Jurnal Indonesia : Manajemen Informatika dan Komunikasi
www.journal.amikindonesia.ac.id/jimik/ Vol 5 No 1, Januari (2024)
E-ISSN: 2723-7079, P-ISSN: 2776-8074

Implementasi Wazuh Integritas File untuk Perlindungan Keamanan Berdasarkan Aktivitas Log di BTSI UKSW

Bagas Haryanto [1*], Dian W. Chandra [2]

[1*,2] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Kota Salatiga, Provinsi Jawa Tengah, Indonesia.

Email: 672018338@student.uksw.edu [1*], dian.c@uksw.edu [2]

Histori Artikel:
Dikirim 28 Agustus 2023; *Diterima dalam bentuk revisi* 22 September 2023; *Diterima* 1 November 2023; *Diterbitkan* 10 Januari 2024.

Abstrak

Perkembangan teknologi saat ini sudah semakin canggih terutama pada keamanan data. Keamanan data dan integritas File memiliki peran yang penting dan menjadi salah satu perhatian utama dalam lingkungan perusahaan. Diperlukan langkah - langkah efektif untuk sistem keamanan data yang mendeteksi ancaman data terutama integritas File di lingkungan BTSI UKSW. Sistem Wazuh memberikan fitur pemantauan dan pendeteksian aktivitas perubahan File. Fitur tersebut dapat bekerja karena adanya aktivitas perubahan File dan analisis log yang berjalan secara Real-Real. Untuk menjaga keamanan sistem adalah memonitor integritas File, yaitu memastikan bahwa File kritis tidak mengalami perubahan yang tidak sah oleh pihak yang tidak berwenang. Oleh karena itu, dilakukan penelitian sekaligus implementasi Wazuh integritas File untuk perlindungan keamanan berdasarkan aktivitas log di BTSI UKSW. Hasil penelitian menunjukkan bahwa implementasi sistem Wazuh integritas File dapat mengidentifikasi kejadian keamanan terhadap aktivitas mencurigakan terhadap sebuah File dan secara efektif mampu memberikan notifikasi kepada administrator terhadap aktivitas yang tidak sah.

Kata Kunci: Wazuh; Integritas File; Log.

Abstract

Technological developments are now increasingly sophisticated, especially in data security. Data security and File Integrity have an essential role and are one of the main concerns in the corporate environment. Practical steps are needed for a data security system that detects data threats, especially File Integrity within the SWCU BTSI environment. The Wazuh system provides monitoring and detection of File change activity. This feature works because of Real-Real File change activity and log analysis. To maintain system security is to monitor File Integrity, namely ensuring that critical Files are not subject to unauthorized changes by unauthorized parties. Therefore, research was carried out and implementation of File Integrity Wazuh for security protection based on log activity at SWCU BTSI. The results showed that the implementation of the File Integrity Wazuh system can identify security incidents against suspicious activity on a File and is effectively able to provide notifications to administrators against unauthorized activity.

Keyword: Wazuh; Integritas File; Log.

1. Pendahuluan

Teknologi informasi menjadi sangat penting dalam kehidupan sehari-hari. Berbagai jenis teknologi informasi seperti komputer dan internet telah memungkinkan dalam mengakses informasi dengan lebih mudah dan efisien [1]. Oleh karena itu, penting bagi organisasi untuk mengimplementasikan solusi keamanan yang efektif untuk melindungi integritas dan kerahasiaan suatu data. Integritas File merupakan aspek penting dalam keamanan sistem komputer, yang melibatkan pemantauan dan deteksi perubahan yang terjadi pada File - File penting [2]. Jika File atau data tidak terjaga integritasnya, maka dapat terjadi manipulasi data yang dapat mengancam keutuhan data yang berisikan informasi penting [3].

Wazuh adalah platform keamanan yang terfokus pada deteksi ancaman dan pemantauan keamanan. Salah satu fitur utamanya adalah memiliki kemampuan untuk mengawasi dan memantau integritas File dalam system [4]. Dengan menggunakan *Wazuh* Integritas File, *BTSI UKSW* dapat memantau aktivitas sistem dan memeriksa integritas File untuk mencegah perubahan yang tidak diizinkan. *Wazuh* akan memberikan peringatan jika ada perubahan atau aktivitas mencurigakan pada File. Untuk itu, Seberapa efektif implementasi sistem Wazuh dalam mendeteksi perubahan yang tidak sah pada File sistem?

Penelitian yang berjudul Pengujian Integritas File Operasi Tanda Tangan Digital Menggunakan Kombinasi *Hash MD5*, *RSA* dan *Skema Qr-Cod*, Penelitian ini bertujuan untuk mengembangkan perangkat lunak guna melakukan pengujian integritas dokumen dengan tanda tangan digital yang dibangun menggunakan fungsi *hash MD5* dan algoritma *RSA* yang kemudian di-generate menjadi *Qr-Code* pada dokumen yang terdiri dari 1000 kata dengan ekstensi .docx. Dokumen yang akan diuji tersebut diberikan tanda tangan digital dengan perangkat lunak yang dibangun dan selanjutnya dilakukan pengujian integritas dengan melakukan operasi modifikasi terhadap File teks tersebut [5].

Pada penelitian yang berjudul *A ReView of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis*, Tujuan dari penelitian ini adalah untuk menyajikan fungsionalitas Wazuh dalam mendeteksi serangan yang didemonstrasikan di *server web*. *Server web* adalah komponen yang sangat terpapar ke internet dan jika tidak dilindungi dengan baik, mereka sangat rentan terhadap berbagai jenis serangan. Untuk mencegah serangan, mereka harus dideteksi terlebih dahulu dan itulah mengapa sistem *Host Intrusion Detection* digunakan. Salah satu solusi yang bisa membantu adalah Wazuh. Ini adalah alat yang ampuh yang menampilkan semua serangan yang terdeteksi dengan sangat detail dan *RealReal* [6].

Pada penelitian yang berjudul Implementasi *Wazuh* 4.0 untuk Perlindungan Keamanan Integritas File, Penelitian ini bertujuan untuk memantau setiap perubahan dalam *registry* tercatat dalam *event log Wazuh*, *Event Log* menampilkan data yang lengkap beserta *Real stamp*, Data dari *Event Log* dapat digunakan untuk keperluan forensik digital, Pemenuhan standar *FIM* pada *com-pliance* dapat di lakukan menggunakan aplikasi *Wazuh* [7].

Pada penelitian yang berjudul Implementasi *Secury Information and Event Management* (SIEM) pada Aplikasi SMS Center Pemerintah Daerah Provinsi Nusa Tenggara Barat, Penelitian ini bertujuan untuk pengimplementasian SIEM pada salah satu aplikasi SMS Center Pemerintah Daerah Provinsi NTB. SMS Center merupakan sebuah aplikasi yang menyediakan layanan SMS *Gateway* Pemerntah Provinsi NTB yang digunakan untuk broadcast dan mengirim pesan berbasis sms. *Tools* yang akan digunakan sebagai solusi yang ditawarkan adalah menggunakan aplikasi *Wazuh* [3].

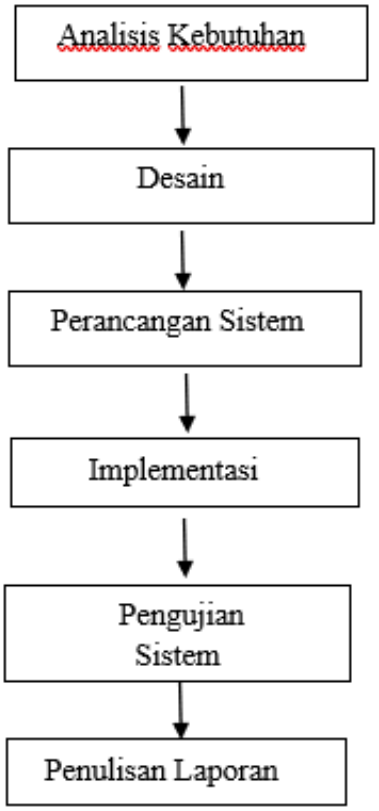
Pada penelitian yang berjudul *Wazuh* sebagai *Log Event Management* dan Deteksi Celah Keamanan pada *Server* dari Serangan *Dos*, Penelitian ini bertujuan untuk memonitoring secara rutin menggunakan Wazuh Manager untuk mendapat informasi berupa log mengenai aktivitas yang dilakukan oleh *Agent*. Kemudian *log* tersebut dapat divisualisasikan oleh *Wazuh* dengan beragam bentuk statistik agar mudah dipahami. Pada menu *Integrity monitoring* menampilkan *log* dari aktivitas berupa membuat,memodifikasi dan menghapus *File*. Untuk mendeteksi adanya *malware* berbahaya, diperlukan integrasi antara *Wazuh Manager* dan Virus Total. Suricata dapat mendeteksi adanya serangan *DoS*. Kemudian *alert* dari suricata tersebut diteruskan *Wazuh* agar ditampilkan pada *web interface Wazuh*. *Alert* dari *Wazuh* akan dikirmkan kepada administrator melalu *e-mail* [4]. Berdasarkan penelitian tersebut, Peneliti memilih untuk membuat penelitian mengenai implementasi sistem pengamanan integritas File. Dari penelitian

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 5 No 1, Januari (2024), pp. 183-192
DOI : https://doi.org/10.35870/jimik.v5i1.447

sebelumnya, sistem *Wazuh* menggunakan metode analisis data pasca kejadian dalam memeriksa integritas sebuah File. Sedangkan, penelitian yang dilakukan sekarang menggunakan sistem *Wazuh* sebagai alat untuk memantau dan memeriksa integritas File secara *Real-Real*.

2. Metode Penelitian

Penelitian ini dilakukan dengan beberapa tahapan, Berikut ini tahap penelitian yang akan digunakan untuk pembuatan penelitian:



Gambar 1. Tahapan Penelitian

Tahapan penelitian pada Gambar 1, dapat dijelaskan sebagai berikut. Tahap pertama adalah analisa kebutuhan. Pada tahap ini untuk menentukan detail kebutuhan yang akan digunakan selama penelitian. Kebutuhan perangkat pendukung seperti hardware dan software sangat diperlukan untuk melakukan implementasi Wazuh Integritas File. Tahap kedua adalah desain yang meliputi sebuah skema sistem Wazuh Integritas File yang akan diimplementasikan di *BTSI UKSW*. Tahap ketiga adalah Perancangan Sistem melakukan perancangan sebuah sistem, diperlukan tools atau aplikasi yang dirancang agar sistem tersebut dapat bekerja secara maksimal. Tahap keempat adalah implementasi, yaitu melakukan implementasi sebuah sistem. Sistem yang sudah dirancang pada tahap sebelumnya, akan diterapkan dan dilakukan uji coba untuk menentukan apakah sistem tersebut berhasil atau gagal. Tahap kelima adalah pengujian sistem hasil, yaitu membahas mengenai pengujian untuk memastikan apakah setiap perubahan pada sistem tersebut terpantau dengan baik. Pengujian sistem ini juga dilakukan bersamaan dengan aktivitas monitoring dan analisa terkait keamanan pada integritas File. Tahap kelima adalah penulisan laporan, yaitu mendokumentasikan setiap proses dalam bentuk laporan tertulis dan akan menjadi laporan yang berbentuk artikel ilmiah.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 5 No 1, Januari (2024), pp. 183-192
DOI : https://doi.org/10.35870/jimik.v5i1.447

3. Hasil dan Pembahasan

3.1 Analisis kebutuhan untuk implementasi Wazuh Integritas File

1) Kebutuhan hardware yang digunakan

Tabel 1. Daftar perangkat keras

No	Nama Perangkat	Spesifikasi
1	Laptop sebagai Wazuh-Server dan Client	Processor : Intel(R) Core i3 1005G1 RAM : 12 GB SSD : 128 GB HDD : 1 TB
2	Laptop sebagai Client	Processor : Intel Core i7-8750H RAM : 16 GB SSD : 128 GB HDD : 1 TB
3	Laptop sebagai Client	Processor : Intel Core i7-8750H RAM : 8 GB SSD : 128 GB HDD : 1 TB

2) Kebutuhan *software* yang digunakan

Tabel 2. Daftar perangkat lunak

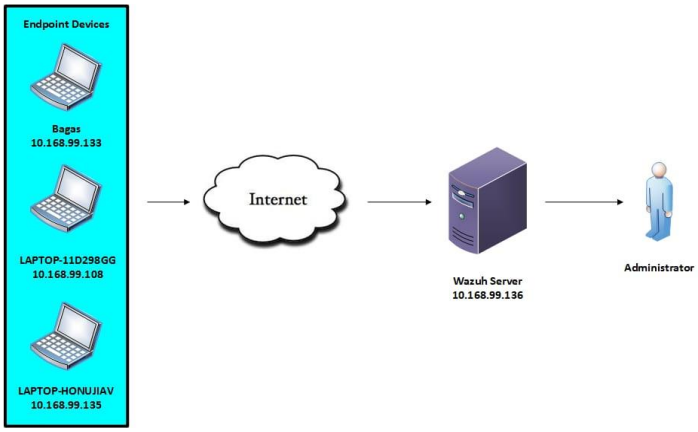
No	Nama Perangkat	Keterangan
1	Ubuntu Server	Sebagai tempat Wazuh-server
2	VirtualBox	Aplikasi virtualisasi untuk menjalankan beberapa sistem operasi yang berbeda secara bersamaan pada satu computer [8].
3	Wazuh	Perangkat berbasis open open yang berfungsi sebaga sistem deteksi intrusi berbasis host (endpoint) [2].
4	Wazuh Indexer	Sebuah komponen dalam Wazuh yang digunakan untuk mengindeks data log yang dikumpulkan oleh Wazuh Agent [9].
5	Wazuh Server	Komponen Wazuh untuk menganalisi data yang diterima dari Wazuh-Agent memicu peringatan jika ada anomali yang terdeteksi [10].
6	Wazuh Dashboard	Komponen ini menampilkan berbagai informasi keamanan yang berguna seperti indikator ancaman, log aktivitas sistem, dan laporan keamanan [11].
7	Wazuh-Agent	Sebuah software atau progRAM yang digunakan untuk mengumpulkan informasi keamanan pada suatu sistem atau jaringan komputer dan mengirimkannya ke server Wazuh untuk dianalisis lebih lanjut [4].

3.2 Desain Skema Sistem Wazuh Integritas File

Tahap ini berisi skema sistem *Wazuh* Integritas File. Skema ini dibuat berdasarkan data dan informasi secara langsung dari BTSI. *Wazuh* Integritas File bekerja sebagai sistem yang terdapat fitur untuk mengumpulkan data dalam bentuk log File dan melakukan monitoring terhadap suatu integritas File. Dalam hal ini, terdapat 3 bagian penting yaitu perangkat *endpoint*, sumber jaringan (internet), dan sistem *Wazuh Server*. *Wazuh* akan memindai File pada ketiga *client* yang ada di sistem dan membuat database File hash yang akan digunakan sebagai acuan. Setelah database hash File dibuat, *Wazuh* akan

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 5 No 1, Januari (2024), pp. 183-192
DOI : https://doi.org/10.35870/jimik.v5i1.447

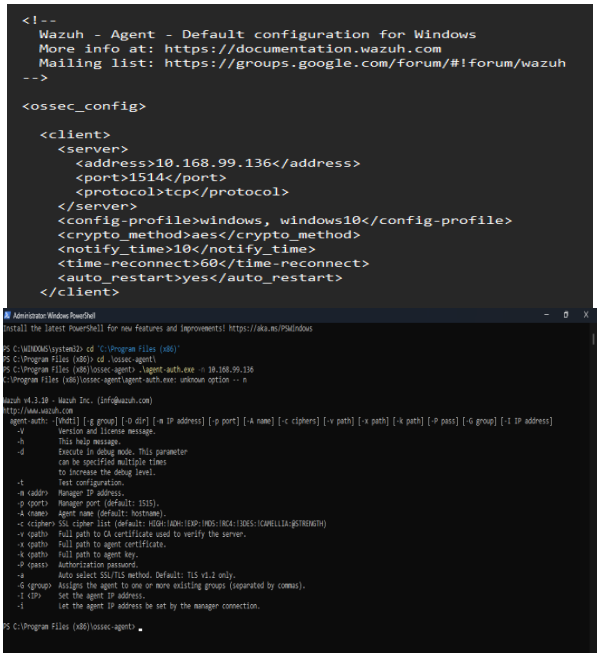
terus memantau perubahan yang terjadi pada File-File di sistem. Jika terdapat perbedaan antara hash baru dengan hash yang ada pada *database*, maka *Wazuh* akan memberikan peringatan atau notifikasi kepada administrator atau pengguna sistem melalui *dashboard Wazuh*.



Gambar 2. Skema Sistem Wazuh Server

3.3 Perancangan sistem Wazuh Integritas File

Pada tahapan ini, menjelaskan mengenai pengaturan system *Wazuh* sebelum dilakukan monitoring integritas File. Konfigurasi ini berisi langkah awal dengan menambahkan alamat IP *Wazuh Server* ke *Wazuh Agent* agar saling terkoneksi. Hasil konfigurasi awal sistem *Wazuh* ini nantinya dapat dilihat dengan menggunakan aplikasi *Wazuh Agent Manager* melalui *View View* dan *Windows Windows*. Untuk detail konfigurasi tersebut dapat dilihat pada Gambar 3.



Gambar 3. Detail konfigurasi ip server Wazuh

Setelah konfigurasi awal telah dilakukan, maka aktivitas selanjutnya adalah menambahkan direktori File tertentu sesuai dengan kebutuhan. Hal ini bertujuan agar sistem *Wazuh* nantinya mendapatkan akses untuk melakukan monitoring ke direktori File secara otomatis. Direktori yang akan dimonitoring yaitu sub-direktori "TA 2" yang terletak di dalam direktori "Kuliah" pada disk drive D:\. Perintah tersebut akan memonitoring direktori "TA 2" dan sub-direktori yang berada di

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 5 No 1, Januari (2024), pp. 183-192
DOI : https://doi.org/10.35870/jimik.v5i1.447

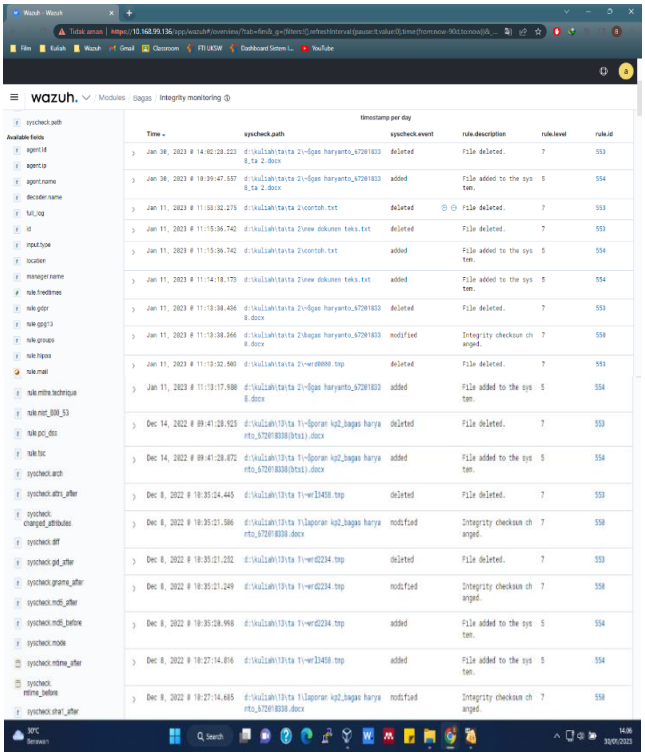
dalamnya untuk melihat apakah ada perubahan data pada file dan sekaligus membuat laporan untuk aktivitas tersebut secara *Real-Real*. Untuk lebih jelasnya dapat dilihat pada Gambar 4 dibawah ini. Setelah proses konfigurasi selesai, *Wazuh Agent* akan memantau integritas File pada direktori yang sudah ditentukan dan mengambil tindakan yang sesuai dengan kebijakan dan telah ditetapkan jika ada perubahan pada File.

```
<directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>

<directories check_all="yes" report_changes="yes" realtime="yes">D:\\Kuliah\TA\TA 2</directories>

<ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>

<ignore type="sregex">.log$|.htm$|.jpg$|.png$|.chm$|.pnf$|.evtx$</ignore>
```

Gambar 4. Direktori yang akan dimonitoring

3.4 Pengujian dan pengimplementasian sistem Wazuh Integritas File

Pada Tahap pengujian sistem Wazuh Integritas *File Monitoring* aktivitas *Log File* secara *Real-Real* perlu dilakukan untuk memastikan bahwa sistem berfungsi dengan baik. Aktivitas tersebut adalah melakukan *Integrity monitoring* terhadap sebuah *File Directory*. Jika suatu *File Directory* sudah terdeteksi, maka secara *Real-Real*. *Wazuh* akan memberikan notifikasi berupa informasi detail *Integrity monitoring* dan waktu aktivitas perubahan File. Untuk tampilan detail monitoring ini kemudian akan dianalisis dan sekaligus *Wazuh* akan melakukan pelacakan aktivitas yang tidak sah atau mencurigakan. Untuk lebih jelasnya mengenai detail *Integrity monitoring* dapat dilihat pada Gambar 5.



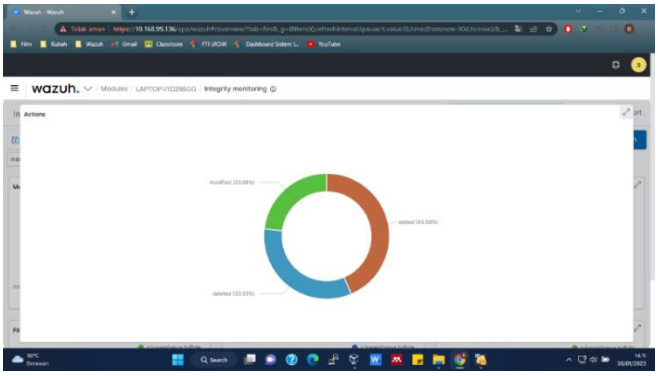
Gambar 5. *Detail File Integrity Monitoring (FIM) Log*

Dari hasil aktivitas yang didapatkan dari aktivitas berupa *Added File*, *Modified File*, dan *Deleted File* yang dilakukan oleh semua *Wazuh Agent* di rentang waktu ±1 bulan. *Wazuh Manager* akan memberikan peringatan bahwa File tersebut sudah dilakukan modifikasi. Dari hasil monitoring, Dapat dilihat bahwa Implementasi Wazuh Integritas File Untuk Perlindungan Keamanan Berdasarkan Aktifitas Log di BTSI UKSW sudah berhasil dilakukan. Berikut adalah bukti screenshot hasil pengujian Wazuh Integritas File dari Agent Bagas pada Gambar 6 dan Gambar 7, untuk Agent LAPTOP-l1D298GG

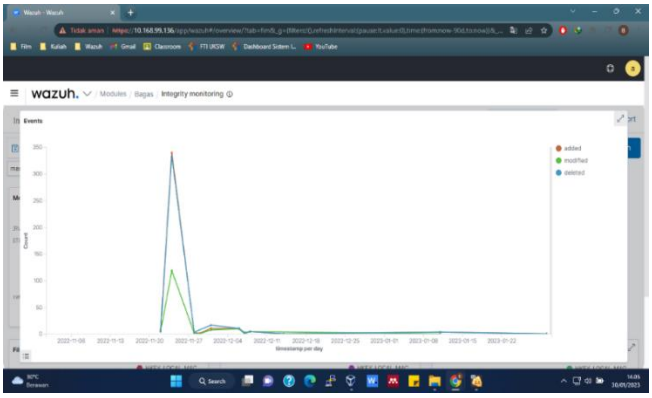
Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 5 No 1, Januari (2024), pp. 183-192
DOI : https://doi.org/10.35870/jimik.v5i1.447

dapat dilihat pada Gambar 8 dan Gambar 9, Sedangkan untuk Agent LAPTOP-HONUJIAV dapat dilihat pada Gambar 10 dan Gambar 11.

1) Bagas

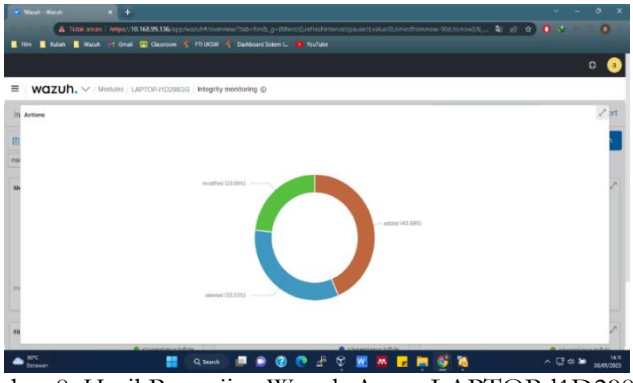


Gambar 6. Hasil Pengujian Wazuh Agent Bagas



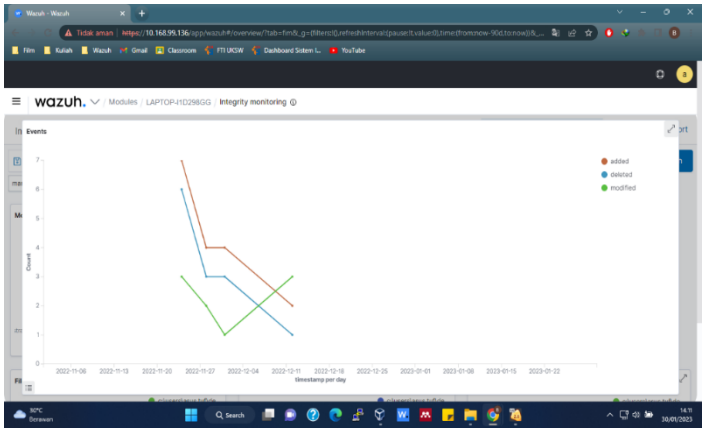
Gambar 7. Hasil Realstamp Per Day Agent Bagas

2) LAPTOP-l1D298GG



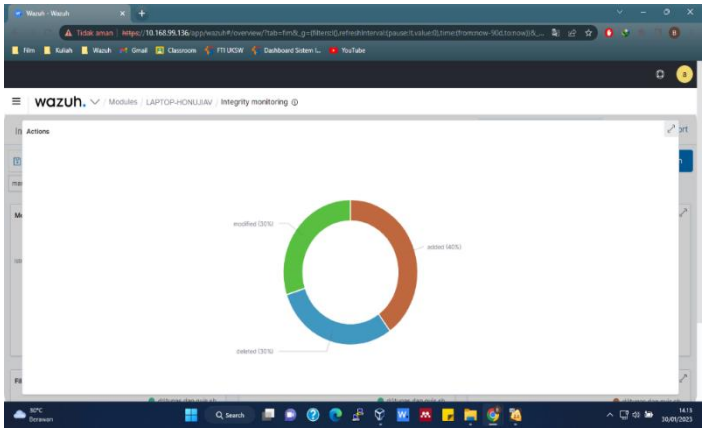
Gambar 8. Hasil Pengujian Wazuh Agent LAPTOP-l1D298GG

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 5 No 1, Januari (2024), pp. 183-192
DOI : https://doi.org/10.35870/jimik.v5i1.447

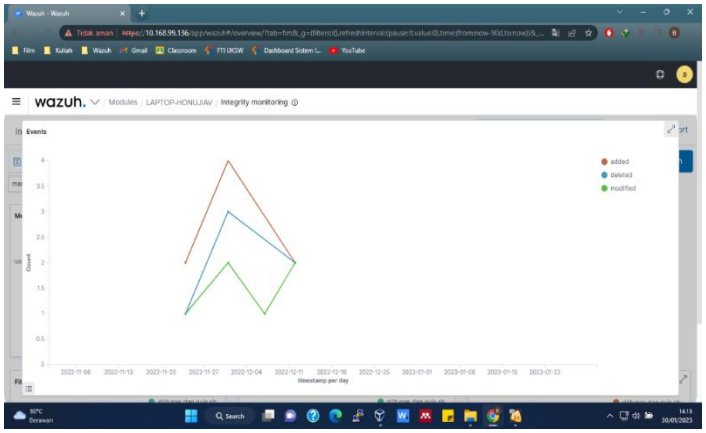


Gambar 9. Hasil Realstamp Per Day Agent LAPTOP-l1D298GG

3) PTOP-HONUJIAV



Gambar 10. Hasil Pengujian Wazuh Agent LAPTOP-HONUJIAV



Gambar 11. Hasil Realstamp Per Day Agent LAPTOP-HONUJIAV

Dari Hasil pengujian menggunakan Wazuh diukur pada tingkat keakuratan Wazuh dalam memantau dan mengaudit integritas File. Wazuh Integritas File bekerja sangat baik dan memiliki fitur yang sangat berguna sebagai pendeteksi keamanan pada komputer client. Dalam hal ini, Wazuh melakukan audit dan analisis log File untuk mengidentifikasi kejadian keamanan yang tidak biasa atau mencurigakan. Berikut adalah persentase hasil dari pengujian Wazuh Integritas File yang telah dilakukan pada Tabel 3.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 5 No 1, Januari (2024), pp. 183-192
DOI : https://doi.org/10.35870/jimik.v5i1.447

Tabel 3. Detail Integrity File

No	Nama *Agent*	*Integrity File*		
		Added	*Delete*	*Modified*
1	Bagas	42,05%	41,41%	16,54%
2	LAPTOP-l1D298GG	43,59%	33,33%	23,08%
3	LAPTOP-HONUJIAV	40%	30%	30%

4. Kesimpulan

Penelitian ini Berdasarkan hasil pengujian Wazuh Integritas File di *BTSI UKSW*, dapat di ketahui bahwa implementasi sistem ini dapat dijadikan rekomendasi dalam mempertahankan keamanan data. Selain itu, Wazuh Integritas File ini juga dapat mendeteksi perubahan aktivitas yang tidak sah pada File, serta memantau File untuk memastikan bahwa tidak ada perubahan yang tidak diizinkan akan terjadi. Dalam uji coba yang sudah dilakukan. Wazuh Integritas File mampu secara efektif mendeteksi perubahan pada File yang diawasi oleh fitur–fitur khusus dan memberikan notifikasi kepada administrator. Selain itu, Wazuh Integritas File juga mampu melakukan validasi integritas File dengan membandingkan checksum dari File yang diawasi dengan nilai checksum yang disimpan di dalam database Wazuh. Secara keseluruhan, implementasi Wazuh Integritas File dapat menjadi pilihan yang tepat untuk meningkatkan keamanan sistem dan memantau aktivitas yang mencurigakan pada aktivitas penggunaan File.

5. Daftar Pustaka

[1] Munawar, Z., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *J-SIKA | Jurnal Sistem Informasi Karya Anak Bangsa*, *2*(01), 14-20.

[2] Fahrudi, M. A., & Suartana, I. M. (2023). Integrasi End-point Security Berbasis Agent dan Bot Messenger untuk Deteksi dan Monitoring Serangan pada Web Server secara Real-time. *Journal of Informatics and Computer Science (JINACS)*, 275-282. DOI: https://doi.org/10.26740/jinacs.v4n03.p275-282.

[3] Khotimah, H., Bimantoro, F., Kabanga, R. S., & Widiartha, I. B. K. (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). DOI: https://doi.org/10.29303/jbegati.v3i2.752.

[4] Nova, F., Pratama, M. D., & Prayama, D. (2022). Wazuh Sebagai log event management Dan Deteksi Celah Keamanan Pada server dari serangan dos. *JITSI: Jurnal Ilmiah Teknologi Sistem Informasi*, *3*(1), 1-7. DOI: https://doi.org/10.30630/jitsi.3.1.59.

[5] Mursid, H., Supardi, J., & Rizkie, M. Q. (2022). Pengujian Integritas File Operasi Tanda Tangan Digital Menggunakan Kombinasi Hash MD5, RSA dan Skema Qr-Cod. *Generic*, *14*(2), 30-37.

[6] Stanković, S., Gajin, S., & Petrović, R. A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis.

[7] Laksmiati, D. (2021). IMPLEMENTASI WAZUH 4.0 UNTUK PERLINDUNGAN KEAMANAN INTEGRITAS FILE. *Akrab Juara: Jurnal Ilmu-ilmu Sosial*, *6*(3), 164-174. DOI: https://doi.org/10.58487/akrabjuara.v6i3.1513.