SKRIPSI

ANALISIS KINERJA FILE INTEGRITY MONITORING BERBASIS WAZUH SIEM MENGGUNAKAN METODE PPDIOO PADA SERVER FAKULTAS ILMU KOMPUTER UPNVJT

ENGIE RAMADHANI
NPM 22082010029

DOSEN PEMBIMBING
Dr. Eng. Agussalim, S.Pd., M.T
Nur Cahyo Wibowo, S.Kom., M.Kom

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI SISTEM INFORMASI
SURABAYA
2026

LEMBAR PENGESAHAN

ANALISIS KINERJA FILE INTEGRITY MONITORING BERBASIS WAZUH SIEM MENGGUNAKAN METODE PPDIOO PADA SERVER FAKULTAS ILMU KOMPUTER UPNVJT

Oleh:

ENGIE RAMADHANI

NPM.22082010029

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi Prodi Sistem Informasi Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jawa Timur Pada tanggal 11 Mei 2026.

Menyetujui,

Dr. Eng. Agussalim, S.Pd., M.T. **NIP. 19850811 2019031 005**	.....	**(Pembimbing I)**
Nur Cahyo Wibowo, S.Kom, M.Kom. **NIP. 19790317 2021211 002**	.....	**(Pembimbing II)**
Eka Dyar Wahyuni, S.Kom, M.Kom **NIP. 19841201 2021212 005**	.....	**(Ketua Penguji)**
Seftin Fitri Ana Wati, S.Kom, M.Kom **NPT. 212199 10 320267**	.....	**(Anggota Penguji I)**
Dhian Satria Yudha Kartika, S.Kom, M.Kom **NIP. 19860522 2025211 048**	.....	**(Anggota Penguji II)**

Mengetahui,

Dekan Fakultas Ilmu Komputer

Prof. Dr. Ir. Novirina Hendrasarie, MT.

NIP. 19681126 199403 2 001

LEMBAR PERSETUJUAN

ANALISIS KINERJA FILE INTEGRITY MONITORING BERBASIS WAZUH SIEM MENGGUNAKAN METODE PPDIOO PADA SERVER FAKULTAS ILMU KOMPUTER UPNVJT

Oleh :

ENGIE RAMADHANI

NPM. 2208201029

Menyetujui,

Koordinator Program Studi Sistem Informasi

Fakultas Ilmu Komputer

Siti Mukaromah, S.Kom, M.Kom

NIP. 19810704 2021212 011

SURAT PERNYATAAN BEBAS PLAGIASI

Saya yang bertandatangan di bawah ini:

Nama Mahasiswa	: Engie Ramadhani
NPM	: 22082010029
Program	: Sarjana (S1)
Program Studi	: Sistem Informasi
Fakultas	: Fakultas Ilmu Komputer

Menyatakan bahwa dalam dokumen Skripsi ini tidak terdapat bagian dari karya ilmiah lain yang telah diajukan untuk memperoleh gelar akademik di suatu lembaga Pendidikan Tinggi, dan juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang/lembaga lain, kecuali yang secara tertulis disitasi dalam dokumen ini dan disebutkan secara lengkap dalam daftar pustaka.

Dan saya menyatakan bahwa dokumen ilmiah ini bebas dari unsur-unsur plagiasi. Apabila dikemudian hari ditemukan indikasi plagiat pada Skripsi ini, saya bersedia menerima sanksi sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya tanpa ada paksaan dari siapapun juga dan untuk dipergunakan sebagaimana mestinya.

Surabaya, 18 Mei 2026

Yang Membuat Pernyataan,

Engie Ramadhani

NPM. 22082010029

ABSTRAK

Nama Mahasiswa / NPM	:	Engie Ramadhani / 22082010029
Judul Skripsi	:	Analisis File Integrity Monitoring Berbasis Wazuh Siem menggunakan Metode PPDIOO pada Server Fakultas Ilmu Komputer UPNVJT
Dosen Pembimbing	:	1. Dr. Eng. Agussalim, S.Pd, M.T. 2. Nur Cahyo Wibowo, S.Kom, M.Kom

Ancaman keamanan siber pada server institusi pendidikan tidak hanya berasal dari serangan jaringan, tetapi juga dari perubahan file internal yang tidak terdeteksi. Pada Fakultas Ilmu Komputer UPN "Veteran" Jawa Timur, pernah terjadi gangguan layanan web akibat perubahan konfigurasi file server yang menyebabkan kegagalan akses layanan, sehingga menunjukkan perlunya sistem monitoring integritas file yang lebih optimal. Penelitian ini bertujuan menerapkan dan menganalisis kinerja File Integrity Monitoring (FIM) berbasis Wazuh SIEM pada server Fakultas Ilmu Komputer menggunakan metode PPDIOO. Penelitian dilakukan melalui tahapan perencanaan, implementasi, pengoperasian, dan evaluasi sistem pada tiga server fakultas. Analisis kinerja difokuskan pada waktu deteksi, akurasi alert, dan efisiensi monitoring melalui pengujian penambahan, modifikasi, dan penghapusan file sebanyak 90 skenario pengujian. Hasil penelitian menunjukkan bahwa Wazuh FIM mampu mendeteksi seluruh perubahan file yang diuji dengan tingkat akurasi alert 100% dan rata-rata waktu deteksi berkisar antara 1,2 hingga 1,9 detik. Sistem juga mampu memberikan visibilitas aktivitas file secara *real-time* tanpa mengganggu operasional server. Hasil tersebut menunjukkan bahwa implementasi Wazuh SIEM efektif digunakan sebagai mekanisme deteksi dini perubahan file tidak sah untuk memperkuat keamanan server Fakultas Ilmu Komputer.

Kata kunci: File Integrity Monitoring, Wazuh, SIEM, PPDIOO, Keamanan Server.

ABSTRACT

Student Name / NPM	:	Engie Ramadhani / 22082010029
Thesis Title	:	*Analisis File Integrity Monitoring Berbasis Wazuh Siem menggunakan Metode PPDIOO pada Server Fakultas Ilmu Komputer UPNVJT*
Advisors	:	1. Dr. Eng. Agussalim, S.Pd, M.T. 2. Nur Cahyo Wibowo, S.Kom, M.Kom.

Cybersecurity threats to educational institution servers do not only originate from network attacks, but also from undetected internal file changes. At the Faculty of Computer Science, UPN "Veteran" East Java, web service disruptions had occurred due to changes in server configuration files that caused service access failures, indicating the need for a more optimal file integrity monitoring system. This study aimed to implement and analyze the performance of Wazuh SIEM-based File Integrity Monitoring (FIM) on the Faculty of Computer Science servers using the PPDIOO method. The research was conducted through the stages of planning, implementation, operation, and system evaluation on three faculty servers. Performance analysis focused on detection time, alert accuracy, and monitoring efficiency through 90 testing scenarios consisting of file addition, modification, and deletion. The results showed that Wazuh FIM successfully detected all tested file changes with an alert accuracy rate of 100% and an average detection time ranging from 1.2 to 1.9 seconds. The system also provided real-time visibility of file activities without disrupting server operations. These results indicated that the implementation of Wazuh SIEM was effective as an early detection mechanism for unauthorized file changes to strengthen server security at the Faculty of Computer Science.

Keywords: *File Integrity Monitoring, Wazuh, SIEM, PPDIOO, Server Security.*

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis File Integrity Monitoring Berbasis Wazuh Siem menggunakan Metode PPDIOO pada Server Fakultas Ilmu Komputer UPNVJT" sebagai salah satu persyaratan untuk memperoleh gelar sarjana pada program studi yang sedang ditempuh.

Dalam proses penyusunan skripsi ini, penulis menyadari bahwa penelitian ini tidak dapat terselesaikan tanpa adanya dukungan, bantuan, serta bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan rasa terima kasih kepada semua pihak yang telah memberikan kontribusi secara langsung maupun tidak langsung dalam penyelesaian skripsi ini:

1. Ayah, Ibu, serta adik-adik, yang senantiasa memberikan doa, dukungan, kasih sayang, serta pengorbanan yang tiada henti kepada penulis selama menempuh pendidikan hingga penyusunan skripsi ini.
2. Dr. Eng. Agussalim, S.Pd, M.T. selaku dosen pembimbing I dan Nur Cahyo Wibowo, S.Kom, M.Kom. selaku dosen pembimbing II, yang telah meluangkan waktu, tenaga, serta pikiran untuk memberikan arahan, bimbingan, dan masukan yang sangat berharga selama proses penyusunan skripsi ini.
3. Mohamad Irwan Afandi, S.T, M.Sc selaku dosen wali yang telah memberikan arahan, bimbingan, serta motivasi kepada penulis selama menjalani proses perkuliahan.
4. Tim National Komunitas Wo-Men in Tech Security yang telah memberikan pengalaman, dukungan, serta kesempatan bagi penulis untuk berkembang dan belajar dalam bidang teknologi dan keamanan siber. Khususnya Kak Riana dan Kak Alief atas arahan dan diskusi terkait penyusunan skripsi ini, serta rekan-rekan lainnya atas dukungan yang diberikan.
5. Mentor dan teman-teman Computer and Network Security di Infinite Learning yang telah menjadi rekan selama proses internship serta memberikan dukungan, kebersamaan, dan semangat dalam proses belajar dan pengembangan diri.

6. Teman-teman AMN Surabaya, yang berasal dari berbagai daerah di Indonesia, dari Sabang hingga Merauke, dan Bersama-sama merantau sebagai penerima beasiswa. Terima kasih atas kebersamaan, dukungan, serta semangat yang saling diberikan selama menjalani masa perkuliahan.
7. Laila Karima, Zahrah Hayat Arka Putri, Nayli Amirah Firdaus, Rifda Nasywatul Affah, Devita Fahliza Ulfa, Risma Paramesti, Ayu Arfina, Shania Chairunnisa, Beauty Restuning Sari, Nafila Putri yang telah menjadi teman seperjuangan sejak awal perkuliahan hingga proses penyusunan skripsi. Terima kasih atas kebersamaan, dukungan, motivasi, serta semangat yang selalu diberikan dalam menghadapi berbagai tantangan selama masa studi.
8. Teman-teman seperbimbingan, yaitu Iqbal, Bisma, Sadrakh, Saipul, dan Dirga, serta teman-teman lainnya yang saling memberikan motivasi, dukungan, dan kebersamaan dalam menghadapi berbagai tantangan selama proses penyusunan skripsi.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat berbagai kekurangan. Oleh sebab itu, penulis sangat mengharapkan kritik dan saran yang konstruktif demi perbaikan penelitian di masa yang akan datang. Semoga skripsi ini dapat memberikan kontribusi serta menjadi referensi bagi penelitian selanjutnya.

Surabaya, 11 Mei 2026

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR SINGKATAN DAN ARTI SIMBOL

Singkatan	Arti / Keterangan
APT	Advanced Persistent Threat Serangan siber jangka panjang yang dilakukan secara terencana untuk mencuri data atau merusak sistem tanpa terdeteksi.
CDN	Content Delivery Network Jaringan server global yang digunakan untuk mempercepat distribusi konten web kepada pengguna.
CIA	Confidentiality, Integrity, Availability Prinsip dasar keamanan informasi yang berfokus pada kerahasiaan, integritas, dan ketersediaan data.
Cloudflare	Layanan keamanan siber dan CDN yang melindungi situs web dari serangan siber serta membantu meningkatkan performa akses web.
CPU	Central Processing Unit Komponen utama komputer yang berfungsi memproses data dan menjalankan instruksi sistem.
DDoS	Distributed Denial of Service Jenis serangan siber yang membanjiri server dengan trafik berlebihan hingga layanan tidak dapat diakses.
DLP	Data Loss Prevention Kebijakan dan teknologi untuk mencegah kehilangan maupun kebocoran data penting.

DoS	Denial of Service Serangan yang bertujuan mengganggu ketersediaan layanan dengan membebani sistem target.
ELK Stack	Elasticsearch, Logstash, dan Kibana. Rangkaian perangkat lunak open-source untuk pengumpulan, pengelolaan, dan visualisasi data log.
FIM	File Integrity Monitoring Sistem untuk mendeteksi perubahan terhadap file penting pada server.
HTTP/HTTPS	Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure Protokol komunikasi web, di mana HTTPS menggunakan enkripsi untuk mengamankan pertukaran data.
IDS	Intrusion Detection System Sistem keamanan yang digunakan untuk mendeteksi aktivitas mencurigakan atau serangan pada jaringan maupun sistem.
IP	Internet Protocol Protokol jaringan yang digunakan untuk pengalamatan dan pengiriman data antar perangkat komputer.
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission organisasi internasional yang menetapkan standar teknologi dan keamanan informasi.
JSON	JavaScript Object Notation Format pertukaran data ringan yang digunakan untuk komunikasi antar sistem.

MITRE ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge Framework keamanan siber yang digunakan untuk mengidentifikasi dan mengklasifikasikan teknik serta taktik serangan siber.
NIST	National Institute of Standards and Technology Lembaga yang mengembangkan standar dan pedoman keamanan siber.
PCI-DSS	Payment Card Industry Data Security Standard Standar keamanan untuk melindungi data transaksi kartu pembayaran.
PPDIOO	Prepare, Plan, Design, Implement, Operate, Optimize Metodologi siklus hidup jaringan untuk perencanaan, implementasi, operasional, dan optimasi sistem.
RAM	Random Access Memory Memori sementara yang digunakan sistem untuk menyimpan data saat proses berjalan.
SIEM	Security Information and Event Management Sistem untuk mengumpulkan, memantau, dan menganalisis log keamanan secara terpusat.
SOC	Security Operations Center Pusat operasional keamanan yang bertugas memantau, menganalisis, dan menangani insiden keamanan siber.
SQL Injection	Teknik serangan yang mengeksploitasi celah keamanan pada query database melalui input pengguna.

SSH	Secure Shell Protokol jaringan untuk mengakses dan mengelola server secara aman dari jarak jauh.
SSL	Secure Socket Layer Protokol keamanan yang digunakan untuk mengenkripsi komunikasi data pada jaringan.
TCP	Transmission Control Protocol Protokol komunikasi yang memastikan pengiriman data berlangsung secara andal dan berurutan.
TLS	Transport Layer Security Protokol keamanan penerus SSL yang digunakan untuk mengenkripsi komunikasi data.
VM / Virtualmin	Platform virtualisasi dan pengelolaan layanan server dalam satu mesin fisik.
WAF	Web Application Firewall Sistem keamanan yang melindungi aplikasi web dari berbagai serangan berbasis HTTP.
Wazuh	Platform open-source untuk Security Information and Event Management (SIEM) dan monitoring keamanan sistem.
Wazuh Agent	Komponen Wazuh yang diinstal pada endpoint untuk mengirimkan log dan data keamanan ke server.
Wazuh Dashboard	Antarmuka visual Wazuh untuk monitoring, analisis keamanan, dan visualisasi alert secara real-time.
Wazuh Indexer	Komponen Wazuh yang berfungsi mengindeks dan menyimpan data log untuk pencarian dan analisis cepat.

Wazuh Server	Komponen utama Wazuh yang menerima, memproses, dan mengelola data keamanan dari agent.
XDR	Extended Detection and Response Teknologi keamanan yang mengintegrasikan deteksi dan respons ancaman pada berbagai lapisan sistem.
XSS	Cross Site Scripting Jenis serangan pada aplikasi web dengan menyisipkan script berbahaya ke halaman web.
ZTNA	Zero Trust Network Architecture Pendekatan keamanan jaringan dengan prinsip “never trust, always verify”, di mana setiap akses harus diverifikasi secara ketat.