STRATEGI SECURITY MONITORING DAN INCIDENT RESPONSE DALAM MENJAGA KEAMANAN SIBER DI PT DEFENDER NUSA SEMESTA

LAPORAN MBKM MAGANG

SYAHID BANDORO SURYO
00000075737

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

STRATEGI SECURITY MONITORING DAN INCIDENT RESPONSE DALAM MENJAGA KEAMANAN SIBER DI PT DEFENDER NUSA SEMESTA

LAPORAN MBKM MAGANG

SYAHID BANDORO SURYO
00000075737

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

HALAMAN PERNYATAAN ORISINALITAS TIDAK PLAGIAT

Dengan ini saya,

Nama	:	Syahid Bandoro Suryo
NIM	:	00000075737
Program Studi	:	Informatika

Menyatakan dengan sesungguhnya bahwa Laporan MBKM Magang saya yang berjudul:

Strategi Security Monitoring dan Incident Response dalam Menjaga Keamanan Siber 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, 22 Juni 2025

(Syahid Bandoro Suryo)

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH MAHASISWA

Yang bertanda tangan di bawah ini:

Nama	:	Syahid Bandoro Suryo
NIM	:	00000075737
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, 22 Juni 2025

Yang menyatakan

Syahid Bandoro Suryo

** 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

”A good name is to be more desired than great wealth, Favor is better than silver and gold.”

Proverbs 22:1 (NASB)

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa atas segala rahmat dan kemudahan yang diberikan, sehingga laporan magang berjudul *"Strategi Security Monitoring dan Incident Response dalam Menjaga Keamanan Siber di PT Defender Nusa Semesta"* 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. Ucapan terima kasih disampaikan 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 Wirawan Istiono, S.Kom., M.Kom., sebagai Pembimbing pertama 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* dalam program magang.
6. Orang Tua, teman-teman dan keluarga saya yang telah memberikan bantuan dukungan material dan moral, sehingga penulis dapat menyelesaikan laporan ini.

Semoga laporan magang ini dapat memberikan manfaat dan menjadi referensi yang berguna bagi para pembaca.

Tangerang, 22 Juni 2025

Syahid Bandoro Suryo

STRATEGI SECURITY MONITORING DAN INCIDENT RESPONSE DALAM MENJAGA KEAMANAN SIBER DI PT DEFENDER NUSA SEMESTA

Syahid Bandoro Suryo

ABSTRAK

Strategi *security monitoring* dan *incident response* di PT Defender Nusa Semesta dijalankan melalui operasional *Security Operations Center* (SOC) yang beroperasi selama 24 jam untuk memastikan deteksi dini dan penanganan cepat terhadap ancaman siber. Sistem SIEM digunakan sebagai alat utama untuk memantau dan menganalisis log dari berbagai perangkat secara real-time. Tantangan dalam proses monitoring, seperti tingginya jumlah *false positive*, dapat mengganggu efisiensi serta menghambat fokus analisis terhadap ancaman yang valid. Untuk mengatasinya, diterapkan tahapan kerja terstruktur berupa validasi alarm, analisis log mendalam, penyusunan notifikasi insiden, serta eskalasi teknis melalui sistem ticketing internal. Selain itu, penggunaan playbook dan dokumentasi berbasis studi kasus turut mendukung konsistensi dalam pengambilan keputusan. Pendekatan ini terbukti meningkatkan efektivitas pemantauan keamanan dan memperkuat respons terhadap insiden siber.

Kata kunci: False Positive, Incident Response, Security Monitoring, SOC (urut abjad)

SECURITY MONITORING AND INCIDENT RESPONSE STRATEGIES IN SAFEGUARDING CYBERSECURITY AT PT DEFENDER NUSA SEMESTA

Syahid Bandoro Suryo

ABSTRACT

The security monitoring and incident response strategy at PT Defender Nusa Semesta is implemented through a 24/7 Security Operations Center (SOC) to ensure early detection and timely handling of cyber threats. A SIEM system is used as the primary tool to monitor and analyze logs from various security devices in real-time. Challenges such as a high volume of false positives may reduce efficiency and hinder the focus on valid threats. To address this, a structured workflow is applied, including alarm validation, in-depth log analysis, incident notification drafting, and technical escalation through an internal ticketing system. Additionally, the use of playbooks and case-based documentation supports consistency in decision-making. This approach improves the effectiveness of security monitoring and strengthens incident response capabilities.

Keywords*: False Positive, Incident Response, Security Monitoring, SOC* (in alphabetical order)

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN