JURNAL PENGABDIAN MASYARAKAT BANGSA
e-ISSN : 2987- 0135
Volume 3, No. 10, Tahun 2025
https://jurnalpengabdianmasyarakatbangsa.com/index.php/jpmba/index

Pelatihan Wazuh dan Integrasi Suricata dengan Notifikasi Telegram Untuk Siswa SMK Magang di Universitas Bina Darma

Suryayusra[1], Delfin Christofa[2]
[1,2] *Universitas Bina Darma, Palembang, Indonesia*

Corresponding Author
Nama Penulis: Suryayusra
E-mail: suryayusra@binadarma.ac.id

Abstrak

Pelatihan ini bertujuan meningkatkan pemahaman dan keterampilan siswa SMK dalam menerapkan sistem keamanan jaringan melalui Wazuh File Integrity Monitoring dan integrasi Suricata dengan notifikasi Telegram. Kegiatan dilakukan dengan metode hands-on training yang meliputi penyampaian konsep dasar keamanan jaringan, instalasi dan konfigurasi Wazuh Agent, implementasi FIM, pemasangan Suricata sebagai IDS, integrasi log Suricata ke Wazuh, serta pembuatan Telegram Bot untuk notifikasi real-time. Siswa juga melakukan simulasi serangan, seperti perubahan file dan port scanning, untuk menguji kemampuan sistem mendeteksi ancaman. Hasil pelatihan menunjukkan bahwa siswa mampu memahami cara kerja FIM, membaca log keamanan, mengidentifikasi aktivitas jaringan mencurigakan, dan menerima peringatan otomatis melalui Telegram. Secara keseluruhan, pelatihan berbasis praktik ini terbukti efektif meningkatkan kompetensi siswa serta memberikan pengalaman langsung terkait implementasi sistem keamanan modern berbasis open-source. Model pelatihan ini dapat diterapkan secara berkelanjutan untuk mempersiapkan siswa menghadapi tantangan keamanan siber di dunia pendidikan dan industri.

Kata kunci - *wazuh, suricata, telegram, keamanan jaringan, monitoring log*

Abstract

This training aims to improve the understanding and skills of vocational high school students in implementing network security systems through Wazuh File Integrity Monitoring and the integration of Suricata with Telegram notifications. The activities were carried out using a hands-on training method that included the delivery of basic network security concepts, installation and configuration of Wazuh Agent, implementation of FIM, installation of Suricata as an IDS, integration of Suricata logs into Wazuh, and creation of Telegram Bots for real-time notifications. Students also simulated attacks, such as file changes and port scanning, to test the system's ability to detect threats. The training results showed that students were able to understand how FIM works, read security logs, identify suspicious network activity, and receive automatic alerts via Telegram. Overall, this practice-based training proved effective in improving student competency and providing direct experience in implementing modern, open-source security systems. This training model can be applied sustainably to prepare students to face cybersecurity challenges in education and industry.

Keywords - *wazuh, suricata, telegram, network security, log monitoring*

PENDAHULUAN

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam berbagai sektor, termasuk dunia pendidikan. Salah satu dampak besar dari perkembangan tersebut adalah meningkatnya kebutuhan akan pemahaman keamanan siber (cybersecurity) sebagai bagian fundamental dalam pengelolaan sistem informasi modern. Serangan siber yang semakin kompleks dan beragam menuntut adanya peningkatan kemampuan dalam hal deteksi, monitoring, dan penanggulangan ancaman (Garg et al., 2023). Di lingkungan pendidikan, khususnya Sekolah Menengah Kejuruan (SMK), siswa perlu dibekali kompetensi yang relevan dengan kebutuhan industri, termasuk keterampilan praktis dalam mengelola keamanan sistem dan jaringan (Mulyono et al., 2023).

Masalah yang sering ditemui di lingkungan SMK adalah minimnya media pembelajaran praktis berbasis *tools* keamanan jaringan yang digunakan di dunia kerja (Pasha et al., 2024). Pembelajaran keamanan siber sering kali hanya disampaikan secara teoritis, sehingga siswa kurang mendapatkan pengalaman langsung mengenai implementasi sistem pertahanan jaringan (Mukherjee et al., 2024). Kondisi ini berdampak pada kurangnya kesiapan siswa dalam mengidentifikasi ancaman siber dan memahami cara kerja alat keamanan yang saat ini menjadi standar industri. Oleh karena itu, diperlukan sebuah kegiatan pelatihan yang mampu memberikan pengalaman langsung melalui penggunaan perangkat keamanan open-source yang mudah diimplementasikan (Prasetia et al., 2024).

Wazuh, sebagai platform keamanan *open-source* berbasis SIEM (Security Information and Event Management), menawarkan berbagai fitur penting seperti monitoring sistem, analisis log, deteksi ancaman, hingga *File Integrity Monitoring* (FIM) (Haryanto & Chandra, 2024). FIM merupakan komponen penting dalam menjaga keamanan, karena mampu mendeteksi perubahan pada file dan direktori yang dapat mengindikasikan tindakan berbahaya seperti modifikasi tidak sah, malware, atau aktivitas pengguna yang mencurigakan (Kamil et al., 2024). Sementara itu, Suricata dikenal sebagai sistem deteksi dan pencegahan intrusi (IDS/IPS) yang mampu menganalisis trafik jaringan secara mendalam dan mendeteksi berbagai pola serangan berdasarkan *signature* maupun metode analisis lainnya. Integrasi kedua sistem ini memberikan pendekatan keamanan komprehensif yang efektif dan relevan untuk kebutuhan pembelajaran (Rivaldi & Marpaung, 2024).

Beberapa penelitian terdahulu menunjukkan bahwa penggunaan perangkat *open-source* seperti Wazuh dan Suricata efektif dalam memberikan pemahaman mendalam mengenai keamanan jaringan. Pelatihan berbasis praktik menggunakan IDS/IPS dan SIEM terbukti meningkatkan kemampuan peserta dalam membaca log, memahami pola serangan, serta menganalisis respons keamanan (Bhavsar & Thakar, 2025). Selain itu, penelitian lain mengungkapkan bahwa penyediaan notifikasi real-time, misalnya melalui Telegram Bot, mampu mempercepat respons terhadap insiden serta meningkatkan keterlibatan peserta dalam proses belajar. Notifikasi instan membuat peserta lebih mudah memahami alur deteksi ancaman dari awal sampai munculnya peringatan.

Masuknya teknologi Telegram Bot dalam kegiatan pelatihan memberikan nilai tambah karena mempermudah peserta dalam menerima peringatan secara langsung melalui perangkat seluler (Kurnaedi & Widodo, 2023). Hal ini meniru praktik yang digunakan dalam industri, di mana sistem keamanan sering kali diintegrasikan dengan platform notifikasi untuk mempercepat mitigasi insiden. Dengan demikian, penggunaan notifikasi Telegram dalam pelatihan ini tidak hanya menambah pemahaman teknis siswa, tetapi juga memperlihatkan bagaimana teknologi monitoring modern bekerja pada lingkungan nyata. Pengalaman ini sangat bermanfaat bagi siswa SMK yang dipersiapkan untuk memasuki dunia kerja di bidang teknologi informasi (Rakhmat Sani et al., 2025).

Berdasarkan latar belakang tersebut, kegiatan pengabdian kepada masyarakat ini disusun untuk memberikan pelatihan kepada siswa SMK mengenai implementasi Wazuh *File Integrity Monitoring* serta integrasi Suricata dengan notifikasi Telegram. Kegiatan ini bertujuan untuk meningkatkan pengetahuan dan keterampilan siswa dalam memahami keamanan jaringan, menganalisis ancaman, serta memanfaatkan *tools open-source* secara efektif. Selain itu, pelatihan ini diharapkan dapat memperkaya pengalaman belajar siswa melalui praktik langsung, sehingga mereka

memiliki bekal yang lebih kuat dalam menghadapi tantangan dunia industri di masa mendatang. Tujuan utama pelatihan ini adalah memberikan kemampuan teknis mengenai instalasi, konfigurasi, integrasi, dan analisis hasil monitoring menggunakan Wazuh dan Suricata, serta meningkatkan kesiapan siswa dalam menghadapi isu-isu keamanan siber secara nyata.

METODE

Pelaksanaan kegiatan pengabdian ini dilakukan melalui pendekatan pelatihan langsung (hands-on training) dengan tiga tahapan utama, yaitu:

1. Tahap Persiapan Teknis dan Materi

Gambar 1.
Persiapan Teknis dan Materi Pelatihan

Tahap ini meliputi seluruh kegiatan awal yang diperlukan agar proses pelatihan dapat berjalan secara terstruktur. Tim pelaksana terlebih dahulu menyusun materi pelatihan yang mencakup konsep dasar keamanan jaringan, pengenalan Wazuh dan Suricata, serta pemahaman mengenai *File Integrity Monitoring* (FIM). Selain penyusunan materi, dilakukan pula instalasi seluruh perangkat lunak yang dibutuhkan, termasuk pembuatan lingkungan virtual menggunakan VirtualBox yang berisi Wazuh Server, beberapa Wazuh Agent dengan sistem operasi berbeda, serta instalasi Suricata sebagai sistem deteksi intrusi. Konfigurasi Telegram Bot juga dilakukan pada tahap ini untuk memastikan notifikasi dapat dikirim secara otomatis. Penyiapan teknis yang matang pada tahap ini sangat penting karena menentukan kelancaran pelatihan dan meminimalkan kendala teknis yang mungkin muncul saat praktik berlangsung.

2. Tahap Pelaksanaan Pelatihan dan Praktik Terbimbing

Gambar 2.
Pelaksanaan Pelatihan dan Praktik Terbimbing

Tahap ini merupakan inti dari kegiatan pelatihan karena siswa mendapatkan materi sekaligus melakukan praktik secara langsung. Pelatihan dimulai dengan penyampaian teori mengenai keamanan jaringan, fungsi IDS/IPS, mekanisme FIM, dan cara kerja integrasi sistem keamanan. Setelah pemahaman dasar diberikan, peserta dibimbing untuk melakukan praktik instalasi Wazuh Agent di berbagai sistem operasi, konfigurasi FIM untuk memantau perubahan file, serta pemasangan Suricata dan integrasi log Suricata ke dalam Wazuh. Pada tahap ini peserta juga mempelajari cara membuat dan menghubungkan Telegram Bot dengan sistem agar notifikasi real-time dapat diterima saat terjadi perubahan file atau saat Suricata mendeteksi adanya aktivitas mencurigakan. Pendekatan praktik terbimbing ini memastikan peserta dapat memahami alur sistem keamanan secara terintegrasi mulai dari proses monitoring, deteksi, hingga munculnya alert otomatis.

3. Tahap Evaluasi, Diskusi, dan Dokumentasi Kegiatan

Gambar 3.
Evaluasi, Diskusi Dan Dokumentasi Kegiatan

Pada tahap ini, peserta melakukan berbagai simulasi serangan seperti perubahan file tanpa izin, percobaan *port scanning*, atau aktivitas jaringan lainnya untuk menguji respon Wazuh dan Suricata. Hasil simulasi kemudian dianalisis melalui log dan dashboard Wazuh untuk melihat bagaimana sistem mencatat dan menampilkan aktivitas berpotensi berbahaya tersebut. Peserta kemudian diajak berdiskusi untuk memahami hasil deteksi, mengidentifikasi pola serangan, serta menilai efektivitas konfigurasi yang telah dilakukan. Selain evaluasi teknis, seluruh proses pelatihan didokumentasikan secara lengkap, meliputi konfigurasi sistem, hasil percobaan, tampilan dashboard, dan bukti keberhasilan notifikasi Telegram. Dokumentasi ini berfungsi sebagai bahan laporan pengabdian dan dapat digunakan kembali sebagai referensi pembelajaran bagi siswa atau kegiatan pelatihan di masa mendatang.

HASIL DAN PEMBAHASAN

Pelaksanaan pelatihan memberikan dampak positif terhadap peningkatan kompetensi siswa dalam memahami konsep keamanan jaringan menggunakan perangkat *open-source*. Selama kegiatan berlangsung, siswa menunjukkan peningkatan pengetahuan mengenai mekanisme deteksi ancaman serta peran penting sistem keamanan terintegrasi dalam melindungi infrastruktur jaringan. Salah satu pencapaian utama adalah kemampuan siswa dalam menginstal dan mengonfigurasi Wazuh Agent pada berbagai sistem operasi, baik Windows maupun Linux. Selain itu, siswa mampu mengidentifikasi bagaimana *File Integrity Monitoring* (FIM) bekerja dalam mendeteksi perubahan file, termasuk modifikasi yang berpotensi mengindikasikan aktivitas berbahaya atau tidak sah. Pemahaman terhadap FIM ini menjadi salah satu elemen penting dalam membangun kesadaran siswa terhadap ancaman internal pada sistem.

Dalam proses implementasi bagian jaringan, siswa juga memperoleh pemahaman mendalam mengenai penggunaan Suricata sebagai sistem deteksi dan pencegahan intrusi. Mereka berhasil memasang Suricata, mengonfigurasi rule set, dan memastikan integrasinya dengan Wazuh melalui mekanisme log forwarder. Dengan integrasi tersebut, setiap aktivitas jaringan yang mencurigakan dapat dipantau secara langsung melalui dashboard Wazuh. Siswa mampu melakukan simulasi serangan sederhana, seperti *port scanning* dan SSH *brute force*, untuk melihat bagaimana Suricata mengidentifikasi pola serangan tersebut melalui *signature* yang tersedia. Kemampuan siswa dalam menganalisis output hasil deteksi Suricata menunjukkan bahwa pendekatan praktik langsung memberikan kontribusi signifikan dalam pembangunan pemahaman mereka terkait ancaman siber berbasis jaringan.

Selain itu, integrasi notifikasi otomatis menggunakan Telegram Bot memberikan pengalaman praktis tambahan bagi siswa dalam memahami bagaimana sistem keamanan modern bekerja secara real-time. Setiap kali terjadi perubahan file penting atau Suricata mendeteksi aktivitas berbahaya, peringatan langsung dikirimkan ke aplikasi Telegram. Notifikasi ini tidak hanya mempercepat respons terhadap insiden, tetapi juga memperlihatkan alur kerja lengkap dari deteksi hingga munculnya peringatan. Respons cepat yang ditunjukkan melalui mekanisme Telegram Bot membantu siswa lebih memahami pentingnya sistem alert dalam operasi keamanan jaringan. Mereka juga mempelajari bagaimana teknologi messaging dapat dimanfaatkan sebagai alat respons insiden yang efisien dan mudah digunakan.

Hasil pengamatan selama kegiatan menunjukkan bahwa pendekatan pelatihan berbasis praktik sangat efektif dalam meningkatkan pemahaman siswa SMK. Dengan melihat sendiri bagaimana konfigurasi dilakukan, bagaimana serangan terdeteksi, serta bagaimana peringatan dikirimkan, siswa memperoleh pengalaman belajar yang lebih komprehensif daripada metode ceramah semata. Kombinasi antara teori dan praktik ini memungkinkan siswa untuk menghubungkan konsep abstrak mengenai keamanan jaringan dengan contoh nyata yang mereka lakukan sendiri selama pelatihan. Hal ini memperkuat pemahaman mereka terhadap berbagai komponen sistem keamanan dan hubungan antar perangkat keamanan yang saling mendukung dalam suatu ekosistem.

Secara keseluruhan, kegiatan ini menunjukkan bahwa penggunaan perangkat *open-source* seperti Wazuh dan Suricata sangat ideal digunakan sebagai media pembelajaran bagi siswa SMK karena sifatnya yang fleksibel, bebas lisensi, dan mudah dikonfigurasikan. Integrasi kedua perangkat tersebut dengan Telegram Bot semakin memperkaya pengalaman belajar karena memberikan gambaran langsung tentang bagaimana sistem keamanan modern di dunia industri bekerja dalam mendeteksi, mencatat, dan memberikan peringatan terhadap ancaman. Dengan demikian, pelatihan ini tidak hanya meningkatkan kemampuan teknis siswa, tetapi juga menumbuhkan kesadaran mereka terhadap pentingnya keamanan siber dalam pengelolaan sistem informasi masa kini.

KESIMPULAN

Pelatihan Wazuh File Integrity Monitoring dan integrasi Suricata dengan notifikasi Telegram memberikan dampak positif dalam meningkatkan pemahaman serta keterampilan siswa SMK mengenai konsep keamanan jaringan modern. Melalui kegiatan ini, siswa tidak hanya diperkenalkan pada teori deteksi ancaman dan monitoring integritas file, tetapi juga memahami implementasinya secara langsung dalam lingkungan simulasi yang menyerupai kondisi nyata. Penggunaan platform open-source seperti Wazuh dan Suricata memungkinkan siswa mengenal perangkat keamanan yang banyak digunakan di industri, sekaligus mempraktikkan bagaimana sistem keamanan bekerja dalam mendeteksi aktivitas mencurigakan dan memberikan peringatan secara real-time melalui Telegram.

Secara keseluruhan, seluruh tujuan kegiatan pengabdian dapat dicapai dengan baik, yang terlihat dari kemampuan siswa dalam melakukan instalasi, konfigurasi, serta analisis log dari kedua platform keamanan tersebut. Kegiatan ini membuktikan bahwa pendekatan pelatihan berbasis praktik sangat efektif dalam membangun kompetensi siswa SMK di bidang keamanan siber.

Sebagai saran, kegiatan pelatihan selanjutnya dapat dikembangkan dengan menambahkan skenario serangan yang lebih kompleks, seperti *lateral movement, privilege escalation*, dan korelasi *multi-log*, serta penerapan *active response* untuk mitigasi otomatis. Selain itu, integrasi dengan teknologi keamanan tambahan seperti *firewall, threat intelligence*, atau dashboard analitik lanjutan dapat diterapkan untuk memperluas wawasan peserta. Penerapan evaluasi berbasis proyek dan studi kasus nyata juga disarankan untuk meningkatkan kemampuan analitis siswa sehingga mereka lebih siap menghadapi kebutuhan industri teknologi informasi yang semakin kompleks di masa depan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Universitas Bina Darma yang telah memberikan dukungan dan pendanaan dalam pelaksanaan kegiatan pengabdian kepada masyarakat ini. Dukungan tersebut memungkinkan seluruh rangkaian kegiatan, mulai dari persiapan, pelatihan, hingga penyusunan laporan ilmiah, dapat terlaksana dengan baik dan memberikan manfaat nyata bagi peserta pelatihan. Penulis juga menyampaikan apresiasi kepada pihak sekolah mitra serta seluruh peserta yang telah berpartisipasi aktif sehingga kegiatan ini dapat berjalan dengan lancar dan mencapai tujuan yang diharapkan.

DAFTAR PUSTAKA

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/V2

Garg, A., Pandey, A., Sharma, N., Kumar, A., Jha, P. K., & Singhal, R. K. (2023). An In-Depth Analysis of the Constantly Changing World of Cyber Threats and Defences: Locating the Most Recent Developments. *2023 International Conference on Power Energy, Environment and Intelligent Control, PEEIC 2023*, 181–186. https://doi.org/10.1109/PEEIC59336.2023.10451963

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

Kamil, A., Rizaludin, D., Studi, A. N.-S. D. J., & 2024, undefined. (2024). Implementasi Wazuh FIM (File Integrity Monitoring) untuk Perlindungan Keamanan Sistem Informasi pada Unit Kegiatan Mahasiswa di Universitas Trunojoyo Madura. *Pub.Nuris.Ac.IdA Kamil, D Rizaludin, AT Ni'mahSains Data Jurnal Studi Matematika Dan Teknologi, 2024•pub.Nuris.Ac.Id*. Retrieved December 9, 2025, from https://pub.nuris.ac.id/sainsdata/article/view/127

Kurnaedi, D., & Widodo, A. D. (2023). Implementation of Telegram Chatbot as an Effective Communication Means at SMK PGRI 1 Tangerang. *Bit-Tech*, *6*(2), 183–189. https://doi.org/10.32877/BT.V6I2.1054

Mukherjee, M., Le, N. T., Chow, Y.-W., Susilo, W., Mukherjee, M., Le, N. T., Chow, Y.-W., & Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information 2024, Vol. 15, 15*(2). https://doi.org/10.3390/INFO15020117

Mulyono, H., Pratama, A., & Novita, R. (2023). Peningkatan Kompetensi Siswa pada Network Security di SMKN 6 Padang. *Jurnal Pustaka Mitra (Pusat Akses Kajian Mengabdi Terhadap Masyarakat)*, *3*(3), 131–134. https://doi.org/10.55382/JURNALPUSTAKAMITRA.V3I3.476

Pasha, D., Rahayu, M., & Saputra, V. H. (2024). Pelatihan Keamanan Jaringan untuk Antisipasi Kejahatan Cyber Untuk Siswa SMK N 1 Padang Cermin. *Jurnal Abdimas Teknologi Inforamasi Dan Digitalisasi (JATI-DIG)Jati-Dig*, *1*(2), 44–48. https://doi.org/10.58602/jati-dig.v1i2.32

Prasetia, O., Machfud, S., & Ibnurhus, G. A. (2024). Sosialiasi Pengenalan Pentingnya Cyber Security Guna Menjaga Keamanan Data di Era Digital Pada Siswa/i SMK Bakti Idhata Jakarta. *JIPM: Jurnal Inovasi Pengabdian Masyarakat*, *2*(1), 16–20. https://doi.org/10.55903/JIPM.V2I1.141

Rakhmat Sani, R., Ghozi, W., Adi Rafrastara, F., Rahmawan Pramudya, E., & Shinta Sari, W. (2025). Penyuluhan dan Pelatihan Dasar Keamanan Siber pada Siswa SMK Muhammadiyah 1 Semarang. In *Jurnal Nasional Pengabdian Masyarakat Ilmu Komputer)* (Vol. 4, Issue 2).

Rivaldi, O., & Marpaung, N. L. (2023). *Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata*. *8*(1), 2023.