BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan digital serta teknologi informasi membawa dampak besar terhadap operasional bisnis. Namun, di balik manfaat tersebut, terdapat pula risiko keamanan siber yang semakin kompleks, salah satunya adalah serangan siber. Berbagai ancaman ini tidak hanya menyerang sistem informasi, tetapi juga dapat merugikan reputasi dan kepercayaan pengguna terhadap sebuah organisasi atau perusahaan. Serangan siber kini lebih terorganisir dan menggunakan berbagai teknik canggih yang sulit untuk dideteksi, serta seringkali berdampak destruktif bagi perusahaan. Hal ini memaksa perusahaan untuk terus beradaptasi dan memperkuat pertahanan mereka dalam melindungi informasi yang bersifat *confidential* [1].

Serangan siber modern cenderung lebih terorganisir, canggih, dan persisten. Para pelaku kejahatan siber kini memanfaatkan berbagai teknik serta taktik yang sulit dideteksi secara konvensional, seperti *social engineering*, *fileless malware*, hingga *Advanced Persistent Threats* (APT) [2]. Dampak dari serangan ini tidak hanya mencakup gangguan operasional dan kerugian finansial, tetapi juga dapat merusak reputasi serta menurunkan tingkat kepercayaan publik terhadap perusahaan.

Dalam menghadapi kondisi ini, organisasi perlu membangun sistem pertahanan siber yang adaptif dan responsif. Salah satu langkah strategis yang dilakukan adalah dengan membentuk *Security Operations Center* (SOC), yaitu unit yang bertugas untuk melakukan *monitoring*, deteksi, analisis, dan respons terhadap insiden keamanan secara *real-time*. Di lingkungan SOC, khususnya pada level 1 (L1), proses deteksi awal menjadi sangat krusial karena menjadi garda terdepan dalam mengidentifikasi indikasi serangan siber [3] [4].

Namun, efektivitas proses deteksi dan mitigasi di SOC Level 1 sangat bergantung pada standar, prosedur, dan kerangka kerja yang digunakan. Dalam hal ini, MITRE ATT&CK Framework (*Adversarial Tactics, Techniques, and Common Knowledge*) menjadi salah satu referensi yang banyak digunakan secara global [2] [4]. Framework ini menyediakan basis pengetahuan yang komprehensif mengenai taktik, teknik, dan prosedur (TTP) yang digunakan oleh pelaku ancaman siber.

Dengan menggunakan MITRE ATT&CK untuk beberapa *case*, tim SOC dapat memahami pola serangan, melakukan analisis perilaku musuh, serta merespons insiden dengan pendekatan berbasis intelijen [4] [5].

1.2 Maksud dan Tujuan Kerja Magang

Kegiatan magang ini dilaksanakan dengan tujuan utama untuk memberikan pengalaman langsung di dunia kerja, khususnya dalam bidang keamanan siber sebagai *Security Analyst*. Tujuan yang ingin dicapai melalui kegiatan magang ini meliputi:

1. Menerapkan *softskill* dan *hardskill* yang telah diperoleh selama masa studi ke dalam praktik nyata di lingkungan *Security Operation Center (SOC)*.
2. Mengembangkan pengalaman profesional dalam bidang *cyber security*, sebagai bentuk persiapan memasuki dunia kerja secara penuh.
3. Memperdalam pengetahuan teknis dan operasional dalam *monitoring* keamanan jaringan dan sistem informasi secara *real-time*.
4. Memahami proses dan prosedur kerja di dalam SOC, termasuk dalam penggunaan *tools monitoring*, pelaporan insiden, dan penerapan *framework* keamanan.
5. Berkontribusi langsung dalam kegiatan operasional SOC, khususnya dalam *monitoring* dan analisis keamanan terhadap *appliance/customer* yang menjadi tanggung jawab tim.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Kegiatan magang ini dimulai pada tanggal 3 Februari 2025 dan berakhir pada bulan Juli 2025. Sistem kerja yang diterapkan adalah sistem kerja *shifting*, menyesuaikan kebutuhan pemantauan keamanan yang berlangsung selama 24 jam setiap hari (24/7). *Shifting* ini terbagi ke dalam tiga jadwal kerja sebagai berikut:

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

Selain pembagian shift, sistem kerja juga dibagi menjadi dua kelompok rotasi mingguan berdasarkan hari kerja, yaitu:

- Sayap Kiri: bekerja pada hari Minggu, Senin, Selasa, dan Rabu
- Sayap Kanan: bekerja pada hari Rabu, Kamis, Jumat, dan Sabtu

Setiap peserta magang juga akan ditempatkan dalam salah satu dari dua tim operasional, yaitu Tim A dan Tim B. Masing-masing tim memiliki tanggung jawab untuk memantau *appliance* atau *customer* tertentu yang menjadi bagian dari layanan SOC.

Selama magang, peserta diwajibkan untuk menjaga komunikasi aktif dengan tim melalui platform komunikasi internal dan memastikan seluruh kegiatan operasional tercatat dan dilaporkan sesuai dengan prosedur yang berlaku di SOC.