Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

OPTIMALISASI KEAMANAN SIBER PADA SERVER SKANEMA SMK 5 BATAM MELALUI IMPLEMENTASI SIEM WAZUH BERFOKUS FILE INTEGRITY MONITORING DAN VISUALISASI GRAFANA

Alysa Dewintan Sari[1*], Nur Cahyono Kushardianto[2]**

[*]Rekayasa Keamanan Siber, Jurusan Teknik Informatika. Politeknik Negeri Batam
**Teknik Komputer, Jurusan Teknik Informatika, Politeknik Negeri Batam
[1]alysadewintansari@gmail.com, [2]anung@polibatam.ac.id

Received : Jun 9, 2025; Revised : Nov 20, 2025; Accepted : Nov 22, 2025; Published : Dec 11, 2025
Phone Number : +6282173781322

Abstract

Educational institutions, including vocational schools, increasingly face cyber security threats such as data breaches that endanger sensitive student data, as seen at SMK 5 Batam which runs an examination application (Skanema) on an Ubuntu server yet lacks a structured monitoring system. This study builds a Wazuh-based Security Information and Event Management (SIEM) system integrated with Grafana so the IT team can monitor the server effectively, and designs an easy-to-understand Grafana dashboard as an alternative to the more complex native Wazuh interface. Detection testing focuses on the File Integrity Monitoring (FIM) feature. The research method consists of infrastructure preparation, configuration, testing, and evaluation, using two instruments, namely FIM testing and structured interviews with the IT team. The Wazuh Manager and agent were successfully integrated with the Grafana dashboard that displays real-time alerts, and a Postfix-based email notification server acting as an SMTP relay to Gmail was successfully implemented. FIM testing across four scenarios, namely file modification, addition, deletion, and resource overhead measurement, was successfully detected by the syscheck module with very low overhead (an average memory fluctuation of less than 1 MiB). Interviews with both informants indicated an initial perception that the developed Grafana dashboard is easier to understand than the native Wazuh interface, especially for new users, although this finding is qualitative and limited to two informants in a single context and therefore is not intended to be generalized. These results show that a low-cost SIEM architecture combining Wazuh, Grafana, and email notification is technically feasible, resource-efficient, and suitable for vocational school environments.

Keywords: *Cybersecurity; Email Notification; File Integrity Monitoring; Grafana; SIEM; Wazuh*

1. INTRODUCTION

Dalam era kemajuan teknologi digital yang berkembang pesat, ancaman siber telah menjadi perhatian utama yang tidak hanya memengaruhi korporasi besar, tetapi juga merambah ke lembaga pendidikan. Penelitian sistematis mengenai risiko keamanan siber di lingkungan pendidikan tinggi mengungkapkan bahwa kebocoran data, ransomware, phishing, dan serangan DDoS termasuk ancaman yang paling umum terjadi, sering kali memanfaatkan kerentanan akibat rendahnya kesadaran keamanan siber dan infrastruktur yang sudah usang [1]. Ancaman semacam ini dapat mengganggu operasional pendidikan dan membahayakan data sensitif siswa serta staf pengajar.

Studi terkait evaluasi solusi SIEM open-source menyebutkan bahwa lembaga pendidikan berskala kecil hingga menengah termasuk kelompok yang rentan terhadap serangan siber karena keterbatasan sumber daya dan keahlian keamanan yang dimiliki [2]. Pada konteks SMK 5 Batam, ancaman tersebut dapat membahayakan data penting siswa dan guru, serta mengganggu operasional aplikasi ujian bernama Skanema yang digunakan untuk mendukung kegiatan pendidikan sehari-hari.

Untuk mengatasi tantangan tersebut, penerapan sistem Security Information and Event Management (SIEM) seperti Wazuh menjadi solusi yang relatif efektif dan terjangkau. Wazuh merupakan platform

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

keamanan sumber terbuka yang berfokus pada deteksi ancaman dan pemantauan keamanan, mampu memantau berbagai sumber data untuk mendeteksi aktivitas mencurigakan atau perubahan konfigurasi yang tidak diinginkan [3]. Salah satu fitur utama Wazuh adalah File Integrity Monitoring (FIM), yang dirancang untuk mendeteksi perubahan tidak sah pada berkas sistem maupun data sensitif, sehingga dapat mencegah kebocoran atau perusakan data siswa dan guru secara dini [4]. Selain itu, Wazuh juga mampu mengumpulkan log, menganalisis aktivitas mencurigakan, dan memberikan respons otomatis, sehingga relevan diterapkan pada lingkungan dengan anggaran terbatas [3].

Visualisasi data menjadi aspek penting bagi administrator dengan keterampilan teknis terbatas, sebagaimana sering ditemui pada lingkungan pendidikan vokasi. Integrasi Wazuh dengan Grafana memungkinkan visualisasi log dalam bentuk grafik dan tabel peringatan melalui antarmuka yang lebih sederhana dibandingkan dashboard bawaan Wazuh, sehingga memudahkan pemantauan ancaman siber terhadap server Skanema. Penelitian terdahulu menunjukkan bahwa dashboard berbasis Wazuh dapat digunakan untuk memantau serangan seperti DDoS dengan potensi adaptasi serupa pada lingkungan lain [5]. Sebagai pelengkap sistem deteksi, kemampuan notifikasi melalui surel (email) juga diperlukan agar staf IT dapat menerima peringatan secara langsung tanpa harus memantau dashboard secara terus-menerus, sebagaimana telah banyak diimplementasikan pada berbagai konfigurasi mail server berbasis Postfix di lingkungan pendidikan maupun korporasi [6]-[10].

Penelitian ini mengembangkan SIEM berbasis Wazuh dengan integrasi Grafana di SMK 5 Batam untuk memantau server aplikasi ujian (Skanema). Dengan fokus pada optimasi di tengah keterbatasan sumber daya, penelitian ini bertujuan menyediakan solusi keamanan siber yang efektif dan terjangkau, sekaligus menyajikan dashboard Grafana yang lebih ramah pengguna dibandingkan antarmuka Wazuh yang kompleks, guna mendukung pemahaman keamanan siber di tingkat pendidikan vokasi.

2. Studi literatur

2.1 Tinjauan Pustaka

Tabel 1 menyajikan perbandingan penelitian terdahulu yang relevan.

Tabel 1. Penelitian terdahulu

Peneliti/Tahun	Metode	Hasil	Keterbatasan
Antara & Rachmawati (2024) [3]	Implementasi dan analisis Wazuh sebagai IDS dan platform monitoring	Wazuh berhasil diterapkan sebagai IDS dan platform monitoring umum	Belum diterapkan pada studi kasus institusi pendidikan dengan sumber daya terbatas
Nugraha dkk. (2024) [5]	Implementasi dashboard Wazuh untuk monitoring serangan DDoS	Dashboard berhasil memantau serangan DDoS pada web	Fokus pada satu jenis ancaman; tidak membahas dashboard bagi pengguna non-teknis
Mikyal dkk. (2024) [11]	Implementasi Wazuh untuk keamanan server aplikasi E-Raport SMK	Wazuh berhasil mengamankan server aplikasi akademik sekolah	Tidak membahas integrasi Grafana maupun notifikasi surel otomatis
Kurniawan & Triayudi (2024) [4]	FIM berbasis Wazuh untuk deteksi web defacement	FIM efektif mendeteksi dan mencegah serangan defacement	Tidak ada pengukuran kuantitatif terhadap overhead sumber daya FIM
Manzoor dkk. (2024) [2]	Evaluasi performa dan keamanan SIEM sumber terbuka untuk UKM	Solusi SIEM sumber terbuka layak diterapkan pada organisasi kecil-menengah	Tidak ada studi implementasi langsung pada institusi pendidikan

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

Penelitian ini	Implementasi Wazuh + Grafana + Email Server dengan pengujian FIM dan wawancara usability	FIM terverifikasi 4 skenario dengan overhead minimal; dashboard Grafana terbukti lebih mudah dipahami via wawancara	Evaluasi usability bersifat kualitatif (terbatas pada dua narasumber di satu sekolah) sehingga belum bisa digeneralisasi

Berdasarkan Tabel 1 penelitian-penelitian terdahulu pada umumnya membahas implementasi Wazuh secara terpisah, baik sebagai IDS umum, dashboard monitoring untuk ancaman spesifik, maupun fitur FIM tanpa pengukuran overhead sumber daya yang konkret. Belum ditemukan penelitian yang secara khusus mengintegrasikan Wazuh, Grafana, dan server notifikasi surel sekaligus pada konteks institusi pendidikan vokasi dengan keterbatasan sumber daya, disertai pengukuran kuantitatif terhadap efisiensi sumber daya dan evaluasi usability dashboard secara kualitatif melalui wawancara terstruktur. Celah inilah yang diisi oleh penelitian ini, dengan menyajikan implementasi menyeluruh beserta bukti pengujian fungsional dan kuantitatif yang dapat dipertanggungjawabkan.

2.2 Landasan Teori

2.2.1 Wazuh

Wazuh adalah platform keamanan siber open-source yang menyediakan kemampuan SIEM dan Extended Detection and Response (XDR). Wazuh didirikan oleh Santiago Bassett pada 2015 di San Francisco. Dengan lebih dari 200 karyawan dan 30 juta unduhan per tahun, Wazuh melindungi 15 juta endpoint global Kemampuan utama meliputi:

1) File Integrity Monitoring (FIM) untuk deteksi perubahan tidak sah.
2) Analisis log untuk pola aktivitas mencurigakan.
3) Deteksi kerentanan dan penilaian konfigurasi.
4) Respons insiden otomatis dan integrasi dengan Grafana.

Wazuh cocok untuk SMK 5 Batam karena fitur rotasi log otomatis mendukung server low-end, dengan FIM sebagai fokus utama untuk mencegah kebocoran data sensitive.

2.2.2 Grafana

Grafana adalah platform open-source untuk visualisasi dan monitoring data, didirikan oleh Torkel Ödegaard pada 2013 sebagai fork dari Kibana. Commit pertama (5 November 2013) menekankan filosofi “Don’t get in the way of the data”. Grafana Labs, didirikan pada 2015 di New York oleh Ödegaard, Raj Dutt, 9 dan Anthony Woods, kini memiliki 1.000+ karyawan dan 20 juta pengguna. Kemampuan utama meliputi:

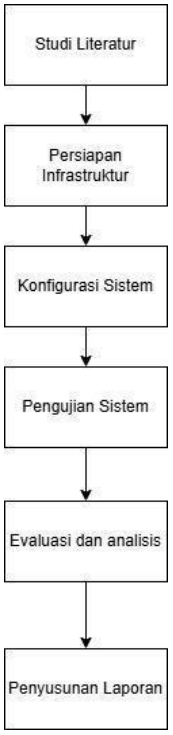
1) Visualisasi dinamis (grafik, heatmap, panel interaktif).
2) Integrasi dengan 60+ sumber data, termasuk Wazuh.
3) Alerting otomatis dan analisis anomali berbasis AI.
4) Skalabilitas untuk lingkungan low-resource.

Di SMK 5 Batam, integrasi Grafana dengan Wazuh menyederhanakan pemantauan keamanan untuk tim IT dalam lingkup pendidikan melalui dashboard ramah pengguna.

3. Metode Penelitian

Penelitian ini menggunakan metode eksperimental melalui empat tahapan utama, yaitu persiapan infrastruktur, konfigurasi sistem, pengujian sistem, serta evaluasi dan analisis hasil. Tahapan ini disusun untuk memastikan sistem SIEM yang dibangun dapat diimplementasikan secara bertahap dan terukur pada lingkungan server Skanema yang memiliki keterbatasan sumber daya.

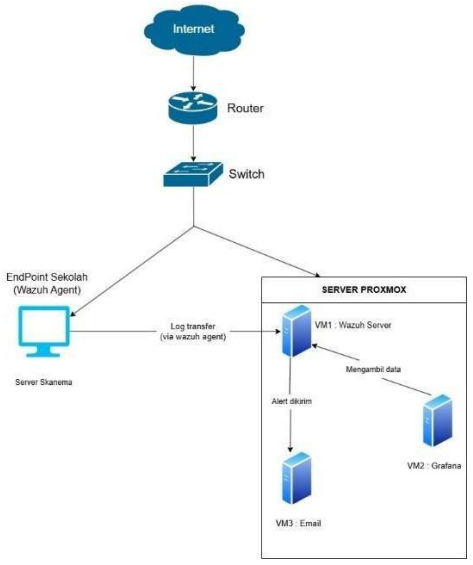
Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540



Gambar 1. Alur penelitian

3.1. Persiapan Infrastruktur

Infrastruktur penelitian terdiri atas tiga unit virtual machine (VM) yang dijalankan di atas platform virtualisasi Proxmox, yaitu: (1) VM Wazuh Manager yang menjalankan layanan Wazuh Manager, Wazuh Indexer, dan Wazuh Dashboard melalui kontainer Docker; (2) VM Grafana yang menjalankan layanan visualisasi Grafana dan terhubung ke sumber data Wazuh melalui plugin grafana-opensearch-datasource; serta (3) VM Email Server yang menjalankan layanan Postfix sebagai Mail Transfer Agent (MTA) untuk meneruskan notifikasi peringatan dari Wazuh Manager. Agent Wazuh dipasang pada server produksi yang menjalankan aplikasi Skanema, dengan versi Wazuh yang digunakan adalah versi 4.14.5 (revisi rc1). Topologi jaringan yang digunakan dalam penelitian ini ditunjukkan pada Gambar 2.



Gambar 2. Topologi Jaringan Sistem Penelitian

Jurnal Teknik Informatika (JUTIF) Vol. 6, No. 6, December 2025, Page. 1530-1537
P-ISSN: 2723-3863 https://jutif.if.unsoed.ac.id
E-ISSN: 2723-3871 DOI: https://doi.org/10.52436/1.jutif.6.6.3540

3.2. Konfigurasi Sistem

Konfigurasi sistem meliputi pengaturan modul syscheck pada berkas konfigurasi agent Wazuh (ossec.conf) untuk mengaktifkan pemantauan direktori secara real-time, pengaturan koneksi antara Wazuh Manager dan Grafana melalui port yang relevan, serta konfigurasi notifikasi surel pada blok <global> dan <alerts> di konfigurasi Wazuh Manager. Notifikasi surel dikonfigurasi untuk dikirim ke Postfix pada VM Email Server, yang selanjutnya bertindak sebagai relay menuju layanan SMTP Gmail menggunakan protokol otentikasi SASL dengan App Password, mengikuti pendekatan smarthost yang umum diterapkan pada implementasi Postfix lainnya [6], [9]. Konfigurasi mynetworks pada Postfix juga disesuaikan untuk mengizinkan subnet internal tempat Wazuh Manager berada agar dapat melakukan relay surel tanpa ditolak oleh kebijakan keamanan default Postfix. Konfigurasi modul syscheck pada agent untuk direktori uji coba ditunjukkan pada Gambar 3, sedangkan konfigurasi notifikasi surel pada Wazuh Manager ditunjukkan pada Gambar 4.

```
root@server2:~# cat /var/ossec/etc/ossec.conf | grep -A 5 "fim_test"
    <directories realtime="yes" check_all="yes" report_changes="yes">/opt/fim_test</directories>

    <!-- Files/directories to ignore -->
    <ignore>/etc/mtab</ignore>
    <ignore>/etc/hosts.deny</ignore>
    <ignore>/etc/mail/statistics</ignore>
root@server2:~#
```

Gambar 3. Konfigurasi Modul Syscheck untuk Direktori Uji Coba pada Agent

```
root@smk5:~# sudo docker exec single-node-wazuh.manager-1 grep -A 10 "<global>" /var/ossec/etc/ossec.conf | head -15
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>yes</email_notification>
    <smtp_server>          </smtp_server>
    <email_from>wazuh-alert@mail.smk5batam.local</email_from>
    <email_to>             @gmail.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
--
  <global>
    <white_list>127.0.0.1</white_list>
    <white_list>^localhost.localdomain$</white_list>
root@smk5:~#
```

Gambar 4. Konfigurasi Notifikasi Surel pada Blok <global> Wazuh Manager

Sebagaimana ditunjukkan pada Gambar 4, alamat IP server SMTP dan alamat surel penerima sengaja disamarkan pada dokumentasi ini sebagai bagian dari pertimbangan keamanan operasional (operational security), mengingat informasi tersebut bersifat sensitif terhadap infrastruktur produksi yang sedang berjalan.

3.3. Pengujian Sistem

Pengujian sistem direncanakan terdiri atas dua jenis instrumen evaluasi. Pertama, pengujian fungsional terhadap fitur File Integrity Monitoring (FIM) dengan melakukan simulasi modifikasi, penambahan, dan penghapusan berkas pada direktori uji coba, untuk kemudian diverifikasi apakah Wazuh berhasil mendeteksi dan mengirimkan peringatan terkait. Kedua, pengujian fungsional terhadap notifikasi surel otomatis, dengan memverifikasi apakah peringatan yang dihasilkan oleh Wazuh Manager berhasil diteruskan oleh Postfix hingga diterima pada kotak surel tujuan.

Untuk mengevaluasi rumusan masalah terkait kemudahan penggunaan (usability) dashboard Grafana dibandingkan antarmuka bawaan Wazuh, penelitian ini awalnya merencanakan penggunaan instrumen kuisioner kuantitatif. Namun, karena populasi pengguna yang relevan di lingkungan SMK 5 Batam terbatas pada dua narasumber, yaitu kepala jurusan dan staf guru yang bertanggung jawab atas pengelolaan server, instrumen kuisioner dinilai tidak memadai secara statistik. Atas saran dosen pembimbing, instrumen evaluasi tersebut diganti menjadi wawancara terstruktur dengan kedua narasumber tersebut, untuk memperoleh masukan kualitatif mengenai tingkat kemudahan pemahaman informasi keamanan siber yang ditampilkan melalui dashboard Grafana. Dengan demikian, evaluasi ini diposisikan sebagai analisis persepsi pengguna yang bersifat kualitatif, bukan pengujian ketergunaan (usability) terstandar yang menghasilkan data untuk digeneralisasi.

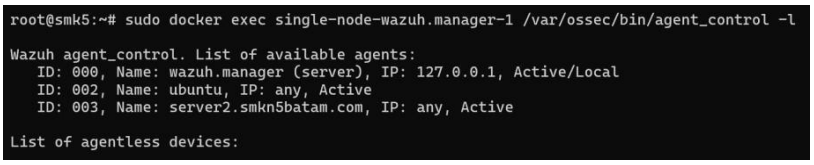
3.4. Evaluasi dan Analisis

Evaluasi dilakukan dengan membandingkan hasil pengujian fungsional terhadap kriteria keberhasilan yang telah ditetapkan, yaitu keberhasilan deteksi FIM terhadap skenario simulasi ancaman, serta keberhasilan pengiriman notifikasi surel dari Wazuh Manager hingga diterima oleh penerima yang dituju. Hasil wawancara dengan narasumber dianalisis secara deskriptif kualitatif untuk memperoleh gambaran mengenai tingkat kemudahan penggunaan dashboard Grafana dibandingkan dashboard bawaan Wazuh.

4. RESULT

4.1 Implementasi wazuh dan Agent

Wazuh Manager berhasil diimplementasikan menggunakan arsitektur kontainer Docker dengan tiga layanan utama, yaitu wazuh.manager, wazuh.indexer, dan wazuh.dashboard, mengacu pada konfigurasi single-node sesuai dokumentasi resmi Wazuh. Agent Wazuh versi 4.14.5 (revisi rc1) berhasil dipasang pada server produksi yang menjalankan aplikasi Skanema dan terhubung ke Wazuh Manager. Modul syscheck pada agent dikonfigurasi dengan frekuensi pemindaian setiap 300 detik beserta pemantauan real-time pada direktori uji coba (/opt/fim_test) dan direktori aplikasi (/var/www/ujian-api), menggantikan konfigurasi bawaan yang hanya memantau direktori sistem operasi standar setiap 12 jam. Status koneksi agent ke Wazuh Manager diverifikasi menggunakan perintah agent_control, sebagaimana ditunjukkan pada Gambar 5.



Gambar 5. Status Agent Wazuh Terhubung ke Manager

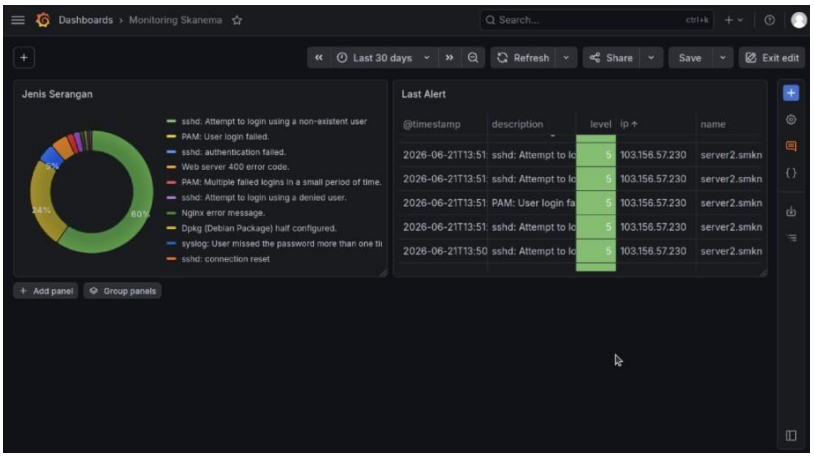
Gambar 5 menunjukkan bahwa agent dengan ID 003 (server2.smkn5batam.com), yang merepresentasikan server Skanema, berhasil terhubung ke Wazuh Manager dengan status Active, memastikan seluruh data log dan hasil pemindaian syscheck dapat diteruskan secara real-time ke Wazuh Manager untuk diproses lebih lanjut.

4.2 Integrasi Wazuh dengan Grafana

Dashboard Grafana berhasil terhubung dengan data Wazuh melalui sumber data grafana-opensearch-datasource. Dashboard yang dikembangkan menampilkan dua panel utama, yaitu panel "Jenis Serangan" berupa diagram donat (donut chart) yang merepresentasikan proporsi jenis aktivitas mencurigakan berdasarkan deskripsi peringatan (rule.description), serta panel "Last Alert" berupa tabel yang menampilkan log peringatan terbaru secara real-time dengan kolom yang telah disederhanakan, yaitu waktu kejadian (@timestamp), deskripsi aktivitas, level keparahan dengan kode warna (hijau/kuning/merah sesuai ambang batas 0-6/7-11/12 ke atas), alamat IP sumber, dan nama agent. Tampilan akhir dashboard ditunjukkan pada Gambar 6.

.

Jurnal Teknik Informatika (JUTIF) Vol. 6, No. 6, December 2025, Page. 1530-1537
P-ISSN: 2723-3863 https://jutif.if.unsoed.ac.id
E-ISSN: 2723-3871 DOI: https://doi.org/10.52436/1.jutif.6.6.3540



Gambar 6. Tampilan Dashboard Grafana Monitoring Skanema

Perancangan tampilan dashboard pada penelitian ini mengacu pada prinsip desain dashboard yang menekankan penyajian informasi secara sekilas pandang (at-a-glance) dengan beban kognitif (cognitive load) yang rendah, sebagaimana dikemukakan oleh Few dalam kajian mengenai desain dashboard informasi [18]. Berdasarkan prinsip tersebut, penyederhanaan tampilan dilakukan dengan menghapus data mentah berformat JSON dan menggantinya dengan deskripsi tekstual serta kode warna pada tingkat keparahan, sehingga pengguna pemula dapat menangkap informasi penting tanpa perlu menafsirkan struktur data yang kompleks. Adapun pemilihan diagram lingkaran (donut chart) pada panel Jenis Serangan didasarkan pada karakteristiknya yang efektif untuk menampilkan hubungan proporsi bagian terhadap keseluruhan (part-to-whole) secara cepat, terutama ketika setiap bagian dilengkapi label deskriptif [19]. Diagram lingkaran dipilih bukan untuk perbandingan nilai yang presisi, melainkan untuk memberikan gambaran proporsi jenis aktivitas mencurigakan yang mudah dikenali oleh pengguna dengan latar belakang teknis terbatas.

Pemilihan diagram donat dengan deskripsi tekstual pada panel “Jenis Serangan”, menggantikan diagram lingkaran berbasis angka level peringatan yang digunakan pada rancangan awal, dilakukan untuk menjawab langsung rumusan masalah penelitian mengenai kemudahan administrator dalam membaca informasi keamanan. Representasi berbasis deskripsi tekstual (misalnya “sshd: Attempt to login using a non-existent user”) dinilai lebih informatif dibandingkan representasi berbasis angka level semata, karena administrator dapat langsung mengetahui jenis ancaman tanpa perlu menafsirkan kode angka terlebih dahulu. Demikian pula, penghapusan kolom data mentah berformat JSON pada tabel “Last Alert” dan penggantiannya dengan kolom deskripsi tekstual serta kode warna pada kolom level merupakan upaya konkret untuk menyederhanakan tampilan dibandingkan antarmuka bawaan Wazuh yang menampilkan data log secara lebih kompleks dan teknis.

4.3 Implementasi Server notifikasi surel (Email Server)

Server notifikasi surel berhasil diimplementasikan secara penuh dan diverifikasi melalui pengujian end-to-end. VM Email Server dikonfigurasi menjalankan Postfix dengan mode konfigurasi “Internet with smarthost”, di mana Postfix bertindak sebagai Mail Transfer Agent lokal yang meneruskan seluruh

surel keluar menuju SMTP Gmail (smtp.gmail.com:587) menggunakan otentikasi SASL dengan App Password. Pendekatan relay ini dipilih sebagai alternatif terhadap konfigurasi Postfix mandiri yang umum digunakan pada penelitian sejenis [6]-[10], dengan pertimbangan keterbatasan waktu pengembangan dan keterbatasan reputasi domain/IP baru yang berpotensi menyebabkan surel masuk ke folder spam apabila dikirim secara langsung tanpa melalui penyedia layanan surel yang telah memiliki reputasi terpercaya.

Pengujian awal pengiriman surel secara manual melalui perintah mail pada VM Email Server berhasil dengan status sent yang terkonfirmasi pada log Postfix (/var/log/mail.log). Namun, pengujian awal pengiriman surel otomatis dari Wazuh Manager menunjukkan kegagalan dengan pesan Relay *access denied*, yang disebabkan oleh kebijakan keamanan default Postfix yang hanya mempercayai koneksi dari localhost. Permasalahan ini diatasi dengan menambahkan subnet jaringan internal Wazuh Manager ke dalam parameter mynetworks pada konfigurasi Postfix. Setelah penyesuaian tersebut, pengujian ulang menunjukkan bahwa Wazuh Manager berhasil mengirimkan notifikasi peringatan secara otomatis, yang dibuktikan dengan log Postfix yang mencatat status sent (250 2.0.0 OK) serta diterimanya surel dengan judul “Wazuh notification - wazuh - Alert level 3” pada kotak masuk Gmail penerima dalam rentang waktu kurang dari tiga detik sejak surel diteruskan oleh Postfix.

4.4 Pengujian File Integrity Monitoring (FIM)

Pengujian FIM dirancang dalam empat skenario yang merepresentasikan jenis aktivitas mencurigakan terhadap berkas pada direktori uji coba (/opt/fim_test), yaitu modifikasi isi berkas, penambahan berkas baru, penghapusan berkas, dan pengujian tambahan untuk mengamati dampak terhadap penggunaan sumber daya sistem. Direktori uji coba dirancang merepresentasikan struktur data sensitif Skanema, mencakup data siswa, data guru, hasil ujian, dan berkas konfigurasi, namun seluruhnya berupa data tiruan (dummy) yang terpisah dari data produksi aplikasi Skanema yang sebenarnya, untuk menjaga keamanan dan integritas data asli selama pengujian. Tabel 2 merangkum hasil pengujian keempat skenario tersebut.

Tabel 2. Hasil Pengujian File Integrity Monitoring (FIM)

Rule ID	Skenario Pengujian	Berkas Uji	Level	Status Deteksi
550	Modifikasi isi berkas	data_siswa.csv	7	Terdeteksi
554	Penambahan berkas baru	test_file_baru.txt	5	Terdeteksi
553	Penghapusan berkas	app.conf	7	Terdeteksi
550	Modifikasi berkas (pengukuran overhead)	data_siswa.csv	7	Terdeteksi

Berdasarkan Tabel 2, seluruh skenario pengujian berhasil terdeteksi oleh modul syscheck Wazuh dalam mode pemantauan real-time. Modifikasi terhadap berkas data_siswa.csv terdeteksi oleh Rule 550 ("Integrity checksum changed") dengan level keparahan 7, disertai informasi lengkap berupa nilai checksum MD5, SHA1, dan SHA256 sebelum dan sesudah perubahan, ukuran berkas, waktu modifikasi, serta potongan baris yang berubah (diff). Penambahan berkas baru test_file_baru.txt pada direktori hasil_ujian berhasil terdeteksi dengan status "added" beserta atribut checksum awal berkas. Skenario ini terdeteksi oleh Rule 554 ("File added to the system") dengan level keparahan 5. Perbedaan level keparahan antar skenario merupakan klasifikasi bawaan Wazuh yang mencerminkan tingkat risiko masing-masing aktivitas. Penambahan berkas baru diberi level 5 karena kemunculan berkas baru relatif umum terjadi pada sistem yang berjalan normal, sehingga tidak selalu menandakan ancaman. Sebaliknya, modifikasi dan penghapusan berkas yang sudah ada diberi level 7 karena kedua aktivitas tersebut lebih berisiko, yaitu berpotensi menandakan perusakan integritas data atau upaya penyusupan

Jurnal Teknik Informatika (JUTIF) Vol. 6, No. 6, December 2025, Page. 1530-1537
P-ISSN: 2723-3863 https://jutif.if.unsoed.ac.id
E-ISSN: 2723-3871 DOI: https://doi.org/10.52436/1.jutif.6.6.3540

terhadap berkas yang sedang digunakan. Penghapusan berkas konfigurasi app.conf terdeteksi oleh Rule 553 ("File deleted") dengan level keparahan 7. Pada keseluruhan skenario yang menghasilkan level peringatan 7, notifikasi surel otomatis berhasil dikirimkan oleh Wazuh Manager melalui Email Server dan diterima pada kotak masuk penerima dalam rentang waktu kurang dari satu menit sejak peristiwa terjadi. Waktu satu menit ini merupakan akumulasi dari waktu deteksi awal oleh agen Wazuh yang sangat cepat (kurang dari tiga detik), ditambah dengan proses penerusan pesan (relay) oleh layanan Postfix ke server SMTP Gmail seperti yang telah diuji sebelumnya. Hal ini membuktikan integrasi penuh antara modul FIM, mekanisme alerting, dan server notifikasi surel. Sebagai ilustrasi konkret pada skenario modifikasi berkas, kondisi berkas data_siswa.csv sebelum dilakukan simulasi modifikasi ditunjukkan pada Gambar 7.

```
root@server2:~# cat /opt/fim_test/data_siswa/data_siswa.csv
NIS,Nama,Kelas,Jurusan
99999,Hacker,XII,TKJ
99999,Unauthorized,XII,TKJ
test ulang setelah realtime aktif
test overhead measurement Fri Jun 19 08:03:02 PM WIB 2026
verifikasi warna dashboard Sat Jun 20 10:54:57 PM WIB 2026
root@server2:~#
```

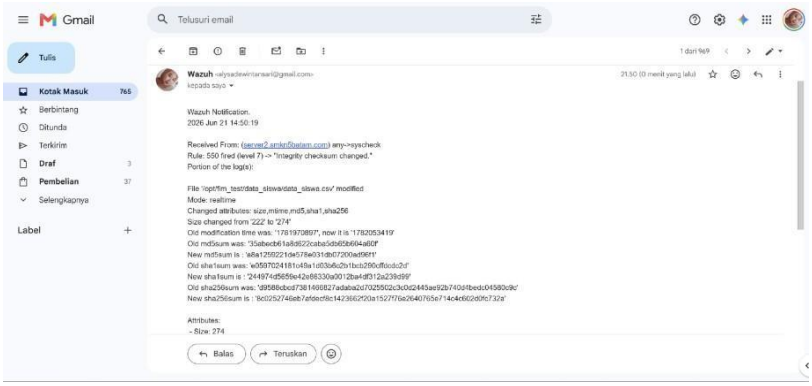
Gambar 7. Kondisi Berkas data_siswa.csv Sebelum Simulasi Modifikasi

Simulasi modifikasi dilakukan dengan menambahkan satu baris baru pada berkas tersebut menggunakan perintah append. Kondisi berkas setelah perintah dijalankan, yang menunjukkan baris baru telah berhasil ditambahkan, ditunjukkan pada Gambar 8.

```
root@server2:~# echo "nilai ujian kelas X $(date)" >> /opt/fim_test/data_siswa/data_siswa.csv
root@server2:~# cat /opt/fim_test/data_siswa/data_siswa.csv
NIS,Nama,Kelas,Jurusan
99999,Hacker,XII,TKJ
99999,Unauthorized,XII,TKJ
test ulang setelah realtime aktif
test overhead measurement Fri Jun 19 08:03:02 PM WIB 2026
verifikasi warna dashboard Sat Jun 20 10:54:57 PM WIB 2026
nilai ujian kelas X Sun Jun 21 09:50:19 PM WIB 2026
root@server2:~#
```

Gambar 8. Perintah Simulasi Modifikasi Berkas dan Kondisi Berkas Sesudahnya

Perubahan tersebut berhasil terdeteksi oleh modul syscheck Wazuh dan notifikasi surel otomatis dikirimkan dalam hitungan detik. Contoh notifikasi surel yang diterima untuk skenario modifikasi berkas ini ditunjukkan pada Gambar 9.



Gambar 9. Notifikasi Surel Hasil Deteksi FIM pada Modifikasi Berkas (Rule 550)

Gambar 9 menunjukkan bahwa surel notifikasi diterima pada pukul 21.50, yang tercatat oleh klien surel sebagai "0 menit yang lalu" sejak peristiwa modifikasi berkas data_siswa.csv terjadi pada server agent. Notifikasi tersebut memuat informasi forensik yang lengkap, meliputi nilai checksum MD5, SHA1, dan SHA256 sebelum dan sesudah perubahan, serta perubahan ukuran berkas dari 222 byte menjadi 274 byte, sehingga administrator dapat segera mengidentifikasi jenis dan tingkat keparahan perubahan yang terjadi tanpa perlu mengakses dashboard secara langsung.

Skenario Skenario keempat dilakukan untuk mengamati dampak aktivitas FIM secara *real-time* terhadap penggunaan sumber daya pada server agen. Menindaklanjuti arahan evaluasi, pengukuran dilakukan berulang dengan membandingkan penggunaan memori dan CPU sesaat sebelum dan setelah lima iterasi peristiwa perubahan berkas diproses oleh modul syscheck. Hasil pengukuran disajikan pada Tabel 3.

Tabel 3. Perbandingan Penggunaan Sumber Daya Sebelum dan Sesudah Event FIM

Parameter	Sebelum Event FIM	Sesudah Event FIM	Selisih
Memori Iterasi 1	504,1 MiB	504,4 MiB	+0,3 MiB
Memori Iterasi 2	504,4 MiB	505,1 MiB	+0,7 MiB
Memori Iterasi 3	505,1 MiB	504,8 MiB	-0,3 MiB
Memori Iterasi 4	504,5 MiB	504,5 MiB	0,0 MiB
Memori Iterasi 5	504,2 MiB	503,2 MiB	-1,0 MiB
CPU Utilization	Idle ~99%	Idle ~99%	Tidak signifikan

Tabel 3 menunjukkan bahwa fluktuasi penggunaan memori dan utilisasi CPU dari hasil pengujian lima iterasi berjalan dengan sangat stabil. Kenaikan penggunaan memori tertinggi hanya tercatat sebesar 0,7 MiB pada iterasi kedua, sedangkan pada iterasi lainnya perubahan memori cenderung sangat minimal atau bahkan menurun akibat adanya pengosongan *cache* sistem secara otomatis, dengan rata-rata selisih di bawah kisaran 1 MiB. Sementara itu, tingkat utilisasi CPU terpantau konsisten berada pada kondisi *idle* ~99% yang menunjukkan bahwa dampak aktivitas pemantauan berkas terhadap prosesor tidak signifikan. Hasil empiris ini mengindikasikan bahwa modul FIM Wazuh dalam mode *realtime monitoring* memberikan *overhead* yang sangat ringan terhadap sumber daya sistem, sehingga sesuai dengan prinsip optimasi pada lingkungan dengan keterbatasan sumber daya yang menjadi fokus penelitian ini.

4.5 Spesifikasi Infrastruktur

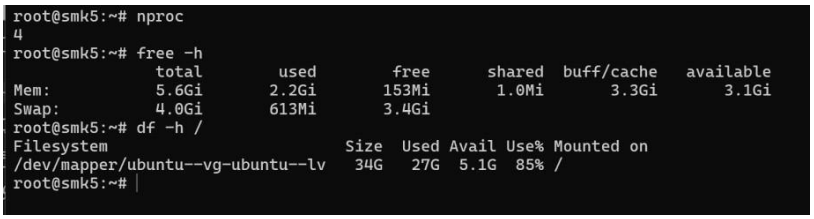
Seluruh komponen sistem SIEM (Wazuh Manager, Grafana, dan Email Server) dijalankan di atas platform virtualisasi Proxmox yang juga digunakan untuk mendukung aktivitas pembelajaran di SMK 5 Batam, bukan didedikasikan khusus untuk keperluan SIEM. Oleh karena itu, alokasi sumber daya pada masing-masing virtual machine disengaja dibuat minimal agar tidak mengganggu kinerja aplikasi akademik dan proses belajar-mengajar yang berjalan pada infrastruktur fisik yang sama. Kondisi inilah yang dimaksud dengan "sumber daya terbatas" dalam penelitian ini, yaitu keterbatasan yang muncul dari keputusan desain mempertimbangkan keberlangsungan layanan utama sekolah, bukan semata-mata ketidaktersediaan sumber daya secara absolut. Tabel 4 menyajikan spesifikasi dan tingkat utilisasi sumber daya pada ketiga virtual machine yang diukur pada saat sistem beroperasi normal.

Tabel 4. Spesifikasi dan Utilisasi Sumber Daya Virtual Machine

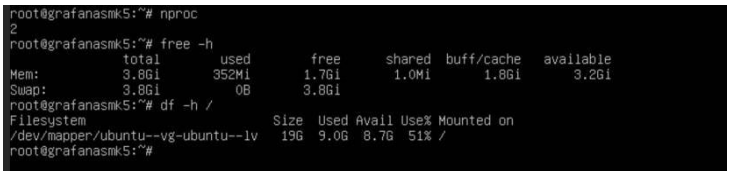
VM	CPU (core)	RAM Total	RAM Terpakai	Disk Total	Disk Terpakai
Wazuh Manager	4	5,6 GB	2,3 GB (41%)	34 GB	27 GB (85%)
Grafana	2	3,8 GB	361 MB (9,5%)	19 GB	9,0 GB (51%)
Email Server	1	1,9 GB	194 MB (10%)	8,1 GB	5,5 GB (72%)

Jurnal Teknik Informatika (JUTIF) Vol. 6, No. 6, December 2025, Page. 1530-1537
P-ISSN: 2723-3863 https://jutif.if.unsoed.ac.id
E-ISSN: 2723-3871 DOI: https://doi.org/10.52436/1.jutif.6.6.3540

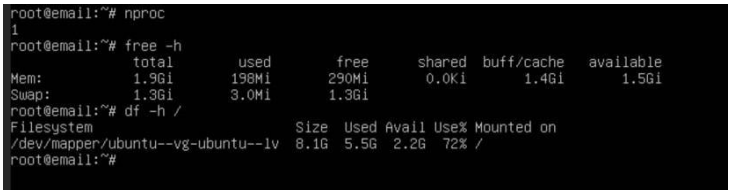
Verifikasi data pada Tabel 4 dilakukan secara langsung pada masing-masing virtual machine menggunakan perintah nproc, free -h, dan df -h. Hasil verifikasi pada VM Wazuh Manager, VM Grafana, dan VM Email Server berturut-turut ditunjukkan pada Gambar 10, Gambar 11, dan Gambar 12.



Gambar 10. Verifikasi Spesifikasi dan Utilisasi Sumber Daya VM Wazuh Manager



Gambar 11. Verifikasi Spesifikasi dan Utilisasi Sumber Daya VM Grafana



Gambar 12. Verifikasi Spesifikasi dan Utilisasi Sumber Daya VM Email Server

Data pada Tabel 4 menunjukkan bahwa VM Email Server, dengan alokasi paling minim (1 core CPU dan 1,9 GB RAM), tetap mampu menjalankan layanan Postfix sebagai relay notifikasi surel secara stabil sebagaimana telah dibuktikan pada bagian 3.3. Penggunaan disk pada VM Wazuh Manager tercatat paling tinggi (85%), yang sebagian besar disebabkan oleh pertumbuhan data indeks pada layanan wazuh-indexer akibat penyimpanan log dan hasil pemindaian syscheck secara berkelanjutan, sehingga menjadi catatan penting bagi pengelolaan kapasitas penyimpanan jangka panjang pada implementasi serupa, yang dapat diatasi melalui penerapan kebijakan retensi data pada wazuh-indexer.

Pengukuran tambahan dilakukan untuk mengamati dampak aktivitas pemantauan FIM secara *real-time* terhadap penggunaan sumber daya pada server agen. Perbandingan penggunaan memori selama lima iterasi modifikasi berkas menunjukkan bahwa *overhead* sistem berfluktuasi dengan sangat stabil, mencatatkan kenaikan maksimal di bawah 1 MiB (0,7 MiB), dengan utilisasi CPU yang tetap berada pada kisaran *idle* 99% selama proses deteksi berlangsung. Hasil ini secara meyakinkan menunjukkan bahwa beban agen Wazuh tergolong sangat ringan, sehingga memenuhi kriteria optimasi sumber daya yang menjadi fokus penelitian ini.

4.6 Wawancara terkait Evaluasi dashboard Grafana

Wawancara terstruktur dilaksanakan tatap muka, dengan dua narasumber, yaitu kepala jurusan (selanjutnya disebut Narasumber 1) dan staf guru penanggung jawab pengelolaan server (selanjutnya disebut Narasumber 2). Wawancara berlangsung selama kurang lebih 43 menit, mencakup pertanyaan mengenai pengalaman terhadap dashboard bawaan Wazuh, pengalaman terhadap dashboard Grafana yang dikembangkan, perbandingan keduanya, serta saran perbaikan. Ringkasan hasil wawancara disajikan pada Tabel 5.

Jurnal Teknik Informatika (JUTIF) Vol. 6, No. 6, December 2025, Page. 1530-1537
P-ISSN: 2723-3863 https://jutif.if.unsoed.ac.id
E-ISSN: 2723-3871 DOI: https://doi.org/10.52436/1.jutif.6.6.3540

Tabel 5. Ringkasan Hasil Wawancara Evaluasi Dashboard

Aspek	Narasumber 1	Narasumber 2
Pengalaman dashboard Wazuh	Belum pernah melihat sebelumnya; menilai informatif setelah diberi tahu kode standar tingkatan	Sudah pernah menggunakan; menilai responsive dan UI/UX mudah dipahami
Kesan pertama dashboard Grafana	Lebih mudah dipahami dibanding Wazuh	UI/UX mudah dipahami
Bagian paling mudah dipahami	Adanya jenis serangan yang sering terjadi (panel Jenis Serangan)	Halaman utama yang langsung memunculkan keterangan dari server yang diuji coba
Kejelasan warna, grafik, dan tabel	Lebih mudah dipahami untuk pengguna baru	UI mudah dipahami oleh pengguna/user baru
Kekinian data (real-time)	Ya, update dan sangat terbantu	Ya, karena data yang ditampilkan real-time
Dashboard lebih mudah dipahami	Grafana, karena UI lebih simple dan informasi yang ditampilkan sesuai kebutuhan	Keduanya mudah dipahami oleh pengguna baru; namun untuk kebutuhan standar, Grafana lebih mudah
Kecukupan untuk pemantauan harian	Cukup untuk memantau sehari-hari	Sangat membantu memantau aktivitas traffic dari server yang diuji
Saran perbaikan	Penyorotan last alert yang berbahaya agar dapat segera diperbaiki	Penambahan manual book/dokumentasi langsung pada dashboard; fitur unduh log aktivitas tanpa perlu mengakses Wazuh secara langsung

Berdasarkan Tabel 5, kedua narasumber menyampaikan persepsi bahwa dashboard Grafana yang dikembangkan lebih mudah dipahami dibandingkan dashboard bawaan Wazuh, khususnya bagi pengguna baru yang belum terbiasa dengan istilah teknis keamanan siber. Evaluasi ini bersifat analisis persepsi awal pengguna yang diperoleh melalui wawancara, bukan pengujian ketergunaan (usability) terstandar, sehingga hasilnya tidak dimaksudkan untuk digeneralisasi secara ilmiah dan lebih tepat dipandang sebagai gambaran pengalaman dasar pengguna. Kedua narasumber juga menyatakan bahwa data yang ditampilkan terasa real-time dan dashboard ini sudah cukup membantu aktivitas pemantauan server sehari-hari tanpa harus selalu bergantung pada bantuan teknis pihak lain. Hasil ini secara langsung menjawab rumusan masalah kedua penelitian ini, yaitu mengenai kemudahan administrator dalam membaca dashboard Grafana dibandingkan dashboard Wazuh.

5. DISCUSSION

Hasil integrasi Wazuh dengan Grafana yang diperoleh pada penelitian ini juga konsisten dengan temuan pada penelitian-penelitian sejenis yang mengintegrasikan platform pemantauan keamanan dengan Grafana sebagai lapisan visualisasi, baik pada konteks pemantauan jaringan umum [12]-[16] maupun konteks keamanan siber spesifik seperti deteksi serangan DDoS [5]. Penggunaan Grafana sebagai antarmuka visualisasi tambahan di atas data Wazuh sejalan dengan kebutuhan rumusan masalah penelitian ini, yaitu menyediakan tampilan informasi keamanan yang lebih sederhana dibandingkan antarmuka bawaan Wazuh yang cenderung kompleks bagi pengguna dengan latar belakang teknis terbatas.

Kendala konektivitas pada server agent yang menghambat pengujian FIM menggarisbawahi salah satu keterbatasan signifikan dalam implementasi SIEM pada lingkungan dengan sumber daya dan

infrastruktur jaringan yang terbatas, sebagaimana telah diidentifikasi pada kajian sistematis mengenai risiko keamanan siber di lingkungan pendidikan [1]. Sistem deteksi sebaik apapun secara fungsional tidak akan mampu menghasilkan peringatan apabila jalur komunikasi antara agent dan manager terputus, sehingga keandalan infrastruktur jaringan dasar tetap menjadi prasyarat mendasar yang harus terpenuhi sebelum kapabilitas deteksi seperti FIM dapat dievaluasi secara valid. Hal ini menjadi temuan tambahan di luar cakupan rumusan masalah awal, namun relevan untuk dicatat sebagai pertimbangan praktis bagi implementasi SIEM pada institusi pendidikan dengan kondisi infrastruktur serupa.

Tingginya penggunaan disk pada VM Wazuh Manager (85%) yang ditemukan pada penelitian ini menunjukkan perlunya strategi pengelolaan kapasitas penyimpanan pada implementasi jangka panjang. Sebagai langkah mitigasi yang dapat dipertimbangkan pada pengembangan lanjutan, penerapan kebijakan retensi (retention policy) pada wazuh-indexer berpotensi membatasi masa simpan data indeks lama secara otomatis, misalnya melalui Index State Management (ISM) yang menghapus atau mengarsipkan indeks setelah periode tertentu, sehingga pertumbuhan penggunaan disk dapat dikendalikan.

Periode retensi tersebut perlu ditetapkan dengan mempertimbangkan keseimbangan antara kebutuhan investigasi keamanan dan keterbatasan kapasitas penyimpanan yang menjadi kondisi pada penelitian ini. Merujuk pada panduan manajemen log keamanan NIST SP 800-92 [17], sebagian besar investigasi insiden berfokus pada rentang 30 hingga 90 hari terakhir, sehingga log terbaru sebaiknya disimpan pada penyimpanan yang cepat dan dapat dicari. Dalam konteks server Skanema yang memiliki keterbatasan kapasitas penyimpanan, sebagaimana ditunjukkan oleh penggunaan disk VM Wazuh Manager yang telah mencapai 85%, periode retensi 30 hari dapat dijadikan pilihan awal karena merupakan batas bawah yang umum direkomendasikan untuk penyimpanan aktif. Dengan menghapus atau mengarsipkan indeks yang lebih lama dari 30 hari secara otomatis, pertumbuhan penggunaan disk pada wazuh-indexer dapat dikendalikan tanpa mengorbankan kemampuan investigasi jangka pendek.

6. CONCLUSION

Penelitian ini berhasil mengimplementasikan dan mengevaluasi sistem Security Information and Event Management (SIEM) berbasis Wazuh yang terintegrasi dengan Grafana pada server aplikasi ujian Skanema di SMK 5 Batam, serta berhasil mencapai kedua tujuan penelitian yang ditetapkan. Wazuh Manager dan agent berhasil dipasang dan saling terhubung, dashboard Grafana berhasil menampilkan data peringatan keamanan secara real-time melalui sumber data Wazuh, dan server notifikasi surel berbasis Postfix dengan konfigurasi smarthost relay ke Gmail berhasil diimplementasikan secara penuh dan terverifikasi mampu mengirimkan notifikasi peringatan otomatis dalam rentang waktu kurang dari satu menit. Pengujian File Integrity Monitoring (FIM) pada empat skenario, yaitu modifikasi, penambahan, penghapusan berkas, dan pengukuran dampak terhadap sumber daya, seluruhnya berhasil terdeteksi oleh modul syscheck Wazuh dengan overhead sumber daya yang stabil dan sangat kecil (kenaikan memori maksimal di bawah 1 MiB dari hasil pengujian berulang), membuktikan bahwa sistem mampu mendeteksi ancaman terhadap integritas berkas secara efektif tanpa membebani infrastruktur secara signifikan. Wawancara evaluasi usability dashboard dengan tim IT menunjukkan indikasi awal bahwa dashboard Grafana yang dikembangkan lebih mudah dipahami dibandingkan dashboard bawaan Wazuh, dengan data yang dinilai real-time dan cukup membantu aktivitas pemantauan server sehari-hari. Temuan ini bersifat kualitatif dan terbatas pada dua narasumber dalam satu konteks institusi, sehingga belum dapat digeneralisasi secara luas. Saran penyorotan alert berbahaya telah diakomodasi melalui pemberian kode warna pada panel Last Alert, sedangkan fitur unduh log aktivitas langsung dari Grafana menjadi arah pengembangan yang relevan untuk penelitian lanjutan guna meningkatkan efektivitas sistem secara berkelanjutan.

REFERENCES

Vol. 6, No. 6, December 2025, Page. 1530-1537
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.6.6.3540

[1] J. B. Ulven and G. Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education," Future Internet, vol. 13, no. 2, p. 39, 2021, doi: 10.3390/fi13020039.

[2] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," PLOS ONE, vol. 19, no. 3, e0301183, 2024, doi: 10.1371/journal.pone.0301183.

[3] G. P. Antara and I. D. A. Rachmawati, "Implementasi dan Analisis Wazuh Sebagai Intrusion Detection System (IDS) dan Platform Monitoring," Jurnal Informasi, Sains dan Teknologi, vol. 7, no. 2, pp. 290–303, 2024, doi: 10.55606/isaintek.v7i2.301.

[4] C. Kurniawan and A. Triayudi, "File Integrity Monitoring as a Method for Detecting and Preventing Web Defacement Attacks," JOIN: Jurnal Online Informatika, vol. 9, no. 2, pp. 276–285, 2024, doi: 10.15575/join.v9i2.1326.

[5] A. Nugraha, Y. Muhyidin, and I. Kurniawan, "Implementasi Wazuh Dashboard pada Server untuk Monitoring Serangan DDoS terhadap Web XYZ," Scientica: Jurnal Ilmiah Sains dan Teknologi, vol. 2, no. 11, pp. 215–228, 2024.

[6] S. Hawari, A. Ammar, A. N. I. Purwanto, and A. D. Goenawan, "Membangun Mail Server Berbasis Linux Menggunakan Postfix dan Dovecot," Jurnal Teknik Mesin, Industri, Elektro dan Informatika, vol. 1, no. 1, pp. 38–47, 2022, doi: 10.55606/jtmei.v1i1.781.

[7] M. S. Husein, S. Supriyadi, and J. Mulyana, "Membangun Server Mail Menggunakan Postfix Pada Kubuntu 16.04," Jurnal INSTEK, vol. 5, no. 1, pp. 47–56, 2020, doi: 10.24252/instek.v5i1.13297.

[8] H. Mukhtar, D. A. P. Sitorus, and Y. Fatma, "Analisa Dan Implementasi Security Mail Server," Jurnal Fasilkom, vol. 10, no. 1, pp. 25–32, 2020, doi: 10.37859/jf.v10i1.190.

[9] T. Chandra and E. Adelia, "Membangun Mail Server Berbasis Postfix pada Sistem Operasi Linux," Jurnal Ilmiah Core IT, vol. 6, no. 2, 2018.

[10] A. Rismayadi, S. Topiq, and R. Nurtantho, "Membangun Mail Server Berbasis Linux Menggunakan Postfix Admin Di PT. Kemuning Televisi," Jurnal Responsif, vol. 2, no. 1, pp. 92–98, 2020.

[11] M. Mikyal, M. Lamada, and A. Wahid, "Implementasi Keamanan Server Aplikasi E-Raport SMK Negeri 1 Sinjai Menggunakan Wazuh," JIMU: Jurnal Ilmiah Multidisipliner, vol. 3, no. 1, pp. 103–125, 2024.

[12] M. A. G. Sihotang, "Implementasi Sistem Monitoring Jaringan Komputer dengan Grafana dan Prometheus di PT. Nata Digital Solution," Tugas Akhir, Univ. Pembangunan Panca Budi, 2024.

[13] N. Yudyanto, S. Syaifuddin, and Y. Azhar, "Integrasi Modern Honey Network Dengan Grafana Untuk Visualisasi," Jurnal Repositor, vol. 2, no. 10, 2024.

[14] M. A. Husna and P. Rosyani, "Implementasi Sistem Monitoring Jaringan dan Server Menggunakan Zabbix yang Terintegrasi dengan Grafana dan Telegram," JURIKOM, vol. 8, no. 6, p. 247, 2021, doi: 10.30865/jurikom.v8i6.3631.

[15] B. Rasyidi and F. Pratama, "Sistem Monitoring Server di PT. XYZ Media Indonesia Berbasis Grafana dan Prometheus," MALCOM: Indonesian Journal of Machine Learning and Computer Science, vol. 4, no. 4, pp. 1456–1465, 2024, doi: 10.57152/malcom.v4i4.1546.

[16] M. F. Rafi and E. Marpanaji, "Pengembangan Sistem Monitoring Cloud LMS berbasis Grafana, Prometheus dan Telegram di SMK Negeri 2 Yogyakarta," Journal of Information Technology and Education (JITED), vol. 3, no. 1, pp. 91-100, 2025, doi: 10.21831/jited.v3i1.1052.

[17] K. Kent and M. Souppaya, "Guide to Computer Security Log Management," NIST Special Publication 800-92, National Institute of Standards and Technology, Gaithersburg, MD, 2006, doi: 10.6028/NIST.SP.800-92.

[18] S. Few, Information Dashboard Design: The Effective Visual Communication of Data. Sebastopol,

CA: O'Reilly Media, 2006.

[19] X. Cai, K. Efstathiou, X. Xie, Y. Wu, Y. Shi, and L. Yu, "A Study of the Effect of Doughnut Chart Parameters on Proportion Estimation Accuracy," Computer Graphics Forum, vol. 37, no. 3, pp. 300-311, 2018, doi: 10.1111/cgf.13325.