BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan Teknologi Informasi (TI) yang pesat mendorong transformasi digital di berbagai sektor, seperti pemerintahan, bisnis, dan industri. Teknologi ini meningkatkan efisiensi dan akses informasi, namun juga memperbesar risiko serangan siber. Ketergantungan tinggi terhadap sistem digital membuka celah bagi ancaman seperti *phishing*, *ransomware, data breach*, dan eksploitasi celah keamanan yang berdampak pada kerugian finansial dan reputasi organisasi[1].

Laporan Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 330 juta trafik anomali di Indonesia selama tahun 2024, dengan aktivitas tertinggi berasal dari Mirai Botnet yang menargetkan perangkat IoT untuk serangan DDoS. Selain itu, tercatat 2,48 juta aktivitas APT, 514 ribu *ransomware*, dan 26,7 juta *phishing*. Sebanyak 241 dugaan kebocoran data dan 56 juta data *exposure* berdampak pada 461 *stakeholder*, dengan target utama sektor keuangan, pemerintahan, dan infrastruktur kritis[2]. Pada tahun 2021, terhitung 741 juta lebih insiden siber, termasuk kasus besar seperti peretasan 91 juta akun Tokopedia, kebocoran data 279 juta penduduk melalui BPJS Kesehatan, dan insiden kebocoran data 2 juta nasabah BRI Life[3]. Lonjakan kasus kebocoran data hingga 143% dalam satu kuartal (Surfshark, 2022) memperkuat bukti bahwa sistem keamanan TI di Indonesia masih tergolong lemah, sebagaimana dinyatakan oleh *Global Cybersecurity Index (GCI)* 2017[4].

Dalam konteks ini, keamanan data harus dipandang sebagai aset strategis sekaligus investasi jangka panjang yang membutuhkan dukungan teknologi, regulasi, dan kesiapan sumber daya manusia[5]. Salah satu peran strategis dalam menjaga keamanan informasi adalah *Security Analyst*, yang bertugas menganalisis ancaman, merancang perlindungan, serta memberikan solusi teknis untuk mencegah insiden siber[6]. Peran ini diperkuat oleh sistem *Security Information and Event Management (SIEM),* yang memudahkan pemantauan aktivitas jaringan secara *real-time*, analisis log, serta respons cepat terhadap insiden (Muhammad et al., 2023)[7].

SIEM menyediakan data dan alat analisis untuk mendeteksi pola serangan dan menghasilkan peringatan dini, sementara *Security Analyst* menerjemahkan

data tersebut menjadi tindakan mitigasi nyata. Salah satu *platform* yang umum digunakan adalah *Elastic Stack,* di mana komponen seperti *Elasticsearch*, *Logstash*, dan Kibana dapat diintegrasikan untuk membangun sistem SIEM yang fleksibel, *open-source*, dan efektif dalam mendukung kebutuhan *monitoring* keamanan. Integrasi keduanya membentuk sistem *monitoring* yang proaktif dan adaptif dalam menghadapi ancaman siber.

Integrasi peran *Security Analyst* dan SIEM ini diimplementasikan secara nyata oleh PT. Defender Nusa Semesta (Defenxor), penyedia layanan keamanan TI di bawah CTI Group. Sebagai *Managed Security Service Provider (MSSP)*, Defenxor telah bersertifikasi ISO 27001 sejak 2016 untuk layanan *Security Operation Center (SOC)*, dan menyediakan layanan SOC, *penetration testing*, konsultasi keamanan, serta perangkat keamanan untuk berbagai sektor. Operasionalnya terbagi dalam tiga divisi utama: DISC (operasional SOC), DIMS (*monitoring* dan dukungan teknis), dan DISI (implementasi keamanan). Dalam strukturnya, *Security Analyst* berada di bawah DIMS dengan tugas memantau keamanan, menganalisis insiden, dan menangani ancaman secara berkelanjutan.

Berdasarkan latar belakang tersebut, laporan kerja magang ini difokuskan pada peran *Security Analyst* dalam *monitoring* keamanan data *customer* menggunakan SIEM pada PT. Defender Nusa Semesta. Permasalahan utamanya adalah meningkatnya ancaman siber yang menuntut sistem *monitoring* yang andal serta sumber daya manusia yang mampu merespons insiden secara efektif. Pengalaman kerja selama magang di divisi DIMS menjadi dasar untuk menggambarkan kontribusi peran *Security Analyst* dan SIEM dalam mendukung pengamanan data *customer*.

1.2 Maksud dan Tujuan Kerja Magang

Program kerja magang di PT. Defender Nusa Semesta bertujuan untuk mengimplementasikan secara langsung ilmu dan keterampilan dalam bidang keamanan siber yang diperoleh selama studi di Universitas Multimedia Nusantara. Melalui peran sebagai *Security Analyst*, kegiatan difokuskan pada pemantauan keamanan data menggunakan platform *Security Information and Event Management* (*SIEM*).

Tujuan utamanya adalah memperkuat kompetensi teknis dalam analisis log, deteksi dan penanganan insiden, serta koordinasi dalam lingkungan *Security Operation Center* (*SOC*). Selain itu, magang ini juga mendorong pengembangan

soft skill seperti komunikasi, kerja tim, dan manajemen waktu.

Partisipasi aktif dalam operasional keamanan siber memberikan pemahaman mendalam tentang prosedur, teknologi, dan tantangan industri dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Dengan demikian, program ini menjadi jembatan antara teori akademik dan praktik profesional dalam membentuk sumber daya manusia yang kompeten di bidang keamanan informasi.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Program kerja di PT. Defender Nusa Semesta dilaksanakan selama 25 minggu, terhitung sejak 3 Februari 2025 hingga 31 Juli 2025. Sistem kerja terbagi dalam dua periode, yaitu jam kerja *reguler* (Senin–Jumat) dan *shifting* (Rabu–Sabtu) sesuai dengan kebijakan tim. Selama masa kerja, jadwal tetap berjalan meskipun bertepatan dengan hari libur nasional maupun akhir pekan apabila termasuk dalam rotasi shift. Total hari kerja selama periode ini mencapai 109 hari, dengan estimasi total 1.026 jam kerja.

Periode : 3 Februari 2025 – 31 Juli 2025
Hari kerja : Menyesuaikan sistem kerja (lihat prosedur di bawah)
Jam kerja : Menyesuaikan sistem kerja dan shift
Posisi : *Security Analyst*

Adapun prosedur pelaksanaan kegiatan kerja magang adalah sebagai berikut:

1. Durasi Kerja Program magang dilaksanakan selama 25 minggu, dengan sistem kerja yang terbagi dalam dua periode berbeda:
    - Periode 1 (03 Maret – 09 Mei 2025) Magang dilaksanakan 5 hari kerja per minggu, yaitu dari hari Senin sampai Jumat, pukul 09.00 – 18.00 WIB. Sistem kerja dilakukan secara *Work from Office (WFO)* penuh dengan waktu istirahat dari pukul 12.00 – 13.00 WIB.
    - Periode 2 (14 Mei – 31 Juli 2025) Sistem kerja berubah menjadi *shift* dengan pola kerja 4 hari per minggu. Peserta magang dibagi menjadi dua tim:
        - Tim A (Sayap Kiri): Masuk Minggu – Rabu
        - Tim B (Sayap Kanan): Masuk Rabu – Sabtu

Tergabung dalam Tim B (Sayap Kanan), dengan jadwal kerja yang berlangsung dari hari Rabu hingga Sabtu setiap minggunya. Dalam sistem ini, waktu kerja dilakukan secara *rolling* dalam tiga jenis *shift* berikut:

- *Early Shift*: 05.00 – 15.00 WIB
- *Mid Shift*: 10.00 – 20.00 WIB
- *Night Shift*: 19.30 – 05.30 WIB

Pergantian shift dilakukan secara bergilir setiap pekan.

2. Kehadiran

   - Selama Periode 1: Kehadiran dicatat secara langsung melalui sistem tap *ID card* saat WFO.
   - Selama Periode 2: Kehadiran disesuaikan dengan jadwal *shift* dan tim, dan tetap dicatat secara langsung melalui sistem tap *ID card* saat masuk *shift*.

3. Pembimbing dan Struktur Tim

   Tim SOC pada PT. Defender Nusa Semesta dipimpin serta dibimbing oleh Bapak Andi dan Bapak Mario yang menjabat sebagai *Team Leader*. Seluruh kegiatan operasional tim berada dalam arahan dan supervisi langsung dari kedua pemimpin tersebut.