ANALISIS INTEGRASI WAZUH HIDS UNTUK SIMULASI FILE INTEGRITY MONITORING PADA LINGKUNGAN SOC

LAPORAN CAREER ACCELERATION PROGRAM

SYAHID BANDORO SURYO
00000075737

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2026

ANALISIS INTEGRASI WAZUH HIDS UNTUK SIMULASI FILE INTEGRITY MONITORING PADA LINGKUNGAN SOC

LAPORAN CAREER ACCELERATION PROGRAM

Diajukan sebagai Salah Satu Syarat untuk Memperoleh

Gelar Sarjana S.Kom

SYAHID BANDORO SURYO
00000075737

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2026

HALAMAN PERNYATAAN ORISINALITAS TIDAK PLAGIAT

Dengan ini saya,

Nama	:	Syahid Bandoro Suryo
NIM	:	00000075737
Program Studi	:	Informatika

Menyatakan dengan sesungguhnya bahwa Laporan Career Acceleration Program saya yang berjudul:

Analisis Integrasi Wazuh HIDS untuk Simulasi File Integrity Monitoring pada Lingkungan SOC

merupakan hasil karya saya sendiri, bukan merupakan hasil plagiat, dan tidak pula dituliskan oleh orang lain; Semua sumber, baik yang dikutip maupun dirujuk, telah saya cantumkan dan nyatakan dengan benar pada bagian Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan karya ilmiah, saya bersedia menerima konsekuensi untuk dinyatakan TIDAK LULUS. Saya juga bersedia menanggung segala konsekuensi hukum yang berkaitan dengan tindak plagiarisme ini sebagai kesalahan saya pribadi dan bukan tanggung jawab Universitas Multimedia Nusantara.

Tangerang, 23 Desember 2025

(Syahid Bandoro Suryo)

HALAMAN PERNYATAAN PENGGUNAAN BANTUAN KECERDASAN ARTIFISIAL (AI)

Saya yang bertanda tangan di bawah ini:

Nama	:	Syahid Bandoro Suryo
NIM	:	00000075737
Program Studi	:	Informatika
Judul Laporan	:	Analisis Integrasi Wazuh HIDS untuk Simulasi File Integrity Monitoring pada Lingkungan SOC

Dengan ini saya menyatakan secara jujur menggunakan bantuan Kecerdasan Artifisial (AI) dalam pengerjaan Laporan sebagai berikut :

- ☑ Menggunakan AI sebagaimana diizinkan untuk membantu dalam menghasilkan ide-ide utama saja
- ☐ Menggunakan AI sebagaimana diizinkan untuk membantu menghasilkan teks pertama saja
- ☐ Menggunakan AI untuk menyempurnakan sintaksis dan tata bahasa untuk pengumpulan tugas
- ☐ Karena tidak diizinkan: Tidak menggunakan bantuan AI dengan cara apa pun dalam pembuatan tugas

Saya juga menyatakan bahwa:

(1) Menyerahkan secara lengkap dan jujur penggunaan perangkat AI yang diperlukan dalam tugas melalui Formulir Penggunaan Perangkat Kecerdasan Artifisial (AI)

(2) Mengakui telah menggunakan bantuan AI dalam tugas saya baik dalam bentuk kata, paraphrase, penyertaan ide atau fakta penting yang disarankan oleh AI dan saya telah menyantumkan dalam sitasi serta referensi

(3) Terlepas dari pernyataan di atas, tugas ini sepenuhnya merupakan karya saya sendiri

Tangerang, 23 Desember 2025

(Syahid Bandoro Suryo)

HALAMAN PERNYATAAN KEABSAHAN PERUSAHAAN

Nama	:	Syahid Bandoro Suryo
NIM	:	00000075737
Program Studi	:	Informatika
Fakultas	:	Teknik dan Informatika

menyatakan bahwa saya melaksanakan kegiatan di:

Nama Perusahaan/Organisasi	:	PT. Defenxor Nusa Semesta (Defenxor)
Alamat	:	Graha BIP 6th Floor Jalan Jend. Gatot Subroto Kav. 23, Jakarta 12930
Email Perusahaan/Organisasi	:	info@defenxor.com

1. Perusahaan/Organisasi tempat saya melakukan kegiatan dapat di validasi keberadaannya.
2. Jika dikemudian hari, terbukti ditemukan kecurangan/penyimpangan data yang tidak valid di perusahaan/organisasi tempat saya melakukan kegiatan, maka:
    a. Saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah yang telah saya tempuh.
    b. Saya bersedia menerima semua sanksi yang berlaku sebagaimana ditetapkan dalam peraturan yang berlaku di Universitas Multimedia Nusantara.

Pernyataan ini saya buat dengan sebenar-benarnya dan digunakan sebagaimana mestinya

Tangerang, 23 Desember 2025

Mengetahui	Menyatakan
Defenxor PT. DEFENDER NUSA SEMESTA	METERAI TEMPEL FC6BCANX067074742
(Andi Wahyudi)	(Syahid Bandoro Suryo)

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH MAHASISWA

Yang bertanda tangan di bawah ini:

Nama	:	Syahid Bandoro Suryo
NIM	:	00000075737
Program Studi	:	Informatika
Jenjang	:	S1
Jenis Karya	:	Laporan Career Acceleration Program

Menyatakan dengan sesungguhnya bahwa:

☑ Saya bersedia memberikan izin sepenuhnya kepada Universitas Multimedia Nusantara untuk mempublikasikan hasil karya ilmiah saya di repositori Knowledge Center, sehingga dapat diakses oleh Civitas Akademika/Publik. Saya menyatakan bahwa karya ilmiah yang saya buat tidak mengandung data yang bersifat konfidensial dan saya juga tidak akan mencabut kembali izin yang telah saya berikan dengan alasan apapun.

☐ Saya tidak bersedia karena dalam proses pengajuan untuk diterbitkan ke jurnal/konferensi nasional/internasional (dibuktikan dengan *letter of acceptance*)**.

Tangerang, 23 Desember 2025

Yang menyatakan

Syahid Bandoro Suryo

** Jika tidak bisa membuktikan LoA jurnal/HKI selama enam bulan ke depan, saya bersedia mengizinkan penuh karya ilmiah saya untuk diunggah ke KC UMN dan menjadi hak institusi UMN.

Halaman Persembahan / Motto

”The journey of a thousand miles begins with a single step.”

Lao Tzu

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa atas segala rahmat dan kemudahan yang diberikan, sehingga laporan magang berjudul ”Analisis Integrasi Wazuh HIDS untuk Simulasi File Integrity Monitoring pada Lingkungan SOC” dapat diselesaikan dengan baik. Laporan ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) pada Program Studi Informatika, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara.
Mengucapkan terima kasih

1. Bapak Dr. Ir. Andrey Andoko, M.Sc., selaku Rektor Universitas Multimedia Nusantara.
2. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Bapak Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Ibu Alethea Suryadibrata, S.Kom., M.Eng., sebagai Pembimbing pertama yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya laporan ini.
5. Bapak Andi Wahyudi, sebagai *Team Leader* DIMS PT Defender Nusa Semesta dan *supervisor* dalam program magang.
6. Orang Tua, teman-teman dan keluarga saya yang telah memberikan bantuan dukungan material dan moral, sehingga penulis dapat menyelesaikan laporan ini.

Semoga laporan magang ini dapat memberikan manfaat dan menjadi referensi yang berguna bagi para pembaca.

Tangerang, 23 Desember 2025

Syahid Bandoro Suryo

ANALISIS INTEGRASI WAZUH HIDS UNTUK SIMULASI FILE INTEGRITY MONITORING PADA LINGKUNGAN SOC

Syahid Bandoro Suryo

ABSTRAK

Peningkatan ancaman siber terhadap sistem host menjadikan perubahan integritas berkas sebagai salah satu indikator awal terjadinya kompromi sistem, sehingga diperlukan mekanisme pemantauan yang mampu mendukung deteksi dini dalam lingkungan *Security Operations Center* (SOC). Penelitian ini bertujuan untuk menganalisis kemampuan *File Integrity Monitoring* (FIM) pada Wazuh *Host Intrusion Detection System* (HIDS) dalam mendeteksi dan menyajikan informasi perubahan berkas pada sistem yang dipantau. Metode yang digunakan meliputi konfigurasi FIM pada Wazuh HIDS, pengumpulan log perubahan berkas, serta analisis data melalui integrasi dengan Elastic Stack untuk mendukung visualisasi dan korelasi *event* keamanan. Pengujian difokuskan pada aktivitas perubahan berkas berupa penambahan dan modifikasi file pada direktori yang telah ditentukan. Hasil analisis menunjukkan bahwa mekanisme FIM mampu memberikan visibilitas yang jelas terhadap perubahan berkas serta mendukung proses identifikasi aktivitas yang berpotensi mencurigakan. Namun demikian, efektivitas pemantauan dipengaruhi oleh cakupan direktori yang dipilih, potensi *false positive*, serta keterbatasan informasi pendukung dari integrasi *threat intelligence*. Berdasarkan hasil tersebut, FIM pada Wazuh HIDS dapat berperan sebagai komponen pendukung *security monitoring* dan deteksi dini ancaman berbasis perubahan integritas berkas dalam lingkungan SOC.

Kata kunci: Elastic Stack, *File Integrity Monitoring*, *Security Monitoring*, *Security Operations Center*, Wazuh HIDS

ANALYSIS OF WAZUH HIDS INTEGRATION FOR FILE INTEGRITY MONITORING SIMULATION IN A SOC ENVIRONMENT

Syahid Bandoro Suryo

ABSTRACT

The increasing complexity of information technology infrastructures is accompanied by a rise in cyber threats targeting organizational systems and data, highlighting the need for reliable early detection mechanisms within a Security Operations Center (SOC) environment. One critical indicator of system compromise is unauthorized changes to file integrity on monitored hosts. This study analyzes the use of File Integrity Monitoring (FIM) through the Host-based Intrusion Detection System (HIDS) module provided by Wazuh, integrated with the Elastic Stack, to support security monitoring activities. The method involves configuring monitored directories, observing file change events, and analyzing security alerts generated by the FIM mechanism through centralized log management and visualization. The results show that the FIM module is capable of detecting file modification events on critical system components and providing meaningful security alerts that support early detection and analysis of potential threats. This study concludes that Wazuh HIDS-based File Integrity Monitoring can serve as an effective supporting mechanism for host-level security monitoring within a SOC simulation environment.

***Keywords**: Elastic Stack, File Integrity Monitoring, Security Monitoring, Security Operations Center, Wazuh HIDS*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN