JURNAL PENGABDIAN MASYARAKAT BANGSA
e-ISSN : 2987- 0135
Volume 4, No. 4, Tahun 2026
https://jurnalpengabdianmasyarakatbangsa.com/index.php/jpmba/index

Pelatihan Sistem Deteksi Intruksi Menggunakan Wazuh Berbasis Notifikasi Real-Time Telegram di Universitas Bina Darma

Tia Meliana[1], Jemakmun[2], Suryayusra[3]
[1,2,3] *Universitas Bina Darma, Palembang, Indonesia*

Received : 18 Mei 2026, Revised : 3 Juni 2026, Published : 15 Juni 2026

Corresponding Author
Nama Penulis: Tia Meliana
E-mail: tiameliana730@gmail.com

Abstrak

Kegiatan magang di Direktorat Sistem dan Teknologi Informasi (DSTI) Universitas Bina Darma dilaksanakan untuk mendukung peningkatan keamanan jaringan melalui implementasi sistem deteksi intrusi menggunakan Wazuh yang terintegrasi dengan notifikasi real-time Telegram. Kegiatan ini meliputi observasi lingkungan kerja, analisis kebutuhan sistem, instalasi dan konfigurasi Wazuh Server serta Wazuh Agent, integrasi Telegram Bot API, dan pengujian fungsional sistem. Implementasi dilakukan pada lingkungan virtual menggunakan VirtualBox dengan Ubuntu Desktop sebagai endpoint yang dipantau dan Kali Linux sebagai media simulasi aktivitas mencurigakan. Hasil implementasi menunjukkan bahwa Wazuh mampu mendeteksi percobaan login tidak sah dan perubahan file melalui fitur File Integrity Monitoring (FIM). Selain itu, notifikasi alert berhasil dikirimkan secara otomatis dan real-time ke Telegram administrator sehingga proses monitoring keamanan menjadi lebih cepat dan efisien. Implementasi sistem ini memberikan manfaat dalam meningkatkan efektivitas monitoring keamanan jaringan serta membantu administrator dalam merespons ancaman keamanan secara lebih cepat di lingkungan Universitas Bina Darma.

Kata kunci *– wazuh, intrusion detection system, telegram bot, monitoring keamanan*

Abstract

The internship activities conducted at the Directorate of Systems and Information Technology (DSTI), Universitas Bina Darma, aimed to support network security improvement through the implementation of an intrusion detection system using Wazuh integrated with real-time Telegram notifications. The activities included workplace observation, system requirement analysis, installation and configuration of Wazuh Server and Wazuh Agent, Telegram Bot API integration, and functional system testing. The implementation was carried out in a VirtualBox-based virtual environment using Ubuntu Desktop as the monitored endpoint and Kali Linux to simulate suspicious activities. The implementation results showed that Wazuh successfully detected unauthorized login attempts and file modifications through the File Integrity Monitoring (FIM) feature. In addition, alert notifications were automatically delivered in real time to administrators via Telegram, enabling faster and more efficient security monitoring. This implementation contributed to improving the effectiveness of network security monitoring and assisting administrators in responding more quickly to potential security threats within Universitas Bina Darma.

Keywords *- wazuh, intrusion detection system, telegram bot, security monitoring*

How To Cite : *Meliana, T., Jemakmun, J., & Suryayusra, S. (2026). Pelatihan Sistem Deteksi Intruksi Menggunakan Wazuh Berbasis Notifikasi Real-Time Telegram di Universitas Bina Darma . Jurnal Pengabdian Masyarakat Bangsa, 4(4), 1282 - 1289. https://doi.org/10.59837/jpmba.v4i4.4413*

Copyright *©2026 Tia Meliana, Jemakmun Jemakmun, Suryayusra Suryayusra*

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

PENDAHULUAN

Perkembangan teknologi informasi pada era digital memberikan dampak yang sangat besar terhadap berbagai sektor, termasuk sektor pendidikan. Perguruan tinggi saat ini memanfaatkan sistem informasi dan jaringan komputer untuk mendukung proses akademik, administrasi, hingga penyimpanan data penting (Nova et al., 2022). Semakin meningkatnya penggunaan teknologi tersebut menyebabkan risiko ancaman keamanan jaringan juga semakin tinggi. Ancaman seperti brute force, malware, perubahan file tanpa izin, maupun akses ilegal dapat mengganggu stabilitas sistem dan menyebabkan kerugian bagi institusi (Fernando et al., 2020).

Perkembangan teknologi jaringan yang semakin pesat membuat aktivitas akademik di perguruan tinggi bergantung pada sistem berbasis digital. Berbagai layanan seperti e-learning, sistem informasi akademik, perpustakaan digital, dan penyimpanan data mahasiswa membutuhkan jaringan yang stabil dan aman (Azzahra et al., 2025). Ketergantungan terhadap teknologi tersebut menyebabkan keamanan sistem informasi menjadi aspek yang sangat penting untuk diperhatikan oleh setiap institusi Pendidikan (Dewi, 2017).

Keamanan jaringan merupakan salah satu faktor utama dalam menjaga kerahasiaan, integritas, dan ketersediaan data (Erlansari et al., 2020). Jika sistem keamanan tidak dikelola dengan baik, maka berbagai ancaman dapat masuk dan menyebabkan gangguan operasional. Ancaman tersebut tidak hanya berasal dari pihak luar, tetapi juga dapat berasal dari kesalahan pengguna maupun perubahan sistem yang tidak terkontrol. Oleh karena itu, dibutuhkan sistem monitoring keamanan yang mampu bekerja secara optimal dan berkelanjutan (Jumiaty, 2024).

Universitas Bina Darma sebagai salah satu perguruan tinggi yang berfokus pada pengembangan teknologi informasi memiliki infrastruktur jaringan dan sistem informasi yang digunakan secara aktif dalam kegiatan operasional kampus. Infrastruktur tersebut mencakup server, jaringan internet, laboratorium komputer, dan berbagai layanan digital yang digunakan oleh mahasiswa maupun staf kampus (R. A. Dwi Ayu, 2021). Dengan banyaknya aktivitas digital yang berlangsung, risiko terhadap ancaman keamanan jaringan juga semakin meningkat (Rizky et al., 2025).

Dalam pengelolaan sistem jaringan, administrator memiliki tanggung jawab untuk memastikan seluruh layanan berjalan dengan baik tanpa adanya gangguan keamanan (Antara et al., 2024). Namun, proses monitoring secara manual sering kali menjadi kendala karena administrator harus memantau dashboard sistem secara terus-menerus. Kondisi tersebut dapat menyebabkan keterlambatan dalam mengetahui adanya ancaman atau aktivitas mencurigakan yang terjadi pada jaringan.

Salah satu solusi yang dapat diterapkan adalah penggunaan Wazuh sebagai sistem monitoring keamanan dan Intrusion Detection System (IDS). Wazuh merupakan platform keamanan open-source yang mampu melakukan monitoring log, File Integrity Monitoring (FIM), serta analisis ancaman secara real-time. Selain itu, Wazuh juga dapat diintegrasikan dengan berbagai sistem lain untuk meningkatkan efektivitas monitoring keamanan (Erlansari et al., 2020).

Wazuh memiliki kemampuan untuk mendeteksi berbagai aktivitas mencurigakan pada sistem maupun jaringan. Sistem ini dapat menganalisis log dari server dan endpoint untuk mengetahui adanya percobaan login ilegal, perubahan file penting, maupun aktivitas abnormal lainnya. Dengan fitur File Integrity Monitoring, Wazuh mampu memantau perubahan file secara otomatis sehingga administrator dapat mengetahui jika terjadi modifikasi file tanpa izin (Islam & Rafique, 2024). Selain monitoring pada sisi host, keamanan jaringan juga membutuhkan sistem yang mampu mendeteksi aktivitas mencurigakan pada lalu lintas jaringan. Dalam implementasi keamanan modern, deteksi ancaman secara cepat menjadi hal yang sangat penting untuk meminimalkan dampak serangan. Oleh karena itu, sistem monitoring perlu didukung dengan mekanisme notifikasi yang mampu memberikan informasi ancaman secara langsung kepada administrator(Bhavsar & Thakar, 2025).

Dalam implementasinya, proses monitoring yang hanya mengandalkan dashboard masih memiliki keterbatasan karena administrator harus memantau sistem secara terus-menerus. Jika

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

administrator tidak sedang membuka dashboard monitoring, maka terdapat kemungkinan ancaman terlambat diketahui. Kondisi ini dapat menyebabkan proses penanganan insiden keamanan menjadi kurang efektif dan berpotensi menimbulkan kerusakan yang lebih besar pada system (Anggraeni et al., 2022). Untuk mengatasi permasalahan tersebut, diperlukan sistem notifikasi otomatis yang dapat memberikan informasi ancaman secara langsung kepada administrator(Aditya et al., 2024). Telegram dipilih sebagai media notifikasi karena memiliki Telegram Bot API yang mudah diintegrasikan serta mampu mengirimkan pesan secara cepat dan real-time. Selain itu, Telegram juga dapat diakses melalui berbagai perangkat seperti smartphone maupun desktop sehingga memudahkan administrator menerima informasi kapan saja dan di mana saja.

Integrasi antara Wazuh dan Telegram memungkinkan setiap alert keamanan dikirimkan secara otomatis melalui pesan notifikasi. Informasi yang dikirim dapat berupa jenis ancaman, waktu kejadian, tingkat severity, serta perangkat yang terdeteksi mengalami gangguan keamanan. Dengan adanya notifikasi real-time tersebut, administrator dapat segera melakukan analisis dan tindakan mitigasi terhadap ancaman yang terjadi (Andika & Efendi, M.Kom, 2025).

Penerapan sistem deteksi intrusi menggunakan Wazuh dan notifikasi Telegram juga memberikan manfaat dalam meningkatkan efektivitas monitoring keamanan jaringan di lingkungan kampus. Sistem ini membantu administrator dalam memantau aktivitas jaringan secara lebih cepat, efisien, dan responsif. Selain itu, implementasi sistem ini juga dapat menjadi sarana pembelajaran dalam bidang keamanan siber, khususnya terkait monitoring jaringan dan intrusion detection system (Alvan et al., 2025).

Berdasarkan permasalahan tersebut, kegiatan magang ini difokuskan pada implementasi sistem deteksi intrusi menggunakan Wazuh yang terintegrasi dengan notifikasi real-time Telegram di lingkungan Universitas Bina Darma. Implementasi ini bertujuan untuk membantu administrator dalam melakukan monitoring keamanan jaringan secara lebih efektif, mempercepat respons terhadap ancaman keamanan, serta mendukung pengelolaan keamanan sistem yang lebih optimal. Selain memberikan manfaat bagi lingkungan kerja, kegiatan ini juga memberikan pengalaman praktis dalam penerapan teknologi keamanan jaringan berbasis open-source. (Haryanto & Chandra, 2024).

METODE

Pelaksanaan kegiatan dilakukan melalui beberapa tahapan yang meliputi observasi dan pengumpulan data, analisis kebutuhan sistem, instalasi dan konfigurasi Wazuh, integrasi Telegram Bot API, serta pengujian fungsional sistem. Seluruh kegiatan dilaksanakan selama program magang di Direktorat Sistem dan Teknologi Informasi (DSTI) Universitas Bina Darma.

1. Observasi dan Pengumpulan Data

   Tahap awal dilakukan dengan observasi langsung di Direktorat Sistem dan Teknologi Informasi (DSTI) Universitas Bina Darma. Pada tahap ini dilakukan pengamatan terhadap sistem monitoring yang sedang berjalan serta wawancara dengan administrator jaringan mengenai kebutuhan keamanan sistem.

Gambar 1.
Pengumpulan data di DSTI Bina Darma

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

2. Analisis Kebutuhan Sistem

Berdasarkan hasil observasi yang telah dilakukan di lingkungan Direktorat Sistem dan Teknologi Informasi (DSTI) Universitas Bina Darma, tahap selanjutnya adalah melakukan analisis kebutuhan sistem untuk menentukan perangkat lunak, spesifikasi perangkat, serta konfigurasi jaringan yang diperlukan dalam implementasi sistem deteksi intrusi. Analisis ini dilakukan untuk memastikan bahwa sistem yang dibangun dapat berjalan dengan baik sesuai kebutuhan monitoring keamanan jaringan. Pada tahap ini juga dilakukan identifikasi terhadap komponen yang akan digunakan, seperti Wazuh Server, Wazuh Agent, VirtualBox, Ubuntu Desktop, Kali Linux, serta integrasi Telegram Bot API sebagai media notifikasi real-time. Selain itu, dilakukan penyesuaian konfigurasi sistem agar proses monitoring, pengiriman log, dan deteksi ancaman dapat berjalan secara optimal dan efisien.

Gambar 2.
Analisis Jaringan di DSTI Bina Darma

3. Instalasi dan Konfigurasi Wazuh

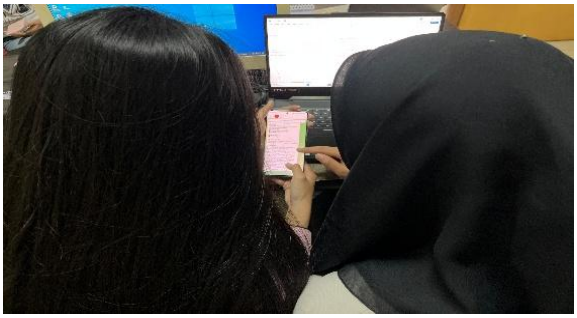
Tahap berikutnya adalah proses instalasi dan konfigurasi Wazuh Server serta Wazuh Agent menggunakan lingkungan virtual berbasis VirtualBox. Penggunaan VirtualBox bertujuan untuk mempermudah proses implementasi dan pengujian sistem dalam lingkungan virtual tanpa mengganggu sistem utama yang sedang berjalan. Pada tahap ini, Wazuh Server berfungsi sebagai pusat monitoring dan pengelolaan log keamanan, sedangkan Wazuh Agent dipasang pada sistem endpoint untuk mengirimkan data log dan informasi aktivitas sistem ke server. Ubuntu Desktop digunakan sebagai endpoint yang dipantau oleh Wazuh Agent karena memiliki dukungan yang baik terhadap implementasi sistem monitoring keamanan berbasis open-source. Setelah proses instalasi selesai, dilakukan konfigurasi koneksi antara Wazuh Server dan Wazuh Agent agar proses pengiriman log, monitoring aktivitas sistem, serta deteksi ancaman dapat berjalan secara real-time dan optimal.

Gambar 3.
Instalasi Wazuh

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

4. Integrasi Telegram Bot

Integrasi Telegram dilakukan dengan memanfaatkan Telegram Bot API sebagai media notifikasi real-time. Pada tahap ini, sistem dikonfigurasi agar setiap alert atau peringatan keamanan yang dihasilkan oleh Wazuh dapat dikirimkan secara otomatis ke akun atau grup Telegram administrator. Dengan adanya integrasi ini, administrator dapat menerima informasi ancaman dengan lebih cepat tanpa harus terus-menerus memantau dashboard Wazuh.



Gambar 4.
Integrasi Bot Telegram Ke Wazuh

5. Pengujian Sistem

Pengujian sistem dilakukan menggunakan Kali Linux sebagai media simulasi serangan untuk menguji kemampuan sistem keamanan yang telah diterapkan. Pada tahap ini dilakukan beberapa simulasi aktivitas mencurigakan, seperti percobaan login tidak sah dan perubahan file pada endpoint yang dipantau oleh Wazuh Agent. Pengujian bertujuan untuk mengetahui kemampuan Wazuh dalam mendeteksi ancaman serta memastikan notifikasi alert dapat dikirimkan secara real-time melalui Telegram kepada administrator.

Gambar 5.
Hasil Pengujian Wazuh

HASIL DAN PEMBAHASAN

Selama pelaksanaan kegiatan magang di Direktorat Sistem dan Teknologi Informasi (DSTI) Universitas Bina Darma, penulis terlibat secara langsung dalam implementasi sistem monitoring keamanan jaringan menggunakan Wazuh yang terintegrasi dengan Telegram. Kegiatan yang dilakukan meliputi instalasi sistem, konfigurasi perangkat, integrasi notifikasi, serta pengujian fungsional untuk memastikan sistem berjalan sesuai kebutuhan monitoring keamanan jaringan.

1. Implementasi Sistem

Implementasi sistem dilakukan menggunakan VirtualBox dengan beberapa komponen utama, yaitu Wazuh Server, Ubuntu Desktop sebagai endpoint, dan Kali Linux sebagai media

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

simulasi serangan. Wazuh Agent dipasang pada Ubuntu Desktop untuk memantau aktivitas sistem dan mengirimkan log ke Wazuh Server.

Pada tahap implementasi, Wazuh berhasil melakukan monitoring terhadap aktivitas sistem dan mendeteksi perubahan file melalui fitur File Integrity Monitoring (FIM). Selain itu, Wazuh juga mampu mendeteksi aktivitas login yang mencurigakan berdasarkan rule yang telah dikonfigurasi.

2. Integrasi Telegram

   Integrasi Telegram dilakukan menggunakan Telegram Bot API. Setelah proses konfigurasi selesai, setiap alert yang dihasilkan oleh Wazuh akan dikirimkan secara otomatis ke akun atau grup Telegram administrator.

   Notifikasi yang diterima berisi informasi terkait jenis ancaman, waktu kejadian, hostname perangkat, serta tingkat severity dari alert yang terdeteksi. Dengan adanya notifikasi ini, administrator dapat mengetahui ancaman keamanan secara cepat tanpa harus membuka dashboard Wazuh.

3. Pengujian Sistem

   Pengujian sistem dilakukan menggunakan simulasi serangan brute force dan perubahan file pada endpoint. Hasil pengujian menunjukkan bahwa:

   a) Wazuh berhasil mendeteksi percobaan login tidak sah.
   b) Wazuh mampu mendeteksi perubahan file pada direktori yang dimonitor.
   c) Alert berhasil dikirimkan secara real-time ke Telegram.
   d) Administrator dapat menerima notifikasi dengan cepat dan melakukan respons lebih awal.

   Hasil implementasi menunjukkan bahwa integrasi Wazuh dan Telegram mampu meningkatkan efektivitas monitoring keamanan jaringan. Sistem yang dibangun membantu administrator dalam mendeteksi ancaman secara lebih cepat dan efisien.

4. Pembahasan

   Penerapan sistem deteksi intrusi menggunakan Wazuh memberikan manfaat dalam meningkatkan keamanan jaringan di lingkungan Universitas Bina Darma. Dengan fitur monitoring log dan File Integrity Monitoring, administrator dapat mengetahui aktivitas mencurigakan yang terjadi pada sistem.

   Integrasi Telegram sebagai media notifikasi juga memberikan peningkatan dalam proses monitoring karena administrator tidak perlu terus-menerus memantau dashboard. Informasi ancaman dapat diterima secara langsung melalui perangkat mobile maupun desktop. Selain itu, sistem ini dapat dikembangkan lebih lanjut dengan menambahkan fitur active response agar sistem mampu melakukan tindakan otomatis ketika ancaman terdeteksi. Dengan demikian, keamanan jaringan dapat ditingkatkan secara lebih optimal.

KESIMPULAN

Berdasarkan hasil pelaksanaan kegiatan magang di Direktorat Sistem dan Teknologi Informasi (DSTI) Universitas Bina Darma, implementasi sistem deteksi intrusi menggunakan Wazuh yang terintegrasi dengan notifikasi real-time Telegram berhasil diterapkan dengan baik. Sistem mampu mendeteksi aktivitas mencurigakan seperti percobaan login tidak sah dan perubahan file secara otomatis melalui mekanisme monitoring yang tersedia.

Integrasi Telegram membantu administrator menerima informasi ancaman secara real-time sehingga proses monitoring keamanan jaringan menjadi lebih cepat dan efisien. Melalui kegiatan ini, penulis memperoleh pengalaman praktis dalam implementasi sistem keamanan jaringan berbasis open-source, sekaligus memberikan kontribusi terhadap peningkatan efektivitas monitoring keamanan di lingkungan Universitas Bina Darma.

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Bina Darma, khususnya Direktorat Sistem dan Teknologi Informasi (DSTI), yang telah memberikan kesempatan dan dukungan selama pelaksanaan kegiatan magang dan penelitian. Penulis juga mengucapkan terima kasih kepada dosen pembimbing serta seluruh pihak yang telah membantu selama pelaksanaan kegiatan magang, proses implementasi sistem, dan penyusunan artikel ini.

DAFTAR PUSTAKA

Aditya, R., Muhyidin, Y., & Singasatia, D. (2024). Implementasi Security Information And Event Management (SIEM) Untuk Monitoring Keamanan Server Menggunakan Wazuh. *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika*, *2*(5), 137–144. https://doi.org/10.61132/MERKURIUS.V2I5.289

Alvan, M., Putra, E., Hariyadi, I. P., & Marzuki, K. (2025). Otomatisasi Konfigurasi Wazuh Terintegrasi VirusTotal Menggunakan Ansible Untuk Mendeteksi dan Memproteksi Serangan Malware. *Melek IT : Information Technology Journal*, *11*(1), 55–66. https://doi.org/10.30742/MELEKITJOURNAL.V11I1.403

Andika, A., & Efendi, M.Kom, R. (2025). Simulasi Dan Analisis Efektivitas Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System (Ips) Berbasis Wazuh. *Jurnal Pendidikan Teknologi Informasi (JUKANTI)*, *8*(1), 17–24. https://doi.org/10.37792/JUKANTI.V8I1.1454

Anggraeni, D. P., Zen, B. P., & Pranata, M. (2022). Security Analysis On Websites Using The Information System Assessment Framework (Issaf) And Open Web Application Security Version 4 (Owaspv4) Using The Penetration Testing Method. *Jurnal Pertahanan: Media Informasi Tentang Kajian Dan Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism Dan Integrity*, *8*(3), 497–506. https://doi.org/10.33172/JP.V8I3.1777

Antara, G. P., Dyah, I., & Rachmawati, A. (2024). Implementasi dan Analisis Wazuh Sebagai Intrusion Detection System (IDS) dan Platform Monitoring. *Jurnal Informasi, Sains Dan Teknologi*, *7*(2), 290–303. https://doi.org/10.55606/ISAINTEK.V7I2.301

Azzahra, W. S., Toni, & Purwanto, M. (2025). Rancangan Monitoring Alarm Transmission Oil Level Pada Gearbox Radar Berbasis Esp8266 Dengan Notifikasi Telegram. *Teknika STTKD: Jurnal Teknik, Elektronik, Engine*, *11*(2), 192–200. https://doi.org/10.56521/TEKNIKA.V11I2.1566

Bhavsar, R., & Thakar, V. (2025). *WITHDRAWN: Design and Implementation of an Open-Source Security Operations Center for Effective Cyber Threat Detection and Response*. https://doi.org/10.21203/RS.3.RS-5795888/V1

Dewi, E. K. (2017). Analisis Log Snort Menggunakan Network Forensic. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *2*(2). https://doi.org/10.29100/JIPI.V2I2.370

Erlansari, A., Coastera, F. F., & Husamudin, A. (2020). Early Intrusion Detection System (IDS) using Snort and Telegram approach. *SISFORMA*, *7*(1), 21–27. https://doi.org/10.24167/SISFORMA.V7I1.2629

Fernando, N., Humaira, & Asri, E. (2020). Monitoring Jaringan dan Notifikasi dengan Telegram pada Dinas Komunikasi dan Informatika Kota Padang. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *1*(4), 121–126. https://doi.org/10.62527/JITSI.1.4.17

Haryanto, B., & Chandra, D. W. (2024). Implementasi Wazuh Integritas File untuk Perlindungan Keamanan Berdasarkan Aktivitas Log di BTSI UKSW. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *5*(1), 183–192. https://doi.org/10.35870/JIMIK.V5I1.447

Islam, M. R., & Rafique, R. (2024). Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries. *International Journal of Engineering Materials and Manufacture*, *9*(4), 136–144. https://doi.org/10.26776/IJEMM.09.04.2024.02

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

Jumiaty, B. S. (2024). SIEM and Threat Intelligence: Protecting Applications with Wazuh and TheHive. *International Journal of Advanced Computer Science and Applications*, *15*(9), 239–251. https://doi.org/10.14569/IJACSA.2024.0150923

Nova, F., Pratama, M. D., & Prayama, D. (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *3*(1), 1–7. https://doi.org/10.62527/JITSI.3.1.59

R. A. DWI AYU, P. (2021). *Analisa Sistem Informasi Akademik (Sisfo) Dan Jaringan Di Universitas Bina Darma*. https://www.binadarma.ac.id/

Rizky, M., Pahlevi, R., Umam, C., & Handoko, L. B. (2025). Deteksi dan Pencegahan Web Defacing Judi Online dengan Wazuh SIEM dan Snort IDS Berbasis Signature. *Jurnal Algoritma*, *22*(1), 197–208. https://doi.org/10.33364/ALGORITMA/V.22-1.2220

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license