Sains Data Jurnal Studi Matematika dan Teknologi
ISSN 2986-903X
v2i2(2024); p. 80-92

Implementasi Wazuh FIM (*File Integrity Monitoring*) untuk Perlindungan Keamanan Sistem Informasi pada Unit Kegiatan Mahasiswa di Universitas Trunojoyo Madura

Alvin Kamil[1], Darian Rizaludin[2], Ana Tsalitsatun Ni'mah[3]
[1,3]Pendidikan Informatika, Universitas Trunojoyo Madura; Jl Raya Telang, Kamal Bangkalan Kode Pos 69162;
[2]PT Radnet Digital Indonesia; Trillium Office & Residence, Jl. Pemuda, Genteng Surabaya, Kode Pos 60271
Correspondence: 220631100006@student.trunojoyo.ac.id, ana.tsalits@trunojoyo.ac.id, rizaludindarian@gmail.com

DOI : https://doi.org/10.52620/sainsdata.v2i2.127

Abstrak

Keamanan data menjadi semakin penting dengan pesatnya perkembangan tekhnologi saat ini. Perkembangan tekhnologi yang pesat, terutama dalam keamanan data semakin menekankan pentingnya integritas file dan perlindungan data dalam lingkungan organisasi. Langkah-langkah efektif diperlukan untuk mendeteksi ancaman terhadap integritas file, khususnya di UKM Triple-C. Sistem Wazuh memiliki modul file integrity monitoring (FIM), FIM digunakan untuk memantau aktifitas perubahan yang terjadi pada file yang bersifat penting secara Realtime. Memantau integritas file dan memastikan bahwa file penting tidak mengalami perubahan yang tidak sah, sangat penting untuk menjaga keamanan sistem. Oleh kerena itu, dilakukan penelitian dan implementasi sistem Wazuh pemantauan integritas file (FIM) sebagai perlindungan keamanan di UKM Triple-C Universitas Trunojoyo Madura. Penelitian ini dilakukan menggunakan metode waterfall. Hasil penelitian menunjukkan bahwa implementasi Wazuh mampu mengidentifikasi kejadian keamanan terkait aktifitas mencurigakan yang terjadi pada file yang di monitoring dan memberikan notifikasi secara efektif kepada administrator.

Kata Kunci: Wazuh, Integritas File, File Integrity Monitoring (FIM), Keamanan Data.

Abstract

Data security is becoming increasingly important with the rapid development of technology today. The rapid development of technology, especially in data security, further emphasises the importance of file integrity and data protection in an organisational environment. Effective measures are needed to detect threats to file integrity, especially in UKM Triple-C. The Wazuh system has a file integrity monitoring (FIM) module, FIM is used to monitor the activity of changes that occur in important files in real time. Monitoring file integrity and ensuring that important files do not undergo unauthorised changes, is very important to maintain system security. Therefore, research and implementation of the file integrity monitoring (FIM) Wazuh system as security protection at UKM Triple-C Trunojoyo Madura University was conducted. This research was conducted using the waterfall method. The results showed that the implementation of Wazuh was able to identify security events related to suspicious activities that occurred in the files being monitored and provide notifications effectively to the administrator.

Keywords: *Wazuh, File Integrity, File Integrity Monitoring (FIM), Data Security.*

PENDAHULUAN

Pada era digital yang terus berkembang saat ini, keamanan informasi menjadi hal yang sangat diperlukan bagi setiap individu maupun organisasi. Dengan semakin luas dan cepatnya perkembangan internet, akses untuk memperoleh data dan informasi dapat lebih mudah, cepat, dan praktis (Aziz Saputra, 2023). Namun, dengan mudahnya untuk mendapatkan akses informasi tersebut menyebabkan munculnya sebuah permasalahan baru yakni potensi pencurian dan

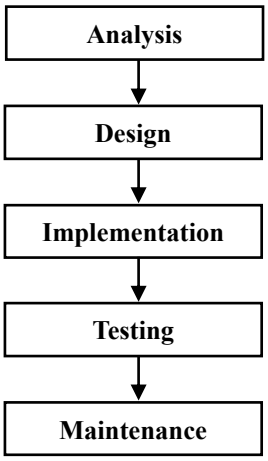
penyalahgunaan data penting oleh pihak yang tidak bertanggung jawab demi keuntungan pribadi (Fahrudi & Suartana, 2023). Oleh karena itu, sangat penting bagi organisasi untuk menerapkan solusi keamanan yang efektif guna melindungi integritas dan keamana data mereka. Integritas file merupakan salah satu aspek penting dalam keamanan sistem komputer, yang mencakup pemantauan serta pendeteksian terhadap setiap perubahan yang terjadi pada file-file penting (Adzimi et al., 2024). Apabila integritas file tidak terjaga, maka dapat terjadi manipulasi data, yang pada akhirnya bisa membahayakan keutuhan informasi penting yang terkandung di dalamnya (Haryanto & Chandra, 2024).

Untuk menjaga integritas file dan mencegah file agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab, diperlukan sebuah aplikasi keamanan yang efektif untuk memantau dan mendeteksi setiap perubahan dan manipulasi yang terjadi pada setiap file atau folder penting. Wazuh merupakan perangkat lunak *open souce* yang terfokus pada deteksi keamanan dan pemantauan integritas file (Haryanto & Chandra, 2024). Wazuh mempunyai modul File Integrity Monitoring (FIM) yang berfungsi dalam memantau integritas file jika terjadi perubahan pada file, baik pada konten, grup, kontrol akses, dan properti lainnya yang dilakukan oleh pengguna yang berwenang maupun pengguna yang tidak berwenang (Hilmi Abdullah et al., 2011). Wazuh dipilih karena *open source* dan kemampuannya yang handal serta fleksibel dalam memantau integritas file secara realtime serta menyediakan *alret* segera jika terjadi perubahan yang mencurigakan pada file atau folder.

Penelitian ini berjudul "Implementasi Wazuh pemantauan integritas file sebagai perlindungan keamanan data di UKM Triple-C Universitas Trunojoyo Madura" bertujuan untuk mengimplementasikan Wazuh sebagai solusi keamanan integritas file di Seketariat Unit Kegiatan Mahasiswa (UKM) Triple-C. UKM Triple-C adalah UKM tingkat Universitas di Universitas Trunojoyo Madura (UTM) yang bergerak di bidang Teknologi Informasi dan Komunikasi sehingga integritas file harus menjadi perhatian khusus untuk UKM Triple-C untuk menjaga keabsahan data (Paramita et al., 2022). UKM Triple-C perlu melakukan monitoring terhadap keamanan dan integritas file mereka. Ini melibatkan pemantauan aktifitas pengguna, pencatatan log, dan analisis aktivitas mencurigakan. Dengan pemantauan aktivitas ini, UKM Triple-C dapat mengidentifikasi potensi pelanggaran keamanan dan integritas file mereka (Susanto et al., 2023). Sehingga dapat memantau dan mencegah aktivitas pelanggaran baik modifikasi, penghancuran, dan penyalahgunaan oleh pengguna maupun pihak yang tidak berwenang (Nurul et al., 2022).

METODE PENELITIAN

Penelitian ini menggunakan metode waterfall, metode waterfall memilki beberapa tahapan yang terstruktur dan sistematis. Berikut adalah tahapan dari metode waterfall:



Gambar 1 Metode Waterfall
Sumber: (Wahyuningsih U, 2023)

Pada gambar 1 menunjukkan tahapan-tahapan metode waterfall yang akan dilakukan dalam penelitian ini, tahapan-tahapan tersebut dapat dijelaskan sebagai berikut : 1) *Analysis* (Analisis), tahapan ini dilakukan untuk mengidentifikasi dan menentukan detail yang diperlukan untuk penelitian. Perangkat pendukung, seperti software dan hardware sangat penting untuk implementasi Wazuh dalam pemantauan integritas file; 2) *Design* (Desain), pada tahap ini rencana atau skema sistem Wazuh untuk pemantauan integritas file dibuat, yang akan diimplementasikan di sekret UKM Tiple-C; 3) *Implementation* (Implementasi), pada tahap ini sistem yang sudah dirancang pada tahap sebelumnya diterapkan dan mengkonfigurasi perangkat yang digunakan; 4) *Testing* (Pengujian), Pada tahap ini peneliti melakukan pengujian terhadap sistem untuk memastikan bahwa setiap perubahan pada file penting dapat dipantau dengan baik untuk memastikan keamanan integritas file dan memastikan Wazuh bekerja seperti yang diharapkan serta menampilkan peringatan jika terjadi perubahan pada file penting; 5) *Maintenance* (Pemeliharaan), tahap terakhir ini dilakukan pemeliharaan terhadap sistem yang telah dikembangkan;

HASIL DAN PEMBAHASAN

1. Analysis (Analisis)

Kebutuhan Hardware

Tabel 1 Kebutuhan Hardware

No	Nama Perangkat	Spesifikasi
1	Laptop sebagai Wazuh-Server dan Client	Processor : 12th Gen Intel(R) Core i3-1215U RAM : 16 GB SSD : 512 GB
2	Komputer sebagai Client	Processor : Intel(R) Core i5-8250U RAM : 4 GB SSD : 120 GB

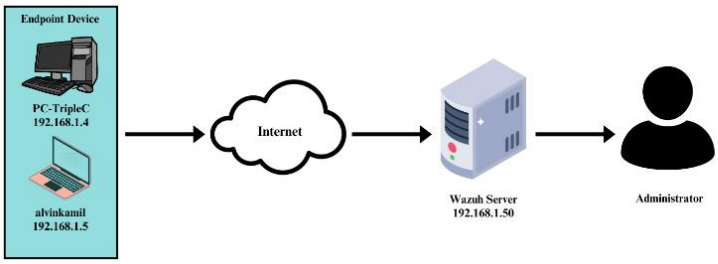
Kebutuhan Software

Tabel 2 Kebutuhan Software

No	Nama Perangkat	Keterangan
1	Ubuntu Server	Tempat Wazuh-server di install (Haryanto & Chandra, 2024).
2	VirtualBox	Aplikasi *hypervisor* tipe 2 yang dapat menjalankan beberapa sistem operasi tamu di dalamnya sehingga dapat melakukan percobaan dengan beberapa tools sesuai dengan keperluan (Aziz Saputra, 2023).
3	Wazuh Server	Komponen dari Wazuh yang bertugas menganalisi data yang diterima dari Wazuh agent dan memberikan peringatan jika terjadi perubahan pada file (Punta Dewa & Windarto, 2024).
4	Wazuh Indexer	Mesin pencari yang digunakan untuk mengindeks dan menyimpan peringatan yang dihasilkan oleh Wazuh-server (Punta Dewa & Windarto, 2024).
5	Wazuh Dashboard	Antarmuka web yang menampilkan dan memvisualisasikan berbagai informasi keamanan yang berguna seperti pemantauan integritas file, indikator ancaman, log aktivitas sistem, dan laporan keamanan (Punta Dewa & Windarto, 2024).
6	Wazuh Agent	Sebuah komponen yang di pasang pada perangkat *Endpoint* seperti *Linux, Windows, macOS,* dan sistem operasi lainnya, untuk mendeteksi dan mengumpulkan informasi keamanan pada suatu sistem lalu mengirimkannya ke Wazuh-server (Punta Dewa & Windarto, 2024).

2. Design (Desain)

Pada tahap ini berisi skema sistem Wazuh integritas file. Skema ini dibuat berdasarkan data dan informasi secara langsung dari Tiple-C. Wazuh berfungsi sebagai sistem yang memiliki fitur untuk mengumpulkan data dalam bentuk log file dan memonitor integritas file. Ada tiga komponen utama dalam sistem ini, yaitu *device endpoint,* sumber jaringan (internet), dan Wazuh server. Wazuh akan memindai file pada kedua agent yang terhubung dalam sistem dan membuat database hash file. Setelah hash file dibuat, Wazuh akan terus memantau perubahan yang terjadi pada file di sistem. Jika ditemukan perbedaan antara hash baru dengan hash yang tersimpan di database, Wazuh akan memberikan *alert* kepada administrator atau pengguna sistem melalui *dashboard* Wazuh.



Gambar 2 Skema Sistem Wazuh

3. Implementation (Implementasi)

Konfigurasi IP Wazuh-server

Peneliti melakukan konfigurasi ip Wazuh-server dengan ip statis 192.168.1.50/24 seperti yang ditunjukkan pada gambar 3 agar Wazuh-server memiliki IP yang pasti.

```
root@servertriplec: /home/tri
root@servertriplec:/home/triplec# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4e:67:7d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.50/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
root@servertriplec:/home/triplec#
```

Gambar 3 Mengkonfigurasi static IP Wazuh-server

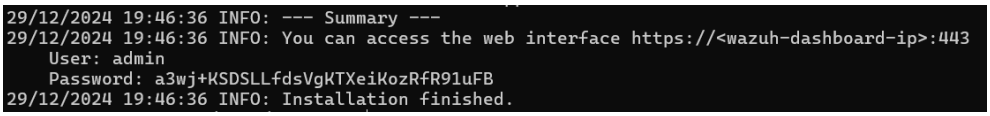
Konfigurasi Wazuh

Peneliti melakukan pemasangan Wazuh pada laptop server yang dijadikan tempat Wazuh-Server seperti yang ditunjukkan oleh gambar 4. Wazuh memiliki beberapa komponen yakni Wazuh-*indexer*, Wazuh-server, dan Wazuh-*dashboard* yang harus terpasang agar sistem Wazuh bisa berjalan dengan nornal. Pemasangan Wazuh dilakukan dengan menginputkan perintah :

```
Curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh install.sh -a
```

Gambar 4 instalasi Wazuh-server, Wazuh-*indexer,* Wazuh-*dashboard*

Setelah pemasangan wazuh-indexer, wazuh-server, dan wazuh-dashboard akan ditampilkan *summary* yang berisi cara mengakses wazuh-dashboard, username, dan password default untuk login ke wazuh-dashboard.



Gambar 5 username dan password default untuk login ke wazuh-dashboard

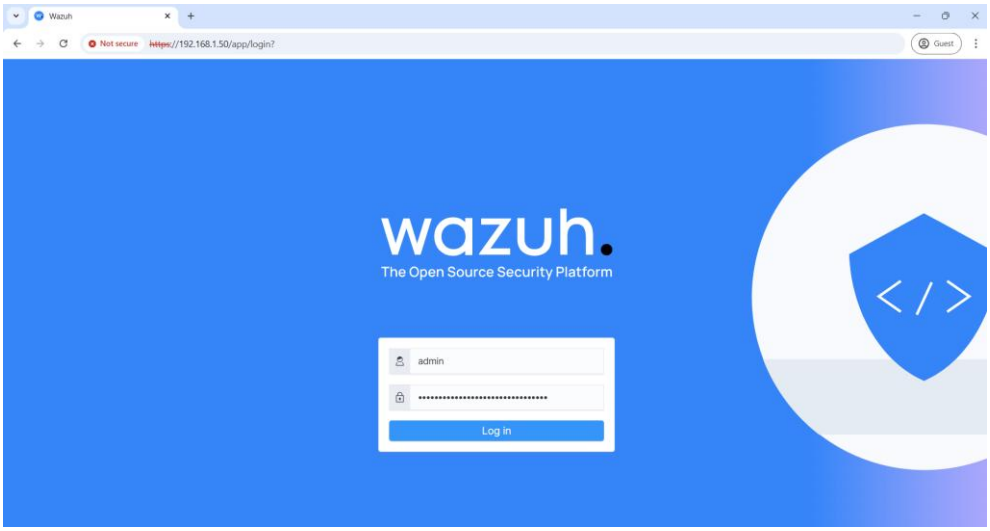
Pengecekan IP Address Wazuh *Dashboard*

Setelah pemasangan Wazuh peneliti melakukan pengecekan ip Wazuh-server untuk login ke wazuh-*dashboard.* Pengecekan *IP address* dapat dilakukan dengan mengetikkan perintah "ip a" pada terminal Wazuh-server, seperti yang tertera pada gambar 6, *IP address* Wazuh-server adalah 192.168.1.50.

Gambar 6 Pengecekan IP Wazuh-server

Login Wazuh *Dashboard*

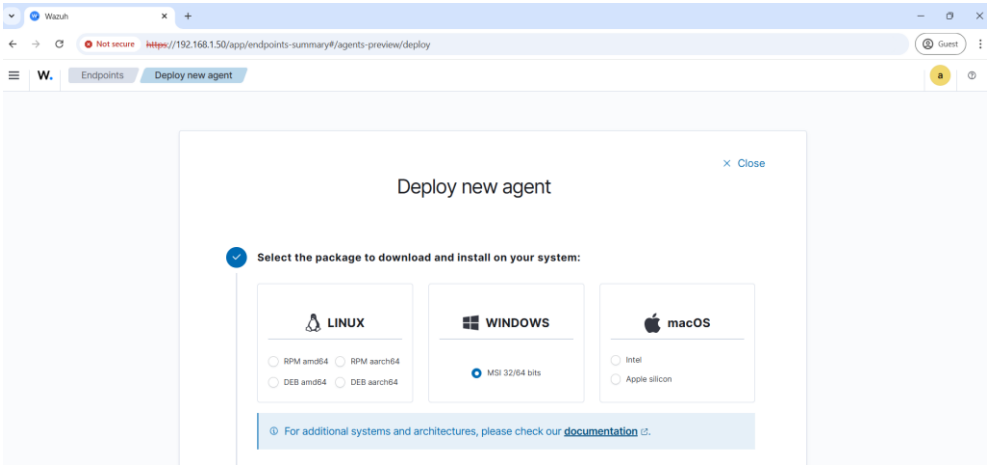
Setelah mendapatkan ip Wazuh-server langkah selanjutnya peneliti masuk ke Wazuh-*dashboard* menggunakan *IP address* di peramban web broser yang tersedia di *device endpoint.* Peneliti menggunakan google chrome untuk masuk ke wazuh *dashboard* dengan menggunakan https://(ip server wazuh). Setelah masuk menggunakan https://192.168.1.50 kemudian akan ditampilkan menu *login* dari Wazuh-*dashboard*. Peneliti memasukkan *username* dan *password default* yang disediakan oleh Wazuh.



Gambar 7 *Login* Wazuh-*dashboard*

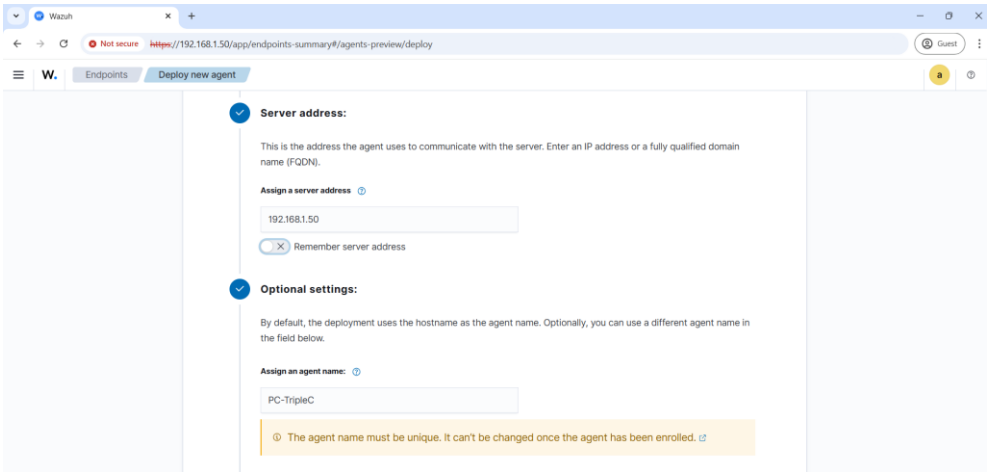
Penambahan Wazuh Agent

Setelah peneliti melakukan login pada wazuh-*dashboard*. Peneliti menambahkan Wazuh agent baru menggunakan fitur *Deploy New Agent* agar Wazuh server dapat terhubung dengan Wazuh *agent* untuk memantau aktifitas pada Wazuh *agent.* Pada gambar 8 peneliti memilih sistem operasi windows sesuai dengan sistem operasi yang digunakan oleh *agent.*



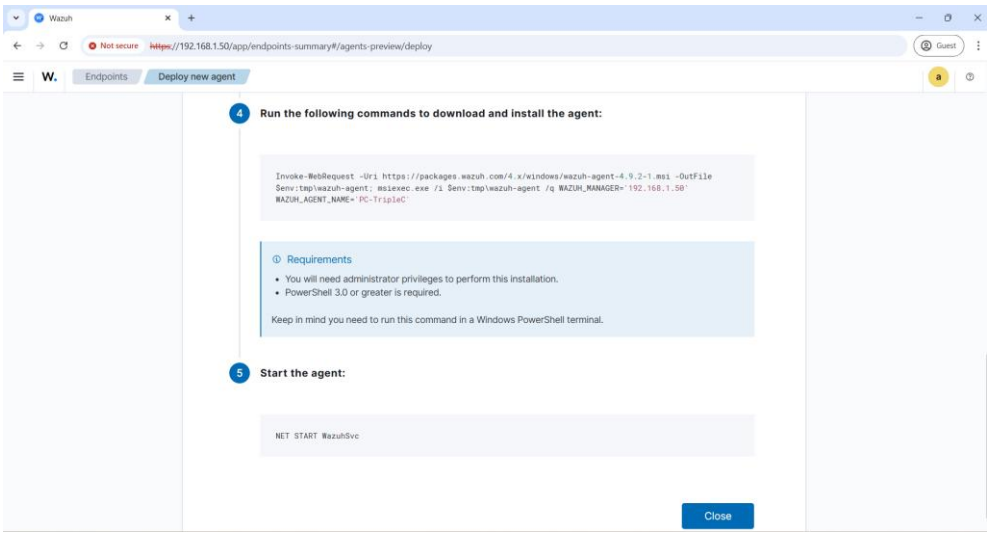
Gambar 8 Pemilihan SIstem Operasi *Endpoint* Untuk Pembuatan Wazuh *Agent* Baru

Pada gambar 9, peneliti memasukkan IP address Wazuh-server. Server address dimasukkan ke dalam pembuatan Wazuh *agent* agar *agent* dapat terhubung dengan wazuh-server. Pada bagian *Optional Settings*, peneliti menggunakan nama “PC-TripleC” sebagai nama *agent*.



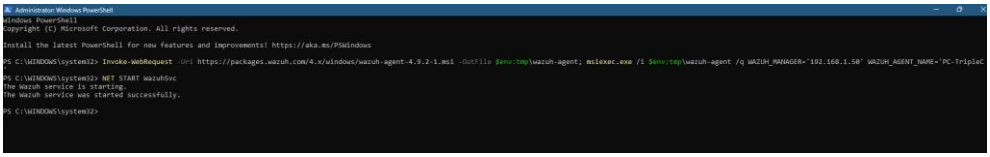
Gambar 9 Input IP Server Address Dan Nama *Agent*

Setelah melakukan pengisian server address dan nama *agent* selesai, Wazuh memberikan dua *command line* yang berisikan perintah untuk menginstall Wazuh-*agent* dan perintah untuk menjalankan Wazuh-*agent,* seperti yang tertera pada gambar 10.



Gambar 10 *Command Line* Untuk Menginstall Dan Menjalankan Wazuh *Agent*

Pada gambar 11, peneliti menjalankan kedua perintah *command line* yang diberikan Wazuh menggunakan Powershell Administrator untuk installasi Wazuh *agent* dan menjalankan wazuh *agent* agar berfungsi pada *Device Endpoint.*



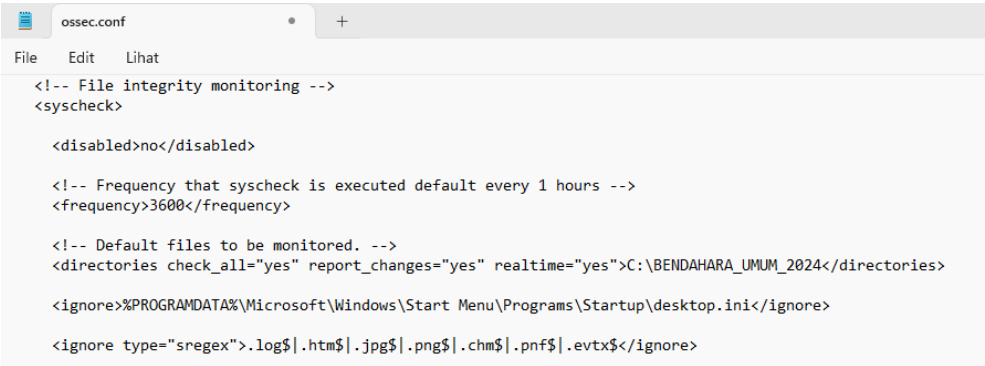
Gambar 11 Menjalankan Wazuh *Agent* Pada Windows *Endpoint*

Konfigurasi *File Integrity Monitoring* (FIM) pada *agent* PC-TripleC

Pada tahap konfigurasi *File Integrity Monitoring* (FIM), peneliti membuat syscheck pada Wazuh *agent* melalui direktori C pada *folder* ossec-agent bagian file ossec.conf. Syscheck dibuat menjadi aktif agar Wazuh *agent* dapat melakukan *monitoring* file secara *real time* untuk memastikan integritas file. Pada gambar 12 peneliti menambahkan direktori yang akan

dimonitoring secara *realtime* yaitu direktori BENDAHARA_UMUM_2024 yang terletak pada lokal disk C: dengan perintah :

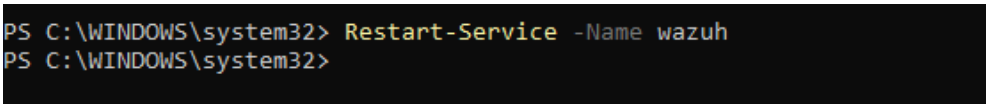
```
<directories check_all="yes" report_changes="yes" realtime="yes">
C:\BENDAHARA_UMUM_2024</directories>
```



Gambar 12 Mengaktifkan *file integrity monitoring* (FIM)

setelah mengkonfigurasi *File Integrity Monitoring* (FIM) lakukan restart service Wazuh agar konfigurasi bisa diterapkan oleh Wazuh menggunakan perintah :

```
Restart-Service -Name wazuh
```

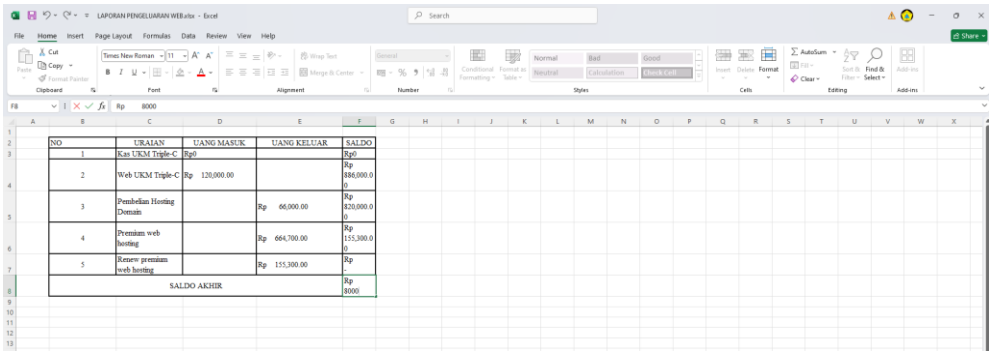


Gambar 13 Memulai Ulang *Service* Wazuh pada Wazuh *Agent*

4. Testing (Pengujian Sistem Wazuh Integritas File)

Pada tahap pengujian
sistem Wazuh *File Integrity Monitoring* (FIM) aktivitas log file secara *Realtime* perlu dilakukan untuk memastikan sistem dapat berfungsi dengan baik. Aktivitas tersebut adalah melakukan *Integrity Monitoring* terhadap sebuah *File Directory.* Pada gambar 14,15,16 peneliti melakukan pengujian berupa *Added File, Modified File,* dan *Deleted File* pada file LAPORAN_PENGELUARAN_WEB yang berada di *Directory* BENDAHARA_UMUM_2024.

Gambar 14 *Added File* LAPORAN_PENGELUARAN_WEB



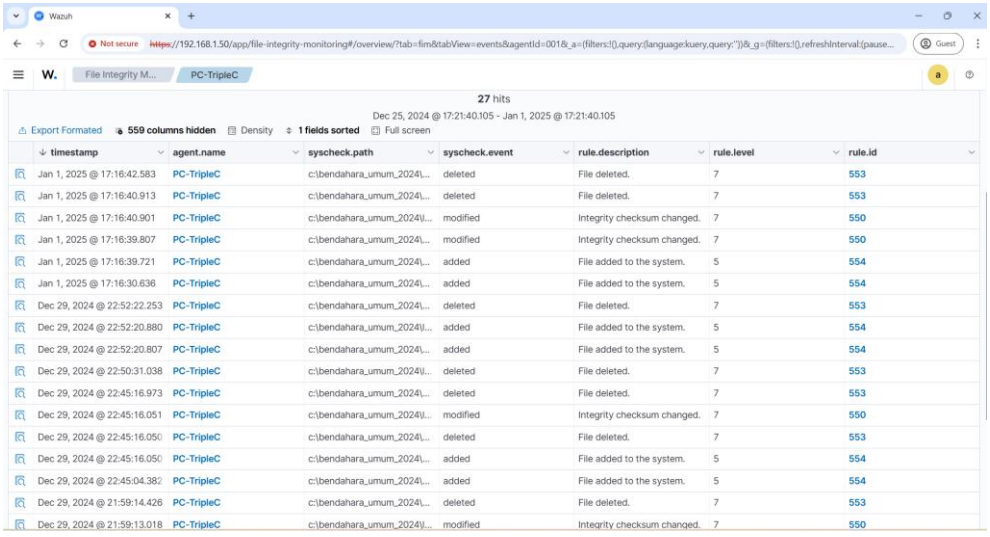
NO	URAIAN	UANG MASUK	UANG KELUAR	SALDO
1	Kas UKM Triple-C	Rp0		Rp0
2	Web UKM Triple-C	Rp 120,000.00		Rp 886,000.00
3	Pembelian Hosting Domain		Rp 66,000.00	Rp 820,000.00
4	Premium web hosting		Rp 664,700.00	Rp 155,300.00
5	Renew premium web hosting		Rp 155,300.00	Rp -
SALDO AKHIR				Rp 8000

Gambar 15 Modified File LAPORAN_PENGELUARAN_WEB

Gambar 16 Deleted File LAPORAN_PENGELUARAN_WEB

Hasil Pengujian Sistem Wazuh Integritas File

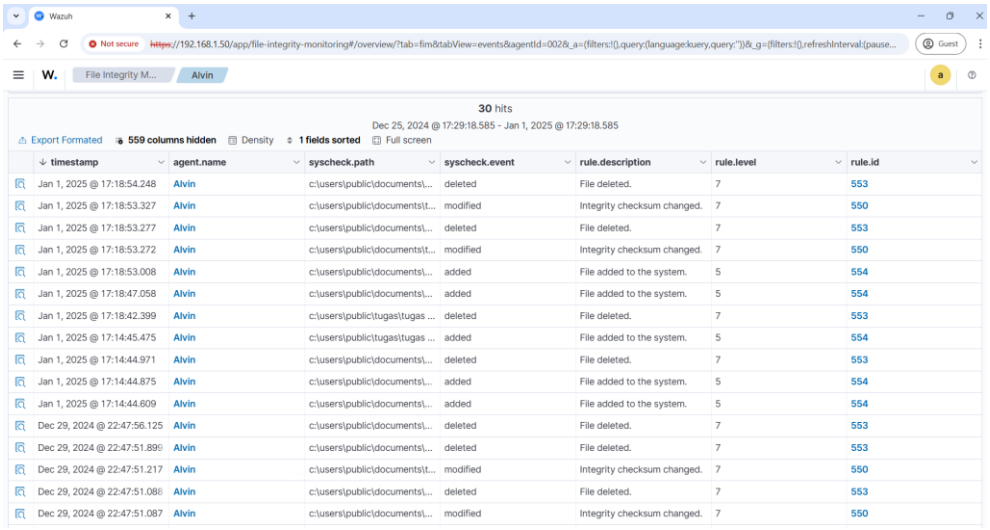
Pada gambar 17,18 dari hasil aktivitas yang didapatkan, seperti *Added File*, *Modified File,* dan *Deleted File* yang dilakukan oleh *agent* PC-TripleC dan *agent* Alvin dalam rentang waktu ± 4 hari. Wazuh Manager memberikan peringatan, bahwa File tersebut sudah dilakukan modifikasi. Dari hasil *monitoring*, dapat dilihat bahwa Implementasi Wazuh Pemantauan Integritas File Sebagai Perlindungan Keamanan Di UKM Triple-C Universitas Trunojoyo Madura berhasil dilakukan.



27 hits
Dec 25, 2024 @ 17:21:40.105 - Jan 1, 2025 @ 17:21:40.105

timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Jan 1, 2025 @ 17:16:42.583	PC-TripleC	c:\bendahara_umum_2024\...	deleted	File deleted.	7	553
Jan 1, 2025 @ 17:16:40.913	PC-TripleC	c:\bendahara_umum_2024\...	deleted	File deleted.	7	553
Jan 1, 2025 @ 17:16:40.901	PC-TripleC	c:\bendahara_umum_2024\...	modified	Integrity checksum changed.	7	550
Jan 1, 2025 @ 17:16:39.807	PC-TripleC	c:\bendahara_umum_2024\...	modified	Integrity checksum changed.	7	550
Jan 1, 2025 @ 17:16:39.721	PC-TripleC	c:\bendahara_umum_2024\...	added	File added to the system.	5	554
Jan 1, 2025 @ 17:16:30.636	PC-TripleC	c:\bendahara_umum_2024\...	added	File added to the system.	5	554
Dec 29, 2024 @ 22:52:22.253	PC-TripleC	c:\bendahara_umum_2024\...	deleted	File deleted.	7	553
Dec 29, 2024 @ 22:52:20.880	PC-TripleC	c:\bendahara_umum_2024\...	added	File added to the system.	5	554
Dec 29, 2024 @ 22:52:20.807	PC-TripleC	c:\bendahara_umum_2024\...	added	File added to the system.	5	554
Dec 29, 2024 @ 22:50:31.038	PC-TripleC	c:\bendahara_umum_2024\...	deleted	File deleted.	7	553
Dec 29, 2024 @ 22:45:16.973	PC-TripleC	c:\bendahara_umum_2024\...	deleted	File deleted.	7	553
Dec 29, 2024 @ 22:45:16.051	PC-TripleC	c:\bendahara_umum_2024\...	modified	Integrity checksum changed.	7	550
Dec 29, 2024 @ 22:45:16.050	PC-TripleC	c:\bendahara_umum_2024\...	deleted	File deleted.	7	553
Dec 29, 2024 @ 22:45:16.050	PC-TripleC	c:\bendahara_umum_2024\...	added	File added to the system.	5	554
Dec 29, 2024 @ 22:45:04.382	PC-TripleC	c:\bendahara_umum_2024\...	added	File added to the system.	5	554
Dec 29, 2024 @ 21:59:14.426	PC-TripleC	c:\bendahara_umum_2024\...	deleted	File deleted.	7	553
Dec 29, 2024 @ 21:59:13.018	PC-TripleC	c:\bendahara_umum_2024\...	modified	Integrity checksum changed.	7	550

Gambar 17 *Detail File Integrity Monitoring (FIM) Log*

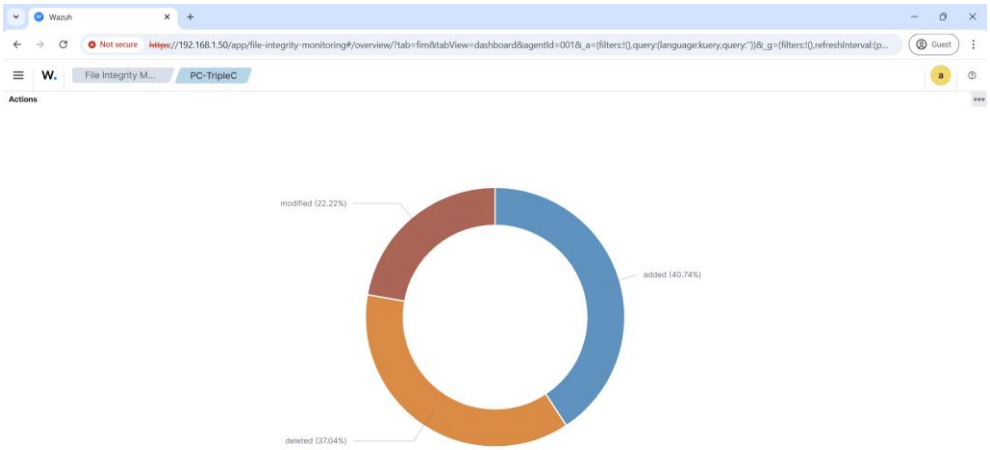


timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Jan 1, 2025 @ 17:18:54.248	Alvin	c:\users\public\documents\...	deleted	File deleted.	7	553
Jan 1, 2025 @ 17:18:53.327	Alvin	c:\users\public\documents\t...	modified	Integrity checksum changed.	7	550
Jan 1, 2025 @ 17:18:53.277	Alvin	c:\users\public\documents\...	deleted	File deleted.	7	553
Jan 1, 2025 @ 17:18:53.272	Alvin	c:\users\public\documents\t...	modified	Integrity checksum changed.	7	550
Jan 1, 2025 @ 17:18:53.008	Alvin	c:\users\public\documents\...	added	File added to the system.	5	554
Jan 1, 2025 @ 17:18:47.058	Alvin	c:\users\public\documents\...	added	File added to the system.	5	554
Jan 1, 2025 @ 17:18:42.399	Alvin	c:\users\public\tugas\tugas ...	deleted	File deleted.	7	553
Jan 1, 2025 @ 17:14:45.475	Alvin	c:\users\public\tugas\tugas ...	added	File added to the system.	5	554
Jan 1, 2025 @ 17:14:44.971	Alvin	c:\users\public\documents\...	deleted	File deleted.	7	553
Jan 1, 2025 @ 17:14:44.875	Alvin	c:\users\public\documents\...	added	File added to the system.	5	554
Jan 1, 2025 @ 17:14:44.609	Alvin	c:\users\public\documents\...	added	File added to the system.	5	554
Dec 29, 2024 @ 22:47:56.125	Alvin	c:\users\public\documents\...	deleted	File deleted.	7	553
Dec 29, 2024 @ 22:47:51.899	Alvin	c:\users\public\documents\...	deleted	File deleted.	7	553
Dec 29, 2024 @ 22:47:51.217	Alvin	c:\users\public\documents\t...	modified	Integrity checksum changed.	7	550
Dec 29, 2024 @ 22:47:51.088	Alvin	c:\users\public\documents\...	deleted	File deleted.	7	553
Dec 29, 2024 @ 22:47:51.087	Alvin	c:\users\public\documents\...	modified	Integrity checksum changed.	7	550

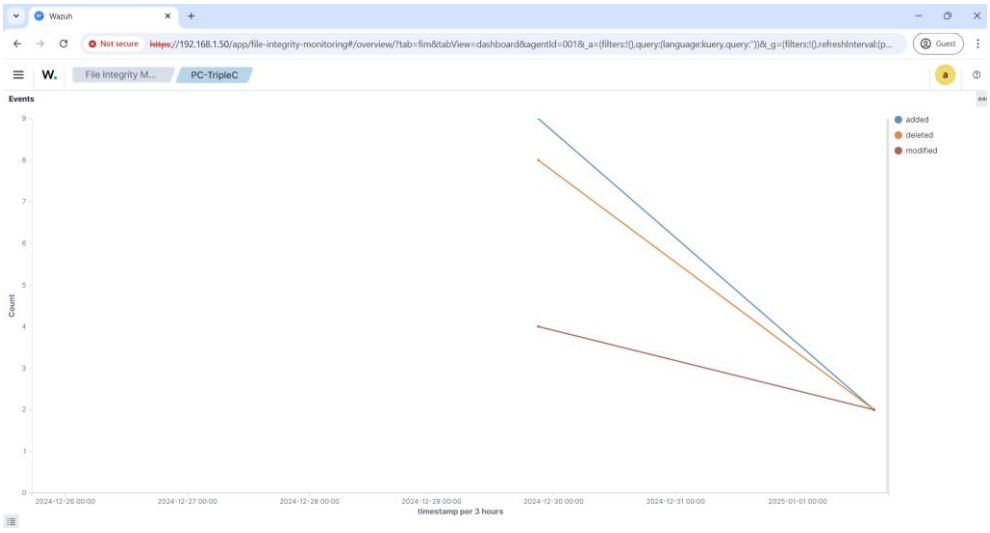
Gambar 18 *Detail File Integrity Monitoring (FIM) Log*

Berikut adalah bukti dari hasil pengujian Wazuh Integritas File dari *agent* PC-TripleC pada gambar 19 dan gambar 20, untuk *agent* Alvin pada gambar 21 dan gambar 22.

1. Agent PC-TripleC

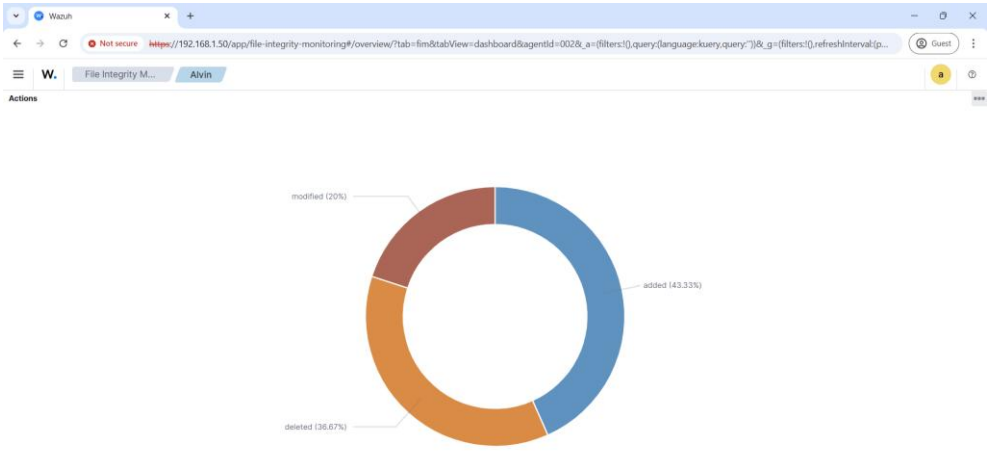


Gambar 19 Hasil Pengujian Wazuh *Agent* PC-TripleC

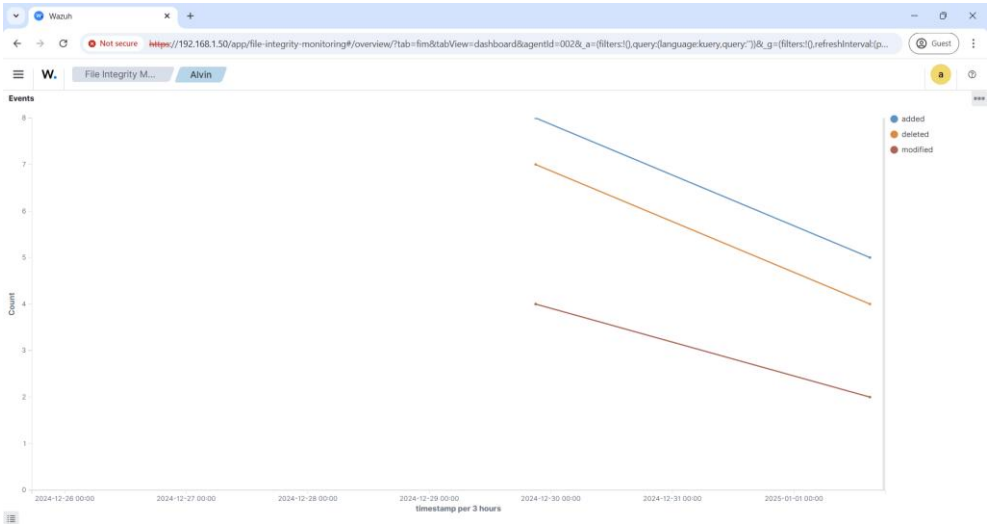


Gambar 20 Hasil *Timestamp* Per Tiga Jam

2. Agent Alvin



Gambar 21 Hasil Pengujian Wazuh *Agent* Alvin



Gambar 22 Hasil *Timestamp* Per Tiga Jam

Dari hasil pengujian menggunakan Wazuh, diukur pada tingkat keakuratan Wazuh dalam memantau dan mangaudit integritas File. Wazuh integritas file berkerja dengan sangat baik dan memiliki fitur yang sangat berguna sebagai pendeteksi keamanan pada *device agent.* Dalam hal ini, Wazuh melakukan audit dan analisis Log File untuk mengidentifikasi kejadian keamanan yang tidak biasa dan mencurigakan. Pada table 3 ditunjukkan presentase hasil dari pengujian Wazuh Integritas File yang telah dilakukan.

Tabel 3 Detail Integrity File

No	Nama *Agent*	*Integrity File*		
		Added	*Deleted*	*Modified*
1	PC-TripleC	40,74%	37,04%	22,22%
2	Alvin	43,33%	36,67%	20%

5. Maintenance (Pemeliharaan)

Pada tahap ini dilakukan pemeliharaan terhadap sistem yang telah dikembangkan. Tahap ini peneliti bekerjasama dengan pihak UKM Triple-C untuk melakukan pemeliharaan sistem yang telah diimplementasikan oleh peneliti dengan cara, secara rutin mengecek dan memonitoring sistem yang telah diimplementasikan.

KESIMPULAN

Berdasarkan hasil pengujian Wazuh Pemantauan Integritas File (FIM) Sebagai Perlindungan Keamanan Di UKM Triple-C Universitas Trunojoyo Madura yang telah dilakukan oleh peneliti, diketahui bahwa penerapan sistem ini dapat direkomendasikan untuk menjaga keamanan data. Wazuh Pemantauan Integritas File, mampu mendeteksi perubahan aktivitas yang tidak sah pada file dan memantau file untuk memastikan tidak ada perubahan yang tidak diizinkan. Dalam uji coba, Wazuh Pemantauan Integritas File, berhasil secara efektif mendeteksi perubahan pada file yang dipantau dan memberikan notifikasi dan *alert* kepada administrator. Selain itu, sistem ini juga mampu memvalidasi integritas file dengan membandingkan nilai hash yang dipantau dengan nilai hash yang tersimpan di dalam database Wazuh. Secara keseluruhan, penerapan Wazuh Pemantauan Integritas File merupakan pilihan yang tepat untuk meningkatkan keamanan sistem dan memantau aktivitas mencurigakan terkait perubahan yang terjadi pada file serta menjaga integritas file.

SARAN

Beberapa saran yang dapat dilakukan untuk meningkatkan sistem ini lebih baik lagi, yaitu :

1. Untuk penelitian selanjutnya bisa menghubungkan notifikasi/alert keamanan dengan BOT aplikasi Telegram.
2. Memperluas penerapan sistem dengan lebih banyak Agent.
3. Menambahkan fitur respon otomatis terhadap ancaman yang terdeteksi.

REFERENSI

Adzimi, S. N., Alfasih, H. A., Ramadhan, F. N. G., Neyman, S. N., & Setiawan, A. (2024). Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi menggunakan Debian. *Journal of Internet and Software Engineering*, *1*(4), 12. https://doi.org/10.47134/pjise.v1i4.2681

Aziz Saputra, F. (2023). *Implementasi Security Information And Event Management (Siem) Menggunakan Wazuh Pada Pesantren Teknologi Informasi Dan Komunikasi Jombang* [Thesis, SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI]. https://repository.nurulfikri.ac.id/id/eprint/530

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*, *4*(3), 275–282. https://doi.org/https://doi.org/10.26740/jinacs.v4n03.p275-282

Haryanto, B., & Chandra, D. W. (2024). Implementasi Wazuh Integritas File untuk Perlindungan Keamanan Berdasarkan Aktivitas Log di BTSI UKSW. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *5*(1), 183–192. https://doi.org/10.35870/jimik.v5i1.447

Hilmi Abdullah, Z., Izura Udzir, N., Mahmod, R., & Samsudin, K. (2011). Towards a Dynamic File Integrity Monitor through a Security Classification. *International Journal on New Computer Architectures and Their Applications (IJNCAA)*, *1*(3), 766–779.

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). *JEMSI: Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(5), 564–573. https://doi.org/10.31933/jemsi.v3i5

Paramita, S., Siregar, S. A., Damanik, R. A., & Dedi Irawan, M. (2022). Bulletin of Information Technology (BIT) Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013. *Bulletin of Information Technology (BIT)*, *3*(4), 374–379. https://doi.org/10.47065/bit.v3i1

Punta Dewa, R., & Windarto. (2024). Network Anomaly Detection Using Isolation Forest on Wazuh Logs with WhatsApp Notifications at PT XYZ. *KRESNA: Jurnal Riset Dan Pengabdian Masyarakat*, *4*(2), 208–216. https://doi.org/https://doi.org/10.36080/kresna.v4i2.170

Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber di Era Digital. *Journal of Business and Entrepreneurship*, *11*(1), 23–33. https://doi.org/10.46273/job&e.v11i1.365

Wahyuningsih U, T. M. (2023). *Pengembangan Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata terhadap Distributed Denial of Service Development of Network Security Using Intrusion Prevention System Based on Suricata against Distributed Denial of Service* [Skripsi]. Universitas Trunojoyo Madura.