BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan transformasi digital di sektor swasta maupun pemerintahan telah meningkatkan ketergantungan terhadap sistem informasi. Kondisi ini memperluas *attack surface* dan sekaligus meningkatkan risiko terjadinya insiden siber. Di balik kemudahan dalam transaksi, komunikasi, dan pengelolaan data, tetap tersembunyi berbagai potensi ancaman seperti kebocoran data, sabotase layanan, hingga serangan terhadap infrastruktur kritis yang dapat menimbulkan kerugian finansial maupun reputasional[1].

Secara global, kerugian akibat kejahatan siber diproyeksikan mencapai USD 10,5 triliun per tahun pada 2025, meningkat signifikan dari USD 3 triliun pada tahun 2015[2]. Di Indonesia, Badan Siber dan Sandi Negara (BSSN) mencatat bahwa sepanjang tahun 2024 terjadi 330 juta trafik anomali, 2,48 juta aktivitas *Advanced Persistent Threats* (APT), 514 ribu insiden ransomware, 26,7 juta upaya phishing, serta 56 juta data yang terpapar dan berdampak pada 461 entitas[3]. Kondisi ini menegaskan urgensi peningkatan ketahanan dan kapabilitas keamanan siber yang lebih adaptif dan responsif.

Selain itu, lanskap ancaman siber juga mengalami pergeseran. Serangan tidak hanya bersifat masif, tetapi semakin sering dilakukan secara terarah (*targeted attacks*) terhadap sasaran-sasaran bernilai tinggi. Laporan industri menunjukkan tingginya paparan malware di lingkungan korporasi, peningkatan tren ransomware, serta lonjakan serangan terhadap perangkat *Internet of Things* (IoT) di sektor industri, kesehatan, dan transportasi[4]. Serangan semacam ini umumnya mengeksploitasi kelemahan pada konfigurasi sistem, celah perangkat lunak, serta kesalahan perilaku pengguna. Oleh karena itu, diperlukan sistem yang mampu memberikan deteksi dini yang akurat dan respons insiden yang cepat serta terukur.

Untuk menghadapi dinamika ancaman tersebut, organisasi membutuhkan sistem pemantauan keamanan yang tidak hanya reaktif, tetapi juga proaktif. *Security Information and Event Management* (SIEM) menjadi solusi terintegrasi yang mampu mengumpulkan, menormalkan, dan mengorelasikan log dari berbagai sumber untuk mendeteksi anomali secara *real-time*. Proses ini membantu penyaringan informasi yang relevan, mempercepat eskalasi insiden, serta menekan

risiko kebocoran data. Selain itu, integrasi SIEM ke dalam infrastruktur keamanan yang ada meningkatkan efisiensi operasional dan pengawasan terhadap aset digital[5].

Sebaliknya, pendekatan manual berbasis aturan statis tidak mampu mengimbangi volume dan variasi data yang terus meningkat. Ketergantungan pada analisis log secara tradisional berisiko menimbulkan *alert fatigue*, *false positive*, bahkan *blind spot* dalam lingkungan *Security Operations Center* (SOC)[6]. Oleh karena itu, dibutuhkan arsitektur pemantauan yang terpusat, otomatis, dan skalabel untuk mengumpulkan, mengorelasikan, serta menganalisis peristiwa keamanan dari berbagai perangkat dan aplikasi secara efektif[7].

Salah satu platform open-source yang banyak digunakan sebagai SIEM adalah Elastic Stack, yang terdiri dari Elasticsearch, Logstash, Kibana, dan Beats atau Elastic Agent. Integrasi komponen-komponen ini memungkinkan *log ingestion* secara *real-time*, normalisasi serta pemrosesan data, penyimpanan terindeks untuk pencarian cepat, dashboard interaktif, pembuatan *detection rules*, serta aktivitas *threat hunting* berbasis *timeline* insiden[8]. Dengan kapabilitas tersebut, Elastic Stack mendukung visibilitas menyeluruh dan *situational awareness* yang lebih baik.

Dalam konteks PT Defender Nusa Semesta (Defenxor) penyedia layanan keamanan TI di bawah naungan CTI Group yang telah tersertifikasi ISO 27001 untuk layanan SOC peran *Security Analyst* menjadi garda terdepan dalam proses pemantauan keamanan. Tugas utama meliputi pemantauan log melalui Elastic Stack, analisis dan korelasi alert lintas sumber, serta investigasi insiden pada lingkungan klien. Seluruh proses diperkuat dengan validasi menggunakan *threat intelligence* seperti VirusTotal, AbuseIPDB, dan MXToolbox, yang digunakan untuk menilai reputasi IP, *file hash*, URL, serta konfigurasi DNS/email. Validasi ini bertujuan untuk menekan *false positive* dan memprioritaskan indikator kompromi (IOC) yang valid.

Untuk mendukung efektivitas pemantauan, Defenxor juga mengimplementasikan arsitektur monitoring berbasis multi-platform. Grafana digunakan untuk observabilitas dan pemantauan ketersediaan sistem melalui metrik dan dashboard *real-time*. Check Point Harmony Endpoint menyediakan pertahanan sisi *endpoint* dengan fitur deteksi ransomware, *threat emulation*, dan forensik otomatis sebagai sinyal awal insiden. Sementara itu, SolarWinds memberikan visibilitas terhadap *infrastructure & availability monitoring*, sehingga keterkaitan antara insiden keamanan dan kondisi perangkat atau jaringan dapat dianalisis secara menyeluruh. Kombinasi ini memungkinkan tim SOC melihat *big picture*

dari jejak serangan, dari sisi endpoint, log keamanan, hingga dampaknya terhadap performa server dalam satu ekosistem pemantauan terpadu.

Melihat kondisi tersebut, laporan ini berfokus pada analisis monitoring keamanan dan respons insiden di PT Defender Nusa Semesta menggunakan Elastic Stack sebagai SIEM utama. Tujuan laporan ini adalah mengevaluasi efektivitas korelasi log, validasi ancaman, dan integrasi multi-platform dalam meningkatkan akurasi deteksi dan kecepatan respons insiden.

1.2 Maksud dan Tujuan Kerja Magang

Program magang di PT Defender Nusa Semesta disusun sebagai wadah untuk menerapkan secara langsung pengetahuan serta keterampilan di bidang keamanan siber yang telah diperoleh selama perkuliahan di Universitas Multimedia Nusantara. Dalam posisi sebagai *Security Analyst*, kegiatan berfokus pada pemantauan keamanan data melalui penggunaan platform *Security Information and Event Management (SIEM)*.

Tujuan utama pelaksanaan magang ini adalah untuk meningkatkan kemampuan teknis dalam menganalisis log, mendeteksi dan menangani insiden, serta menjalin koordinasi di lingkungan kerja *Security Operation Center (SOC)*. Selain aspek teknis, kegiatan ini juga menumbuhkan kemampuan *soft skill* seperti komunikasi, kolaborasi tim, serta pengelolaan waktu secara efektif.

Partisipasi langsung dalam kegiatan operasional keamanan siber memberikan wawasan yang lebih mendalam mengenai alur kerja, penggunaan teknologi, serta tantangan nyata dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi. Oleh karena itu, program magang ini berperan sebagai jembatan antara teori akademik dan penerapan profesional untuk membentuk sumber daya manusia yang kompeten di bidang keamanan informasi.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Kegiatan magang di PT. Defender Nusa Semesta berlangsung selama 15 minggu, dimulai pada 1 Juli 2025 hingga 10 Oktober 2025. Pelaksanaan kerja menggunakan sistem *shift* (Rabu–Sabtu) sesuai dengan kebijakan yang diterapkan oleh tim. Selama periode tersebut, jadwal kerja tetap berjalan meskipun bertepatan dengan hari libur nasional atau akhir pekan, apabila hari tersebut termasuk dalam rotasi *shift*. Secara keseluruhan, total hari kerja yang dijalani selama masa magang

berjumlah 63 hari, dengan estimasi durasi waktu kerja mencapai sekitar 649 jam.

Periode : 01 Juli 2025 – 10 Oktober 2025
Hari kerja : Rabu - Sabtu
Jam kerja : Menyesuaikan sistem kerja dan shift
Posisi : *Security Analyst*

Prosedur pelaksanaan kegiatan magang di PT. Defender Nusa Semesta dilaksanakan selama 15 minggu dengan sistem kerja *shift* selama empat hari setiap minggu. Peserta magang dibagi menjadi dua kelompok, yaitu Tim A (Sayap Kiri) yang bertugas dari hari Senin hingga Rabu, dan Tim B (Sayap Kanan) yang bertugas dari hari Rabu hingga Sabtu. Peserta magang yang tergabung dalam Tim B (Sayap Kanan) menjalankan jadwal kerja secara rutin setiap hari Rabu hingga Sabtu.

Sistem kerja diterapkan secara *rolling shift* yang terdiri dari tiga jenis *shift*, yaitu *Early Shift* (pukul 04.00–16.00 WIB), *Mid Shift* (pukul 09.00–21.00 WIB), dan *Night Shift* (pukul 19.00–06.00 WIB). Pergantian jadwal *shift* dilakukan secara bergiliran setiap minggu untuk menjaga keseimbangan waktu kerja.

Kehadiran setiap peserta disesuaikan dengan jadwal *shift* masing-masing dan tercatat secara otomatis melalui sistem tap *ID card* pada saat memulai *Shift*. Seluruh kegiatan dilaksanakan di bawah arahan dan supervisi langsung Tim SOC yang dipimpin oleh Bapak Andi dan Bapak Mario selaku *Team Leader* di PT. Defender Nusa Semesta.