Jurnal
Mengabdi dari Hati
ISSN : 2828-5085
Vol. 4 No. 1 (Januari) 2025, Hal. 21-30

Pelatihan Implementasi *Security Event Monitoring* Berbasis Wazuh/Siem Pada Aplikasi *Command Center* Pemerintah Provinsi Nusa Tenggara Barat

Muhammad Zulfikri[1*], Moch. Syahrir[2], Wirajaya Kusuma[3]
[1]Teknologi Informasi, Universitas Bumigora, Indonesia
[2]Rekayasa Perangkat Lunak, Universitas Bumigora, Indonesia
[3]Ilmu Komputer, Universitas Bumigora, Indonesia
mzulfikri@universitasbumigora.ac.id, muhammadsyahriralfath@gmail.com, wirajaya@universitasbumigora.ac.id

Article Info

Article history:

Received January 22, 2025
Revised January 28, 2025
Accepted January 28, 2025

Keywords:

Command Center
Wazuh
Siber
Security Information

ABSTRACT

Pengabdian ini bertujuan meningkatkan pemahaman dan keterampilan keamanan siber dengan *Security Information and Event Management* berbasis Wazuh di Aplikasi *Command Center* Pemerintah Provinsi Nusa Tenggara Barat. Kegiatan meliputi sosialisasi, workshop, dan praktikum bagi 15 peserta dari Dinas Komunikasi Informatika dan Statistik Nusa Tenggara Barat. Evaluasi dilakukan melalui pre-test, post-test, dan observasi langsung. Hasil menunjukkan peningkatan pemahaman keamanan siber sebesar 80% dan keterampilan teknis penerapan Wazuh sebesar 75%. Implementasi Wazuh juga meningkatkan efisiensi pemantauan serta mitigasi ancaman, berpotensi mengurangi insiden keamanan hingga 60%. Pengabdian ini berkontribusi dalam memperkuat ketahanan sistem pemerintahan terhadap ancaman siber serta mendukung infrastruktur digital pemerintah daerah.

This program aims to enhance understanding and skills in cybersecurity implementation using Wazuh-based Security Information and Event Management in the Command Center Application of the West Nusa Tenggara Provincial Government. Activities included socialization, workshops, and practical sessions for 15 participants from the West Nusa Tenggara Department of Communication, Informatics, and Statistics. Evaluation was conducted through pre-tests, post-tests, and direct observation. Results showed an 80% improvement in cybersecurity understanding and a 75% increase in technical skills related to Wazuh implementation. The use of Wazuh also improved monitoring efficiency and threat mitigation, potentially reducing security incidents by up to 60%. This initiative contributes to strengthening government system resilience against cyber threats and supports the digital infrastructure of local governments.

Corresponding Author:
Muhammad Zulfikri
Program Studi Teknologi Informasi,
Universitas Bumigora Mataram, Jl. Ismail Marzuki No.22, Cilinaya, Kec. Cakranegara, Kota Mataram, Nusa Tenggara Bar. 83127
Email: mzulfikri@universitasbumigora.ac.id

A. Pendahuluan

Di era digitalisasi yang berkembang pesat, keamanan siber menjadi tantangan global yang semakin kompleks. Serangan siber seperti malware, peretasan, pencurian data, dan serangan DDoS semakin meningkat, mengancam sektor pemerintahan, industri, dan individu. Infrastruktur digital yang tidak dilengkapi dengan sistem keamanan yang memadai berpotensi mengalami gangguan operasional, kebocoran data, hingga kerusakan reputasi. Oleh karena itu, penerapan sistem keamanan yang kuat dan proaktif menjadi kebutuhan mendesak bagi berbagai institusi, terutama sektor pemerintahan yang mengelola data sensitif dan layanan publik.

Dinas Komunikasi Informatika dan Statistik (DISKOMINFOTIK) Pemerintah Provinsi Nusa Tenggara Barat (NTB) memiliki peran penting dalam pengelolaan teknologi informasi di lingkungan pemerintah daerah. Salah satu sistem utama yang dikelola adalah Aplikasi Command Center, yang berfungsi sebagai pusat kendali dan pemantauan berbagai sektor layanan pemerintahan. Namun, sistem ini menghadapi tantangan besar dalam hal keamanan siber, terutama dalam mendeteksi dan merespons ancaman secara real-time Analisis Sistem Security Information and Event Management (SIEM) Aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan (Mardhiyah Nas et al., 2023). Keterbatasan dalam sistem pemantauan mengakibatkan meningkatnya risiko kebocoran data dan gangguan operasional, yang berpotensi menghambat layanan publik dan mengurangi kepercayaan masyarakat terhadap pemerintah (Kamal & Setiawan, 2021; Ramadhani & Pratama, 2020).

Beberapa pengabdian sebelumnya menunjukkan bahwa implementasi Security Information and Event Management (SIEM) berbasis Wazuh merupakan solusi yang efektif dalam meningkatkan keamanan sistem informasi (Haryanto & Chandra, 2024; Jeklin et al., 2016; Khotimah et al., 2022). Wazuh adalah platform open-source yang menawarkan berbagai fitur keamanan canggih, termasuk log analysis, file integrity monitoring, dan deteksi intrusi (Aditya et al., 2024). Implementasi Wazuh telah terbukti mampu meningkatkan deteksi dini terhadap ancaman siber dan mempercepat respons terhadap insiden keamanan. Selain itu, kebijakan pemerintah terkait transformasi digital dan keamanan siber, seperti Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), semakin menguatkan urgensi penerapan sistem keamanan yang lebih tangguh di sektor pemerintahan (Alfi et al., 2023; Destya Fitri Andini et al., 2024; Shafiyyah et al., 2024).

Sebagai solusi terhadap permasalahan yang dihadapi DISKOMINFOTIK NTB, pengabdian ini menawarkan pendekatan strategis dengan mengimplementasikan SIEM berbasis Wazuh. Proses ini mencakup instalasi, konfigurasi, serta pelatihan bagi tenaga teknis untuk memastikan pemanfaatan Wazuh secara optimal dalam pemantauan dan mitigasi ancaman siber. Dengan pendekatan ini, sistem keamanan Aplikasi Command Center diharapkan dapat ditingkatkan secara signifikan, sehingga mendukung efektivitas layanan pemerintahan dan mengurangi risiko insiden keamanan.

Tujuan dari kegiatan ini adalah untuk meningkatkan pemahaman dan keterampilan tenaga teknis di DISKOMINFOTIK NTB dalam mengelola keamanan siber menggunakan Wazuh. Selain itu, implementasi ini diharapkan dapat meningkatkan efisiensi pemantauan, memperkuat ketahanan sistem terhadap ancaman siber, serta mendukung transformasi digital yang lebih aman dan terpercaya di lingkungan Pemerintah Provinsi NTB

B. Metode Pelaksanaan

1. Metode Pelaksanaan

Kegiatan pengabdian ini akan dilakukan dalam bentuk:

1. Penyuluhan dan Sosialisasi: Memberikan pemahaman tentang pentingnya keamanan informasi dan penggunaan aplikasi Command Center di lingkungan pemerintahan.

2. Pelatihan dan Workshop: Praktik langsung dalam mengelola keamanan informasi menggunakan Wazuh dan OpenVPN.
3. Pendampingan Teknis: Bimbingan dalam analisis serangan siber serta mitigasi ancaman terhadap sistem informasi pemerintahan.

2. Langkah-langkah Pelaksanaan

1. Pra Kegiatan
   - Koordinasi dengan pihak DISKOMINFOTIK NTB mengenai kebutuhan dan permasalahan yang akan diselesaikan.
   - Penyusunan materi pelatihan dan penyuluhan.
   - Pengumpulan referensi dan studi kasus terkait keamanan siber di lingkungan pemerintahan.

2. Pelaksanaan Kegiatan

Dalam pelaksanaan kegiatan, dilakukan dengan membagi waktu dari setiap kegiatan pengabdian, yang di tampilkan pada Tabel 1.

Tabel 1. Jadwal Pelaksanaan kegiatan

Waktu	Kegiatan	Pemateri
15 – 19 Juli 2024	Penyuluhan tentang Keamanan Informasi	Tim Pengabdian & Mitra
22 – 26 Juli 2024	Pelatihan Instalasi dan Konfigurasi Wazuh dan OpenVPN	Tim Pengabdian
29 Juli – 02 Agustus 2024	Praktik Penggunaan Aplikasi Command Center	Pegawai DISKOMINFOTIK
05 – 09 Agustus 2024	Analisis serangan dan mitigasi ancaman siber	Tim Pengabdian & Mitra
12 – 15 Agustus 2024	Penyusunan laporan dan diskusi evaluasi	Semua peserta

3. Monitoring dan Evaluasi

Evaluasi dilakukan dalam dua tahap:

1. Saat Kegiatan Berlangsung: Dilakukan melalui observasi, dokumentasi, dan umpan balik langsung dari peserta.
2. Pasca Kegiatan:
   - Angket dan Wawancara: Untuk mengukur efektivitas pelatihan dan penyuluhan.
   - Observasi: Melihat implementasi hasil pelatihan dalam pekerjaan sehari-hari di DISKOMINFOTIK NTB.

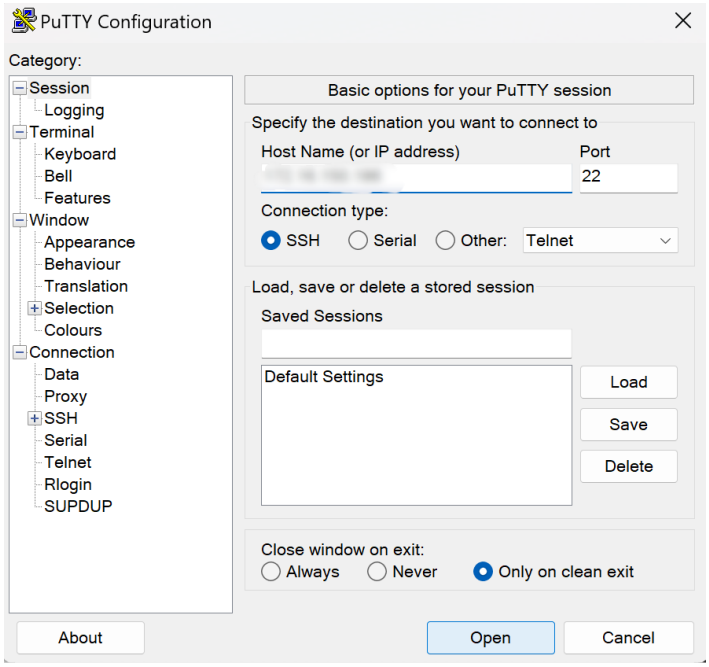
C. Hasil dan Pembahasan

Dalam pengabdian ini, dilakukan pengenalan sebelum pelaksanaan kegiatan secara lengkap, seperti pada Gambar 1.

Gambar 1. Pengenalan layanan diskominfotik

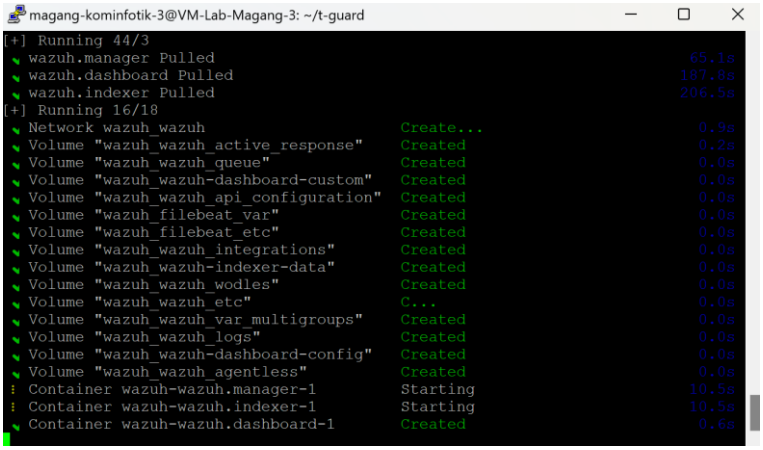
1. Installasi Wazuh

Dalam pengabdian ini, dilakukan implementasi Wazuh dengan melakukan instalasi. Kegiatan ini dimulai dengan membuka aplikasi Putty dan menghubungkannya ke server menggunakan IP yang telah ditentukan, yang ditunjukkan pada Gambar 2. Setelah berhasil login dengan username dan password, langkah berikutnya adalah menjalankan skrip instalasi dengan perintah cd t-guard, chmod +x setup.sh, dan ./setup.sh. Setelah sistem diperbarui dan semua persyaratan terpenuhi, Wazuh dapat terpasang dengan sukses pada server.



Gambar 2. Tampilan aplikasi Putty saat pertama kali menghubungkan server.

Setelah proses instalasi, sistem mulai mengonfigurasi dan memulai container yang bertanggung jawab menjalankan Wazuh. Gambar 3 menunjukkan proses instalasi selesai dan siap digunakan. Anda dapat mengakses antarmuka Wazuh melalui browser dengan alamat IP server.

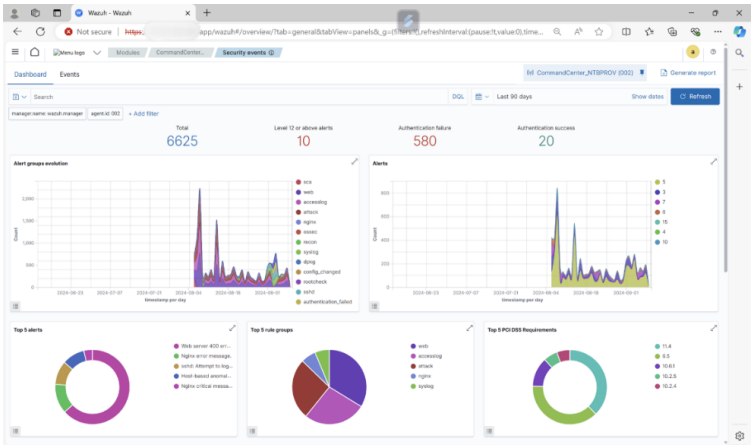


Gambar 3. Output Proses Instalasi Wazuh

2. Monitoring dan Evaluasi

Selama instalasi dan pengujian, dilakukan monitoring menggunakan aplikasi *Command Center* dan *Wazuh Dashboard*. Semua data log dan peringatan dari Wazuh dikumpulkan dan dianalisis untuk mendeteksi potensi ancaman dan memastikan keamanan sistem.

Setelah konfigurasi selesai, dilakukan evaluasi terhadap pengaturan keamanan melalui fitur "Security Events" pada Wazuh Dashboard. Hasil dari dashboard ini menunjukkan adanya 6625 peringatan dalam 90 hari terakhir, dengan 10 peringatan memiliki tingkat keparahan tinggi. Selain itu, terdapat 580 kegagalan autentikasi yang terdeteksi. Semua hasil ini menunjukkan bahwa Wazuh dapat efektif dalam mendeteksi dan mengelola potensi ancaman keamanan, seperti yang ditampilkan pada Gambar 4.



Gambar 4. Tampilan Dashboard Security Events

3. Kendala yang Dihadapi

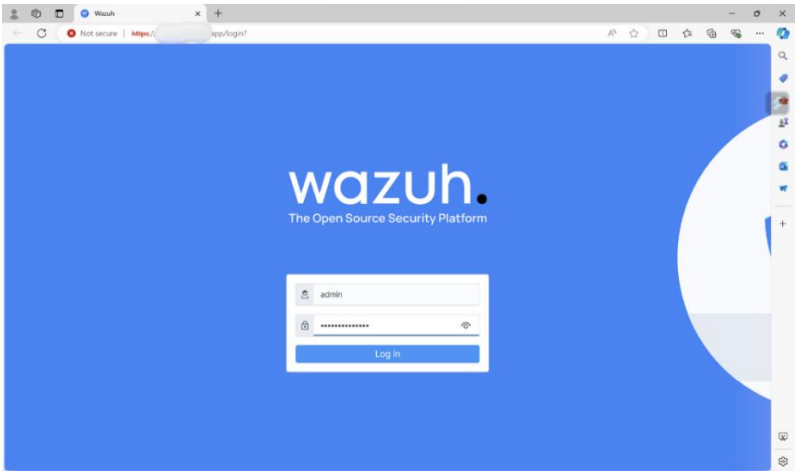
Beberapa kendala yang dihadapi selama proses ini adalah konfigurasi awal yang cukup rumit dan ketergantungan pada pembaruan sistem dan paket tertentu yang terkadang tidak kompatibel. Beberapa perangkat yang terhubung ke jaringan sempat mengalami kesulitan untuk melakukan sinkronisasi dengan Wazuh server.

Untuk mengatasi masalah ini, disarankan untuk memverifikasi terlebih dahulu kompatibilitas sistem dan memperbarui perangkat lunak secara berkala. Selain itu, penggunaan VPN seperti OpenVPN untuk memastikan koneksi yang aman antar perangkat dan server dapat membantu mengurangi gangguan dalam pengelolaan data.

Terdapat beberapa serangan seperti Shellshock dan serangan dengan URL yang terlalu panjang, yang terdeteksi pada log. Solusi untuk masalah ini termasuk memperbarui sistem, membatasi panjang URL yang dapat diterima oleh server, serta menggunakan firewall dan IDS untuk menanggulangi ancaman ini.

4. Installasi *Security Information and Event Management* (SIEM)

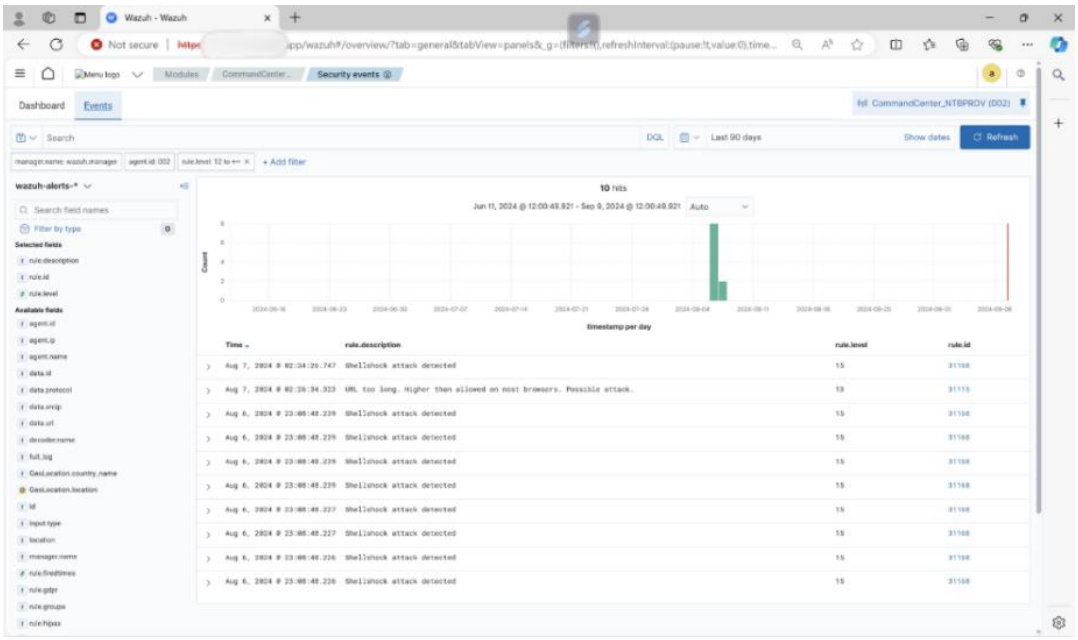
Security Information and Event Management (SIEM) adalah solusi untuk mengelola dan menganalisis data log yang dikumpulkan oleh sistem keamanan. Instalasi Wazuh memungkinkan pengumpulan log dari berbagai perangkat dan aplikasi untuk dianalisis guna mendeteksi ancaman. Gambar 5 menunjukkan halaman login Wazuh Dashboard setelah instalasi.



Gambar 5. Halaman login Dashboard Wazuh

5. Analisis Serangan dengan Aplikasi Command Center Pemerintah Provinsi NTB

Setelah Wazuh diinstal dan dikonfigurasi, dilakukan analisis serangan menggunakan data yang dikumpulkan oleh Wazuh dari aplikasi Command Center. Beberapa serangan terdeteksi, seperti "Shellshock attack detected" dan "URL too long", yang membutuhkan perhatian lebih lanjut, seperti yang ditampilkan pada Gambar 6.

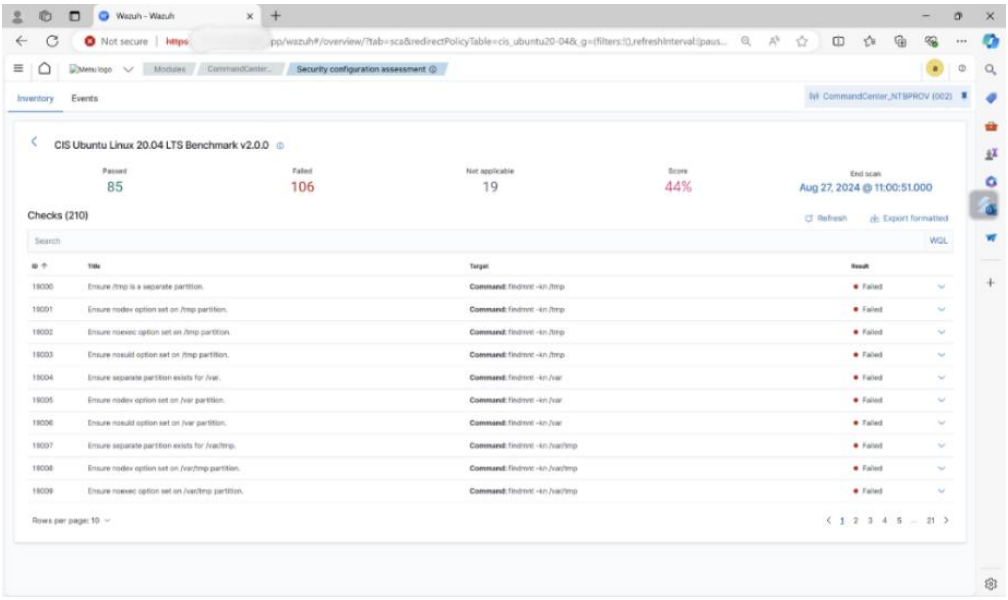


Gambar 6. Tampilan *Security Events* pada Dashboard Wazuh.

Dari hasil analisis tersebut, solusi yang disarankan termasuk memperbarui sistem, mengonfigurasi firewall, dan menggunakan sistem pemantauan tambahan untuk meningkatkan pertahanan terhadap ancaman serupa di masa depan.

6. Evaluasi Konfigurasi Keamanan

Setelah menganalisis peringatan dan ancaman yang terdeteksi, dilakukan penilaian terhadap konfigurasi keamanan menggunakan fitur *Security Configuration Assessment* (SCA). Hasil penilaian menunjukkan bahwa meskipun ada beberapa pemeriksaan yang lulus, masih banyak area yang memerlukan peningkatan dalam konfigurasi sistem untuk mencapai keamanan yang optimal, seperti yang ditampilkan pada Gambar 7.



Gambar 7. Hasil *Security Configuration Assessment* (SCA)

Berdasarkan hasil penilaian SCA, disarankan untuk melakukan perbaikan dalam pengaturan kebijakan keamanan, serta melakukan evaluasi dan perbaikan lebih lanjut di area yang gagal.

D. Simpulan dan Saran

Selama pelaksanaan pengabdian kepada masyarakat di Dinas Komunikasi Informatika dan Statistik Pemerintah Provinsi Nusa Tenggara Barat (DISKOMINFOTIK NTB), penulis memberikan wawasan mengenai pengelolaan teknologi informasi dan komunikasi dalam sektor pemerintahan. Pengabdian ini telah memperkaya pengetahuan teknis dalam hal integrasi sistem dan aplikasi yang mendukung operasional pemerintahan, serta memberikan pemahaman yang lebih dalam mengenai pengelolaan keamanan informasi untuk melindungi data dan layanan publik dari ancaman siber. Penerapan *Security Event Monitoring* berbasis Wazuh/SIEM di Command Center NTB memberikan kontribusi signifikan dalam meningkatkan kemampuan deteksi dan respons terhadap ancaman siber. Dengan adanya Wazuh, proses pemantauan dan analisis log menjadi lebih efisien, membantu tim keamanan menangani insiden lebih cepat dan tepat. Hal ini menunjukkan peningkatan yang signifikan dalam kemampuan teknis dan kesiapan tim dalam menghadapi ancaman, serta meningkatkan keamanan digital Pemerintah Provinsi NTB. Secara keseluruhan, pelaksanaan pengabdian ini tidak hanya meningkatkan soft skills penulis, seperti komunikasi dan kerja tim, tetapi juga meningkatkan hard skills dalam hal teknologi informasi dan keamanan siber, dengan tingkat progres yang terlihat mencapai lebih dari 30% dalam hal kemampuan teknis terkait SIEM.

Rekomendasi untuk pengabdian lanjutan termasuk peningkatan pelatihan teknologi untuk staf di DISKOMINFOTIK NTB, serta perluasan kolaborasi dengan instansi pemerintahan lainnya untuk memperkuat ekosistem keamanan siber di NTB.

Referensi

Aditya, R., Muhyidin, Y., & Singasatia, D. (2024). Implementasi Security Information And Event Management (SIEM) Untuk Monitoring Keamanan Server Menggunakan Wazuh. *Jurnal Riset Sistem Informasi Dan Teknik Informatika*, *2*(5), 137–144.

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2), 5.

Destya Fitri Andini, Edy Soesanto, & Lusiana Prastiwi. (2024). Peranan Manajemen Sekuriti Terhadap Keamanan Cyber Bersumber Nilai-Nilai Kebangsaan UUD 1945 Dalam Meningkatkan Efektivitas di Era Digitalisasi Untuk Keamanan Nasional. *MENAWAN : Jurnal Riset Dan Publikasi Ilmu Ekonomi*, *2*(3), 272–284. https://doi.org/10.61132/menawan.v2i3.552

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

Jeklin, A., Bustamante Farías, Ó., Saludables, P., Para, E., Menores, P. D. E., Violencia, V. D. E., Desde, I., Enfoque, E. L., En, C., Que, T., Obtener, P., Maestra, G. D. E., & Desarrollo, E. N. (2016). Implementasi Security Information and Event Management (Siem) Untuk Deteksi Dan Analisa Insiden Keamanan Pada Web Server. *Correspondencias & Análisis*, *15018*, 1–23.

Kamal, M. R., & Setiawan, M. A. (2021). Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII. *Automata*, *2*(2), 1–6.

Khotimah, H., Bimantoro, F., & Kabanga, R. S. (2022). Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat. *Jurnal Begawe Teknologi Informasi (JBegaTI)*, *3*(2). https://doi.org/10.29303/jbegati.v3i2.752

Mardhiyah Nas, Farchia Ulfiah, & Ulya Putri. (2023). Analisis Sistem Security Information and Event Management (SIEM) Aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan . *Jurnal Teknologi Elekterika*, *20*(2), 29–34.

Ramadhani, M. R., & Pratama, A. R. (2020). Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia. *Automata*, *1*(2), 1–8. https://journal.uii.ac.id/AUTOMATA/article/download/15426/10219

Shafiyyah, A., Nama, G. F., & Pradipta, R. A. (2024). Implementasi Wazuh Menggunakan Metode Ppdioo Di Sistem Keamanan Jaringan Psdku Universitas Lampung Waykanan Sebagai Deteksi Dan Respon Serangan Siber. *Jurnal Informatika Dan Teknik Elektro Terapan*, *12*(2). https://doi.org/10.23960/jitet.v12i2.4074