PERAN SECURITY ANALYST DALAM MONITORING KEAMANAN DATA MENGGUNAKAN SIEM PADA PT. DEFENDER NUSA SEMESTA

LAPORAN MBKM MAGANG

AZALEA KEISHA PUTRI
00000076267

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

PERAN SECURITY ANALYST DALAM MONITORING KEAMANAN DATA MENGGUNAKAN SIEM PADA PT. DEFENDER NUSA SEMESTA

LAPORAN MBKM MAGANG

AZALEA KEISHA PUTRI
00000076267

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

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:

Peran Security Analyst dalam Monitoring Keamanan Data Menggunakan SIEM 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

(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 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, 19 Juni 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

”If my mind can conceive it, if my heart can believe it, then I can achieve it”

- Muhammad Ali

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas terselesaikannya laporan magang berjudul *"Peran Security Analyst* dalam *Monitoring* Keamanan Data Menggunakan *SIEM* pada 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 Alethea Suryadibrata, S.Kom., M.Eng., sebagai 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 Juni 2025

Azalea Keisha Putri

PERAN SECURITY ANALYST DALAM MONITORING KEAMANAN DATA MENGGUNAKAN SIEM PADA PT. DEFENDER NUSA SEMESTA

Azalea Keisha Putri

ABSTRAK

Ketergantungan yang tinggi terhadap sistem digital turut meningkatkan risiko serangan siber yang dapat mengancam keamanan data organisasi. Dalam konteks tersebut, peran *Security Analyst* yang didukung oleh sistem *Security Information and Event Management* (SIEM) menjadi elemen krusial dalam melakukan pemantauan ancaman secara waktu nyata (*real-time*). Implementasi sistem ini pada PT. Defender Nusa Semesta dilaksanakan melalui integrasi perangkat seperti Elastic Stack, Grafana, dan Thruk, yang memungkinkan analisis log, korelasi insiden, serta pelaporan teknis terhadap aktivitas mencurigakan. Selama pelaksanaan program magang selama 18 minggu, kegiatan pemantauan dilakukan secara terstruktur, mencakup proses *monitoring* sistem, validasi objek digital melalui referensi eksternal seperti AbuseIPDB dan VirusTotal, serta komunikasi insiden dengan pihak *customer*. Hasil implementasi menunjukkan bahwa kolaborasi antara SIEM dan peran aktif *Security Analyst* mampu membentuk sistem keamanan data yang adaptif, terdokumentasi, dan selaras dengan standar operasional perusahaan.

Kata kunci: Keamanan Data, *Security Analyst*, *SIEM*

THE ROLE OF SECURITY ANALYSTS IN IMPLEMENTING DATA SECURITY MONITORING USING SIEM AT THE SECURITY OPERATIONS CENTER OF PT. DEFENDER NUSA SEMESTA

Azalea Keisha Putri

ABSTRACT

The high reliance on digital systems has increased the risk of cyberattacks that threaten data security. In this context, the role of a Security Analyst, supported by a Security Information and Event Management (SIEM) system, becomes crucial for real-time threat monitoring. At PT. Defender Nusa Semesta, this system was implemented through the integration of tools such as Elastic Stack, Grafana, and Thruk, enabling log analysis, incident correlation, and technical reporting of suspicious activities. Throughout the 20-week internship program, monitoring activities were carried out in a structured manner, including system observation, validation of digital objects using external references such as AbuseIPDB and VirusTotal, and incident communication with external parties. The implementation demonstrated that collaboration between the SIEM system and the active involvement of the Security Analyst can establish an adaptive, well-documented data security system aligned with the company's operational standards.

Keywords: *Data Security, Security Analyst, SIEM*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN