MONITORING SISTEM SIEM DAN EDR DALAM DIVISI SECURITY OPERATION CENTER (SOC) DI PT VISIONET DATA INTERNASIONAL

LAPORAN MBKM MAGANG

IGNASIUS DENNI HERMAWAN
00000045479

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

MONITORING SISTEM SIEM DAN EDR DALAM DIVISI SECURITY OPERATION CENTER (SOC) DI PT VISIONET DATA INTERNASIONAL

LAPORAN MBKM MAGANG

IGNASIUS DENNI HERMAWAN
00000045479

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

HALAMAN PERNYATAAN ORISINALITAS TIDAK PLAGIAT

Dengan ini saya,

Nama	:	Ignasius Denni Hermawan
NIM	:	00000045479
Program Studi	:	Informatika

Menyatakan dengan sesungguhnya bahwa Laporan MBKM Magang saya yang berjudul:

Monitoring Sistem SIEM dan EDR dalam divisi Security Operation Center (SOC) di PT Visionet Data Internasional

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, 8 Juli 2025

(Ignasius Denni Hermawan)

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH MAHASISWA

Yang bertanda tangan di bawah ini:

Nama	:	Ignasius Denni Hermawan
NIM	:	00000045479
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, 8 Juli 2025

Yang menyatakan

Ignasius Denni Hermawan

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

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

Proverbs 22:1 (NASB)

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

KATA PENGANTAR

Puji Syukur atas berkat dan rahmat kepada Tuhan Yang Maha Esa, atas selesainya penulisan laporan Magang ini dengan judul: Monitoring Sistem SIEM dan EDR dalam Divisi SOC di PT Visionet Data Internasional dilakukan untuk memenuhi salah satu syarat untuk mencapai gelar Sarjana Komputer Jurusan Informatika Pada Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan laporan magang ini, sangatlah sulit bagi saya untuk menyelesaikan laporan magang ini. Oleh karena itu, saya mengucapkan 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 Sy. Yuliani Yakub, S.Kom., M.T., Ph.D, sebagai Pembimbing yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya laporan magang ini.
5. Kepada Bapak Hadi, selaku Supervisor praktik kerja magang yang telah meluangkan waktu untuk memberikan bimbingan serta kepercayaan dalam pelaksanaan praktik kerja magang.
6. Orang Tua dan keluarga saya yang telah memberikan bantuan dukungan material dan moral, sehingga laporan dapat diselesaikan.

Semoga laporan magang ini bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi, bagi para pembaca

Tangerang, 8 Juli 2025

Ignasius Denni Hermawan

MONITORING SISTEM SIEM DAN EDR DALAM DIVISI SECURITY OPERATION CENTER (SOC) DI PT VISIONET DATA INTERNASIONAL

Ignasius Denni Hermawan

ABSTRAK

PT Visionet Data Internasional merupakan perusahaan *IT Managed Services* di Indonesia yang memiliki berbagai klien dari beragam sektor industri. Dalam menjaga keamanan sistem informasi milik klien, Visionet mengandalkan layanan *Security Operations Center* (SOC) yang didukung oleh penerapan teknologi SIEM (*Security Information and Event Management*) dan EDR (*Endpoint Detection and Response*). Dalam rangka mendukung operasional SOC, dilaksanakan praktik kerja magang dengan fokus pada proses monitoring dan eskalasi insiden keamanan siber berdasarkan alert yang muncul dari sistem Wazuh/SOCFortress (SIEM) dan SentinelOne (EDR). Kegiatan magang melibatkan analisis alert, verifikasi melalui platform *threat intelligence*, hingga pelaporan kepada PIC klien. Selain itu, peserta magang juga mengikuti pelatihan (bootcamp) dan diberikan kesempatan untuk mendalami *threat intelligence* serta investigasi insiden saat berada di SOC Level 2. Selama masa magang, praktik kerja ini berhasil memberikan kontribusi nyata terhadap kelancaran operasional SOC serta meningkatkan pengalaman teknis dalam menghadapi tantangan di dunia keamanan siber secara langsung.

Kata kunci: *Alert*, *Endpoint Detection and Response* (EDR), Eskalasi, *Security Information and Event Management* (SIEM), *Security Operation Center* (SOC)

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

SIEM AND EDR SYSTEM MONITORING IN SECURITY OPERATION CENTER (SOC) DIVISION AT PT VISIONET DATA INTERNASIONAL

Ignasius Denni Hermawan

ABSTRACT

PT Visionet Data Internasional is an IT Managed Services company in Indonesia that serves various clients across multiple industries. To ensure the security of clients' information systems, Visionet operates a Security Operations Center (SOC) *supported by Security Information and Event Management* (SIEM) *and Endpoint Detection and Response* (EDR) *technologies. As part of the SOC operations, an internship program was conducted focusing on monitoring and escalating cybersecurity incidents based on alerts generated from the Wazuh* (SIEM) *and SentinelOne* (EDR) *systems. The internship tasks included analyzing alerts, verifying indicators through threat intelligence platforms, and reporting to the appropriate person-in-charge* (PIC) *at the client side. In addition, the intern participated in bootcamp training and gained experience in threat intelligence and incident investigation while working in* SOC *Level 2. This internship provided valuable contributions to* SOC *operations and enhanced the intern's technical skills in dealing with real-world cybersecurity challenges.*

Keywords*: Alert, Endpoint Detection and Response* (EDR), *Escalation, Security Information and Event Management* (SIEM), *Security Operations Center* (SOC)

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR ISI

UNIVERSITAS MULTIMEDIA NUSANTARA

DAFTAR TABEL

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR GAMBAR

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR LAMPIRAN

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA