JURNAL KHATULISTIWA INFORMATIKA VOL. 14 NO. 1 Juni 2026
p-ISSN: 2339-1928 e-ISSN: 2579-633X Halaman : 14 – 20

EVALUASI EFEKTIVITAS SISTEM MONITORING INSIDEN SIBER BERBASIS WAZUH MENGGUNAKAN MODEL KEBERHASILAN SISTEM INFORMASI DELONE DAN MCLEAN PADA INSTANSI PEMERINTAH XYZ

Irman Nurjaman[1];Ismasari Nawangsih;[2] Anggi Alfin[3]

Program Studi Teknik Informatika, Fakultas Teknik
Universitas Pelita Bangsa
irmannurjaman.real@gmail.com, ismasari.n@pelitabangsa.ac.id, anggialfin@pelitabangsa.ac.id

INFO ARTIKEL

Diajukan :
07-04-2026

Diterima :
05-05-2026

Diterbitkan:
01-06-2026

Kata Kunci :
Wazuh, Security Information and Event Management (SIEM), Monitoring Insiden Siber, Keamanan Siber

INTISARI

Transformasi digital pada instansi pemerintah telah meningkatkan ketergantungan terhadap sistem informasi sekaligus memperbesar risiko ancaman keamanan siber. Kondisi tersebut mendorong kebutuhan akan implementasi *Security Information and Event Management* (SIEM) yang mampu mendukung pemantauan, deteksi, dan respons terhadap insiden keamanan secara terintegrasi. Wazuh merupakan salah satu platform SIEM berbasis *open source* yang banyak diimplementasikan karena fleksibilitas dan efisiensi biaya. Namun, sebagian besar penelitian terdahulu masih berfokus pada aspek teknis implementasi, sedangkan evaluasi keberhasilan sistem dari perspektif pengguna, khususnya pada instansi pemerintah, masih relatif terbatas. Penelitian ini bertujuan mengevaluasi efektivitas penerapan sistem monitoring insiden siber berbasis Wazuh di Instansi Pemerintah XYZ menggunakan Model Keberhasilan Sistem Informasi DeLone dan McLean. Penelitian menggunakan metode deskriptif kuantitatif dengan pendekatan evaluatif. Data dikumpulkan melalui observasi terhadap dashboard Wazuh serta penyebaran kuesioner skala Likert kepada pengguna yang dipilih menggunakan teknik *purposive sampling*. Analisis dilakukan melalui uji validitas dan reliabilitas instrumen, perhitungan nilai rata-rata pada setiap dimensi, klasifikasi tingkat efektivitas, serta analisis naratif terhadap log keamanan yang dihasilkan sistem. Hasil penelitian menunjukkan bahwa implementasi Wazuh memperoleh nilai rata-rata keseluruhan sebesar 4,26 yang termasuk dalam kategori Sangat Efektif**.** Dimensi dengan nilai tertinggi adalah Penggunaan (4,43), diikuti Manfaat Bersih (4,36) dan Kualitas Layanan (4,36), sedangkan Kualitas Informasi memperoleh nilai terendah sebesar 4,21 sehingga masih memerlukan optimalisasi, terutama melalui penyempurnaan aturan deteksi (*ruleset*) untuk mengurangi *false positive*. Analisis log juga menunjukkan bahwa sistem mampu mendeteksi percobaan *brute force* dan *failed login* secara hampir *real-time*, sehingga mendukung peningkatan kemampuan deteksi dini dan respons insiden keamanan siber di lingkungan instansi pemerintah.

I. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong transformasi digital pada berbagai sektor, termasuk instansi pemerintah. Digitalisasi proses bisnis melalui penerapan sistem informasi bertujuan meningkatkan efisiensi operasional, kualitas layanan publik, transparansi, serta akuntabilitas penyelenggaraan pemerintahan. Di sisi lain, peningkatan ketergantungan terhadap teknologi informasi juga diikuti oleh meningkatnya risiko ancaman keamanan siber yang berpotensi mengganggu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi sebagai tiga prinsip utama keamanan informasi (CIA Triad) (Putri et al., 2024).

Instansi pemerintah menjadi salah satu sektor yang paling rentan terhadap serangan siber karena mengelola berbagai informasi

strategis dan layanan publik yang harus tersedia secara berkelanjutan. Berbagai bentuk serangan, seperti *brute force attack*, pencurian kredensial (*credential theft*), eksploitasi kerentanan sistem, *malware*, hingga akses ilegal terhadap server dan aplikasi internal, berpotensi menyebabkan gangguan operasional, kebocoran data, maupun penurunan kepercayaan masyarakat terhadap layanan pemerintah. Oleh karena itu, organisasi sektor publik memerlukan mekanisme pemantauan keamanan yang mampu mendeteksi ancaman secara cepat dan mendukung proses respons insiden secara efektif.

Salah satu pendekatan yang banyak diterapkan untuk mendukung pengelolaan keamanan siber adalah *Security Information and Event Management* (SIEM). Teknologi SIEM berfungsi mengumpulkan, mengintegrasikan, mengorelasikan, menganalisis, serta menyajikan data log dari berbagai perangkat dan aplikasi secara terpusat sehingga memudahkan organisasi dalam mendeteksi aktivitas yang mencurigakan, melakukan investigasi insiden, dan mendukung pengambilan keputusan keamanan informasi. (Anggraini & Widhiantoro, 2023).

Di antara berbagai platform SIEM, Wazuh merupakan solusi berbasis *open source* yang banyak diimplementasikan karena menawarkan fleksibilitas konfigurasi, kemudahan integrasi dengan berbagai perangkat keamanan, serta efisiensi biaya implementasi. Wazuh menyediakan berbagai fitur keamanan, seperti *host-based intrusion detection*, analisis log, pemantauan integritas berkas (*file integrity monitoring*), pemindaian kerentanan (*vulnerability assessment*), serta integrasi dengan berbagai perangkat pendukung keamanan lainnya. Karakteristik tersebut menjadikan Wazuh sebagai alternatif yang sesuai bagi instansi pemerintah yang membutuhkan sistem pemantauan keamanan siber dengan biaya implementasi yang relatif rendah namun tetap memiliki kemampuan deteksi yang memadai. (Wazuh, 2025)

Beberapa penelitian terdahulu menunjukkan bahwa implementasi Wazuh mampu meningkatkan efektivitas deteksi ancaman keamanan siber. Sutanto dan Rakhman (2025) melaporkan bahwa integrasi Wazuh dengan Grafana meningkatkan visibilitas terhadap aktivitas keamanan dan mempercepat proses identifikasi ancaman. Sementara itu, Rafiqul Islam dan Rafique (2024) menunjukkan bahwa implementasi Wazuh pada berbagai lingkungan sistem operasi mampu mendukung proses mitigasi ancaman secara efektif melalui pemantauan log secara *real-time*. Meskipun demikian, sebagian besar penelitian tersebut masih berfokus pada aspek teknis implementasi, seperti kemampuan deteksi, integrasi sistem, maupun performa aplikasi. (Sutanto & Rakhman, 2025) (Rafiqul Islam & Rafique, 2024).

Keberhasilan implementasi suatu sistem informasi tidak hanya ditentukan oleh kemampuan teknis sistem, tetapi juga dipengaruhi oleh kualitas informasi yang dihasilkan, kualitas layanan pendukung, tingkat penggunaan, kepuasan pengguna, serta manfaat yang dirasakan oleh organisasi. Dengan kata lain, sistem yang memiliki kemampuan teknis yang baik belum tentu memberikan manfaat optimal apabila tidak diterima dan dimanfaatkan secara efektif oleh penggunanya.

Berdasarkan telaah literatur, penelitian mengenai evaluasi implementasi SIEM berbasis Wazuh dari perspektif pengguna pada lingkungan instansi pemerintah masih relatif terbatas. Sebagian besar penelitian lebih menitikberatkan pada pengujian performa teknis sistem dibandingkan evaluasi keberhasilan implementasi secara menyeluruh. Kondisi tersebut menunjukkan adanya *research gap* yang perlu dikaji lebih lanjut, khususnya mengenai bagaimana kualitas sistem, kualitas informasi, kualitas layanan, tingkat penggunaan, kepuasan pengguna, serta manfaat yang dirasakan setelah implementasi Wazuh di lingkungan pemerintahan.

Untuk mengisi kesenjangan penelitian tersebut, penelitian ini menggunakan Model Keberhasilan Sistem Informasi DeLone dan McLean sebagai kerangka evaluasi. Model ini merupakan salah satu model evaluasi sistem informasi yang paling banyak digunakan karena mampu mengukur keberhasilan implementasi sistem melalui enam dimensi utama, yaitu Kualitas Sistem (*System Quality*), Kualitas Informasi (*Information Quality*), Kualitas Layanan (*Service Quality*), Penggunaan (*Use*), Kepuasan Pengguna (*User Satisfaction*), dan Manfaat Bersih (*Net Benefits*)(DeLone & McLean, 2003).Keenam dimensi tersebut memberikan gambaran yang komprehensif mengenai keberhasilan implementasi sistem informasi, baik dari aspek teknis maupun dari perspektif pengguna.

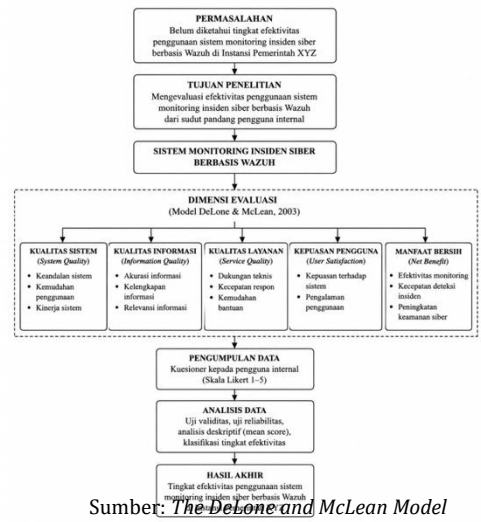
Berdasarkan latar belakang tersebut, penelitian ini bertujuan mengevaluasi efektivitas penerapan sistem monitoring insiden siber berbasis Wazuh pada Instansi Pemerintah XYZ menggunakan Model Keberhasilan Sistem Informasi DeLone dan McLean. Evaluasi dilakukan melalui analisis persepsi pengguna terhadap enam dimensi model tersebut serta

didukung oleh analisis log keamanan yang dihasilkan sistem Wazuh. Hasil penelitian diharapkan dapat memberikan kontribusi praktis sebagai dasar evaluasi implementasi SIEM pada instansi pemerintah sekaligus memperkaya kajian akademik mengenai evaluasi sistem keamanan informasi berbasis *open source* dari perspektif pengguna.

II. BAHAN DAN METODE

Penelitian ini menggunakan metode deskriptif kuantitatif dengan pendekatan evaluatif untuk menilai efektivitas implementasi sistem monitoring insiden siber berbasis Wazuh di Instansi Pemerintah XYZ. Pendekatan evaluatif dipilih karena penelitian tidak hanya mendeskripsikan kondisi implementasi sistem, tetapi juga mengukur tingkat keberhasilan penerapannya berdasarkan persepsi pengguna dengan menggunakan Model Keberhasilan Sistem Informasi DeLone dan McLean (DeLone & McLean, 2003)

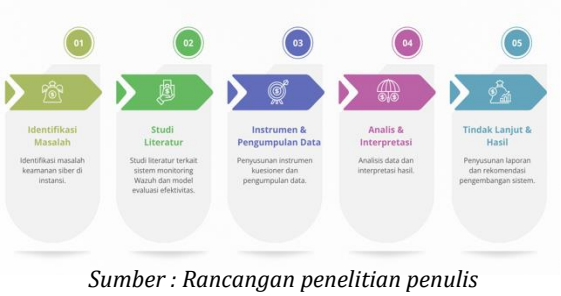
Kerangka evaluasi mengacu pada enam dimensi utama Model Keberhasilan Sistem Informasi DeLone dan McLean, yaitu Kualitas Sistem (*System Quality*), Kualitas Informasi (*Information Quality*), Kualitas Layanan (*Service Quality*), Penggunaan (*Use*), Kepuasan Pengguna (*User Satisfaction*), dan Manfaat Bersih (*Net Benefits*). Keenam dimensi tersebut digunakan untuk mengevaluasi kualitas implementasi sistem monitoring insiden siber secara menyeluruh, baik dari aspek teknis maupun dari perspektif pengguna.



Sumber: *The DeLone and McLean Model*

Gambar *1*. Kerangka Pemikiran

Objek penelitian adalah sistem monitoring insiden siber berbasis Wazuh yang telah diimplementasikan pada Instansi Pemerintah XYZ. Responden penelitian terdiri atas pegawai yang terlibat secara langsung dalam pengoperasian maupun pengelolaan sistem, meliputi administrator sistem, operator dashboard, dan staf teknis keamanan informasi. Pemilihan responden dilakukan menggunakan teknik *purposive sampling*, yaitu teknik pengambilan sampel berdasarkan pertimbangan bahwa responden memiliki pengetahuan dan pengalaman dalam penggunaan sistem Wazuh sehingga mampu memberikan penilaian yang relevan terhadap implementasi sistem.



Sumber : Rancangan penelitian penulis

Gambar 2. Alur Penelitian

Instrumen penelitian berupa kuesioner yang disusun berdasarkan enam dimensi Model Keberhasilan Sistem Informasi DeLone dan McLean dengan menggunakan skala Likert lima tingkat. Skor penilaian terdiri atas: (1) Sangat Tidak Setuju, (2) Tidak Setuju, (3) Netral, (4) Setuju, dan (5) Sangat Setuju. Selain penyebaran kuesioner, pengumpulan data juga dilakukan melalui observasi langsung terhadap dashboard Wazuh untuk memperoleh informasi mengenai aktivitas log, kategori insiden, tingkat keparahan (*severity level*), serta pola serangan yang terdeteksi, seperti *brute force attack* dan *failed login*.

Tabel 1. Skala Penilaian Kuisioner (Skala Likert)

Skor	Kategori
1	Sangat Tidak Setuju
2	Tidak Setuju
3	Netral
4	Setuju
5	Sangat Setuju

Sumber : Data primer penelitian

Sebelum dilakukan analisis, instrumen penelitian diuji melalui uji validitas dan uji reliabilitas untuk memastikan bahwa setiap butir pertanyaan mampu mengukur konstruk yang diteliti secara konsisten. Selanjutnya, analisis deskriptif dilakukan dengan menghitung nilai rata-rata (*mean*) pada setiap dimensi evaluasi.

Persamaan yang digunakan untuk menghitung nilai rata-rata adalah sebagai berikut.

$$Mean = \frac{\sum x}{n}$$

$\sum x$ = Jumlah seluruh skor responden dalam satu dimensi
n = jumlah responden

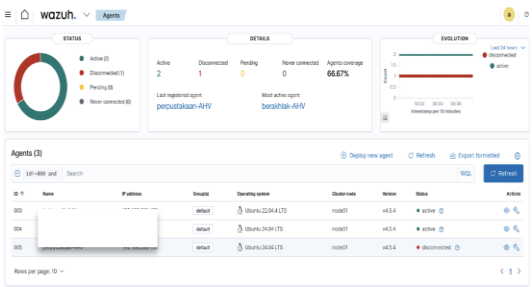
Nilai rata-rata yang diperoleh kemudian diklasifikasikan berdasarkan tingkat efektivitas sebagaimana ditunjukkan pada Tabel 2.

Tabel 2. Klasifikasi Tingkat Efektivitas

Interval Skor	Kategori Efektivitas
4.21 – 5.00	Sangat Efektif
3.41 – 4.20	Efektif
2.61 – 3.40	Cukup Efektif
1.81 – 2.60	Kurang Efektif
1.00 – 1.80	Tidak Efektif

Sumber: Hasil olahan data penelitian

Selain analisis kuantitatif, penelitian ini juga melakukan analisis deskriptif terhadap log keamanan yang dihasilkan oleh sistem Wazuh. Analisis tersebut bertujuan mengidentifikasi pola serangan, frekuensi kejadian, kategori peringatan (*alert*), serta kemampuan sistem dalam mendeteksi insiden keamanan secara hampir *real-time*. Hasil analisis log digunakan sebagai data pendukung untuk memperkuat interpretasi terhadap hasil evaluasi berdasarkan persepsi pengguna.



Sumber : Pusat Data dan Informasi Instansi XYZ
Gambar *3*. Dashboard Wazuh

Data yang telah dianalisis disajikan dalam bentuk tabel, grafik, dan uraian deskriptif untuk memberikan gambaran mengenai tingkat efektivitas implementasi sistem monitoring insiden siber berbasis Wazuh berdasarkan masing-masing dimensi Model Keberhasilan Sistem Informasi DeLone dan McLean. Selain itu, hasil observasi terhadap log keamanan digunakan sebagai data pendukung dalam menginterpretasikan temuan penelitian.

III. HASIL DAN PEMBAHASAN

Hasil Penelitian

Hasil penelitian diperoleh melalui analisis kuesioner yang disusun berdasarkan enam dimensi Model Keberhasilan Sistem Informasi DeLone dan McLean, yaitu Kualitas Sistem (*System Quality*), Kualitas Informasi (*Information Quality*), Kualitas Layanan (*Service Quality*), Penggunaan (*Use*), Kepuasan Pengguna (*User Satisfaction*), dan Manfaat Bersih (*Net Benefits*). Selain itu, observasi terhadap dashboard Wazuh dilakukan untuk mengidentifikasi karakteristik insiden keamanan siber yang terdeteksi selama periode pengamatan.

Berdasarkan hasil analisis, implementasi sistem monitoring insiden siber berbasis Wazuh di Instansi Pemerintah XYZ memperoleh nilai rata-rata keseluruhan sebesar 4,26**,** sehingga termasuk dalam kategori Sangat Efektif**.** Hasil tersebut menunjukkan bahwa sistem telah mampu mendukung aktivitas pemantauan keamanan siber secara efektif berdasarkan persepsi pengguna.

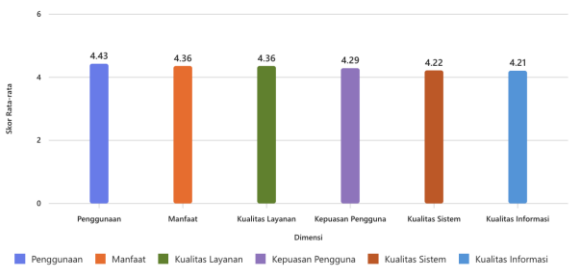
Ringkasan hasil evaluasi pada masing-masing dimensi disajikan pada Tabel 3.

Tabel 3. Ringkasan skor per dimensi (Model DeLone & McLean)

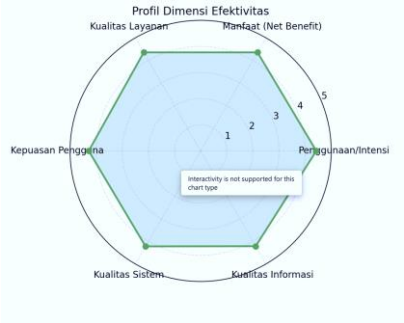
Dimensi	Skor Rata-rata	Kategori
Penggunaan	4,43	Sangat Efektif
Manfaat (Net Benefit)	4,36	Sangat Efektif
Kualitas Layanan	4,36	Sangat Efektif
Kepuasan Pengguna	4,29	Sangat Efektif
Kualitas Sistem	4,22	Sangat Efektif
Kualitas Informasi	4,21	Sangat Efektif

Sumber: (DeLone & McLean, 2003)

Berdasarkan Tabel 3, seluruh dimensi memperoleh nilai rata-rata di atas 4,21 sehingga termasuk dalam kategori Sangat Efektif. Dimensi Penggunaan (*Use*) memperoleh skor tertinggi sebesar 4,43**,** diikuti oleh Manfaat Bersih (*Net Benefits*) dan Kualitas Layanan (*Service Quality*) yang masing-masing memperoleh skor 4,36**.** Sementara itu, dimensi Kualitas Informasi (*Information Quality*) memperoleh skor terendah, yaitu 4,21**,** meskipun masih berada pada kategori Sangat Efektif**.** Temuan ini menunjukkan bahwa implementasi Wazuh telah memberikan manfaat yang signifikan bagi pengguna, namun kualitas informasi yang dihasilkan masih memerlukan optimalisasi lebih lanjut.



Sumber : Hasil olah data penelitian
Gambar *4*. Grafik Batang Rata-rata Skor per Dimensi



Sumber : Hasil olah data penelitian
Gambar *5*. Grafik Radar Profil Dimensi Efektivitas

Selain hasil kuesioner, penelitian ini juga melakukan observasi terhadap log keamanan yang dihasilkan oleh sistem Wazuh selama periode 19–20 Desember 2025. Hasil observasi menunjukkan bahwa sistem berhasil mendeteksi berbagai aktivitas keamanan yang terjadi pada lingkungan Instansi Pemerintah XYZ.

Sebagian besar peringatan (*alert*) berasal dari aktivitas umum sistem sebanyak 18.968 kejadian, diikuti oleh 5.760 percobaan *failed login* yang mengindikasikan adanya upaya *brute force attack*, serta 5.715 aktivitas *successful login*. Temuan tersebut menunjukkan bahwa percobaan akses tidak sah merupakan salah satu jenis aktivitas yang paling sering terdeteksi selama periode pengamatan.

Kemampuan Wazuh dalam menghasilkan notifikasi hampir secara *real-time* memberikan keuntungan bagi administrator untuk melakukan identifikasi dini terhadap aktivitas mencurigakan sebelum berkembang menjadi insiden keamanan yang lebih serius.

Tabel 4. Ringkasan Aktivitas Log Keamanan Wazuh Selama Periode Pengamatan (2025-12-19 s.d. 2025-12-20)

Kategori Serangan/Peristiwa	Jumlah Alert
Lainnya	18.968
Login Berhasil	5.715
Login Gagal	5.760

Sumber: Hasil olahan data penelitian

Pembahasan

Hasil penelitian menunjukkan bahwa implementasi sistem monitoring insiden siber berbasis Wazuh di Instansi Pemerintah XYZ telah berjalan secara efektif berdasarkan enam dimensi Model Keberhasilan Sistem Informasi DeLone dan McLean. Seluruh dimensi memperoleh kategori Sangat Efektif, yang mengindikasikan bahwa sistem tidak hanya memiliki kualitas teknis yang baik, tetapi juga mampu memberikan manfaat nyata bagi pengguna dalam mendukung aktivitas pemantauan keamanan siber.

Tingginya nilai pada dimensi Penggunaan (*Use*) menunjukkan bahwa informasi dan notifikasi yang dihasilkan oleh Wazuh telah dimanfaatkan secara aktif dalam proses operasional keamanan informasi. Kondisi tersebut mengindikasikan bahwa sistem telah terintegrasi dengan alur kerja organisasi sehingga mendukung pengambilan keputusan dalam proses identifikasi dan penanganan insiden keamanan siber. Temuan ini sejalan dengan Model Keberhasilan Sistem Informasi DeLone dan McLean yang menyatakan bahwa tingkat penggunaan sistem merupakan salah satu indikator penting keberhasilan implementasi sistem informasi.

Dimensi Manfaat Bersih (*Net Benefits*) juga menunjukkan bahwa implementasi Wazuh memberikan kontribusi terhadap peningkatan efektivitas pengelolaan keamanan informasi. Penyajian log secara terpusat serta kemampuan mendeteksi aktivitas mencurigakan secara hampir *real-time* membantu administrator mempercepat proses identifikasi ancaman dan meningkatkan efisiensi respons terhadap insiden keamanan.

Sementara itu, dimensi Kualitas Informasi (*Information Quality*) memperoleh nilai paling rendah dibandingkan dimensi lainnya. Meskipun masih termasuk kategori Sangat Efektif, kondisi tersebut menunjukkan bahwa kualitas penyajian informasi masih dapat ditingkatkan. Salah satu upaya yang dapat dilakukan adalah melakukan *fine-tuning* terhadap *ruleset* Wazuh, menyempurnakan mekanisme korelasi *alert*, serta menyesuaikan *custom decoder* sesuai karakteristik lingkungan organisasi. Optimalisasi tersebut berpotensi mengurangi *false positive*, meningkatkan relevansi informasi yang diterima pengguna, serta meminimalkan *alert fatigue* pada administrator keamanan.

Hasil observasi terhadap log keamanan mendukung temuan tersebut. Tingginya jumlah *failed login* yang teridentifikasi sebagai indikasi percobaan *brute force attack* menunjukkan bahwa Wazuh mampu mendeteksi aktivitas mencurigakan secara cepat sehingga administrator dapat melakukan tindakan mitigasi sebelum serangan berkembang menjadi insiden yang berdampak lebih luas. Dengan demikian, hasil penelitian ini memperkuat temuan penelitian terdahulu yang menyatakan bahwa Wazuh merupakan solusi SIEM berbasis

open source yang efektif dalam meningkatkan visibilitas keamanan serta mendukung proses deteksi dan respons insiden pada lingkungan organisasi.

Implikasi Penelitian

Temuan penelitian ini memberikan implikasi praktis, manajerial, dan teoritis terhadap implementasi sistem monitoring insiden siber berbasis *Security Information and Event Management* (SIEM) berbasis *open source* pada instansi pemerintah. Implikasi tersebut menunjukkan bahwa evaluasi keberhasilan implementasi sistem tidak hanya ditinjau dari kemampuan teknis dalam mendeteksi ancaman, tetapi juga dari kualitas sistem, kualitas informasi, kualitas layanan, tingkat penggunaan, kepuasan pengguna, serta manfaat yang dirasakan organisasi berdasarkan Model Keberhasilan Sistem Informasi DeLone dan McLean.

Dari sisi praktis, hasil penelitian ini menunjukkan bahwa penggunaan Wazuh mampu meningkatkan visibilitas terhadap aktivitas keamanan siber melalui penyajian log dan notifikasi insiden secara terpusat dan hampir real-time. Kondisi ini mendukung proses deteksi dini terhadap potensi ancaman, sehingga tim teknis dapat melakukan respons yang lebih cepat dan terkoordinasi. Dengan demikian, Wazuh dapat dipertimbangkan sebagai salah satu solusi pemantauan keamanan yang mendukung peningkatan kesiapsiagaan dan ketahanan siber instansi pemerintah.

Implikasi manajerial dari penelitian ini berkaitan dengan peran sistem Wazuh dalam mendukung pengambilan keputusan terkait keamanan informasi. Informasi keamanan yang dihasilkan oleh sistem menjadi sumber data yang relevan bagi pengelola dan pimpinan unit kerja dalam memahami tingkat risiko, menentukan prioritas pengamanan, serta merencanakan alokasi sumber daya secara lebih tepat. Namun demikian, hasil pada dimensi *Information Quality* menunjukkan bahwa diperlukan perhatian lebih lanjut terhadap pengelolaan dan penyajian informasi, khususnya dalam menyederhanakan struktur alert serta mengoptimalkan aturan deteksi agar informasi yang dihasilkan semakin mudah dipahami dan dimanfaatkan secara optimal.

Dari perspektif teoritis, penelitian ini memberikan kontribusi terhadap kajian evaluasi sistem keamanan informasi dengan mengadopsi Model Keberhasilan Sistem Informasi DeLone dan McLean sebagai kerangka analisis. Temuan penelitian memperkuat relevansi model tersebut dalam menilai keberhasilan implementasi sistem SIEM berbasis open source, khususnya pada lingkungan instansi pemerintah. Keenam dimensi dalam model DeLone dan McLean terbukti mampu memberikan gambaran yang komprehensif mengenai kualitas sistem, kepuasan pengguna, serta manfaat yang dirasakan organisasi. Dengan demikian, model ini dapat dijadikan acuan dalam penelitian selanjutnya yang mengevaluasi sistem keamanan informasi serupa pada skala organisasi yang lebih luas.

IV. KESIMPULAN DAN SARAN

Kesimpulan

Penelitian ini bertujuan mengevaluasi efektivitas implementasi sistem monitoring insiden siber berbasis Wazuh di Instansi Pemerintah XYZ menggunakan Model Keberhasilan Sistem Informasi DeLone dan McLean. Berdasarkan hasil analisis kuesioner dan observasi terhadap log keamanan, implementasi Wazuh memperoleh nilai rata-rata keseluruhan sebesar 4,26**,** sehingga termasuk dalam kategori Sangat Efektif**.**

Seluruh dimensi evaluasi memperoleh kategori Sangat Efektif, dengan dimensi Penggunaan (*Use*) memperoleh nilai tertinggi. Temuan tersebut menunjukkan bahwa sistem telah dimanfaatkan secara optimal dalam mendukung aktivitas pemantauan keamanan siber serta proses pengambilan keputusan terkait penanganan insiden. Selain itu, hasil observasi log memperlihatkan bahwa Wazuh mampu mendeteksi berbagai aktivitas keamanan, termasuk indikasi *brute force attack* melalui *failed login*, secara hampir *real-time*, sehingga mendukung peningkatan kemampuan deteksi dini terhadap ancaman siber.

Meskipun demikian, dimensi Kualitas Informasi (*Information Quality*) memperoleh nilai paling rendah dibandingkan dimensi lainnya. Hal ini menunjukkan bahwa kualitas penyajian informasi masih dapat ditingkatkan melalui optimalisasi aturan deteksi (*ruleset*), penyempurnaan korelasi *alert*, serta penyesuaian konfigurasi sistem agar informasi yang dihasilkan menjadi lebih akurat, relevan, dan mudah dipahami oleh pengguna.

Saran

Berdasarkan hasil penelitian, beberapa rekomendasi yang dapat dipertimbangkan untuk meningkatkan efektivitas implementasi Wazuh di Instansi Pemerintah XYZ adalah sebagai berikut:

1. Melakukan *fine-tuning* terhadap *ruleset* dan mekanisme korelasi *alert* secara berkala untuk mengurangi *false positive* tanpa

mengurangi sensitivitas sistem dalam mendeteksi ancaman.

2. Mengembangkan *custom decoder* dan aturan deteksi yang disesuaikan dengan karakteristik infrastruktur teknologi informasi di lingkungan instansi sehingga kualitas informasi yang dihasilkan menjadi lebih relevan.
3. Mengintegrasikan Wazuh dengan sumber *threat intelligence* atau solusi keamanan lainnya guna meningkatkan kemampuan identifikasi ancaman serta memperkaya konteks analisis keamanan.
4. Menyelenggarakan pelatihan secara berkala bagi administrator dan operator keamanan informasi agar kemampuan dalam menganalisis log, menginterpretasikan *alert*, dan melakukan respons insiden semakin optimal.
5. Penelitian selanjutnya disarankan mengevaluasi hubungan antar dimensi Model Keberhasilan Sistem Informasi DeLone dan McLean menggunakan pendekatan statistik inferensial, seperti SEM-PLS atau metode sejenis, sehingga diperoleh pemahaman yang lebih mendalam mengenai faktor-faktor yang memengaruhi keberhasilan implementasi sistem monitoring insiden siber.

REFERENSI

Sutanto & Rakhman. (2025).Experimental Evaluation of Wazuh-Grafana Integration for Real-Time Cyber Threat Detection in Resource-Constrained Environments. Journal of Applied Informatics and Computing, 9(1), 45–52. https://doi.org/10.30871/jaic.v9i5.10404

Rivera et al., (2024).Penerapan Model DeLone & McLean dalam Menilai Kesuksesan dan Kapabilitas Pengguna Sistem Informasi di Industri Logistik, 7(3), 1407-1417.https://doi.org/10.32493/jtsi.v7i3.41981

Syahrul (2023). Analisis Sistem Security Information and Event Management (SIEM) Aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan. Jurnal Teknik Elektro, 12(2), 123–130. https://repository.poliupg.ac.id/id/eprint/10642/

Putri et al., (2024) .Peran Manajemen Sekuriti pada CIA Triad. Indonesian Journal of Multidisciplinary, 2(3). https://repository.ubharajaya.ac.id/35092/

Anggraini & Widhiantoro.(2023).Mengenal SIEM dan SOAR: Pilar Utama Keamanan Informasi Modern. Prosiding PNJ. https://prosiding.pnj.ac.id/index.php/sniv/article/download/4170/2279/21930

Radhitya, D., et al.(2022). Analisis Implementasi SIEM berbasis Wazuh pada Windows & Linux. UI Library. https://lib.ui.ac.id/detail?id=20523053

Rafiqul Islam & Rafique.(2024) .Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries. https://doi.org/10.26776/ijemm.09.04.2020.02

Nas et al., (2023) .Analisis Sistem Security Information and Event Management (SIEM) Aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan. Jurnal Teknologi Elektrika, 20(2).

DeLone & McLean.(2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. Journal of Management Information Systems, 19(4), 9–30. https://doi.org/10.1080/07421222.2003.11045748

Wazuh. (2025). Wazuh Documentation: Modules Overview.https://documentation.wazuh.com