IMPLEMENTASI PROTOTIPE HOST INTRUSION DETECTION SYSTEM UNTUK SIMULASI OPERASIONAL SIEM PADA LINGKUNGAN SOC

LAPORAN CAREER ACCELERATION PROGRAM

MUHAMMAD AFFRANSYAH BAYULAKSANA
00000077007

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2025

IMPLEMENTASI PROTOTIPE HOST INTRUSION DETECTION SYSTEM UNTUK SIMULASI OPERASIONAL SIEM PADA LINGKUNGAN SOC

LAPORAN CAREER ACCELERATION PROGRAM

Diajukan sebagai Salah Satu Syarat untuk Memperoleh

Gelar Sarjana S.Kom

MUHAMMAD AFFRANSYAH BAYULAKSANA
00000077007

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2025

HALAMAN PERNYATAAN ORISINALITAS TIDAK PLAGIAT

Dengan ini saya,

Nama	:	Muhammad Affransyah Bayulaksana
NIM	:	00000077007
Program Studi	:	Informatika

Menyatakan dengan sesungguhnya bahwa Laporan MBKM Magang saya yang berjudul:

Implementasi Prototipe Host Intrusion Detection System untuk Simulasi Operasional SIEM 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, 19 November 2025

(Muhammad Affransyah Bayulaksana)

HALAMAN PERNYATAAN PENGGUNAAN BANTUAN KECERDASAN ARTIFISIAL (AI)

Saya yang bertanda tangan di bawah ini:

Nama	:	Muhammad Affransyah Bayulaksana
NIM	:	00000077007
Program Studi	:	Informatika
Judul Laporan	:	Implementasi Prototipe Host Intrusion Detection System untuk Simulasi Operasional SIEM 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, 19 November 2025

(Muhammad Affransyah Bayulaksana)

HALAMAN PERNYATAAN KEABSAHAN PERUSAHAAN

Nama	:	Muhammad Affransyah Bayulaksana
NIM	:	00000077007
Program Studi	:	Informatika
Fakultas	:	Teknik dan Informatika

menyatakan bahwa saya melaksanakan kegiatan di:

Nama Perusahaan/Organisasi	:	PT Defender Nusa Semesta (Defenxor)
Alamat	:	Graha BIP 6th Floor Jalan Jend. Gatot Subroto Kav. 23, Jakarta 12930, Indonesia
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, 19 November 2025

Mengetahui	Menyatakan
(Andi Wahyudi)	(Muhammad Affransyah Bayulaksana)

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH MAHASISWA

Yang bertanda tangan di bawah ini:

Nama	:	Muhammad Affransyah Bayulaksana
NIM	:	00000077007
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, 19 November 2025

Yang menyatakan

Muhammad Affransyah Bayulaksana

** 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

”As long as you live, keep learning how to live.”

Seneca

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, sehingga laporan magang yang berjudul ”Implementasi Prototipe Host Intrusion Detection System untuk Simulasi Operasional SIEM pada Lingkungan SOC” ini 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.

Penulis menyadari bahwa tanpa bantuan, dukungan, dan bimbingan dari berbagai pihak, penyusunan laporan magang ini akan sangat sulit untuk diselesaikan. Oleh karena itu, penulis menyampaikan terima kasih kepada:

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. Bapak Dr. Ir. Winarno, M.Kom., sebagai Pembimbing 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/mentor* dalam program magang.
6. Orang Tua dan keluarga yang telah memberikan bantuan dukungan material dan moral, sehingga penulisan laporan magang ini dapat terselesaikan.

Semoga laporan magang ini dapat memberikan manfaat, baik sebagai sumber informasi maupun inspirasi bagi para pembaca.

Tangerang, 19 November 2025

Muhammad Affransyah Bayulaksana

IMPLEMENTASI HOST INTRUSION DETECTION SYSTEM SEBAGAI SIMULASI OPERASIONAL SIEM PADA LINGKUNGAN SOC

Muhammad Affransyah Bayulaksana

ABSTRAK

Peningkatan kompleksitas infrastruktur teknologi informasi sejalan dengan meningkatnya ancaman siber yang menargetkan sistem dan data organisasi, sehingga diperlukan mekanisme deteksi dini yang andal dalam lingkungan Security Operations Center (SOC). Untuk menjawab kebutuhan tersebut, dilakukan implementasi Host Intrusion Detection System (HIDS) berbasis Wazuh dan Elastic Stack (ELK) guna membangun sistem deteksi intrusi yang mampu memantau, menganalisis, serta memberikan peringatan terhadap aktivitas anomali pada tingkat host secara real-time. Perancangan sistem meliputi penyusunan topologi, instalasi, dan konfigurasi komponen utama seperti Wazuh Agent, Wazuh Manager, Filebeat, Elasticsearch, dan Kibana, serta pengujian fungsionalitas yang mencakup integrity monitoring, integrasi dengan VirusTotal API, serta penerapan security alerts dan active response untuk respons otomatis terhadap ancaman. Hasil implementasi menunjukkan bahwa sistem mampu mendeteksi perubahan pada file dan aktivitas mencurigakan secara efisien, menampilkan visualisasi data keamanan melalui dashboard terpusat SIEM, serta meningkatkan efektivitas analisis insiden di SOC. Dengan demikian, rancangan sistem ini memberikan gambaran menyeluruh mengenai penerapan HIDS berbasis Wazuh–ELK sebagai solusi deteksi ancaman yang adaptif dan skalabel dalam lingkungan keamanan informasi modern.

Kata kunci: *Host Intrusion Detection System*, Wazuh, Elastic Stack, SIEM, *Cybersecurity Monitoring*

IMPLEMENTATION OF HOST INTRUSION DETECTION SYSTEM PROTOTYPE FOR SIEM OPERATIONAL SIMULATION IN SOC ENVIRONMENT

Muhammad Affransyah Bayulaksana

ABSTRACT

The increasing complexity of cyber threats requires organizations to implement advanced and adaptive security monitoring mechanisms. To address this challenge, a Host Intrusion Detection System (HIDS) was implemented as a prototype to simulate Security Information and Event Management (SIEM) operations within an SOC environment. The system was developed using the Wazuh ELK Stack, which integrates Wazuh Manager, Filebeat, Elasticsearch, and Kibana to enable centralized log collection, event correlation, and real-time visualization of security data. The implementation process included HIDS deployment, agent configuration, integrity monitoring, alert management, and VirusTotal integration for enhanced threat intelligence. The prototype successfully demonstrated how HIDS can detect system-level anomalies, generate security alerts, and support analysis workflows in SOC operations. This implementation also provided a deeper understanding of how host-based detection complements existing SIEM mechanisms in improving overall cybersecurity monitoring.

***Keywords**: Host Intrusion Detection System, SIEM, Wazuh, ELK Stack, Security Operations Center, Cybersecurity Monitoring*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN