

**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**



**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

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

** 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 yang muncul pada sistem monitoring merupakan insiden yang valid. Sebagian diantaranya merupakan false positive yang memerlukan analisis lanjutan untuk memastikan keabsahannya. Oleh karena itu, setiap potensi ancaman perlu melalui proses investigasi yang sistematis agar tidak terjadi kesalahan dalam penanganan. PT Defender Nusa Semesta (Defenxor) merupakan salah satu perusahaan yang menyediakan layanan SOC untuk membantu klien dalam menjaga keamanan sistem informasi mereka. Selama pelaksanaan program magang, aktivitas utama yang dijalankan 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 lingkungan operasional 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 by monitoring systems represent valid security incidents. Many are false positives that require further analysis to confirm their legitimacy. Therefore, each potential threat must go through a systematic investigation process to avoid handling errors. PT Defender Nusa Semesta (Defenxor) is a company that provides SOC services to help clients protect their information systems. During the internship program, the main activities involved security monitoring and incident handling, carried out based on standard operating procedures established by the Defenxor SOC team. These activities offered hands-on experience in detecting, analyzing, and responding to security incidents occurring in clients' operational environments.

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



DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERNYATAAN ORISINALITAS	ii
HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH	iii
HALAMAN PERSEMBAHAN/MOTO	iv
KATA PENGANTAR	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR TABEL	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN	xi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Maksud dan Tujuan Kerja Magang	3
1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang	4
BAB 2 GAMBARAN UMUM PERUSAHAAN	6
2.1 Sejarah Singkat Perusahaan	6
2.2 Visi dan Misi Perusahaan	7
2.3 Struktur Organisasi Perusahaan	7
BAB 3 PELAKSANAAN KERJA MAGANG	11
3.1 Kedudukan dan Koordinasi	11
3.2 Tugas yang Dilakukan	12
3.3 Uraian Pelaksanaan Magang	15
3.3.1 Implementasi <i>Security Monitoring</i> dalam <i>Workflow</i> Operasional SOC	16
3.3.2 Implementasi <i>Case Incident Handling</i>	30
3.3.3 <i>System Availability Monitoring</i>	35
3.4 Kendala dan Solusi yang Ditemukan	36
BAB 4 SIMPULAN DAN SARAN	37
4.1 Simpulan	37
4.2 Saran	37
DAFTAR PUSTAKA	38

UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR TABEL

Tabel 3.1	Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang	13
Tabel 3.2	Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang (lanjutan)	14
Tabel 3.3	Pekerjaan yang dilakukan tiap minggu selama pelaksanaan kerja magang (lanjutan)	15



DAFTAR GAMBAR

Gambar 2.1	Logo perusahaan PT Defender Nusa Semesta	6
Gambar 2.2	Struktur organisasi perusahaan PT Defender Nusa Semesta	8
Gambar 3.1	Struktur DIMS	11
Gambar 3.2	<i>Flowchart</i> alur analisis dan penanganan insiden SOC	18
Gambar 3.3	Tampilan <i>Alarm List</i>	19
Gambar 3.4	<i>Flowchart</i> Investigasi Log	21
Gambar 3.5	Tampilan detail suatu <i>alarm</i>	22
Gambar 3.6	Tampilan <i>Event Log</i>	23
Gambar 3.7	Tampilan Pemilihan <i>Data View</i> atau <i>Index</i> Perangkat	25
Gambar 3.8	Korelasi dengan aktivitas atau perangkat lain	26
Gambar 3.9	Hasil pengecekan reputasi domain menggunakan VirusTotal	26
Gambar 3.10	Notifikasi Case	28
Gambar 3.11	<i>Alarm Detail</i> dari Case yang dianalisis	30
Gambar 3.12	<i>Event Log</i> dari aktivitas yang terdeteksi	31
Gambar 3.13	Korelasi dengan aktivitas yang berhubungan sesuai konteks alarm	32
Gambar 3.14	Draf notifikasi hasil analisis kasus	34



DAFTAR LAMPIRAN

Lampiran 1	MBKM-01 Cover Letter MBKM Internship Track 1	39
Lampiran 2	MBKM-02 MBKM Internship Track 1 Card	40
Lampiran 3	MBKM-03 Daily Task - Internship Track 1	41
Lampiran 4	MBKM-04 Verification Form of Internship Report MBKM Internship Track 1	68
Lampiran 5	Form Bimbingan	69
Lampiran 6	Pengecekan Hasil Turnitin	71

