THREAT INTELLIGENCE DASHBOARD *WEBSITE* UNTUK ANALISIS *WEBSITE* OPD PEMERINTAH PROVINSI SULAWESI UTARA

Sydney Tesalonika, Sondy Campvid Kumajas*, Quido Conferti Kainde
Teknik Informatika, Fakultas Teknik, Universitas Negeri Manado
sondykumajas@unima.ac.id

ABSTRAK

Magang di Dinas Komunikasi, Informatika, Persandian dan Statistik Daerah Provinsi Sulawesi Utara (DKIPSD) mengungkap permasalahan dalam pemantauan keamanan siber pada *website* Organisasi Perangkat Daerah (OPD). Proses pengecekan ancaman seperti malware, phishing, dan virus yang dilakukan secara manual terbukti tidak efisien dan memperlambat respons terhadap potensi serangan. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sebuah *Threat Intelligence* Dashboard berbasis web sebagai solusi pemantauan terpusat. Metode yang digunakan meliputi integrasi beberapa API *threat intelligence* seperti VirusTotal, PhishTank, URLhaus, dan Google Safe Browsing untuk analisis IP, domain, dan URL, serta pengembangan sistem menggunakan Node.js, React.js, dan MongoDB. Hasil penelitian menunjukkan bahwa dashboard yang dibangun mampu menyederhanakan proses analisis ancaman, menampilkan tingkat risiko secara terintegrasi, serta meningkatkan efisiensi dalam proses monitoring keamanan *website* OPD. Sistem ini membantu pegawai DKIPSD untuk melakukan identifikasi dan mitigasi ancaman siber secara lebih cepat dan akurat.

***Kata kunci** : Magang, DKIPSD, keamanan siber, threat intelligence, website OPD*

1. PENDAHULUAN

Bentuk Kegiatan Pembelajaran (BKP) Magang atau Praktik Kerja merupakan program esensial yang dirancang untuk memberikan kesempatan kepada mahasiswa untuk mendapatkan pengalaman kerja nyata di lingkungan profesional [1]. Melalui kegiatan ini, mahasiswa dapat belajar, meningkatkan, dan menerapkan ilmu pengetahuan serta keterampilan yang telah diperoleh dari Lembaga Pendidikan/Universitas dalam konteks praktis [2]. Selama periode magang, mahasiswa akan dibimbing oleh pembimbing lapangan yang bertanggung jawab dalam memberikan arahan, tugas, dan dukungan, memastikan pengalaman belajar yang optimal dalam batas waktu yang ditentukan. Kegiatan magang juga seringkali melibatkan pengerjaan proyek spesifik yang relevan dengan bidang studi mahasiswa, menjadi sarana konkret untuk mengasah dan mengembangkan *soft skill* maupun *hard skill* yang dibutuhkan di dunia kerja [3].

Dalam pelaksanaannya, penulis melakukan kegiatan magang di Dinas Komunikasi, Informatika, Persandian dan Statistik Daerah Provinsi Sulawesi Utara (DKIPSD). Seiring dengan pesatnya digitalisasi layanan publik, *website* Organisasi Perangkat Daerah (OPD) menjadi komponen penting sebagai media informasi dan layanan kepada masyarakat. Namun, semakin banyaknya *website* OPD juga meningkatkan risiko terhadap ancaman siber seperti *malware*, *phishing* dan serangan berbasis web lainnya.

Permasalahan yang dihadapi adalah proses pemantauan keamanan *website* yang masih dilakukan secara manual, sehingga membutuhkan waktu yang lama, rentan terhadap kesalahan, dan tidak mampu memberikan respons yang cepat terhadap ancaman yang muncul. Hal ini berdampak pada rendahnya efektivitas dalam pengelolaan keamanan siber di lingkungan DKIPSD.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk merancang dan mengimplementasikan sebuah *Threat intelligence Dashboard* berbasis web yang mampu memusatkan proses analisis ancaman terhadap *IP*, *domain*, dan *URL website* OPD.

Solusi yang ditawarkan adalah pengembangan sistem *dashboard* dengan menggabungkan beberapa API *threat intelligence* seperti VirusTotal, PhishTank, URLhaus dan Google Safe Browsing. *Dashboard* ini diharapkan dapat memberikan informasi tingkat risiko secara *real-time* dan terintegrasi sehingga membantu dalam meningkatkan efisiensi dan efektivitas pemantauan keamanan *website* OPD di lingkungan Pemerintah Provinsi Sulawesi Utara.

2. TINJAUAN PUSTAKA

Sebelum melakukan penelitian ini, penulis terlebih dahulu melakukan studi literatur dengan menelusuri berbagai referensi yang relevan, baik berupa jurnal ilmiah, prosiding, maupun sumber lainnya yang berkaitan dengan keamanan siber, *threat intelligence*, serta sistem monitoring berbasis web. Studi literatur ini bertujuan untuk memahami konsep dasar yang digunakan dalam penelitian serta mengidentifikasi penelitian terdahulu yang memiliki keterkaitan dengan pengembangan sistem analisis ancaman pada *website*, khususnya dalam konteks instansi pemerintahan.

Penelitian yang dilakukan oleh Dalimunthe dan Azhari membahas analisis forensik digital terhadap perdagangan data pribadi di *dark web* dengan menggunakan pendekatan *Open Source Intelligence (OSINT)* dan *threat intelligence*. Hasil penelitian menunjukkan bahwa kombinasi kedua metode tersebut

mampu secara efektif mendeteksi serta menganalisis aktivitas kebocoran data, termasuk identifikasi pola distribusi dan validasi data yang diperjualbelikan [4]. Penelitian ini memberikan gambaran bahwa pemanfaatan *threat intelligence* dapat digunakan sebagai dasar dalam memahami ancaman siber secara lebih komprehensif. Namun, penelitian tersebut lebih berfokus pada analisis forensik dan belum mengimplementasikan sistem monitoring dalam bentuk dashboard yang dapat digunakan secara langsung oleh pengguna.

Penelitian lain yang dilakukan oleh Hidayat dkk. mengenai optimasi deteksi malware menggunakan SIEM Wazuh dengan integrasi *cyber threat intelligence* melalui MISP dan DFIR-IRIS menunjukkan bahwa integrasi *threat intelligence* mampu meningkatkan presisi deteksi ancaman secara signifikan. Sistem yang dikembangkan tidak hanya mampu mendeteksi serangan, tetapi juga mendukung respons insiden secara *real-time* [5]. Meskipun demikian, penelitian ini lebih berfokus pada peningkatan performa deteksi *malware* dalam lingkungan SIEM dan belum mengarah pada visualisasi data dalam bentuk *dashboard* terintegrasi yang sederhana dan mudah digunakan oleh instansi pemerintah.

Selanjutnya, penelitian oleh Pratama mengenai perancangan sistem deteksi dini keamanan informasi di lingkungan DISKOMINFO Kabupaten Bandung menunjukkan bahwa penggunaan SIEM berbasis Wazuh dapat membantu dalam melakukan monitoring serangan secara *real-time* melalui pengumpulan dan analisis log dari berbagai sistem [6]. Sistem ini mampu memberikan peringatan dini terhadap potensi ancaman, sehingga meningkatkan kesiapsiagaan dalam menghadapi serangan siber. Namun, penelitian tersebut masih berfokus pada implementasi SIEM sebagai sistem *backend* dan belum mengintegrasikan berbagai sumber *threat intelligence* eksternal untuk memperkaya analisis ancaman.

Penelitian yang dilakukan oleh Nugroho dan Suharjo mengembangkan sistem monitoring trafik web secara *real-time* dengan fitur deteksi anomali menggunakan pendekatan *lightweight* berbasis Node.js dan WebSocket. Hasil penelitian menunjukkan bahwa sistem mampu mendeteksi anomali seperti lonjakan trafik dan *error rate* dengan akurasi tinggi serta memberikan notifikasi secara cepat kepada administrator [7]. Penelitian ini menekankan pentingnya sistem *monitoring real-time* dalam menjaga keamanan dan stabilitas aplikasi web, namun belum memanfaatkan data *threat intelligence* eksternal untuk memberikan konteks ancaman yang lebih luas.

Selain itu, penelitian oleh Susanto dkk. mengenai *website threat* monitoring menunjukkan bahwa sistem monitoring dapat digunakan untuk mendeteksi dan menampilkan hasil serangan terhadap web server melalui teknik penetration testing. Sistem ini mampu memberikan informasi terkait jenis serangan, waktu deteksi, serta tools yang digunakan oleh penyerang [8]. Walaupun demikian, penelitian tersebut masih terbatas pada hasil pengujian serangan dan belum mengintegrasikan berbagai sumber data ancaman secara otomatis untuk analisis yang lebih komprehensif.

Berdasarkan beberapa penelitian terdahulu tersebut, dapat disimpulkan bahwa telah banyak upaya yang dilakukan dalam bidang keamanan siber, baik dari sisi deteksi ancaman, monitoring sistem, maupun analisis data. Namun, sebagian besar penelitian masih berfokus pada aspek tertentu, seperti deteksi *malware*, analisis forensik, atau monitoring trafik secara terpisah. Oleh karena itu, pada penelitian ini penulis mengembangkan sebuah *Threat intelligence* Dashboard *Website* yang mengintegrasikan berbagai sumber *threat intelligence* ke dalam satu platform terpusat. Sistem ini dirancang untuk mempermudah proses analisis ancaman pada *website* OPD dengan menyajikan informasi secara visual, *real-time*, dan komprehensif, sehingga diharapkan mampu meningkatkan efisiensi serta efektivitas dalam proses monitoring dan mitigasi ancaman siber di lingkungan Pemerintah Provinsi Sulawesi Utara.

2.1. *Cyber Security*

Keamanan siber (*cyber security*) merujuk pada serangkaian upaya dan praktik yang dirancang untuk melindungi sistem komputasi, perangkat lunak, dan data dari segala bentuk ancaman, termasuk akses, pengungkapan, transfer, modifikasi, atau penghancuran yang tidak sah, baik yang diakibatkan oleh insiden yang tidak disengaja maupun tindakan jahat yang disengaja [9].

2.2. *Threat intelligence*

Intelijen Ancaman (*threat intelligence*/TI) adalah pengetahuan berbasis bukti, termasuk konteks, mekanisme, indikator, implikasi, dan saran tindakan, mengenai ancaman atau potensi bahaya yang ada atau muncul terhadap aset organisasi [10]. Dalam konteks *cyber security*, *TI* bertujuan untuk mengubah data mentah (seperti *log, IP, URL*) menjadi wawasan yang dapat ditindaklanjuti untuk pertahanan proaktif.

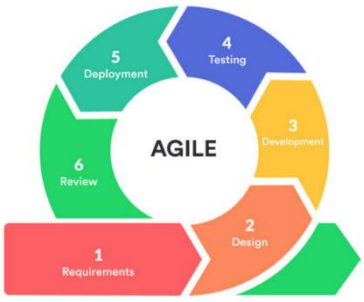
2.3. Deteksi Anomali

Deteksi anomali adalah proses mengidentifikasi pola atau titik data yang tidak sesuai dengan perilaku yang diharapkan atau pola normal dalam suatu dataset [11]. Dalam keamanan siber, anomali sering kali merupakan indikasi serangan *cyber*, *malware,* atau penyalahgunaan sistem [12].

Oleh karena itu, deteksi anomali menjadi sangat penting untuk mengamankan sistem dari ancaman-ancaman tersebut. Metode prediksi berbasis model, seperti *Isolation Forest* atau *Gaussian Mixture Models,* bekerja dengan membangun representasi dari data normal, kemudian menandai setiap penyimpangan yang signifikan dari model tersebut sebagai anomali yang potensial [13].

3. METODE PENELITIAN

Metode pengembangan sistem yang diterapkan dalam pelaksanaan proyek *Threat intelligence Dashboard* ini adalah Metode *Agile*, dengan fokus pada pendekatan Iteratif dan Inkremental. Metode ini dipilih karena sifat proyek pengembangan yang dinamis, di mana kebutuhan dapat berkembang, dan umpan balik berkelanjutan sangat penting untuk menghasilkan solusi yang relevan dan efektif. Pendekatan *Agile* memungkinkan fleksibilitas tinggi untuk mengintegrasikan perubahan dan perbaikan di setiap siklus pengembangan [14].

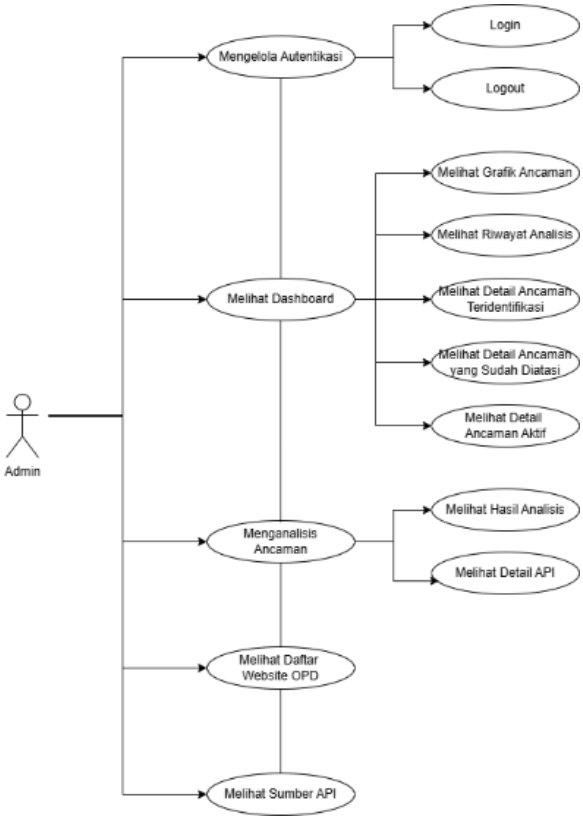


Gambar 1. Metode *Agile*

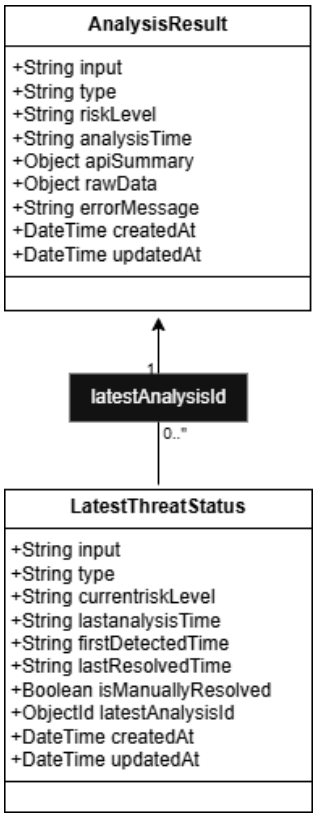
Dalam setiap iterasi pengembangan, proyek ini melalui serangkaian tahapan yang berulang dan saling terkait. Dimulai dengan fase *Requirement* untuk mengidentifikasi dan memprioritaskan kebutuhan fungsionalitas. Selanjutnya, fase *Design* dilakukan untuk merencanakan implementasi teknis dan visual. Fitur-fitur kemudian dibangun pada fase *Development*, diikuti dengan *Testing* secara berkelanjutan untuk memastikan fungsionalitas yang benar. Setelah berhasil diuji, fase *Deployment* dilakukan untuk menyebarkan aplikasi versi terbaru. Setiap siklus diakhiri dengan *Review* bersama stakeholder untuk mendapatkan umpan balik, memastikan produk yang dihasilkan sesuai kebutuhan, dan mempersiapkan iterasi berikutnya. Siklus berulang ini memastikan adaptasi cepat terhadap perubahan dan peningkatan kualitas sistem secara bertahap.

UCD menggambarkan interaksi antara aktor (admin) dengan sistem *Threat Intelligence Dashboard.* Admin memiliki akses untuk melakukan login, melakukan analisis terhadap IP/domain/URL, melihat hasil analisis, serta mengakses riwayat ancaman. Diagram ini menunjukkan bahwa seluruh fungsi sistem berpusat pada admin sebagai pengguna utama yang mengelola proses monitoring keamanan *website* OPD.

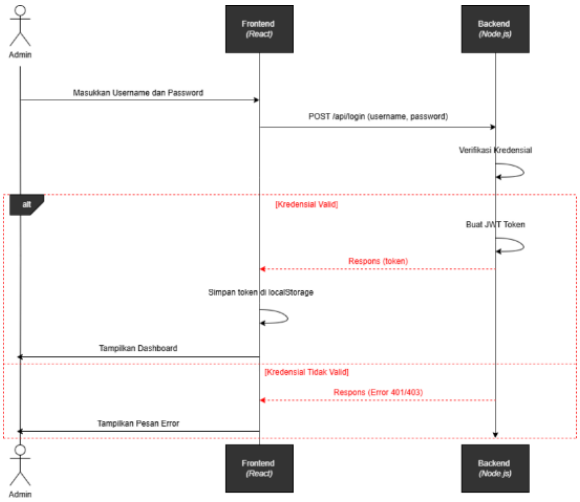
Class Diagram menunjukkan struktur data yang digunakan dalam sistem, khususnya relasi antar model seperti *AnalysisResult* dan *LatestThreatStatus*. Setiap data hasil analisis disimpan dalam *database* MongoDB dan memiliki atribut seperti input, tipe analisis, hasil *API*, serta tingkat risiko. Diagram ini menggambarkan bagaimana data dikelola dan disimpan secara terstruktur untuk mendukung proses analisis dan visualisasi.



Gambar 2. *Use Case Diagram*

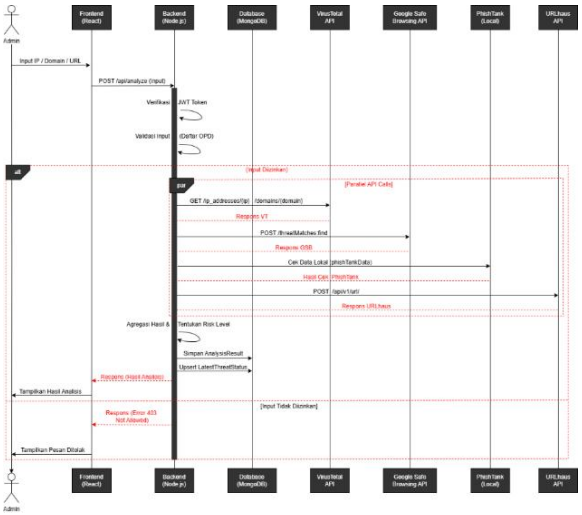


Gambar 3. *Class Diagram*



Gambar 4. *Sequence Diagram (Login Flow)*

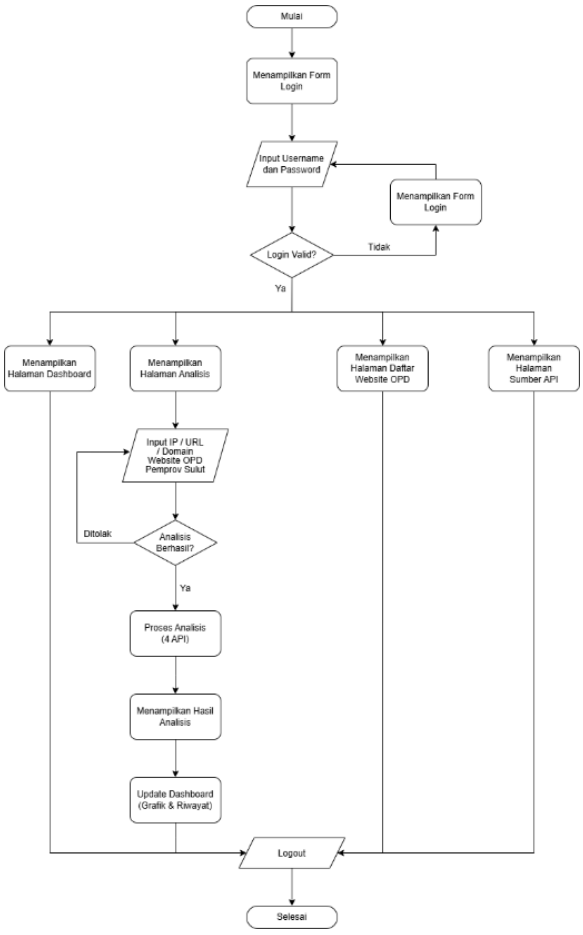
Sequence Diagram ini menggambarkan alur proses autentikasi pengguna. Proses dimulai dari input *username* dan *password* oleh admin, kemudian dikirim ke server untuk diverifikasi. Jika data valid, sistem akan memberikan akses ke *dashboard*, sedangkan jika tidak valid, sistem akan menolak akses.



Gambar 5. *Sequence Diagram (Threat Analysis Flow)*

Diagram ini menggambarkan alur proses autentikasi pengguna. Proses dimulai dari input *username* dan *password* oleh admin, kemudian dikirim ke server untuk diverifikasi. Jika data valid, sistem akan memberikan akses ke *dashboard*, sedangkan jika tidak valid, sistem akan menolak akses.

Gambar 6 menunjukkan *flowchart* sistem yang menggambarkan alur kerja aplikasi secara keseluruhan, dimulai dari *login*, input data analisis, proses pengambilan data dari *API*, pengolahan hasil, hingga penampilan hasil analisis. *Flowchart* ini menunjukkan bahwa sistem bekerja secara tersuktur dan terintegrasi dalam memproses data ancaman.

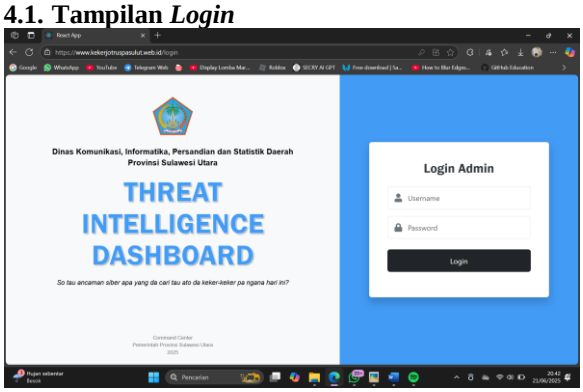


Gambar 6. *Flowchart System*

4. HASIL DAN PEMBAHASAN

Threat intelligence dashboard telah berhasil diimplementasikan sebagai platform terpusat berbasis web yang memungkinkan pegawai Dinas Komunikasi, Informatika, Persandian dan Statistik Daerah Provinsi Sulawesi Utara untuk menganalisis potensi ancaman pada IP, domain, dan URL *website* Organisasi Perangkat Daerah (OPD) secara efisien. Berikut adalah hasil tampilan *website*nya :

4.1. Tampilan *Login*

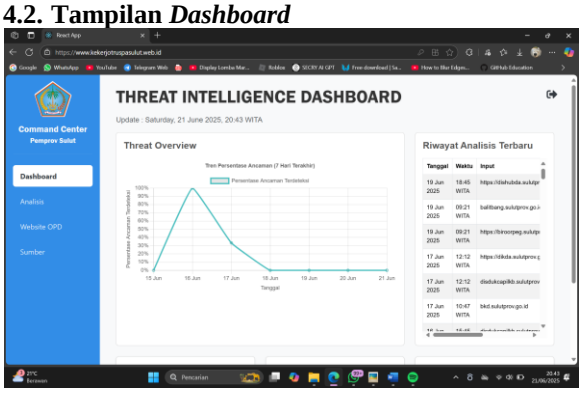


Gambar 7. Tampilan Login

Website hanya bisa diakses oleh admin dari Dinas Komunikasi, Informatika, Persandian dan Statistik

Daerah Provinsi Sulawesi Utara dengan memasukkan *username* dan *password* untuk login mengakses *dashboard.*

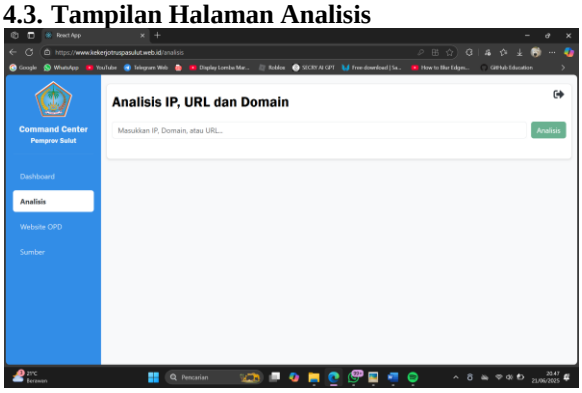
4.2. Tampilan *Dashboard*



Gambar 8. Tampilan Dashboard

Dashboard ini menampilkan grafik garis untuk melihat persentase ancaman yang dianalisis dalam seminggu, riwayat analisis terbaru menampilkan hasil riwayat analisis yang diinput admin dengan menampilkan hasil tanggal, waktu, input dan tingkat resikonya.

4.3. Tampilan Halaman Analisis



Gambar 9. Tampilan Halaman Analisis

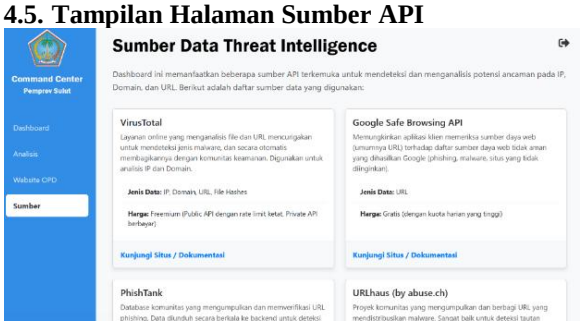
Halaman analisis menampilkan input bar untuk menganalisis *IP*, *URL* atau *domain* pada *website* OPD Pemerintah Provinsi Sulawesi Utara.

4.4. Tampilan Hasil Analisis Berhasil

Ketika admin menginput *website* OPD dari Pemerintah Provinsi Sulawesi Utara, *dashboard* akan menganalisis input tersebut apakah berbahaya atau tidak, bisa dilihat dari tingkat resikonya yang berasal dari hasil gabungan ke-4 API (*Application Programming Interface) Threat intelligence* yaitu VirusTotal, Google Safe Browsing API, PhishTank dan URLhaus.

Gambar 10. Tampilan Hasil Analisis Berhasil

4.5. Tampilan Halaman Sumber API



Gambar 11. Tampilan Halaman Sumber API

Memberikan tampilan sumber data dan informasi dari 4 API *threat intelligence* yang digabungkan.

4.6. Hasil Pengujian

Pengujian sistem dilakukan menggunakan metode *Black Box Testing* yang berfokus pada pengujian fungsionalitas sistem berdasarkan input dan output tanpa melihat struktur internal kode program. Pengujian ini dilakukan dengan melibatkan pengguna langsung dari pihak Dinas Komunikasi, Informatika, Persandian dan Statistik Daerah Provinsi Sulawesi Utara (DKIPSD). Berdasarkan hasil pengujian yang dilakukan, seluruh fitur utama sistem berjalan dengan baik dan sesuai dengan yang diharapkan, sehingga sistem dinyatakan layak untuk digunakan dalam proses monitoring keamanan *website* OPD.

Tabel 1. Hasil Pengujian Black Box Testing

Metode Pengujian	Skenario Utama	Hasil yang Diharapkan	Status
Autentikasi *(Login)*	Admin memasukkan *username* dan *password* yang valid	Sistem berhasil melakukan autentikasi dan mengarahkan ke halaman *dashboard*	Valid
Autentikasi *(Login)*	Admin memasukkan *username* atau *password* yang salah	Sistem menolak *login* dan menampilkan pesan *error*	Valid
Dashboard	Admin mengakses halaman dashboard setelah login	Sistem menampilkan data ringkasan analisis, grafik, dan riwayat ancaman	Valid
Analisis *Threat*	Admin memasukkan input *berupa IP, domain,* atau *URL website* OPD	Sistem memproses input dan mengirim request ke *API threat intelligence*	Valid
Analisis *Threat*	Admin memasukkan input yang bukan *website* OPD	Sistem menolak analisis dan menampilkan notifikasi pembatasan input	Valid

Metode Pengujian	Skenario Utama	Hasil yang Diharapkan	Status
Integrasi API	Sistem mengambil data dari VirusTotal, PhishTank, URLhaus, dan Google Safe Browsing	Sistem berhasil menerima dan menggabungkan hasil analisis dari seluruh *API*	Valid
Hasil Analisis	Sistem menampilkan hasil analisis tingkat risiko (*Low, Medium, High*)	Sistem menampilkan hasil secara akurat dan terintegrasi dalam *dashboard*	Valid
Riwayat Analisis	Admin melihat data riwayat analisis	Sistem menampilkan data analisis sebelumnya (tanggal, waktu, input, risiko)	Valid
Manajemen Data	Sistem menyimpan hasil analisis ke *database* MongoDB	Data tersimpan dengan benar dan dapat ditampilkan kembali	Valid
Navigasi Sistem	Admin berpindah antar halaman (*Dashboard*, Analisis, Daftar *Website*, *API*)	Sistem menampilkan halaman sesuai menu yang dipilih tanpa *error*	Valid

5. KESIMPULAN

Implementasi *Threat intelligence Dashboard* ini secara efektif mengatasi inefisiensi pemantauan ancaman manual pada *website* OPD, menyediakan platform terpusat dan otomatis. Integrasi empat *API Threat intelligence* (VirusTotal, Google Safe Browsing, PhishTank, dan URLhaus) memungkinkan penentuan tingkat risiko yang komprehensif (*Low, Medium, High*) melalui agregasi hasil paralel. Validasi input yang hanya mengizinkan *website* OPD Pemerintah Provinsi Sulawesi Utara memastikan fokus dan relevansi sistem. Meskipun *dashboard* ini meningkatkan kewaspadaan siber instansi secara signifikan, terdapat keterbatasan seperti limitasi analisis harian dari API gratis (VirusTotal 500x, lainnya hingga 1.000x).

Melanjutkan pengembangan dashboard dengan fitur lanjutan (misal: notifikasi, API berbayar) dan menunjuk penanggung jawab internal untuk pemeliharaan serta pelatihan staf.

DAFTAR PUSTAKA

[1] D. Aswita, "Merdeka Belajar Kampus Merdeka (MBKM): Inventarisasi Mitra dalam Pelaksanaan Magang Mahasiswa Fakultas Keguruan dan Ilmu Pendidikan," *Prosiding Seminar Nasional Biotik*, vol. 9, pp. 201–206, Jun. 2022, doi: https://doi.org/10.22373/pbio.v9i2.11747.

[2] Y. N. Adilah, J. Julia, and D. A. Karlina, "Keselarasan Pengalaman Magang Mahasiswa PGSD dengan Pengembangan Kompetensi Pedagogik: Perspektif Mahasiswa Program Magang," *Pedagogika: Jurnal Pedagogik dan Dinamika Pendidikan*, vol. 13, no. 1, pp. 108–119, Apr. 2025, doi: https://doi.org/10.30598/pedagogikavol13issue1page108-119.

[3] S. S. Kusumawardani *et al.*, *Buku Panduan Merdeka Belajar - Kampus Merdeka*, 2nd ed. Jakarta: Direktorat Jenderal Pendidikan Tinggi, Riset, dan Teknologi, 2024. Accessed: Jun. 24, 2025. [Online]. Available: https://kemdiktisaintek.go.id/epustaka/buku-panduan-merdeka-belajar-kampus-merdeka-mbkm-2024/

[4] A. A. Q. A. Dalimunthe and M. Azhari, "Analisis Forensik Digital Terhadap Perdagangan Data Pribadi Di Dark Web Menggunakan OSINT & *Threat intelligence*," *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, vol. 4, no. 1, pp. 254–269, Jun. 2025, doi: 10.62712/juktisi.v4i1.400.

[5] 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," *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, vol. 13, no. 1, Jan. 2025, doi: 10.23960/jitet.v13i1.5686.

[6] N. F. Pratama, "Perancangan Sistem Deteksi Dini Keamanan Informasi DISKOMINFO Kabupaten Bandung," *Jurnal Teknik Informatika dan Sistem Informatika*, vol. 10, no. 1, p. 808, Mar. 2023, [Online]. Available: http://jurnal.mdp.ac.id

[7] F. P. Nugroho and I. Suharjo, "Sistem Monitoring Real-Time dengan Deteksi Anomali untuk Keamanan Aplikasi Web," *JEKIN - Jurnal Teknik Informatika*, vol. 6, no. 1, pp. 37–51, 2026, doi: 10.58794/jekin.v6i1.1913.

[8] M. F. Susanto, A. Nurcahyo, and M. Rahayu, "*Website* Threat Monitoring Untuk Pemantauan dan Analisis Ancaman pada Web Server," *Prosiding Industrial Research Workshop and National Seminar*, vol. 13, pp. 13–14, Jul. 2022, doi: https://doi.org/10.35313/irwns.v13i01.4213.

[9] A. R. Nisa, A. D. Wijayanto, and A. P. J. P. S. Setiawan, "Analisis Log Server untuk mendeteksi Serang DDoS pada Keamanan Jaringan di *Website*," *Journal of Internet and Software Engineering*, vol. 1, no. 3, pp. 1–17, Jun. 2024, doi: 10.47134/pjise.v1i3.2612.

[10] A. M. Aljuhami and D. M. Bamasoud, "*Cyber Threat intelligence* in Risk Management A Survey of the Impact of *Cyber Threat intelligence* on Saudi Higher Education Risk Management," *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 12, no. 10, pp. 156–164, 2021, doi: 10.14569/IJACSA.2021.0121018.

[11] J. Wang and X. Li, "Abnormal Electricity Detection of Users Based on Improved Canopy-Kmeans and Isolation Forest Algorithms," *IEEE*

Access, vol. 12, pp. 99110–99121, Jul. 2024, doi: 10.1109/ACCESS.2024.3429304.

[12] D. Firdaus, Fahira, and R. Rianti, "Deteksi Anomali dan Serangan Low Rate DDOS dalam Lalu Lintas Jaringan Menggunakan Naive Bayes," *NARATIF : Jurnal Nasional Riset, Aplikasi dan Teknik Informatika*, vol. 5, no. 2, pp. 140–148, Dec. 2023, doi: 10.53580/naratif.v5i2.208.

[13] A. Ragil Saputro and V. Atina, "Identifikasi Anomali Keamanan Server Nginx menggunakan Algoritma Isolation Forest," *Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 2, 2025, [Online]. Available: https://example.com

[14] Suhari, A. Faqih, and F. M. Basysyar, "Sistem Informasi Kepegawaian Mengunakan Metode Agile Development di CV. Angkasa Raya," *Jurnal Teknologi dan Informasi (JATI)*, vol. 12, pp. 30–45, Mar. 2022, doi: 10.34010/jati.v12i1