IMPLEMENTASI MEKANISME NOTIFIKASI PERINGATAN BERBASIS WAZUH PADA SIMULASI LINGKUNGAN SOC

LAPORAN CAREER ACCELERATION PROGRAM

RAPHAEL CONSTANTINE KURNIAJAYA
00000069425

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

IMPLEMENTASI MEKANISME NOTIFIKASI PERINGATAN BERBASIS WAZUH PADA SIMULASI LINGKUNGAN SOC

LAPORAN CAREER ACCELERATION PROGRAM

Diajukan sebagai Salah Satu Syarat untuk Memperoleh

Gelar Sarjana S.Kom

RAPHAEL CONSTANTINE KURNIAJAYA
00000069425

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

HALAMAN PERNYATAAN ORISINALITAS TIDAK PLAGIAT

Dengan ini saya,

Nama	:	Raphael Constantine Kurniajaya
NIM	:	00000069425
Program Studi	:	Informatika

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

Perancangan Prototipe Sistem Otomatisasi Peringatan Berbasis HIDS Menggunakan Wazuh 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

(Raphael Constantine Kurniajaya)

HALAMAN PERNYATAAN PENGGUNAAN BANTUAN KECERDASAN ARTIFISIAL (AI)

Saya yang bertanda tangan di bawah ini:

Nama	:	Raphael Constantine Kurniajaya
NIM	:	00000069425
Program Studi	:	Informatika
Judul Laporan	:	Perancangan Prototipe Sistem Otomatisasi Peringatan Berbasis HIDS Menggunakan Wazuh 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

(Raphael Constantine Kurniajaya)

HALAMAN PERNYATAAN KEABSAHAN PERUSAHAAN

Nama	:	Raphael Constantine Kurniajaya
NIM	:	00000069425
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 Sudirman 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
(Andi Wahyudi)	(Raphael Constantine Kurniajaya)

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH MAHASISWA

Yang bertanda tangan di bawah ini:

Nama	:	Raphael Constantine Kurniajaya
NIM	:	00000069425
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

Raphael Constantine Kurniajaya

** 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

”For the Lord gives wisdom; From His mouth come knowledge and understanding.”

Proverbs 2:6 (NASB)

KATA PENGANTAR

Puji syukur dipanjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga laporan magang berjudul "Implementasi Mekanisme Notifikasi Peringatan Berbasis Wazuh pada Simulasi Lingkungan SOC" ini dapat disusun dan 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 mengucapkan terima kasih kepada:

1. Dr. Ir. Andrey Andoko, M.Sc., selaku Rektor Universitas Multimedia Nusantara.
2. Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Moeljono Widjaja, B.Sc., M.Sc., Ph.D., sebagai Pembimbing pertama yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya laporan magang ini.
5. 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 magang ini.

Harapan dari penyusunan laporan ini adalah agar hasil kerja dan pembelajaran selama masa magang dapat memberikan manfaat bagi pembaca, serta memiliki kontribusi positif dalam bidang keamanan informasi.

Tangerang, 23 Desember 2025

Raphael Constantine Kurniajaya

IMPLEMENTASI MEKANISME NOTIFIKASI PERINGATAN BERBASIS WAZUH PADA SIMULASI LINGKUNGAN SOC

Raphael Constantine Kurniajaya

ABSTRAK

Perkembangan ancaman siber yang semakin kompleks menuntut adanya mekanisme deteksi dini dan penyampaian peringatan yang efisien dalam lingkungan *Security Operations Center* (SOC). Salah satu pendekatan yang umum digunakan adalah penerapan *Host-based Intrusion Detection System* (HIDS) untuk memantau aktivitas pada tingkat host. Laporan kerja magang ini membahas perancangan dan implementasi prototipe sistem otomatisasi peringatan berbasis HIDS menggunakan Wazuh dalam lingkungan simulasi SOC. Metode yang digunakan meliputi pemantauan aktivitas host Windows, analisis *log* berbasis *rule-based detection*, serta pengiriman notifikasi *e-mail* secara otomatis ketika terjadi pencocokan (*matching*) antara *event* dan *rule* yang telah dikonfigurasi. Implementasi difokuskan pada penggunaan *rule* sederhana, yaitu deteksi kondisi *agent started* dan *agent stopped*, untuk memverifikasi alur deteksi dan pengiriman peringatan otomatis. Hasil implementasi menunjukkan bahwa sistem mampu menghasilkan *alert* dan mengirimkan notifikasi secara otomatis sesuai dengan kondisi yang terdeteksi. Berdasarkan hasil tersebut, dapat disimpulkan bahwa prototipe sistem otomatisasi peringatan berbasis HIDS ini mampu memberikan gambaran awal mengenai mekanisme peringatan dini serta perannya dalam mendukung aktivitas monitoring dan meringankan beban kerja *Security Analyst* dalam operasional SOC.

Kata kunci: HIDS, keamanan siber, SOC, Wazuh

IMPLEMENTATION OF A WAZUH-BASED ALERT NOTIFICATION MECHANISM IN A SIMULATED SOC ENVIRONMENT

Raphael Constantine Kurniajaya

ABSTRACT

The increasing complexity of cyber threats requires effective early detection and alert delivery mechanisms within a Security Operations Center (SOC) environment. One commonly adopted approach is the use of a Host-based Intrusion Detection System (HIDS) to monitor host-level activities. This internship report discusses the design and implementation of a HIDS-based alert automation prototype using Wazuh in a simulated SOC environment. The applied method includes monitoring Windows host activities, analyzing log data using a rule-based detection approach, and automatically delivering e-mail notifications when predefined rules match incoming events. The implementation focuses on simple detection rules, specifically identifying agent started and agent stopped conditions, to verify the end-to-end detection and automated alerting workflow. The results indicate that the system is capable of generating alerts and delivering notifications automatically according to the detected conditions. Based on these results, it can be concluded that the proposed HIDS-based alert automation prototype provides an initial insight into early warning mechanisms and their role in supporting monitoring activities and reducing the operational workload of Security Analysts in an SOC environment.

***Keywords**: cybersecurity, HIDS, SOC, Wazuh*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR KODE

DAFTAR LAMPIRAN