ANALISIS MONITORING SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) DAN RESPONS INSIDEN DI PT DEFENDER NUSA SEMESTA

LAPORAN CAREER ACCELERATION PROGRAM

AZALEA KEISHA PUTRI
00000076267

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

ANALISIS MONITORING SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) DAN RESPONS INSIDEN DI PT DEFENDER NUSA SEMESTA

LAPORAN CAREER ACCELERATION PROGRAM

Diajukan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Komputer (S.Kom.)

AZALEA KEISHA PUTRI
00000076267

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

HALAMAN PERNYATAAN ORISINALITAS TIDAK PLAGIAT

Dengan ini saya,

Nama	:	Azalea Keisha Putri
NIM	:	00000076267
Program Studi	:	Informatika

Menyatakan dengan sesungguhnya bahwa Laporan MBKM Magang saya yang berjudul:

Analisis Monitoring Security Information and Event Management (SIEM) dan Respons Insiden 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, 10 Oktober 2025

(Azalea Keisha Putri)

HALAMAN PERNYATAAN PENGGUNAAN BANTUAN KECERDASAN ARTIFISIAL (AI)

Saya yang bertanda tangan di bawah ini:

Nama	:	Azalea Keisha Putri
NIM	:	00000076267
Program Studi	:	Informatika
Judul Laporan	:	Analisis Monitoring Security Information and Event Management (SIEM) dan Respons Insiden di PT Defender Nusa Semesta

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, 19 November 2025

(Azalea Keisha Putri)

HALAMAN PERNYATAAN KEABSAHAN PERUSAHAAN

Nama	:	Azalea Keisha Putri
NIM	:	00000076267
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 Subroto Kav.23, Jakarta 12930, Indonesia
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, 19 November 2025

Mengetahui

(Andi Wahyudi)

Menyatakan

(Azalea Keisha Putri)

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH MAHASISWA

Yang bertanda tangan di bawah ini:

Nama	:	Azalea Keisha Putri
NIM	:	00000076267
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, 19 November 2025

Yang menyatakan

Azalea Keisha Putri

** 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

”Fake it till you make it.”

Taylor Swift

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas terselesaikannya laporan magang berjudul ”Analisis Monitoring *Security Information and Event Management* (SIEM) dan Respons Insiden di PT Defender Nusa Semesta.” Laporan ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara. Penulis menyadari bahwa laporan ini tidak akan terselesaikan dengan baik tanpa bantuan berbagai pihak. 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. Ibu Dr. Sy. Yuliani Yakub, S.Kom., M.T., selaku Pembimbing yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya laporan magang ini.
5. Bapak Andi Wahyudi, selaku Team Leader PT. Defender Nusa Semesta yang telah memberikan bimbingan dan bantuan selama praktik kerja magang ini.
6. Orang Tua, keluarga, dan teman-teman saya yang telah memberikan bantuan dukungan material dan moral, sehingga penulis dapat menyelesaikan laporan magang ini.

Semoga laporan magang ini dapat memberikan manfaat, baik sebagai referensi informasi maupun sebagai sumber inspirasi bagi para pembaca.

Tangerang, 19 November 2025

Azalea Keisha Putri

ANALISIS MONITORING SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) DAN RESPONS INSIDEN DI PT DEFENDER NUSA SEMESTA

Azalea Keisha Putri

ABSTRAK

Transformasi digital yang pesat telah memperluas permukaan serangan dan meningkatkan risiko insiden siber, baik di sektor swasta maupun pemerintahan. Untuk menjawab tantangan tersebut, organisasi membutuhkan sistem pemantauan keamanan yang adaptif dan terintegrasi. Laporan ini membahas implementasi dan efektivitas monitoring keamanan serta respons insiden di PT Defender Nusa Semesta (Defenxor) selama program magang 15 minggu pada divisi *Security Operations Center* (SOC). Pemantauan dilakukan dengan memanfaatkan Elastic Stack sebagai platform SIEM utama, didukung oleh integrasi multi-platform seperti Grafana, Check Point Harmony Endpoint, dan SolarWinds. Fokus utama meliputi korelasi log lintas sumber, validasi indikator kompromi menggunakan *threat intelligence*, serta pengawasan infrastruktur dan *endpoint* secara terpadu. Hasil kegiatan menunjukkan bahwa penerapan monitoring berbasis SIEM dan respons insiden terstruktur mampu meningkatkan akurasi deteksi, mempercepat eskalasi insiden, serta memperkuat kesiapan keamanan informasi di lingkungan klien. Program ini tidak hanya mendukung pencapaian tujuan pembelajaran, tetapi juga memberikan kontribusi nyata terhadap operasional SOC perusahaan.

Kata kunci: *Elastic Stack, Incident Response, SIEM*

AN ANALYSIS OF SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) MONITORING AND INCIDENT RESPONSE AT PT DEFENDER NUSA SEMESTA

Azalea Keisha Putri

ABSTRACT

The rapid pace of digital transformation has expanded the attack surface and increased the risk of cyber incidents across both private and public sectors. To address these challenges, organizations require adaptive and integrated security monitoring systems. This report explores the implementation and effectiveness of security monitoring and incident response at PT Defender Nusa Semesta (Defenxor) during a 15-week internship program within the Security Operations Center (SOC) division. The monitoring process utilized Elastic Stack as the primary SIEM platform, supported by multi-platform integration involving Grafana, Check Point Harmony Endpoint, and SolarWinds. The main focus includes cross-source log correlation, validation of indicators of compromise using threat intelligence, and integrated infrastructure and endpoint monitoring. The results show that structured SIEM-based monitoring and incident response improve detection accuracy, accelerate incident escalation, and strengthen information security readiness in client environments. This program not only achieved the intended learning outcomes but also provided tangible contributions to the company's SOC operations.

***Keywords**: Elastic Stack, Incident Response, SIEM*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN