fab30e5388284e612d03be5	MALICIOUS	12/62.	N/A%	Malicious	0	0,1935	1,0000	0,6006
26	6496807d4f83d0996c5edb0299887ce4aee26ce4537012c70777ebad2a351af3	MALICIOUS	9/62.	N/A%	Malicious	0	0,1452	1,0000	0,5767
27	87be42b2e5ffb8d223ee20a9e17cd68f5807c287fd7092e4d2971bd34a63b195	MALICIOUS	14/62.	N/A%	Malicious	0	0,2258	1,0000	0,6166
28	12bba7161d07efcb1b14d30054901ac9ffe5202972437b0c47c88d71e45c7176	MALICIOUS	44/68.	N/A%	Malicious	0	0,6471	1,0000	0,8252
29	8aa0cb69ca2777001e0f4ba0eaab0841592710e4cc5ccd6b0b526d78bbd8bfba	MALICIOUS	45/70.	N/A%	Malicious	0	0,6429	1,0000	0,8231
30	67edc4c3610de89f55259ae86a9155fd59142bc1124f02df85dec98cf2398356	MALICIOUS	27/72.	N/A%	Malicious	0	0,3750	1,0000	0,6905
31	59485D11BE4B46CE30D1FDC6B86E92E3A8D201EAF0BD50C348D740BEFB35F9E6	MALICIOUS	20/61.	N/A%	Malicious	0	0,3279	1,0000	0,6672
32	8D0B8005E271C8CC578824A1E91EA76805A6564F00735787D0891333C213272A	MALICIOUS	22/62.	N/A%	Malicious	0	0,3548	1,0000	0,6805
33	0c129e661bb423f72d6795e6ee421bd2ba1078419aafb627cc591aa1e9064139	MALICIOUS	22/72.	N/A%	Malicious	0	0,3056	1,0000	0,6561
34	b89b5ac8b8cc6c40cc93b2886c61a4a9721123a16e454e235c7a89ca7466ed16	MALICIOUS	13/71.	N/A%	Malicious	0	0,1831	1,0000	0,5955
35	ec857a710d30baf5238dc74c125de34ea2a3e5c49de07a84050de1d96b58b9bd	MALICIOUS	56/70.	N/A%	Malicious	0	0,8000	1,0000	0,9010
36	64a5231340a2c543df22fa4516950bbc7f4926df6e5ff09ff177db6c062c778d	MALICIOUS	60/72.	N/A%	Malicious	0	0,8333	1,0000	0,9175
37	a750fe1eeb4364b3ef69d0939b5aa104c9ee8890d1468984f0c36ae540314225	MALICIOUS	22/46.	N/A%	Malicious	0	0,4783	1,0000	0,7416
38	994fb855cbea0533dda9630a32ccc11f0ab5163e603ead11110732bb19655ef7	MALICIOUS	63/72.	N/A%	Malicious	0	0,8750	1,0000	0,9381
39	e0f8ddf73297a093f986d6e3155d9e305332a37d9f8a383c40c51aa318c3190a	MALICIOUS	54/66.	N/A%	Malicious	0	0,8182	1,0000	0,9100
40	3225435b9328ef4159586fa4e01f6d4057d487fb15d731071941c7c473fe2463	MALICIOUS	60/71.	N/A%	Malicious	0	0,8451	1,0000	0,9233
41	0c1587d8ce9b7b1968994727c1cbc30aff2f9769b9511545f8e3db1535f77273	MALICIOUS	62/72.	N/A%	Malicious	0	0,8611	1,0000	0,9312
42	8e38dbbf489e49b833117da15856f300d364274a96ec4145a7959627486d3f83	MALICIOUS	56/71.	N/A%	Malicious	0	0,7887	1,0000	0,8954
43	6434e5f1bccabd00de72a127a6c0b08148c7111fa0f4d01351b4ce5d70e3c990	MALICIOUS	42/70.	N/A%	Malicious	0	0,6000	1,0000	0,8019
44	f15f8e4701e071aced59c00803f3ca5abf30dd63fad6095aa2fd4d1d2043c909	MALICIOUS	59/72.	N/A%	Malicious	0	0,8194	1,0000	0,9106
45	c1c8cb3fedb1a22f3ed98110aa9e38cdf23a7033f6b6274f1f45d9ac448d5da2	MALICIOUS	44/71.	N/A%	Malicious	0	0,6197	1,0000	0,8117
46	57997f11e51549af9e9f2e70d49774c760b94fcb2f6361213b3966f9cf1ee353	MALICIOUS	61/72.	N/A%	Malicious	0	0,8472	1,0000	0,9243
47	98c5843810 39f2c7272a778c447462749d9d4a75d64546f7a2d5c9e0fb64d025	MALICIOUS	59/72.	N/A%	Malicious	0	0,8194	1,0000	0,9106
48	46a52b7f02c48bbc21e1158648e5d2fb44d1f81b97663dab4b625a700cc6d4d4	MALICIOUS	45/72.	N/A%	Malicious	0	0,6250	1,0000	0,8143
49	330be10bb8e948b983659d21b5ba673dc617aa25dc5f787d1851537d875edff5	MALICIOUS	61/67.	N/A%	Malicious	0	0,9104	1,0000	0,9557
50	6ce0a7d11351b59962e8e6f5f5799fec5c7e6c241bc687a05de41f322a02f8e4	MALICIOUS	63/72.	N/A%	Malicious	0	0,8750	1,0000	0,9381

(Lanjutan)

51	e971feede5c8a07a739548ac7d93881a26e750f0624bf3b78914b9aadff9ff36	MALICIOUS	61/72.	N/A%	Malicious	0	0,8472	1,0000	0,9243
52	a6edec8bb8a1de71eff27deecd7aae78ef4514dc8e2ed3dd83aeaf25a7e4a188	MALICIOUS	50/68.	N/A%	Malicious	0	0,7353	1,0000	0,8689
53	767f3fcee9ffd46b2a4363cffd80174c07ae8d5797f5a8f7805304c04c8f8e9f	MALICIOUS	59/72.	N/A%	Malicious	0	0,8194	1,0000	0,9106
54	d483ab9264c56f627378abbe4b29b1efccda58d70eedef72bf4a1072db5d52e6	MALICIOUS	44/69.	N/A%	Malicious	0	0,6377	1,0000	0,8206
55	fb01be0e521af523d9d97f50deee0a937a61e8cc843ec0b882f5717313560f1c	MALICIOUS	58/71.	N/A%	Malicious	0	0,8169	1,0000	0,9093
56	4426658537673182de9abc33956b29eef3eb18e7f4d2881aab7f4e8837fc97d3	MALICIOUS	44/70.	N/A%	Malicious	0	0,6286	1,0000	0,8161
57	75cc5d86debdd4460f6c4bb8deb3744eaa9ef061a206c3f44e64b82cf719078a	MALICIOUS	64/72.	N/A%	Malicious	0	0,8889	1,0000	0,9450
58	fd3c637591dfa802171102214af18f8434172581de9543adc4e787f84238bb5c	MALICIOUS	61/72.	N/A%	Malicious	0	0,8472	1,0000	0,9243
59	ee60ff1e4073073b7c122c5709f1de810691087b1c0ca0bd128695197149370c	MALICIOUS	54/66.	N/A%	Malicious	0	0,8182	1,0000	0,9100
60	de87e4225ec484e8dceb3be6fe4172e827f8871e9001e4e8566daea1b7197421	MALICIOUS	64/72.	N/A%	Malicious	0	0,8889	1,0000	0,9450
61	aafbd0338ee20af57651a90baaf8504999c072323a9515471fa63c4825a47741	MALICIOUS	61/72.	N/A%	Malicious	0	0,8472	1,0000	0,9243
62	7bc04bac0ba2752d75414cd49cb7b577fb3bba10cf093c4fc0219fced0295686	MALICIOUS	61/72.	N/A%	Malicious	0	0,8472	1,0000	0,9243
63	3b71bbfe8f25fe8cfa088c49145045d0d0b6bad2389c762a2f23677afa2b4edd	MALICIOUS	57/72.	N/A%	Malicious	0	0,7917	1,0000	0,8968
64	ef32a486692c3741b508a13884cbec9f674f2ad0cce280ddfbb0e312e087d1c0	MALICIOUS	50/71.	N/A%	Malicious	0	0,7042	1,0000	0,8535
65	f1e7ad0e00c156b9f927171af0fa415f2d234b6af3b39cd16675d94f52d156a4	MALICIOUS	35/53.	N/A%	Malicious	0	0,6604	1,0000	0,8318
66	ebc90ddb17915f0227f2229feee430afd37fc81c61ae4d703a823b82cab6703c	MALICIOUS	61/72.	N/A%	Malicious	0	0,8472	1,0000	0,9243
67	1c3199a7e3bd6da6647a260d168700d456402a9d751bc26b5a8e1874a035298b	MALICIOUS	61/72.	N/A%	Malicious	0	0,8472	1,0000	0,9243
68	4edc7981542ff530aa6708a8df8f9123335d77d51d4ca3e2b7d0c7797b0926b1	MALICIOUS	61/71.	N/A%	Malicious	0	0,8592	1,0000	0,9303
69	4121140cb90d1022a3b42305b833e04a46e7ab28a0d9dadcc43e2c922c5bf1f0	MALICIOUS	57/68.	N/A%	Malicious	0	0,8382	1,0000	0,9199
70	66b0f28aeef52f270d4ba713a57ac124f9bf711ae291050ef14b1886bba9a1cc	MALICIOUS	64/72.	N/A%	Malicious	0	0,8889	1,0000	0,9450
71	edcff9d9838400262b01881a7100ec7d31369451166b73c2ad65c8481ccc89fa	MALICIOUS	59/71.	N/A%	Malicious	0	0,8310	1,0000	0,9163
72	c61c2244e0367e3b3fbe76b98f6a516a03ab904a1c5d7fcace285c51c4dff43b	MALICIOUS	60/70.	N/A%	Malicious	0	0,8571	1,0000	0,9293
73	ce0a06bd85212a6325cbb0c816ecbed75d173f005f9f9e622d22c4e9aff79dca	MALICIOUS	54/64.	N/A%	Malicious	0	0,8438	1,0000	0,9226
74	a716a94fc0cd31b5d368b65044dad9983c1904e7d51ec64ab30567af59f4e8ca	MALICIOUS	47/71.	N/A%	Malicious	0	0,6620	1,0000	0,8326
75	0d27ddfa897381bf31878ca0af868a83a2746cc8d428c0e11a5f0b2e2d28ec72	MALICIOUS	58/67.	N/A%	Malicious	0	0,8657	1,0000	0,9335
76	37962d265ce4c3d6b0e1a2479522dc2bfc835b23552cdb24c35747d0c22bdd13	MALICIOUS	52/65.	N/A%	Malicious	0	0,8000	1,0000	0,9010
77	c4a11391f44853cf8783e17c14eeb379299d9137e3facf7f32a8cf5aea3b9767	MALICIOUS	52/65.	N/A%	Malicious	0	0,8000	1,0000	0,9010
78	5d20df009a03db5de41320f16acf70fc43137ea774db84b2bd22885ce5a5ced3	MALICIOUS	53/68.	N/A%	Malicious	0	0,7794	1,0000	0,8908
79	8ad4ee4f8c4ec47148635ecd1f3f70506b96752ad0c018fa5bc36596d559ec81	MALICIOUS	49/64.	N/A%	Malicious	0	0,7656	1,0000	0,8839
80	8a87aae368cd9817f313ece0e4bb52568017c01e245b7883b03db4bb03d80a1a	MALICIOUS	60/71.	N/A%	Malicious	0	0,8451	1,0000	0,9233
81	8d330aabb2f7c7ca00d5ace55110f7d4f977f2bae53f5605f2bf4230b19eb494	MALICIOUS	55/69.	N/A%	Malicious	0	0,7971	1,0000	0,8995
82	78c25d10e088fabffa93f29515f370e0c363199e3747b934986569fc7c9f3adb	MALICIOUS	20/65.	N/A%	Normal	0	0,3077	0,0000	0,1524
83	5fd0e67e8a755007259a760ac326b087a716191e42f13870642911cce39c228b	MALICIOUS	52/69.	N/A%	Malicious	0	0,7536	1,0000	0,8780
84	b056e1dfb6566ef0b2e10023d25b5bac3666a93b9f7a699afdff76c33b31793a	MALICIOUS	22/62.	N/A%	Malicious	0	0,3548	1,0000	0,6805
85	e2c0b2a29fb336e68031e00817a7d0808cc21d440bba3cb5b4b0bd835cda31a3	MALICIOUS	22/60.	N/A%	Malicious	0	0,3667	1,0000	0,6864
86	edf67f3e68edcb4e87852cdc10cdeb650a6bf4ab803b7e1fcb9b7f4bfee9fcab	MALICIOUS	21/60.	N/A%	Malicious	0	0,3500	1,0000	0,6781
87	6eb412e139987a8c83ffc920e10d8af81310de375ace0dfd3895f03514ce0a90	MALICIOUS	22/60.	N/A%	Malicious	0	0,3667	1,0000	0,6864
88	7448c841d7b0a02301d8aacbc4651e8492133b5d6077d9b9f9323337b29ba7b3	MALICIOUS	34/62.	N/A%	Malicious	0	0,5484	1,0000	0,7764
89	59e68875b733b15fa766af8d4f1d960b961e81a3b9cab37cf161c8ac9057ebd6	MALICIOUS	25/60.	N/A%	Malicious	0	0,4167	1,0000	0,7111
90	8d0ffcb69cefff7f66be5248e7714549bdaccab163842a86f8baebf7a341ea5d	MALICIOUS	15/50.	N/A%	Malicious	0	0,3000	1,0000	0,6534
91	536e1f8f46ee0f6cced9da56710b7f6996526da9d48e9cb63c0acb53dff14d5b	MALICIOUS	26/62.	N/A%	Malicious	0	0,4194	1,0000	0,7125
92	c03958f4bab9297fdaca6848c6b940002321fde305c3c3d61e0d1714fcdb1cd7	MALICIOUS	48/68.	N/A%	Malicious	0	0,7059	1,0000	0,8544
93	f16deb705d44a9b8bf1ac09128951b660d74bbce751c04293e5988f1bd1192be	MALICIOUS	55/71.	N/A%	Malicious	0	0,7746	1,0000	0,8884
94	32e6e9765b2e1e18699fdcc2817137b22f893457e2a10ae3f66081dd58f811ce	MALICIOUS	34/59.	N/A%	Malicious	0	0,5763	1,0000	0,7902
95	0729f408d5386d401f611358b5b7080afc070d352ad0fbbc45df1e901fb92a57	MALICIOUS	29/61.	N/A%	Malicious	0	0,4754	1,0000	0,7402
96	1966db90a2957b9015efaef6b635c0d96496e5e201b25f65b13f2e7aae7b57b1	MALICIOUS	28/54.	N/A%	Normal	0	0,5185	0,0000	0,2568
97	b0338437cfa0fede611a1f48bc7601482031ffcc4aad597e7aa6d3e44abdf2a0	MALICIOUS	43/60.	N/A%	Malicious	0	0,7167	1,0000	0,8597
98	a6eefc0acd6b5e512514a8933ec9f6059af268c364301e1fe8e11c3fb3888a5b	MALICIOUS	52/68.	N/A%	Malicious	0	0,7647	1,0000	0,8835
99	b7bfcc457284207f51138847c2036298f2e70d98d51bcc35e34a64cc5c591fe5	MALICIOUS	56/71.	N/A%	Malicious	0	0,7887	1,0000	0,8954
100	16007fd9454eecba4a5ae3e696e3a51ab8760323efa0eb57433ce2d5eeabc6ec	MALICIOUS	15/64.	N/A%	Malicious	0	0,2344	1,0000	0,6209

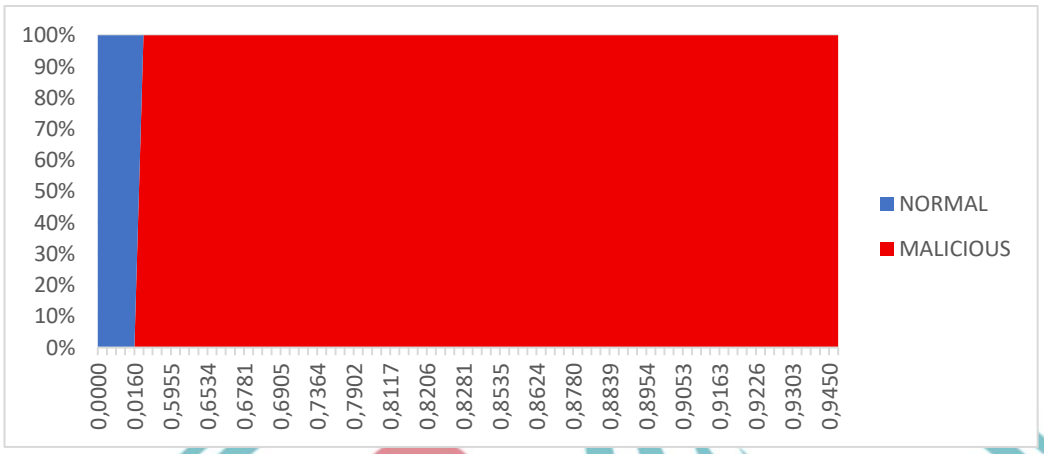
(Lanjutan)

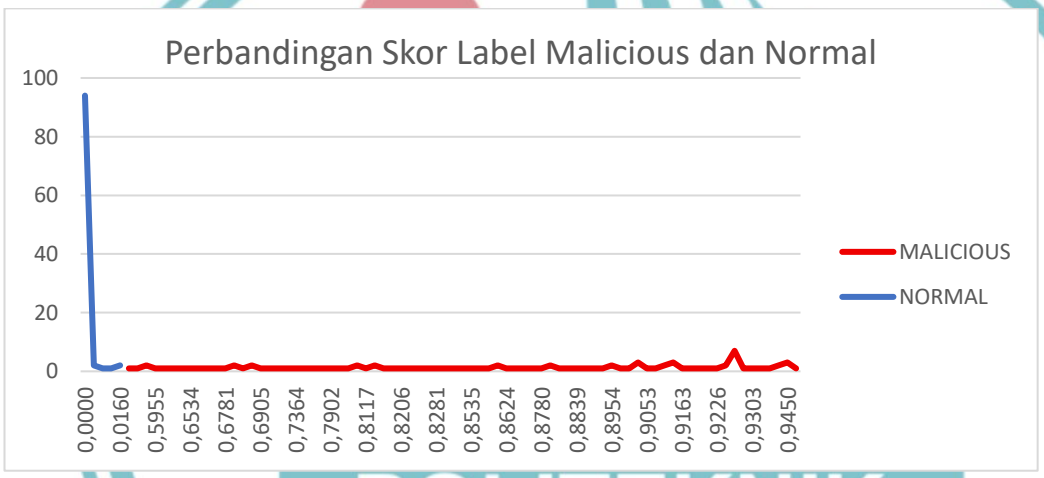
101	017995F270C646A7965FF205F3639B34D9E9F2FC99165C59B271BCA5AEFA80B6	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
102	0242A17D920C12146954B02BA575D9E4D9EEF32BDDD90BAFCF81C38903BE0900	NORMAL	2/62.	N/A%	Normal	0	0,0323	0,0000	0,0160
103	0270797E9DA9B10850424689870789798387B87C639FEB4B840FCBC12A6EB2A4	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
104	05133264950463C1EFD58E20699D540CA8CACCDD53CC1272ABE698773299B3B2	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
105	06E60A78C362502719AAB1D530A16B6EBBCD974C14D792B8C4238DD4D8B2555C	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
106	08DD72F58B5036D8208584FC9E56730522630B59DC659BC8753516734B727045	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
107	0930A8893D3BE7F983BE795889052ECCF28C63E01B909EA6D4A37A8797A6916A	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
108	0A2B20268C556D120CB5D757590BC6A7C35833FEF827D0C6B3335CE73CE70A84	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
109	0A4340E5511800FAD03E6239E1355CBB3B2D6E5062A73CC38418F972FA7A1113	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
110	0B1E352D9C579D0EADDD0F6D080971A16A474D923D9996118390F35C258BEC1D	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
111	0B402F661DE1AD3F51E7189943949D323F26ACA0C4140E58B8942EF02A424EF4	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
112	0FD02CEFC64BAF86B6E75F9027F989719FC58548E1892D3EA14FA2E5A1CDFAC9	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
113	1109EC66BA28F46B494364E26FC146A6207522BF888D028DE1C9E6F6ED9546EE	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
114	12CC9D391437EDEAFE5B3199E2D493C0B5CE79B12594CED53762FACDF2A69A6A	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
115	1351E3D4EDE0A1A83CE7A5CC2FBBA2FA5BA5FA5E318BE0BD1DE385160A110762	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
116	14C5E943D9EF2BC8228F14329AA398F3E879857D3AB2147DE68B7ADAA8E79392	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
117	170E318BC67FA83D89998CF88F32302F2E34A01C1647A9E8AB1D144ECB16C937	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
118	179222BFBB842B612652B04C39964B1F944B464DE16D5CE52D540D8A4BCCB820	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
119	17FBEE270AA0A1975419FD799443838C6AF9978A1489A4479909401DD38A3108	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
120	195FC20C6043E3F7C7FE4929BDC9F3B81CE1CD07FE213D505190653AC21BB46F	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
121	1ACA473DD48E537DD95D4343B2CC108353C0598435625FA74953B167CF2FF43C	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
122	1B096BC695A610576E0B0F34FD5126D2C02117F3BA26473D9151F3E5744A1C8A	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
123	1B8989D423D70F527B0A32BBA803276697D19BF46DDEE8CB5A4CC35719D01CD4	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
124	1E214AADD2D276E199A26A37EA4BD67B50C64D91635537A6BF940A309242D6E2	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
125	2206B0441DE805648B0E587C27C59401D65FFA0CE843058F950AE7B64ABAB44F	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
126	23AFE32CB254A166800C97FF53E48FC32CC2C738732C9A4F3525EA0DC7D34E2D	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
127	242452FEF30C454372237D86FE4BFAB3CDD2A553CBC5C7F9034BB2E526B6880F	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
128	242B92D4A3865D9C936912D742C7995431A1C34F211C2EDF7CCA49DFADE090F5	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
129	24CA1EB366CF0FCCA4B1CF3D2C7E784127530BE192537AECCDD6F840B99BF6BE	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
130	26FFC771E7C3B62A81C30A47DD8D82BB9D104C27F134B8FBA3F5ADE418297145	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
131	2A3385DB2807BB504B560790579255CF08BCC4C759D4BFA518A398B135B30ABB	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
132	2A60C6968118101F8478A04279A688FC03181B6E90C581C2536FE6B39488E87C	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
133	2AC904B8EDFA544867C8E0EF89FAC5696CD2D3206819154C53DC673CC1DDDD75	NORMAL	0/62.	N/A%	Normal	0	0,0000	0,0000	0,0000
134	2B23FD2D745D25AC78A4B5DCD56585589B2741BD6BFF15920B4CA0CF105B496A	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
135	2B81BDB786CA5670C6B11C73C716F8C57EB8B6954A341FB90458C9817F71750E	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
136	2B8BE75AA4DFCCDC8B85C2402A3252BE5B304EFBB1B52CC8767FF41C72402E5B	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
137	2C482BEBC9F63CB91DEA44B92242CBC6C80D8A19630314BD712AA3B6B429B71F	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
138	2F7DE5C44671522400CE7E3D1274988763F9099AAFD99912B70BDBB8237403CA	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
139	3013A0E8FE37EF099BCF8C2C29905BE56F2BABE1400DEA771B1AB672EF057C5C	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
140	30BD05AD63455D066EFCCD89E2E3AB2CBF2BEFFEBBA3AAF80CDF92B37A7DB726	NORMAL	0/62.	N/A%	Normal	0	0,0000	0,0000	0,0000
141	3280961AF5BA3B00E11CE9C892C4D2437D38CB4C0938EAB8B6AD683E759C6585	NORMAL	0/62.	N/A%	Normal	0	0,0000	0,0000	0,0000
142	337532D2E2D3B8FD5EA545C79B10D835719A0B072D502F19414D734342F5DCB4	NORMAL	2/62.	N/A%	Normal	0	0,0323	0,0000	0,0160
143	342EAB3D1EF5186D5C570B6BEE15EE8A988B02D1C38723AEC35F501959953E3C	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
144	353924E7D11B5BCEB903D55018546ADB5DD8345487819AB90E315C04AF93210C	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
145	3641EE8B5867B396103335D53C99AC6C0BEBC7D4341D1831C95728D757548CCA	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
146	366ECF37702DC6588AA31F59C9883BCF730A8C8B7A429A67BC54BCD46FAB6741	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
147	36FD6FAAC5D220BDA87AEFF256B869D13C70A124EB2896D6F307245ED97BB61A	NORMAL	0/62.	N/A%	Normal	0	0,0000	0,0000	0,0000
148	3968227D56EB9F2AD9BE295CDF80EFBEC2EA718F610A9BDAEDFC4521BEC62133	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
149	39758628FD9E06B3DB76E9942694460E84039681FC16857BBFCE058EBA8C416C	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
150	39CDBA0EC1F65D1F0F10B475E33FCA20D9F3B2A5E50F8C39F24A2C0F9A3BD69A	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000

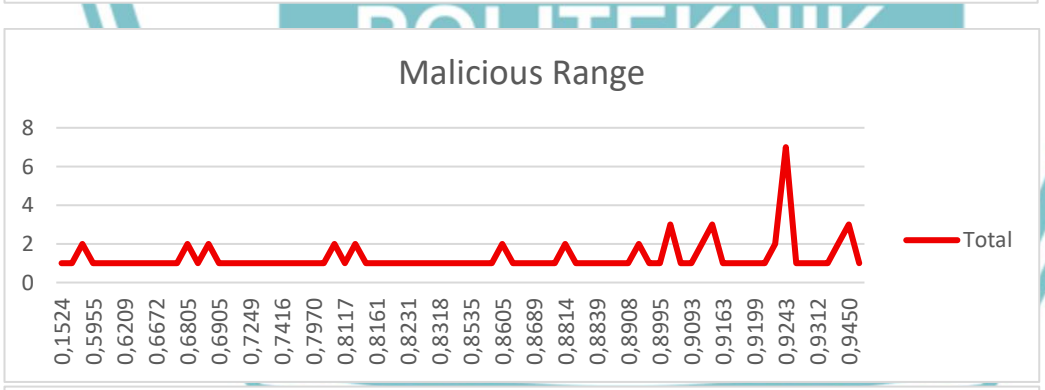
(Lanjutan)

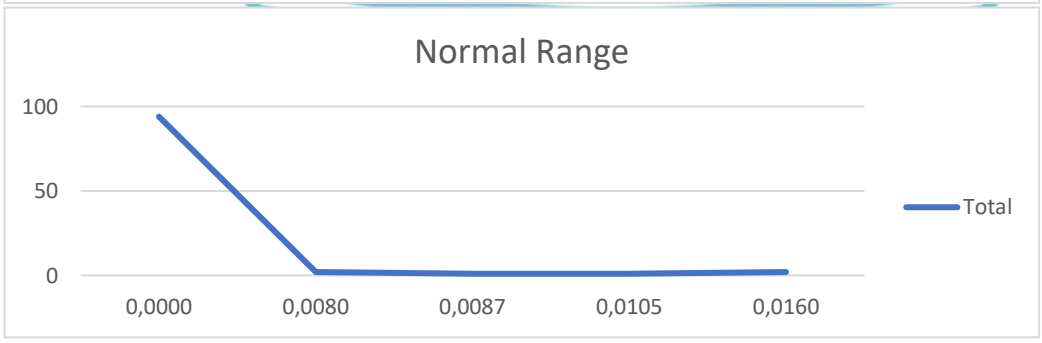
151	3A21D7872B04104E320518E8C692EB683D62BBD4072AF94B2AFDB40A9E417554	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
152	3CEF0A051F789AD29F8C08C2D53C6F495E3FD4490830713DA4F294DBAA6CB348	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
153	3E05357CF8D0A87C8D031C583A30A67FA5BB321F3AEFFA51E4C55E8FA0B05DF9	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
154	4049EBDFD88F088AE69284E38E13568FA10E0B6D15125F1C8A9C1CE6EF9635F2	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
155	40DCE2007A35CB4B5497F04E25669D92B88134902E24C8ABB3C8B910FE002124	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
156	442A87CF7EE48C38CFE7765587B12F125D5306A799EB2116F448999994D8C2C9	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
157	450D8F8E9D3C7F7E2A04137FB09BD790847B9B906BDB8026D14982454F53CE80	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
158	462B88BAB8C8033ABB71C6C1793F16EA894A82DAAD355E6C1D084A6FFB0F3487	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
159	46D9ED1078C5D942F9C3FFE8756747A60CA81FBAF6DD783BFD71A770A4BB8FC9	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
160	4771E2FB446F69B3C254AB159628DCB1A82CBE997091E54EF7A6941A29A41CBE	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
161	48718306BC3694D2DA705DA959DF814793C21F1ED9B4E82DE25383DD69086B42	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
162	489AFC87B0E842EC1FDDA396FF883EAC8B0DB4F85F3D99DC596E2499084A89B0	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
163	4AC0ABD71BA1FC953318587B17F877D5801E87F273CB60B5A70291CE0695EEAA	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
164	4B367FE51907F119823C360FE38F8809320EC48DCFD0EDADDA4D92EDFCD194AA	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
165	4CFFF1F8E0479F3106A1A926FBEFAF2E8018129D5574F8EEFC984C016095F0BA	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
166	4E32F33B2FA57F337F10CB56B4296E9DC4A6AAE35639B3698926AB0D259C8F0D	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
167	5006EECA919DF665052DA5BA4DDABED82B47BE334CC6EB867EB7F3BCF0A40E97	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
168	50701DC3F2CA802836247D254CF0257B75CBDA511BB51D8FE670C06B81EF7CF0	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
169	50C46D95A70CCED676F515600BAF4D2C5FDAB66E7EF67DB3BFBFD0C182ED6C7F	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
170	540DF47ADB43C36C32BE96C62C2F988B454B77A2FFE33575D6970308372D41FB	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
171	555BAA8A7C3016E301AAA3B05DEDCEBDA1B22E16BDC8BDC1523154E8C5AEA017	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
172	558DEDAC46678DE72496A68A5F31EEC002F82E920A5B96A357CEE5B31FCDC032	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
173	55FAED6E44EC4CD8663E2B1F4948986AC4CA40FFA0C72ECE1C4F31D565DB1DE2	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
174	57E6A28A68A32A984F9BE89E6370981E396E590F366715F3B6A03A5FB3740C14	NORMAL	1/62.	N/A%	Normal	0	0,0161	0,0000	0,0080
175	5825BD0858A6DA682FCF64597FCB5403DE3C39E8C4248CBEB69FA36B46DE12EC	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
176	585CF78C74A3A2997C5676AE8140207636E95897C27CB575FA1637CDF42F846A	NORMAL	0/62.	N/A%	Normal	0	0,0000	0,0000	0,0000
177	59B7BBC9F33AD2FBB82E98E88712960E4DD09F1E1E09E5DA4230CB2518F1D337	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
178	59FB3F8E7E0CE08934FC5608A7C7262957E6D5B5536304F622CC9323B4BD73C6	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
179	5DFE821E38D4984FAC615ABD6FED5CB236196C364921FA0DDFE72FB10B77E66B	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
180	5FBC1666BCDC11A194DFF26513BEE84583166610B22DB3294C4D56B96F4DEDFD	NORMAL	1/57.	N/A%	Normal	0	0,0175	0,0000	0,0087
181	6347E3D613D80C83A63CA19F39083DEA94DDEEBAEFBBBE50DF8F1C3497767FBF	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
182	6519E6CA90B20B51D4CBEDA482A354E3FE76CF935ACD94A2EF6EB5B73A204525	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
183	6579FA98B3C1B179D34CE6752CBC792ABE75CD931D78DA682757298F26A975A1	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
184	657ABF716EAE316BD829E1C44F81BFF193A44C5710FCFD5447390EAA1FBE3447	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
185	65D6430E568985364B5C0C7B958D762D26EAE4AD76B20BEE5982300BF8F55AE9	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
186	6641B1D9CDF0969F0DB83D09F587570C540BA103CCB95EC8FD920E3726A9190F	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
187	6750CED46A4EF2D343D1B998EA641A823708E66ECA4A11136A22A46E68FAC3A9	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
188	67E3448AEB088592F759ADEE12D6451082DB269345980CC4DB6B74A77EE80452	NORMAL	1/47.	N/A%	Normal	0	0,0213	0,0000	0,0105
189	69F45B6279D411137B602D162B814A48B4E951074138C15C4DD47A3BB5484D6B	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
190	6A539A2D19B339A504E6AA81F23EF69BB62CB6798348CD85ABD5ADF6A96B6FE6	NORMAL	0/62.	N/A%	Normal	0	0,0000	0,0000	0,0000
191	6ABDF0C5FDB2CE0290590FE35DC68E2BBFEC6EC379AABAEE32A272ECDFEB851B	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
192	6BC929264347D596DB6AEC4B592E318E102A62F8963AD1B7A8422B7B6A9657BB	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
193	6C01FA5464304847B63A23265A5A08995BE03B1A16934B40F21EC0D12B6620B5	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
194	6F6BAB2D8DF9EAE2D28AAF59DAD7F4845D2C47A62B54328972F5E76CE87E2DBA	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
195	700D68A4D38335783D65B3B23BD7B928E95202DCEE9023E1FCB4A160C5187853	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
196	7073B7817BC50F420260E7BD86A30452A96F4294DF04E7848E9E1FAEEE84B7D9	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
197	753A9D215BFED9A0D71B6722A99958381A116ADFD999979B1E81C50395A2DFA5	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000
198	7542A1BFDE04FB0174A77A5D846C1775D324450DE553CCA97C9E2F858E902A46	NORMAL	1/62.	N/A%	Normal	0	0,0161	0,0000	0,0080
199	75C3006576A43EC93B4841565C5184BED1DC0FA2F9C15FC0076CAD9A136FAFAA	NORMAL	0/62.	N/A%	Normal	0	0,0000	0,0000	0,0000
200	7624C7938793B9B2B8606466FC8D624AE45361602B595DC3A186CFB3A782AE6B	NORMAL	0/0.	N/A%	Normal	0	0,0000	0,0000	0,0000

Lampiran 4 Sebaran data pada pengujian awal pembobotan

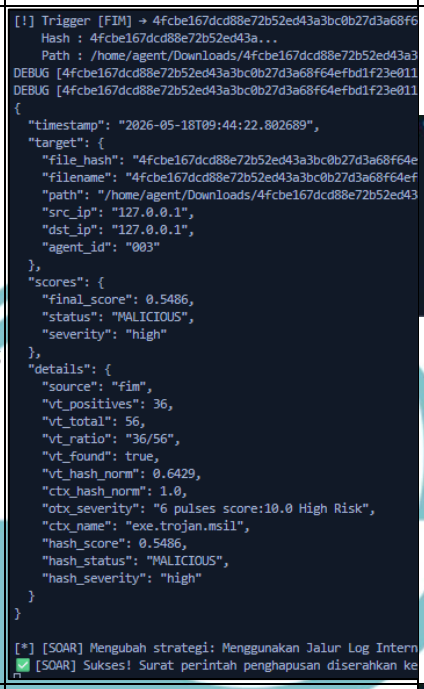
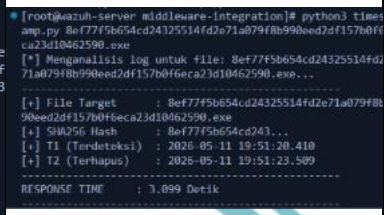
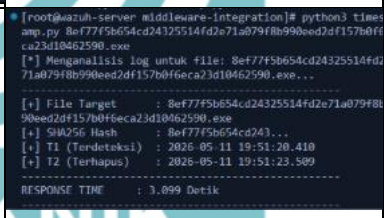


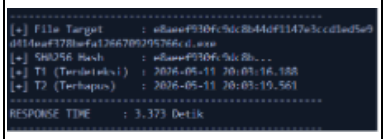
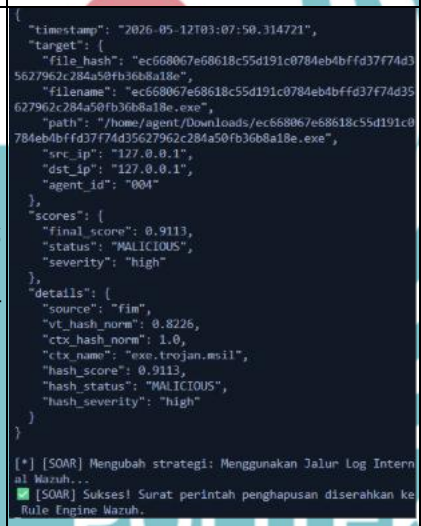
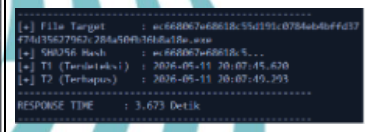
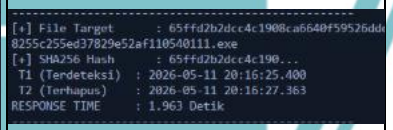






Lampiran 5 Hasil pengujian 428 data IOC pada sistem

No.	SHA 256 (IOC)	Log	Timestamp
1	4fcbe167dcd88e72b52ed43a3bc0b27d3a68f64efbd1f23e0113cd9f55a55f12		 T1 (Terdeteksi) : 2026-05-18 09:44:22.802, T2 (Terhapus) : 2026-05-18 09:44:25.899 RESPONSE TIME : 3.097 Detik
2	8ef77f5b654cd24325514fd2e71a079f8b990eed2df157b0f6eca23d10462590		 T1 (Terdeteksi) : 2026-05-11 19:51:20.410 T2 (Terhapus) : 2026-05-11 19:51:23.509 RESPONSE TIME : 3.099 Detik

3	e8aeef930fc9dc8b44df1147e3ccd1ed5e9d414eaf378befa1266709295766cd		 T1 (Terdeteksi) : 2026-05-11 20:03:16.188 T2 (Terhapus) : 2026-05-11 20:03:19.56 RESPONSE TIME : 3.373 Detik
4	ec668067e68618c55d191c0784eb4bffd37f74d35627962c284a50fb36b8a18e		 T1 (Terdeteksi) : 2026-05-11 20:07:45.620 T2 (Terhapus) : 2026-05-11 20:07:49.293 RESPONSE TIME : 3.673 Detik
5	65ffd2b2dcc4c1908ca6640f59526dde3048255c255ed37829e52af110540111		 T1 (Terdeteksi) : 2026-05-11 20:16:25.400 T2 (Terhapus) : 2026-05-11 20:16:27.363 RESPONSE TIME : 1.963 Detik

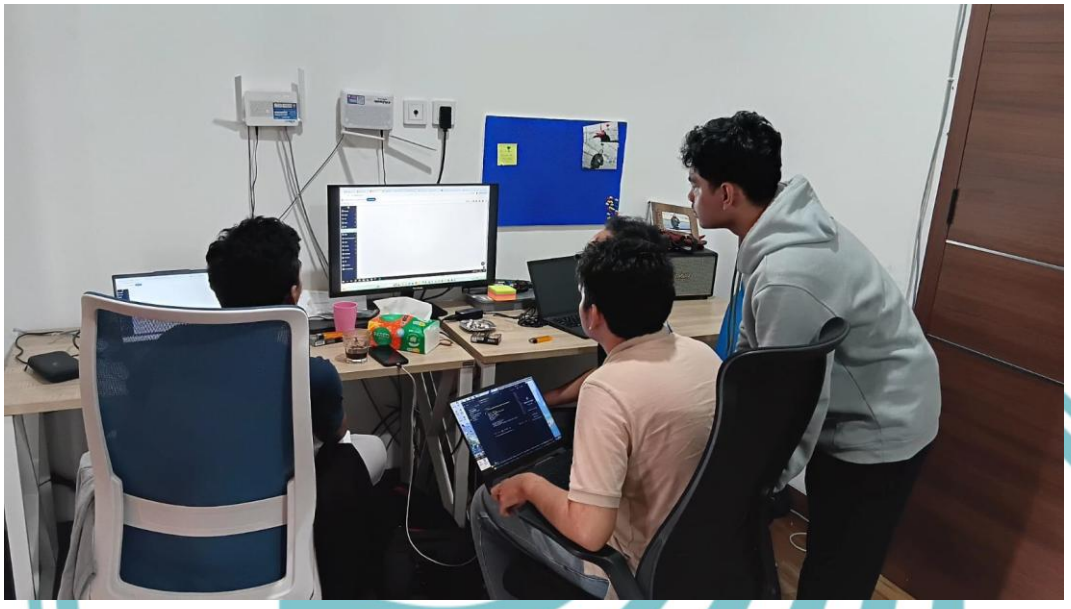
(dokumentasi lengkap dapat dilihat pada link berikut : https://word.cloud.microsoft/open/onedrive/?docId=5FE89369CD32FD12%21se7a621e481fd4dbe9b61ac6923e047e6&driveId=5FE89369CD32FD12)

Lampiran 6 Tabel hasil pengujian 428 data IOC pada sistem

No.	SHA256	Status Awal	VT Ratio	Skor VT	Skor CTX	Status OTX	Bobot Akhir
1	c91183175ce77360006f964841eb4048cf37cb82103f2573e262927be4c7607f	MALICIOUS	23/43	0,5349	1	48 pulses score10.0 High Risk	0,5119
2	c91183175ce77360006f964841eb4048cf37cb82103f2573e262927be4c7607f	MALICIOUS	23/43	0,5349	1	48 pulses score10.0 High Risk	0,5119
3	8c1dc9732884c6078b23953b78314a8d0d8b8d9fe42e5f97a7cd09b8ace943a9	MALICIOUS	29/43	0,6744	1	23 pulses score0 Unknown	0,5593
4	52b6fb40e7efb09c2bebe8550178e7e30009600bdedd1acae085d753761b7598	MALICIOUS	45/70	0,6429	1	23 pulses score1.1 Unknown	0,5486
5	40c2e559992a7f595c593b419930a3f216516c3042ad86fb985348d53b6e01b9	MALICIOUS	46/72	0,6389	1	13 pulses score7.0 Medium Risk	0,5472
6	9f4672c1374034ac4556264f0d4bf96ee242c0b5a9edaa4715b5e61fe8d55cc8	MALICIOUS	28/60	0,4667	1	26 pulses score0 Unknown	0,4887
7	5a17cfaea0cc3a82242fdd11b53140c0b56256d769b07c33757d61e0a0a6ec02	MALICIOUS	24/44	0,5455	1	48 pulses score10.0 High Risk	0,5155
8	b2ba51b4491da8604ff9410d6e004971e3cd9a321390d0258e294ac42010b546	MALICIOUS	41/61	0,6721	1	33 pulses score10.0 High Risk	0,5585
9	fd3f13db41cd5b442fa26ba8bc0e9703ed243b3516374e3ef89be71cbf07436b	MALICIOUS	28/48	0,5833	1	50 pulses score10.0 High Risk	0,5283
10	969d2776df0674a1cca0f74c2fccbc43802b4f2b62ecccecc26ed538e9565eae	MALICIOUS	39/59	0,661	1	41 pulses score10.0 High Risk	0,5547
11	dee1f9121f3a6682101389f432b4dee709507f7ace0a21d9cdbe373a40998e73	MALICIOUS	49/70	0,7	1	4 pulses score10.0 High Risk	0,568
12	4fcbe167dcd88e72b52ed43a3bc0b27d3a68f64efbd1f23e0113cd9f55a55f12	MALICIOUS	36/56	0,6429	1	6 pulses	0,5486
13	a9814c12c8f86a7b13e2d8889f6d0b082bca0cb65747045014707 75ae27e1f26	MALICIOUS	38/52	0,7308	1	4 pulses score13.0 Unknown	0,5785
14	e3c741645c81ba04a1ce8095dce081f7452b67bf2927fe23e0d68d4f7021754b	MALICIOUS	56/66	0,8485	1	4 pulses score16.0 Unknown	0,6185
15	637efa8a39524160858818ff63e2e0e502d5808aee97063ba4e98ee15267d0f7	MALICIOUS	24/56	0,4286	1	4 pulses score0.0 Unknown	0,4757
16	dba68a3035a409a34c848cb1218399fb7c9be87e45d0ed618e2d56f5fba19fb3	MALICIOUS	55/71	0,7746	1	4 pulses score9.0 High Risk	0,5934
17	4b3b9e2e24a56ab342bb517e97acbd203d37a090b0159401bb6a54fc11230b88	MALICIOUS	58/66	0,8788	1	4 pulses	0,6288
18	bda2b0b9985a34ff7589bec1b5f4eabf3c4e452ba479111663dc96253468b115	MALICIOUS	63/72	0,875	1	4 pulses	0,6275
19	e94865b2b225c8fe7e51c224d486c50711441647cf2266a7a698c1e56576036f	MALICIOUS	21/59	0,3559	1	4 pulses	0,451
20	00823f9a400139cf09885081cfa1115fe169df77dc01fe600f1393419fc5a5d6	MALICIOUS	27/60	0,45	1	4 pulses score10.0 High Risk	0,483
21	21117a9986e6c46e6ded575f875b254218d4d9b9588c1391fddf3b8b7cfa7e61	MALICIOUS	60/72	0,8333	1	4 pulses score6.0 Medium Risk	0,6133
22	595ebb854f6512804b3603ac8b63670531bd2c477845fd8b08d3411ae092cc38	MALICIOUS	57/71	0,8028	1	4 pulses score9.0 High Risk	0,603
23	030967003eace6864210b5ac969bd55e91eda783aa60869fe6ff6dae00ee9c96	MALICIOUS	56/71	0,7887	1	4 pulses score10.0 High Risk	0,5982
24	0a2c926442601cdd883dfc4d4b64b2f275d42fdeab88c082ca1cadbce2aad59c	MALICIOUS	26/59	0,4407	1	5 pulses score10.0 High Risk	0,4798
25	13beedd8a3f0a76dd864ff5693f3da4e70f7abf2fa846c9e51f1c87994ee0f61	MALICIOUS	26/60	0,4333	1	6 pulses score10.0 High Risk	0,4773
26	d6775349cb389f4c7a15478fef2c83baaf24540e28a57a40bd7d8e0fd24e65fa	MALICIOUS	21/53	0,3962	1	5 pulses score10.0 High Risk	0,4647
27	050fb15146ce0c354071e0fde7cd4c7948e89c339c37e27a422fa554b27f6d9e	MALICIOUS	26/58	0,4483	1	5 pulses score0.0 Unknown	0,4824
28	2c44a8d802cf2d05fe996e97a27ff9b123ecfba2b9be48cf35172b6489201605	MALICIOUS	25/61	0,4098	1	4 pulses score10.0 High Risk	0,4693
29	74f71cc4cff80b7fcac8e86f595b8d0e55718efde0c0040e2e2a5b66aeb05e1d	MALICIOUS	24/60	0,4	1	4 pulses score10.0 High Risk	0,466
30	7a009bba10f7fdfc958f97511b3c312373723444646fe1833ebb0753c5484b4a	MALICIOUS	25/60	0,4167	1	4 pulses score10.0 High Risk	0,4717
31	4c3b97c157d08ee298edb5d30fa86a3b90b04fedfbe517e7e0307b6013eacbf0	MALICIOUS	56/67	0,8358	1	4 pulses score16.0 Unknown	0,6142
32	da315d9c9c5c31c1cbfdcdbe673b94f236ad46afb6261ee7b22fea878b97a4e5	MALICIOUS	56/71	0,7887	1	4 pulses score10.0 High Risk	0,5982
33	3380d357123e5b81f36a3e606864da12ec9ae2a94c0cd580a89309adf077acd6	MALICIOUS	51/72	0,7083	1	4 pulses score0.2 Unknown	0,5708
34	520aa5f9f233057e70c40f9c7c3f417da4d0e1dd400a2dd4ff61d18b759ce8d0	MALICIOUS	60/70	0,8571	1	4 pulses score13.0 malicious	0,6214
35	55179fcade854308f587291b9bb586f97758ed216a5d773610e3f5f38d25e5e9	MALICIOUS	59/69	0,8551	1	4 pulses score6 Medium Risk	0,6207
36	f10b6634e99ff37ec83b9fecbc7cee089c1c82999eff9a6dc4519071e38f8000	MALICIOUS	60/70	0,8571	1	4 pulses score16.0 Unknown	0,6214
37	017ba68aa41ff6416707ea9fe1482dc231a6c6e2740961f5107c88695e9c4362	MALICIOUS	51/62	0,8226	1	4 pulses score16.0 Unknown	0,6097
38	741508351f8b822d9ce3ecd6d380ac5a37b598b7114c3db5e77a2bacd709c7c8	MALICIOUS	59/71	0,831	1	4 pulses score3.0 malicious	0,6125
39	5722bae97daf54f30f3fcca10ced0c88ec0e64f5c1de3152c332e6178b64acf2	MALICIOUS	56/67	0,8358	1	4 pulses score16.0 Unknown	0,6142
40	dce7346008cc7d3088246fe8bb2924315673e66ee6f939941d4ce73c2de16b08	MALICIOUS	55/68	0,8088	1	4 pulses score13.0 Unknown	0,605
41	909a9da9a1f47e503c348d59216494ade8d1fed8fd97e1435be1b0f98e156835	MALICIOUS	51/69	0,7391	1	4 pulses	0,5813
42	8289c8db41f3396a4353a982e715bba0a2d8b272b5d915f2462ac0578847d76a	MALICIOUS	59/70	0,8429	1	4 pulses score16.0 Unknown	0,6166
43	fb6d4ce94013385b31b30ec1ab8f1a6b2c34252a13062f880eae47b2b5cfc4e7	MALICIOUS	47/64	0,7344	1	4 pulses	0,5797
44	59374902866a6c62f56f32bdfd15a3a3215ec8d6bd2144b111066eff58c8e998	MALICIOUS	54/67	0,806	1	4 pulses score16.0 malicious	0,604
45	cdde3b2650c951e774a8694208c0d151e91b40db5d21da3d790d88ebd702edec	MALICIOUS	50/58	0,8621	1	4 pulses	0,6231
46	b954d66d6cb60a558efff4eb514a87f3ca4e657053090cc1d0770eb17e68560f	MALICIOUS	25/60	0,4167	1	Error Connection Failed	0,4717
47	0001b8219a77f8e206efe2b71ecf3892aed755c26fb2dc5e4b7b42a226b72eaa	MALICIOUS	31/71	0,4366	1	Error Connection Failed	0,4785
48	58d9f039ec38bbe03a1e1bf58a0102ce9c94d6efe39d2450cb44917d4a5c75af	MALICIOUS	56/67	0,8358	1	Error Connection Failed	0,6142
49	1159467031d7e6422cc1dbb955b2bdd50a0552dc433364caeffb5e2204f042aa	MALICIOUS	58/70	0,8286	1	Error Connection Failed	0,6117
50	65b912304a9ea084a79024eb215644b0b3b068da5bc475e681e0f09ba66e6f65	MALICIOUS	21/49	0,4286	1	Error Connection Failed	0,4757

(dokumentasi lengkap dapat dilihat pada link berikut : https://word.cloud.microsoft/open/onedrive/?docId=5FE89369CD32FD12%21se7a621e481fd4dbe9b61ac6923e047e6&driveId=5FE89369CD32FD12

Lampiran 7 Diskusi Sistem dan Treath Hunting di PT.XYZ



Lampiran 8 Kode Middleware

1. Kode main_scoring.py

```python
import os
import re
import json
import threading
import concurrent.futures
from datetime import datetime, timedelta
from dotenv import load_dotenv

try:
    from checkers.virustotal import check_virustotal
    from checkers.ctx import check_ctx
    from checkers.otx import check_otx
    from checkers.abuseipdb import check_abuseipdb
except ImportError as e:
    print(json.dumps({"error": "Module import failed", "details": str(e)}))
    exit()

load_dotenv()

CACHE_FILE         = "cti_cache.json"
CACHE_EXPIRY_HOURS = 24

# ── THREAD LOCKS (SISTEM ANTREAN) ──────────────────────────────
cache_io_lock = threading.Lock()
analysis_locks = {}
locks_manager_lock = threading.Lock()

# ── BOBOT CTI ──────────────────────────────────────────────────
W_IP_ABUSE = 1

# Hash: Diperbarui menjadi fusi 3 CTI (VT, CTX, OTX)
W_HASH_VT  = 0.4927
W_HASH_CTX = 0.5073
W_HASH_OTX = 0

# ── THRESHOLD KLASIFIKASI ──────────────────────────────────────

IP_THRESHOLD_MALICIOUS = 0.35

HASH_THRESHOLD_MALICIOUS = 0.10


# ── CACHE HELPERS ──────────────────────────────────────────────

def load_cache():
    if not os.path.exists(CACHE_FILE):
        return {}
    try:
        with open(CACHE_FILE, 'r') as f:
            return json.load(f)
    except:
        return {}


def save_cache(cache_data):
    try:
        with open(CACHE_FILE, 'w') as f:
            json.dump(cache_data, f, indent=4)
    except:
        pass
```

(Lanjutan)

```python
# ── NORMALISASI ──────────────────────────────────────────────

def normalize_vt(raw):
    if not raw or any(x in str(raw) for x in ["Error", "Not Found"]):
        return 0.0
    match = re.search(r'(\d+)/(\d+)', str(raw))
    return int(match.group(1)) / int(match.group(2)) if match else 0.0


def normalize_ctx(raw):
    safe = ["not found", "error", "none", "normal", "timeout"]
    return 0.0 if not raw or any(s in str(raw).lower() for s in safe) else 1.0


def normalize_otx(raw):
    if not raw or any(x in str(raw).lower() for x in ["none", "error"]):
        return 0.0

    raw_lower = str(raw).lower()

    if "malicious" in raw_lower or "high risk" in raw_lower:
        return 1.0

    # Cuckoo score — handles medium risk dan low risk sekaligus
    score_match = re.search(r'score:([\d\.]+)', raw_lower)
    if score_match:
        return min(float(score_match.group(1)) / 10.0, 1.0)

    return 0.0


def normalize_abuseipdb(raw):
    if not raw or "Error" in str(raw):
        return 0.0
    match = re.search(r'(\d+)', str(raw))
    return min(int(match.group(1)) / 100.0, 1.0) if match else 0.0


def extract_ctx_name(raw):
    if not raw:
        return None
    raw_str = str(raw).strip()
    if any(x in raw_str.lower() for x in ["not found", "error", "none", "normal", "timeout"]):
        return None
    return raw_str

def extract_vt_counts(raw) -> dict:
    """Ekstrak positives dan total dari raw VT string seperti '43/72'."""
    if not raw or any(x in str(raw) for x in ["Error", "Not Found"]):
        return {"vt_positives": 0, "vt_total": 0, "vt_found": False}

    match = re.search(r'(\d+)/(\d+)', str(raw))
    if match:
        positives = int(match.group(1))
        total     = int(match.group(2))
        return {
            "vt_positives": positives,
            "vt_total"    : total,
            "vt_found"    : positives > 0,
            "vt_ratio"    : f"{positives}/{total}"  # ← field ini yang muncul di dashboard
        }
    return {"vt_positives": 0, "vt_total": 0, "vt_found": False, "vt_ratio": "0/0"}


# ── STATUS HELPERS ──────────────────────────────────────────

def classify_hash(score: float) -> tuple[str, str]:
    if score >= HASH_THRESHOLD_MALICIOUS:
        return "MALICIOUS", "high"
    return "NORMAL", "low"


def classify_ip(score: float) -> tuple[str, str]:

    if score >= IP_THRESHOLD_MALICIOUS:
        return "MALICIOUS", "high"
    return "NORMAL", "low"
```

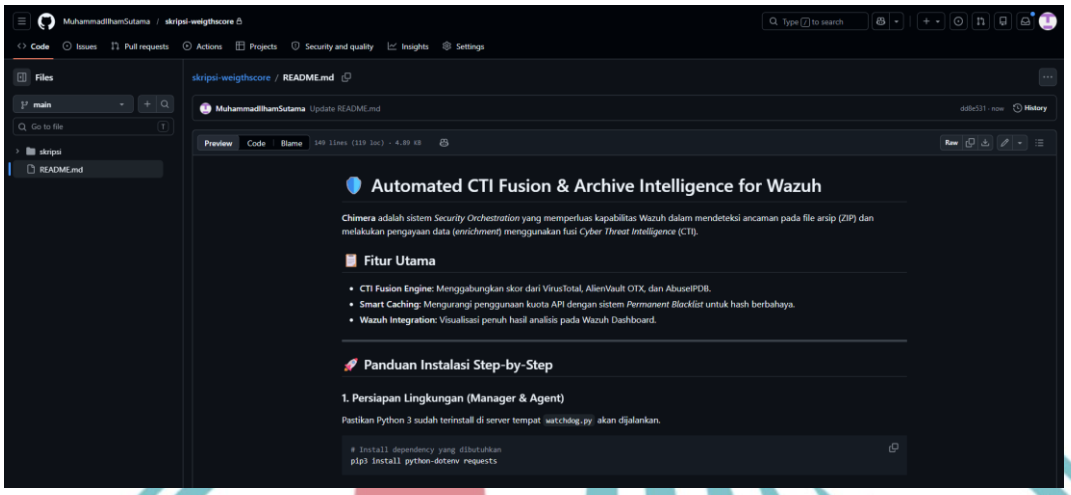
(Lanjutan)

```python
# ── SCORING HELPERS ──────────────────────────────────────────────

def _score_hash(file_hash: str) -> tuple[float, str, str, dict]:

    raw_h_vt  = check_virustotal(file_hash, "hash")
    raw_h_ctx = check_ctx(file_hash, "hash")
    raw_h_otx = check_otx(file_hash, "hash")
    ctx_name  = extract_ctx_name(raw_h_ctx)

    s_h_vt  = normalize_vt(raw_h_vt)
    s_h_ctx = normalize_ctx(raw_h_ctx)
    s_h_otx = normalize_otx(raw_h_otx)

    vt_counts = extract_vt_counts(raw_h_vt)

    # Rumus fusi 3 sumber
    hash_score       = (s_h_vt * W_HASH_VT) + (s_h_ctx * W_HASH_CTX) + (s_h_otx * W_HASH_OTX)
    status, severity = classify_hash(hash_score)

    detail = {
        "vt_positives"  : vt_counts["vt_positives"],   # ← 48
        "vt_total"      : vt_counts["vt_total"],        # ← 72
        "vt_ratio"      : vt_counts.get("vt_ratio", "0/0"),  # ← "48/72"
        "vt_found"      : vt_counts["vt_found"],        # ← True
        "vt_hash_norm" : round(s_h_vt, 4),
        "ctx_hash_norm": round(s_h_ctx, 4),
        "otx_severity" : str(raw_h_otx),
        "ctx_name"     : ctx_name,
        "hash_score"   : round(hash_score, 4),
        "hash_status"  : status,
        "hash_severity": severity,
    }
    return hash_score, status, severity, detail


def _score_ip(src_ip: str) -> tuple[float, str, str, dict]:
    raw_i_abuse = check_abuseipdb(src_ip, "ip")

    s_i_abuse = normalize_abuseipdb(raw_i_abuse)

    ip_score = (
        s_i_abuse * W_IP_ABUSE
    )
    status, severity = classify_ip(ip_score)

    detail = {
        "abuseipdb_norm": round(s_i_abuse, 4),
        "ip_score"      : round(ip_score, 4),
        "ip_status"     : status,
        "ip_severity"   : severity,
    }
    return ip_score, status, severity, detail


# ── CORE ENGINE ──────────────────────────────────────────────────

def get_threat_analysis(file_hash: str, src_ip: str, dest_ip: str,
                        file_path: str, source: str) -> dict:
    cache_key  = f"{source}_{file_hash}_{src_ip}"

    with locks_manager_lock:
        if cache_key not in analysis_locks:
            analysis_locks[cache_key] = threading.Lock()
        item_lock = analysis_locks[cache_key]

    with item_lock:

        with cache_io_lock:
            cache_data = load_cache()

        # ── CEK CACHE ──────────────────────────────────────────────
        if cache_key in cache_data:
            entry  = cache_data[cache_key]
            status = entry['data']['scores']['status']
            if status == "MALICIOUS":
                # MALICIOUS selalu fresh — tidak perlu re-query
                entry['data']['timestamp'] = datetime.now().isoformat()
                return entry['data']
            cached_time = datetime.fromisoformat(entry['cache_timestamp'])
            if datetime.now() - cached_time < timedelta(hours=CACHE_EXPIRY_HOURS):
                entry['data']['timestamp'] = datetime.now().isoformat()
                return entry['data']
```

(Lanjutan)

```
    # ── SCORING PER SOURCE ──────────────────────────────────────────
        if source == "fim":
            hash_score, status, severity, hash_detail = _score_hash(file_hash)

            final_score   = hash_score
            score_details = {
                "source": "fim",
                **hash_detail,
            }

        elif source == "suricata":
            ip_score, status, severity, ip_detail = _score_ip(src_ip)

            final_score   = ip_score
            score_details = {
                "source"  : "suricata",
                "analyzed": "src_ip",
                **ip_detail,
            }

        else:
            raise ValueError(f"Unknown source: {source}")

        # ── BUILD RESULT ────────────────────────────────────────────
        result = {
            "timestamp": datetime.now().isoformat(),
            "target": {
                "file_hash": file_hash,
                "filename" : os.path.basename(file_path) if file_path else "unknown",
                "path"     : file_path,
                "src_ip"   : src_ip,
                "dst_ip"   : dest_ip,
            },
            "scores": {
                "final_score": round(final_score, 4),
                "status"     : status,
                "severity"   : severity,
            },
            "details": score_details,
        }

        with cache_io_lock:
            current_cache = load_cache()
            current_cache[cache_key] = {
                "cache_timestamp": datetime.now().isoformat(),
                "data"           : result,
            }
            save_cache(current_cache)

        return result


if __name__ == "__main__":
    pass
```

(Lanjutan)



(dokumentasi lengkap dapat dilihat pada link berikut :
https://github.com/MuhammadIlhamSutama)