PERAN CYBER SECURITY ANALYST DALAM MONITORING DAN ANALISIS ANCAMAN SIBER PADA PT DEFENDER NUSA SEMESTA

LAPORAN MBKM MAGANG

RAPHAEL CONSTANTINE KURNIAJAYA
00000069425

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

PERAN CYBER SECURITY ANALYST DALAM MONITORING DAN ANALISIS ANCAMAN SIBER PADA PT DEFENDER NUSA SEMESTA

LAPORAN MBKM MAGANG

RAPHAEL CONSTANTINE KURNIAJAYA
00000069425

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

HALAMAN PERNYATAAN ORISINALITAS TIDAK PLAGIAT

Dengan ini saya,

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

Menyatakan dengan sesungguhnya bahwa Laporan MBKM Magang saya yang berjudul:

Peran Cyber Security Analyst dalam Monitoring dan Analisis Ancaman Siber pada 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, 23 Juni 2025

(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 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, 23 Juni 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

”Each of you should give what you have decided in your heart to give, not reluctantly or under compulsion, for God loves a cheerful giver.”

2 Corinthians 9:7 (NIV)

KATA PENGANTAR

Puji syukur dipanjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga laporan magang berjudul "Peran Cyber Security Analyst dalam Monitoring dan Analisis Ancaman Siber pada PT Defender Nusa Semesta" 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. Angga Aditya Permana, S. Kom, M. Kom, 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 Juni 2025

Raphael Constantine Kurniajaya

PERAN CYBER SECURITY ANALYST DALAM MONITORING DAN ANALISIS ANCAMAN SIBER PADA PT DEFENDER NUSA SEMESTA

Raphael Constantine Kurniajaya

ABSTRAK

Dalam kegiatan operasional *Security Operation Center* (SOC), sistem keamanan menghasilkan berbagai *alert* yang harus dianalisis untuk menentukan konteks ancaman serta dampaknya terhadap infrastruktur pelanggan. Proses ini melibatkan pengumpulan data, pemeriksaan log, korelasi antar perangkat keamanan, serta dokumentasi insiden secara terstruktur. PT Defender Nusa Semesta (Defenxor) merupakan perusahaan penyedia layanan keamanan informasi yang melayani berbagai sektor industri, termasuk pemerintahan dan BUMN. Kegiatan magang dilaksanakan di lingkungan SOC Defenxor dengan fokus pada peran sebagai *Level-1 (L1) Security Analyst*, yang mencakup pemantauan *log*, analisis *alert*, dan pengiriman notifikasi insiden kepada pelanggan. Selama program magang, berbagai perangkat keamanan digunakan untuk menunjang proses investigasi teknis. Analisis dilakukan melalui integrasi antara log perangkat, sumber informasi eksternal, serta acuan prosedural dalam *SOC Playbook*. Studi kasus insiden seperti *web scanning*, *brute force login*, dan *malware infection* menjadi bagian dari pengalaman operasional yang memberikan pemahaman praktis mengenai mekanisme deteksi dan respons terhadap ancaman siber secara profesional.

***Kata kunci**: keamanan informasi, L1 Analyst, monitoring, SOC.*

THE ROLE OF CYBER SECURITY ANALYST IN THREAT MONITORING AND ANALYSIS AT PT DEFENDER NUSA SEMESTA

Raphael Constantine Kurniajaya

ABSTRACT

In the operational activities of the Security Operation Center (SOC), security systems generate various alerts that must be analyzed to determine the context of threats and their potential impact on the client's infrastructure. This process involves data collection, log examination, cross-device correlation, and structured incident documentation. PT Defender Nusa Semesta (Defenxor) is a cyber security service provider that supports multiple industrial sectors, including government and state-owned enterprises. The internship program was carried out within Defenxor's SOC environment, with a focus on the role of a Level-1 (L1) Security Analyst, involving log monitoring, alert analysis, and incident notification to clients. Throughout the internship, various security tools were utilized to support the technical investigation process. The analysis was conducted through integrated log correlation, external threat intelligence enrichment, and procedural references based on the SOC Playbook. Case studies involving incidents such as web scanning, brute force login, and malware infection contributed to hands-on experience in understanding the detection and response mechanisms required for professional cyber security operations.

***Keywords**: information security, L1 Analyst, monitoring, SOC.*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN