Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 2 (2026) pp: 26739-26744
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Rancang Bangun Sistem Monitoring Isu Siber Otomatis Berbasis Data Feeding Telegram

Vernanda Iqbal[1], Rizky Santoso[2]
[12]Program Studi Teknik Informatika, Universitas Pamulang
iqbalvernanda3@gmqail.com, rizkysantoso2005@gmail.com

Abstrak

Perkembangan ancaman siber yang semakin kompleks menuntut tersedianya sistem monitoring yang mampu menghimpun, mengelola, dan menyajikan informasi secara cepat serta akurat. Telegram banyak dimanfaatkan oleh komunitas keamanan siber untuk menyebarkan informasi mengenai kerentanan, malware, kebocoran data, phishing, dan berbagai insiden digital. Namun, pemantauan secara manual terhadap banyak kanal membutuhkan waktu, rentan terhadap keterlambatan, dan berpotensi menyebabkan informasi penting terlewatkan. Penelitian ini bertujuan merancang dan membangun Sistem Monitoring Isu Siber Otomatis Berbasis Data Feeding Telegram yang dapat mengumpulkan, menyimpan, mengklasifikasikan, serta menampilkan informasi keamanan siber melalui dashboard berbasis web. Penelitian menggunakan pendekatan pengembangan sistem dengan metode Waterfall yang mencakup analisis kebutuhan, perancangan, implementasi, pengujian, dan evaluasi. Sistem dikembangkan menggunakan Telegram API sebagai sumber data, PHP untuk pemrosesan aplikasi, MySQL sebagai basis data, serta teknologi web untuk penyajian informasi. Pengujian dilakukan menggunakan Black Box Testing guna memastikan kesesuaian fungsi autentikasi, pengambilan data, pengelolaan informasi, visualisasi, dan manajemen pengguna. Hasil penelitian menunjukkan bahwa sistem mampu mengambil data Telegram secara otomatis, menyimpannya secara terstruktur, mengelompokkan informasi berdasarkan kategori isu siber, dan menyajikan hasil monitoring dalam bentuk grafik serta tabel yang mudah dipahami. Seluruh fungsi utama berjalan sesuai kebutuhan yang ditetapkan. Sistem ini meningkatkan efektivitas dan efisiensi monitoring, mengurangi ketergantungan pada proses manual, serta membantu pengguna memperoleh informasi keamanan siber secara cepat, terpusat, dan berkelanjutan.

Kata Kunci: *Keamanan Siber, Monitoring Otomatis, Telegram API, Data Feeding, Dashboard Berbasis Web*

I. Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang semakin pesat telah memberikan berbagai kemudahan dalam pertukaran informasi.Namun, di sisi lain perkembangan tersebut juga meningkatkan risiko terjadinya ancaman siber yang dapat mengganggu keamanan data dan sistem informasi. Berbagai bentuk ancaman seperti malware, phishing, ransomware, kebocoran data,dan eksploitasi kerentanan sistem terus berkembang sehingga memerlukan proses pemantauan yang cepat dan berkelanjutan.dan eksploitasi kerentanan sistem terus berkembang sehingga memerlukan proses pemantauan yang cepat dan berkelanjutan.Telegram merupakan salah satu platform komunikasi yang banyak dimanfaatkan oleh komunitas keamanan siber untuk berbagi informasi terkait ancaman, kerentanan sistem, maupun perkembangan isu keamanan digital. Informasi yang tersebar melalui berbagai channel dan grup Telegram memiliki nilai penting sebagai sumber intelijen siber. Akan tetapi, volume informasi yang sangat besar menyebabkan proses monitoring secara manual menjadi kurang efektif karena membutuhkan waktu yang lama dan berisiko menimbulkan kesalahan dalam identifikasi informasi penting.Telegram merupakan salah satu platform komunikasi yang banyak dimanfaatkan oleh komunitas keamanan siber untuk berbagi informasi terkait ancaman, kerentanan sistem, maupun perkembangan isu keamanan digital. Informasi yang tersebar melalui berbagai channel dan grup Telegram memiliki nilai penting sebagai sumber intelijen siber. Akan tetapi, volume informasi yang sangat besar menyebabkan proses monitoring secara manual menjadi kurang efektif karena membutuhkan waktu yang lama dan berisiko menimbulkan kesalahan dalam identifikasi informasi penting.Telegram merupakan salah satu platform komunikasi yang banyak dimanfaatkan oleh komunitas keamanan siber untuk berbagi informasi terkait ancaman, kerentanan sistem, maupun perkembangan isu keamanan digital. Informasi yang tersebar melalui berbagai channel dan grup Telegram memiliki nilai penting sebagai sumber intelijen siber. Akan tetapi, volume informasi yang sangat besar menyebabkan proses monitoring secara manual menjadi kurang efektif karena membutuhkan waktu yang lama dan berisiko menimbulkan kesalahan dalam identifikasi informasi penting.proses monitoring informasi keamanan siber secara lebih efektif, efisien, dan terintegrasi sehingga mendukung kebutuhan pengguna dalam memperoleh informasi ancaman siber secara real-time.Metode Penelitian

2. Landasan Teori

A. Landasan Teori Variabel I (Data Feeding Telegram)

Data Feeding merupakan proses pengambilan, pengumpulan, dan pengiriman data dari suatu sumber ke dalam sistem secara otomatis untuk selanjutnya diproses menjadi informasi yang bermanfaat. Dalam pengembangan sistem informasi modern, data feeding digunakan untuk memperoleh data secara real-time tanpa memerlukan proses input manual yang berulang.

Telegram merupakan aplikasi pesan instan berbasis cloud yang menyediakan berbagai fitur komunikasi seperti grup, channel, dan bot. Selain digunakan sebagai media komunikasi, Telegram juga banyak dimanfaatkan sebagai sumber informasi pada berbagai bidang, termasuk keamanan siber. Melalui Telegram API, pengembang dapat mengakses data yang tersedia pada channel atau grup tertentu secara otomatis sehingga informasi yang diperoleh dapat diproses lebih lanjut oleh sistem [13].

Pemanfaatan data feeding Telegram memungkinkan proses pengumpulan informasi dilakukan secara cepat, terstruktur, dan berkelanjutan. Dengan adanya mekanisme tersebut, sistem dapat memperoleh data terbaru secara otomatis sehingga mendukung kebutuhan analisis dan monitoring informasi secara real-time

B. Landasan Teori Variabel II (Sistem Monitoring Isu Siber)

Sistem Monitoring Isu Siber merupakan sistem yang digunakan untuk melakukan pengawasan, pengumpulan, pengolahan, dan penyajian informasi yang berkaitan dengan ancaman keamanan siber. Sistem monitoring berfungsi membantu pengguna dalam mengidentifikasi, menganalisis, dan memantau perkembangan berbagai isu keamanan digital yang beredar melalui media elektronik.

Keamanan siber (Cyber Security) adalah serangkaian upaya yang dilakukan untuk melindungi sistem komputer, jaringan, perangkat lunak, dan data dari berbagai ancaman digital seperti malware, ransomware, phishing, kebocoran data, dan serangan siber lainnya. Seiring meningkatnya penggunaan teknologi informasi, kebutuhan terhadap sistem monitoring keamanan siber menjadi semakin penting untuk mendukung proses deteksi dini terhadap potensi ancaman [12].

Sistem monitoring isu siber umumnya dilengkapi dengan kemampuan pengumpulan data otomatis, penyimpanan data pada basis data, proses klasifikasi informasi, serta penyajian hasil monitoring dalam bentuk dashboard. Melalui visualisasi data yang interaktif, pengguna dapat memahami tren ancaman siber, melihat aktivitas terbaru, dan memperoleh informasi yang diperlukan untuk mendukung proses analisis maupun pengambilan keputusan secara lebih efektif [14].

3. Metode Penelitian

A. Jenis Penelitian

Penelitian ini menggunakan jenis penelitian terapan (Applied Research) dengan pendekatan pengembangan sistem (Research and Development). Penelitian dilakukan untuk merancang dan membangun Sistem Monitoring Isu Siber Otomatis Berbasis Data Feeding Telegram yang dapat digunakan sebagai sarana pengumpulan dan monitoring informasi keamanan siber secara otomatis.

B. Pendekatan Penelitian

Pendekatan yang digunakan dalam penelitian ini adalah pendekatan kualitatif dan kuantitatif. Pendekatan kualitatif digunakan untuk menganalisis kebutuhan sistem melalui observasi dan studi literatur, sedangkan pendekatan kuantitatif digunakan untuk mengukur hasil pengujian sistem berdasarkan fungsi-fungsi yang telah dirancang.

C. Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh data informasi keamanan siber yang diperoleh dari channel dan grup Telegram yang digunakan sebagai sumber monitoring.

Sampel penelitian berupa data pesan Telegram yang mengandung informasi terkait ancaman siber, kerentanan sistem, malware, kebocoran data, dan informasi keamanan digital lainnya yang berhasil dikumpulkan oleh sistem selama proses pengujian.

D. Teknik Sampling

Teknik sampling yang digunakan adalah Purposive Sampling, yaitu pengambilan sampel berdasarkan kriteria tertentu. Kriteria yang digunakan adalah pesan Telegram yang memiliki keterkaitan dengan isu keamanan siber dan berasal dari sumber yang telah ditentukan sebagai objek monitoring.

E. Waktu dan Tempat Penelitian

Penelitian dilaksanakan pada periode April 2026 sampai Juni 2026 di lingkungan Kementerian Pertahanan Cyber Security sebagai lokasi pelaksanaan Kerja Praktik. Kegiatan penelitian meliputi observasi, analisis kebutuhan, perancangan sistem, implementasi, pengujian, hingga penyusunan laporan.

F. Instrumen Penelitian

Instrumen yang digunakan dalam penelitian ini meliputi:

1. Perangkat keras berupa komputer atau laptop yang digunakan untuk pengembangan dan pengujian sistem.
2. Perangkat lunak berupa sistem operasi, XAMPP, PHP, MySQL, Telegram API, dan web browser.

DOI: https://doi.org/10.31004/riggs.v5i2.12535

3. Dokumen observasi dan hasil wawancara sebagai sumber informasi kebutuhan sistem.
4. Data pesan Telegram yang digunakan sebagai objek pengujian sistem monitoring.

G. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini meliputi:

1. Observasi, yaitu melakukan pengamatan langsung terhadap proses monitoring informasi keamanan siber dan kebutuhan sistem.
2. Wawancara, yaitu melakukan diskusi dengan pembimbing lapangan dan pihak terkait untuk memperoleh informasi mengenai kebutuhan sistem.
3. Studi Pustaka, yaitu mempelajari buku, jurnal, artikel ilmiah, dan dokumentasi resmi yang berkaitan dengan keamanan siber, Telegram API, database, dan pengembangan sistem informasi.

H. Teknik Analisis Data

Teknik analisis data dilakukan dengan menganalisis kebutuhan sistem berdasarkan hasil observasi, wawancara, dan studi pustaka. Selanjutnya sistem dikembangkan menggunakan metode Waterfall yang terdiri dari tahapan analisis kebutuhan, perancangan sistem, implementasi, pengujian, dan evaluasi.

Pengujian sistem dilakukan menggunakan metode Black Box Testing untuk memastikan seluruh fungsi sistem berjalan sesuai dengan kebutuhan yang telah ditetapkan. Hasil pengujian kemudian dianalisis untuk mengetahui tingkat keberhasilan sistem dalam melakukan pengambilan data, penyimpanan data, klasifikasi informasi, dan penyajian informasi monitoring melalui dashboard berbasis web.

4. Hasil Dan Pembahasan

I. Hasil Implementasi Sistem

Pada tahap implementasi, Sistem Monitoring Isu Siber Otomatis berhasil dikembangkan dengan memanfaatkan Telegram API sebagai sumber data utama, MySQL sebagai media penyimpanan data, serta PHP sebagai bahasa pemrograman untuk membangun aplikasi berbasis web. Sistem mampu melakukan proses pengambilan data secara otomatis dari channel Telegram yang telah ditentukan, kemudian menyimpan dan mengelola data tersebut ke dalam basis data secara terstruktur. Selain itu, sistem juga menyediakan dashboard monitoring yang dapat menampilkan informasi secara real-time sehingga memudahkan pengguna dalam melakukan pemantauan terhadap perkembangan isu keamanan siber yang beredar pada berbagai sumber Telegram.

Pembahasan:

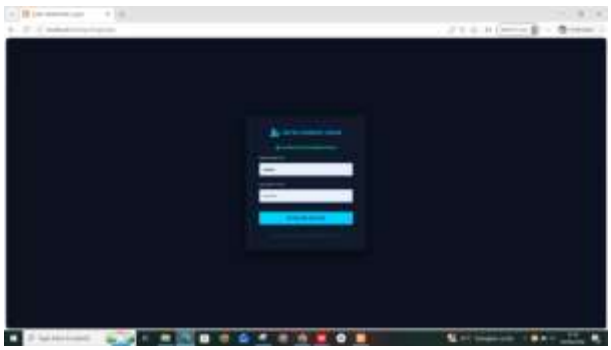
Arsitektur sistem dirancang untuk mendukung proses monitoring yang terintegrasi mulai dari pengambilan data hingga penyajian informasi kepada pengguna. Data yang diperoleh dari Telegram API akan diproses oleh aplikasi, kemudian disimpan ke dalam database sebelum ditampilkan pada dashboard monitoring. Dengan mekanisme tersebut, proses pengumpulan informasi dapat dilakukan secara otomatis tanpa memerlukan intervensi manual yang berlebihan, sehingga meningkatkan efisiensi dan kecepatan dalam memperoleh informasi keamanan siber.

pengelolaan data secara efektif sehingga memudahkan proses monitoring dan analisis informasi keamanan siber.

Pembahasan:

Struktur basis data dirancang dengan mempertimbangkan kebutuhan sistem dalam mengelola data monitoring secara terintegrasi. Setiap tabel memiliki fungsi yang berbeda namun saling berhubungan untuk mendukung proses pengambilan data, penyimpanan informasi, serta pengelolaan pengguna. Dengan rancangan basis data yang terstruktur, sistem mampu menjaga konsistensi data dan meningkatkan performa dalam proses pengolahan informasi.

II. Implementasi Antarmuka Sistem



Gambar 3. Halaman Login

DOI: https://doi.org/10.31004/riggs.v5i2.12535

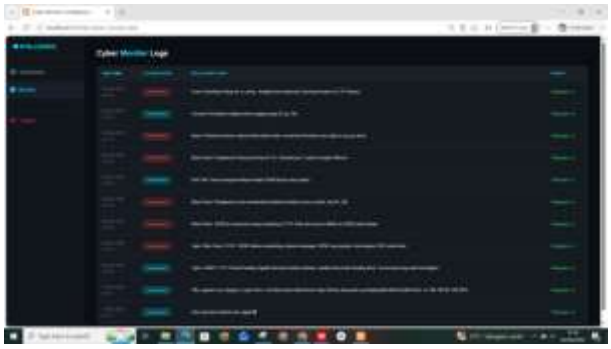
Pembahasan:

Halaman login berfungsi sebagai mekanisme autentikasi yang digunakan untuk memastikan bahwa hanya pengguna yang memiliki hak akses yang dapat memasuki sistem. Pengguna diwajibkan memasukkan username dan password yang valid sebelum dapat mengakses fitur-fitur yang tersedia. Implementasi fitur login ini bertujuan untuk meningkatkan keamanan sistem serta melindungi data monitoring dari akses yang tidak sah.

Gambar 4. Halaman Dashboard

Pembahasan:

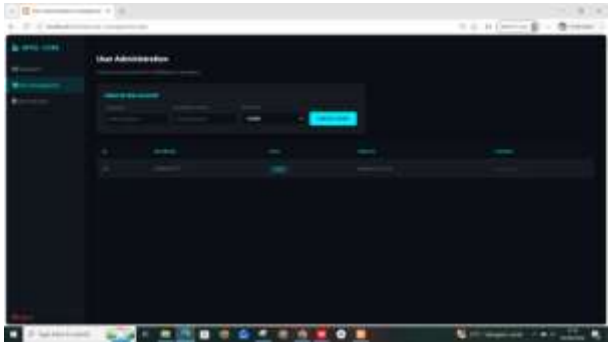
Dashboard merupakan halaman utama yang menyajikan ringkasan informasi hasil monitoring secara visual dan informatif. Halaman ini menampilkan jumlah data yang berhasil dikumpulkan, statistik kategori isu siber, serta grafik aktivitas Telegram yang diperbarui secara berkala. Melalui dashboard, pengguna dapat memperoleh gambaran umum mengenai kondisi dan perkembangan isu keamanan siber tanpa harus melakukan analisis data secara manual.



Gambar 5. Halaman Cyber Monitor

Pembahasan:

Halaman Cyber Monitor digunakan untuk menampilkan seluruh data hasil monitoring yang diperoleh dari Telegram. Informasi yang ditampilkan meliputi judul informasi, kategori isu siber, waktu pengambilan data, dan sumber informasi. Fitur ini memudahkan pengguna dalam melakukan pencarian, pemantauan, serta analisis terhadap data yang telah berhasil dikumpulkan oleh sistem.



Gambar 6. Halaman User Management

Pembahasan:

Halaman User Management berfungsi untuk mengelola akun pengguna yang memiliki akses terhadap sistem monitoring. Administrator dapat menambahkan, mengubah, maupun menghapus data pengguna sesuai

DOI: https://doi.org/10.31004/riggs.v5i2.12535

kebutuhan organisasi. Pengelolaan hak akses yang baik memungkinkan sistem tetap aman dan memastikan setiap pengguna hanya dapat mengakses fitur sesuai dengan perannya masing-masing.

III. Hasil Pengujian Sistem

Pengujian sistem dilakukan menggunakan metode Black Box Testing untuk memastikan seluruh fitur berjalan sesuai dengan kebutuhan pengguna dan rancangan sistem yang telah dibuat.

Berdasarkan hasil pengujian yang telah dilakukan, seluruh fitur utama pada sistem dapat berjalan dengan baik sesuai dengan fungsi yang dirancang. Fitur login berhasil melakukan autentikasi pengguna, proses data feeding Telegram mampu mengambil data secara otomatis, dashboard dapat menampilkan informasi monitoring secara akurat, halaman Cyber Monitor berhasil menampilkan data hasil monitoring, dan fitur User Management dapat mengelola data pengguna tanpa kendala. Hasil pengujian tersebut menunjukkan bahwa sistem telah memenuhi kebutuhan fungsional yang ditetapkan pada tahap analisis dan perancangan.

IV. Analisis Hasil

Grafik aktivitas Telegram digunakan untuk menampilkan jumlah data yang berhasil dikumpulkan oleh sistem dalam periode waktu tertentu. Visualisasi ini memberikan informasi mengenai tren aktivitas informasi keamanan siber yang beredar pada Telegram sehingga pengguna dapat mengidentifikasi peningkatan maupun penurunan aktivitas yang terjadi. Dengan adanya grafik tersebut, proses analisis data menjadi lebih mudah dan informatif.

Diagram distribusi kategori isu siber digunakan untuk menunjukkan persentase masing-masing kategori informasi yang berhasil dikumpulkan oleh sistem. Informasi ini membantu pengguna dalam mengetahui jenis isu keamanan siber yang paling dominan serta memahami pola penyebaran informasi berdasarkan kategori tertentu. Hasil visualisasi menunjukkan bahwa sistem mampu melakukan pengelompokan data dengan baik sehingga informasi yang ditampilkan menjadi lebih terstruktur dan mudah dipahami.

Secara keseluruhan, hasil implementasi menunjukkan bahwa sistem mampu mengotomatisasi proses pengumpulan informasi dari Telegram sehingga mengurangi ketergantungan pada proses monitoring manual. Integrasi antara Telegram API, basis data, dan dashboard monitoring memungkinkan data diperoleh, disimpan, dan disajikan secara terpusat. Dengan demikian, sistem dapat membantu pengguna dalam memperoleh informasi keamanan siber secara lebih cepat, akurat, dan efisien sebagai dasar dalam proses pemantauan maupun pengambilan keputusan [15].

5. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa Sistem Monitoring Isu Siber Otomatis Berbasis Data Feeding Telegram berhasil dirancang dan diimplementasikan sebagai solusi untuk membantu proses pengumpulan, pengelolaan, dan penyajian informasi keamanan siber secara terintegrasi. Sistem mampu melakukan pengambilan data secara otomatis dari sumber Telegram yang telah ditentukan, menyimpan data ke dalam basis data secara terstruktur, serta menyajikan informasi melalui dashboard berbasis web yang informatif dan mudah digunakan. Implementasi fitur monitoring, visualisasi data, dan manajemen pengguna menunjukkan bahwa sistem dapat mendukung kebutuhan pemantauan isu siber secara lebih efektif dibandingkan metode manual yang memerlukan waktu dan tenaga yang lebih besar. Hasil pengujian menggunakan metode Black Box Testing menunjukkan bahwa seluruh fungsi utama sistem, meliputi autentikasi pengguna, proses data feeding Telegram, pengelolaan data monitoring, visualisasi informasi, serta manajemen pengguna, dapat berjalan sesuai dengan kebutuhan yang telah ditetapkan pada tahap analisis dan perancangan. Integrasi antara Telegram API, basis data, dan antarmuka web memungkinkan proses monitoring dilakukan secara berkelanjutan sehingga informasi yang diperoleh dapat diakses secara cepat, akurat, dan terpusat. Dengan demikian, sistem yang dikembangkan mampu meningkatkan efisiensi proses monitoring informasi keamanan siber, mempermudah proses analisis data, serta membantu pengguna dalam memperoleh informasi yang relevan untuk mendukung pengambilan keputusan. Keberadaan sistem ini diharapkan dapat menjadi dasar bagi pengembangan platform monitoring yang lebih cerdas di masa mendatang melalui penerapan teknologi analitik data dan kecerdasan buatan guna meningkatkan akurasi klasifikasi serta kemampuan deteksi dini terhadap berbagai ancaman siber.

Referensi

[1] I. Sommerville, *Software Engineering*, 10th ed. Boston, MA, USA: Pearson, 2016.
[2] R. S. Pressman and B. R. Maxim, *Software Engineering: A Practitioner's Approach*, 9th ed. New York, NY, USA: McGraw-Hill Education, 2020.
[3] R. Elmasri and S. B. Navathe, *Fundamentals of Database Systems*, 7th ed. Boston, MA, USA: Pearson, 2017.
[4] A. Silberschatz, H. F. Korth, and S. Sudarshan, *Database System Concepts*, 7th ed. New York, NY, USA: McGraw-Hill Education, 2019.
[5] D. Comer, *Computer Networks and Internets*, 6th ed. New York, NY, USA: Pearson, 2015.
[6] W. Stallings, *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Boston, MA, USA: Addison-Wesley, 2019.
[7] J. Kim and M. Solomon, *Fundamentals of Information Systems Security*, 4th ed. Burlington, MA, USA: Jones & Bartlett Learning, 2018.
[8] Telegram, "Telegram API Documentation," 2026. Available: https://core.telegram.org. [Accessed: Jun. 2026].
[9] PHP Documentation Team, "PHP Documentation," 2026. Available: https://www.php.net/docs.php. [Accessed: Jun. 2026].
[10] Oracle Corporation, "MySQL Documentation," 2026. Available: https://dev.mysql.com/doc. [Accessed: Jun. 2026].

DOI: https://doi.org/10.31004/riggs.v5i2.12535

[11] Chart.js Contributors, “Chart.js Documentation,” 2026. Available: https://www.chartjs.org/docs. [Accessed: Jun. 2026].
[12] C. Pascoe, S. Quinn, and K. Scarfone, “The NIST Cybersecurity Framework (CSF) 2.0,” NIST Cybersecurity White Papers, NIST CSWP 29, 2024, doi: 10.6028/NIST.CSWP.29.
[13] Telegram, “Telegram APIs,” 2026. Available: https://core.telegram.org/api. [Accessed: Aug. 2026].
[14] OWASP Foundation, “Logging Cheat Sheet,” OWASP Cheat Sheet Series, 2026. Available: https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html. [Accessed: Aug. 2026].
[15] Cybersecurity and Infrastructure Security Agency, “Assessing the Potential Value of Cyber Threat Intelligence Feeds,” 2021. Available: https://www.cisa.gov/resources-tools/resources/assessing-potential-value-cyber-threat-intelligence-feeds-white-paper. [Accessed: Aug. 2026].

DOI: https://doi.org/10.31004/riggs.v5i2.12535