BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi Informasi telah berkembang pesat dalam satu dekade terakhir, dengan tingkat konsumsi internet yang sangat tinggi secara global oleh individu maupun organisasi, termasuk di bidang akademik, pemerintahan, hingga sektor industri [1]. Dengan pesatnya perkembangan teknologi informasi ini muncul juga masalah baru yaitu keamanan siber. Keamanan siber bukan hanya sebuah masalah teknis, tetapi juga sangat dipengaruhi oleh pengguna bukan ahli yang berinteraksi dengan konten daring [2].

Dalam menghadapi tantangan ini, banyak organisasi mengandalkan *Security Operations Center* (SOC) sebagai pusat pengawasan, deteksi, dan respon terhadap insiden keamanan siber. SOC berperan penting dalam menjaga keberlangsungan sistem dan mencegah dampak merugikan akibat serangan siber apabila diimplementasikan dengan benar [3].

Karena itu ancaman terhadap data dan sistem informasi terus berkembang. Pengalaman magang dalam divisi SOC akan memberikan wawasan mendalam mengenai strategi mitigasi risiko, analisis insiden keamanan, serta implementasi kebijakan keamanan siber dalam lingkungan industri.

1.2 Maksud dan Tujuan Kerja Magang

Maksud dari pelaksanaan kerja magang ini adalah untuk mempelajari secara langsung proses *monitoring* sistem SIEM (*Security Information and Event Management*) dan EDR (*Endpoint Detection and Response*) dalam ruang lingkup operasional *Security Operations Center* (SOC).

Tujuan dalam menjalankan proses kerja magang ini adalah:

1. Menambah keterampilan teknis dalam bidang keamanan siber terutama dalam menggunakan sistem SIEM dan EDR.
2. Menambah keterampilan dalam menggunakan *threat intelligence* dalam proses menganalisa insiden keamanan siber.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Program magang ini dilaksanakan selama enam bulan, mulai dari 16 Desember 2024 hingga 16 Juni 2025. Pada empat bulan pertama, kerja magang dilaksanakan di bagian SOC Level 1 (L1), yang berfokus pada pemantauan awal, analisis insiden dasar, dan eskalasi kejadian keamanan siber. Selanjutnya, ditempatkan di bagian SOC Level 2 (L2) selama satu bulan, yang menangani analisis insiden yang lebih mendalam, investigasi lanjutan, serta respons terhadap ancaman keamanan siber yang lebih kompleks.

Selama program magang berlangsung, jadwal kerja yang telah ditetapkan oleh perusahaan adalah setiap hari Senin hingga Jumat, dengan jam kerja dari pukul 09.00 hingga 17.00 WIB. Selain itu, terdapat waktu istirahat makan siang selama 1 jam yang disediakan bagi seluruh karyawan dan peserta magang.

Paralel dengan berlangsungnya program magang di tiga bulan pertama, PT Visionet juga mengadakan bootcamp bagi peserta magang. Bootcamp ini bertujuan untuk meningkatkan pemahaman dan keterampilan dalam bidang *cybersecurity*, khususnya dalam konteks operasional di SOC. Melalui program ini, peserta mendapatkan pelatihan teknis dan praktik langsung yang mendukung tugas-tugas mereka selama magang.