BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi yang sangat pesat dalam beberapa dekade terakhir telah membawa dampak besar terhadap kehidupan manusia di berbagai bidang. Internet, sebagai salah satu penemuan terpenting abad ke-21, telah meruntuhkan batasan ruang dan waktu dalam komunikasi, transaksi, hingga penyimpanan informasi. Transformasi digital ini membuat hampir seluruh aktivitas bisnis, pemerintahan, dan sosial bergantung pada sistem jaringan dan infrastruktur TI.

Namun, di balik kemajuan tersebut, muncul ancaman baru yang tidak bisa diabaikan yaitu ancaman siber. Peningkatan konektivitas dan digitalisasi telah menjadi celah bagi pelaku kejahatan untuk melancarkan serangan siber yang semakin canggih. Ancaman ini meliputi pencurian data, serangan malware, phishing, ransomware, hingga *advanced persistent threat* (APT), yang tidak hanya merugikan individu, tetapi juga institusi besar dan negara. Pertumbuhan eksponensial perangkat yang terhubung ke internet telah meningkatkan kompleksitas infrastruktur siber, menjadikannya target yang rentan terhadap eksploitasi [1].

Seiring dengan meluasnya penggunaan layanan digital, permukaan serangan terhadap sistem informasi juga terus bertambah. Berbagai bentuk ancaman seperti *man-in-the-middle*, *denial-of-service*, eksploitasi kerentanan perangkat lunak, serta rekayasa sosial kini menjadi bagian dari lanskap serangan yang harus dihadapi organisasi modern [2]. Masalah ini diperparah oleh kesenjangan signifikan antara tingkat pengetahuan, sikap, dan perilaku pengguna terhadap praktik keamanan informasi yang masih rendah [3].

Di Indonesia, persoalan keamanan siber tidak hanya berkaitan dengan isu teknis, tetapi juga menyentuh aspek regulasi dan kesiapan nasional. Indonesia masih menempati peringkat ke-70 dari 195 negara dalam Global Cybersecurity Index. Rendahnya literasi digital, belum optimalnya regulasi nasional, serta lemahnya koordinasi antar lembaga menjadikan ruang siber nasional sangat rentan terhadap serangan dan eksploitasi digital [4].

Untuk menjawab tantangan tersebut, keamanan siber harus dibangun

melalui pendekatan yang holistik dan berkelanjutan. Tidak cukup hanya dengan mengandalkan teknologi, tetapi juga harus diperkuat dengan kebijakan yang adaptif, prosedur yang terstandarisasi, serta sumber daya manusia yang kompeten.

Dalam konteks ini, keberadaan *Security Operation Center* (SOC) menjadi sangat penting. SOC berperan sebagai pusat pengendali untuk melakukan pemantauan, analisis, dan respons terhadap insiden keamanan siber secara real-time. Meski demikian, operasional SOC tidak terlepas dari tantangan yang kompleks, seperti beban kerja tinggi, kebutuhan integrasi berbagai sistem keamanan, dan kelangkaan tenaga profesional yang terampil [5].

Peran *Cyber Security Analyst* di lingkungan SOC menjadi komponen krusial dalam proses deteksi dan penanganan insiden. Tugasnya mencakup analisis, validasi, dan eskalasi terhadap berbagai jenis ancaman yang terdeteksi melalui *security tools* seperti *SIEM*, *EDR*, *IDS/IPS*, *firewall*, dan *threat intelligence platform* [6].

Salah satu entitas profesional yang bergerak dalam bidang layanan keamanan siber di Indonesia adalah **PT Defender Nusa Semesta (Defenxor)**. Defenxor menyediakan layanan keamanan informasi melalui tiga pilar utama: DIMS (*Managed Security*), DISC (*Consulting*), dan DISI (*Integrator*). Kegiatan magang dilaksanakan pada unit SOC yang memiliki fokus utama pada pemantauan dan analisis insiden keamanan informasi.

1.2 Maksud dan Tujuan Kerja Magang

Program kerja magang merupakan bagian penting dalam proses pembelajaran di perguruan tinggi yang bertujuan untuk memberikan pengalaman langsung di dunia kerja. Melalui kegiatan magang ini, mahasiswa memiliki kesempatan untuk memahami bagaimana teori-teori yang dipelajari di kelas diterapkan dalam lingkungan profesional yang nyata. Pada pelaksanaannya di Defenxor, kegiatan magang difokuskan pada bidang keamanan informasi, khususnya dalam operasional *Security Operations Center*, di mana keterlibatan secara langsung dalam proses monitoring, analisis, dan eskalasi insiden menjadi bagian utama dari peran yang dijalankan.

Program kerja magang bertujuan untuk memahami dan mendalami peran seorang *Cyber Security Analyst* dalam kegiatan *monitoring* dan analisis ancaman siber menggunakan *security tools* di lingkungan SOC Defenxor.

Selain itu, kegiatan magang ini juga difokuskan pada peningkatan kemampuan teknis dan praktis dalam menghadapi berbagai skenario insiden keamanan informasi, termasuk praktik analisis log, pemrosesan alert, serta pemahaman prosedur penanganan insiden dan komunikasi kepada pelanggan sesuai standar operasional yang berlaku di Defenxor.

Secara khusus, tujuan dari pelaksanaan kerja magang ini adalah sebagai berikut:

1. Mengembangkan keterampilan teknis dalam mendeteksi, menganalisis, dan merespons insiden siber berdasarkan data yang diperoleh dari sistem keamanan seperti *SIEM*, *EDR*, *IDS/IPS*, *WAF*, dan *threat intelligence*.
2. Mempelajari alur kerja SOC yang mencakup proses *alert triage*, investigasi insiden, hingga penyusunan laporan dan notifikasi kepada pihak pelanggan.
3. Mendukung kegiatan operasional harian SOC sebagai *supporting analyst* melalui kontribusi nyata dalam analisis insiden, dokumentasi, dan kolaborasi teknis.
4. Menghubungkan pengetahuan akademik dari perkuliahan dengan praktik nyata di industri keamanan siber, serta membangun kesiapan profesional dalam menghadapi tantangan di bidang ini.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Program magang dilaksanakan di Defenxor pada divisi SOC, di bawah pilar DIMS. Kegiatan magang berlangsung selama satu tahun, dari tanggal 3 Februari 2025 hingga 2 Februari 2026, secara *onsite* penuh waktu di kantor pusat operasional yang berlokasi di Graha BIP lantai 6, Jalan Jenderal Gatot Subroto Kavling 23, Karet Semanggi, Jakarta Selatan.

Setelah menyelesaikan masa pelatihan awal, peserta magang mengikuti sistem kerja *shifting* yang diterapkan di lingkungan SOC. Pembagian kerja dibagi menjadi dua sayap, yaitu sayap kiri (Minggu–Rabu) dan sayap kanan (Rabu–Sabtu), dengan rotasi jadwal mingguan: *Early Shift* (05.00–15.00 WIB), *Mid Shift* (10.00–20.00 WIB), dan *Late Shift* (19.30–05.30 WIB). Penempatan awal berada di sayap kanan dengan jadwal *Late Shift*.

Tahap pelatihan berlangsung selama satu bulan pertama, setiap hari kerja (Senin–Jumat, pukul 08.00–17.00 WIB), mengacu pada silabus *CompTIA*

Security+. Materi meliputi pengamanan perangkat, ancaman jaringan, *malware*, *system hardening*, kriptografi, manajemen risiko, serta penanganan insiden dan protokol jaringan. Kegiatan pelatihan mencakup presentasi topik teknis dan penyelesaian dua *case analysis* berdasarkan skenario nyata, yang kemudian dievaluasi oleh tim *Senior Security Analyst*.