IMPLEMENTASI SECURITY MONITORING DAN INCIDENT HANDLING DALAM OPERASIONAL SOC DI PT DEFENDER NUSA SEMESTA

LAPORAN MBKM MAGANG

MUHAMMAD AFFRANSYAH BAYULAKSANA
00000077007

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

IMPLEMENTASI SECURITY MONITORING DAN INCIDENT HANDLING DALAM OPERASIONAL SOC DI PT DEFENDER NUSA SEMESTA

LAPORAN MBKM MAGANG

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 Magang saya yang berjudul:
Implementasi Security Monitoring dan Incident Handling Dalam Operasional SOC di PT Defender Nusa Semesta

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, 20 Juni 2025

(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 MBKM Magang

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, 20 Juni 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

”Luck is when preparation meets opportunity.”

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 Security Monitoring dan Incident Handling Dalam Operasional SOC di PT Defender Nusa Semesta” 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 Vincentius Kurniawan, S.Kom., M.Eng.Sc, 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, 20 Juni 2025

Muhammad Affransyah Bayulaksana

IMPLEMENTASI SECURITY MONITORING DAN INCIDENT HANDLING DALAM OPERASIONAL SOC DI PT DEFENDER NUSA SEMESTA

Muhammad Affransyah Bayulaksana

ABSTRAK

Dalam operasional Security Operations Center (SOC), tidak semua alarm yangmuncul pada sistem monitoring merupakan insiden yang valid. Sebagian diantaranya merupakan false positive yang memerlukan analisis lanjutan untukmemastikan keabsahannya. Oleh karena itu, setiap potensi ancaman perlu melaluiproses investigasi yang sistematis agar tidak terjadi kesalahan dalam penanganan. PT Defender Nusa Semesta (Defenxor) merupakan salah satu perusahaan yangmenyediakan layanan SOC untuk membantu klien dalam menjaga keamanan sisteminformasi mereka. Selama pelaksanaan program magang, aktivitas utama yangdijalankan meliputi security monitoring dan incident handling yang dilakukan berdasarkan prosedur operasional standar yang telah ditetapkan oleh tim SOC Defenxor. Kegiatan ini memberikan pengalaman langsung dalam mendeteksi,menganalisis, serta merespons insiden keamanan yang terjadi di lingkunganoperasional klien

Kata kunci: *False positive*, *incident handling*, *security monitoring*, SOC

IMPLEMENTATION OF SECURITY MONITORING AND INCIDENT HANDLING FOR SOC OPERATIONAL AT PT DEFENDER NUSA SEMESTA

Muhammad Affransyah Bayulaksana

ABSTRACT

In Security Operations Center (SOC) operations, not all alarms generated bymonitoring systems represent valid security incidents. Many are false positives thatrequire further analysis to confirm their legitimacy. Therefore, each potential threatmust go through a systematic investigation process to avoid handling errors. PTDefender Nusa Semesta (Defenxor) is a company that provides SOC services to helpclients protect their information systems. During the internship program, the mainactivities involved security monitoring and incident handling, carried out basedon standard operating procedures established by the Defenxor SOC team. Theseactivities offered hands-on experience in detecting, analyzing, and responding tosecurity incidents occurring in clients' operational environments.

***Keywords**: False positive, incident handling, security monitoring, SOC*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN