BAB I
PENDAHULUAN

1.1 Latar Belakang Kerja Profesi

Cybersecurity atau keamanan siber adalah langkah yang diambil untuk melindungi sistem informasi dari berbagai potensi ancaman, baik itu serangan *malware*, peretasan, pencurian data, atau bentuk serangan siber lainnya. Di dunia yang semakin terkoneksi, perlindungan terhadap data dan sistem informasi tidak hanya menjadi tanggung jawab departemen IT, tetapi juga menjadi aspek kritis yang harus dikelola dengan cermat di seluruh organisasi.

Kerja profesi dalam bidang *cyber security* berperan penting dalam mengidentifikasi, menganalisis, dan mengurangi risiko keamanan yang mungkin terjadi. Salah satu komponen utama dalam *cyber security* adalah *monitoring* dan analisis. Kegiatan *monitoring* dilakukan untuk memantau secara terus-menerus aktivitas dalam sistem, mendeteksi potensi ancaman, serta memastikan bahwa sistem berjalan dengan aman dan lancar. Sedangkan analisis *cyber security* mengacu pada pemahaman lebih dalam terhadap pola ancaman yang muncul, serta mengidentifikasi titik lemah dalam sistem yang perlu diperkuat.

Monitoring dan analisis ini tidak hanya penting untuk mendeteksi serangan secara dini, tetapi juga untuk meningkatkan strategi keamanan yang diterapkan. Dengan terus melakukan evaluasi dan perbaikan berdasarkan data yang didapatkan dari *monitoring* dan analisis, perusahaan dapat mengurangi risiko keamanan dan meminimalisir kerugian yang muncul.

Kerja profesi atau magang sebagai *Cybersecurity Intern* di PT NOOSC Security Global memberikan kesempatan bagi praktikan untuk terlibat langsung dalam kegiatan yang terkait dengan keamanan siber. Sebagai bagian dari tim *Security Operation Center Analyst*, praktikan akan belajar tentang pemantauan *real-time* terhadap aktivitas jaringan dan sistem untuk mendeteksi potensi ancaman. Praktikan akan berlatih menggunakan berbagai alat keamanan siber, seperti *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), *Service Desk*, *Security*

Information and Event Management (SIEM), pengalaman ini sangat berharga untuk memahami bagaimana tim SOC beroperasi dan bagaimana informasi dikumpulkan serta dianalisis untuk memberikan respons yang tepat terhadap insiden siber. Di sisi lain, sebagai *Cybersecurity Analyst*, praktikan akan terlibat dalam menganalisis data kerentanan yang ada dan melakukan evaluasi terhadap potensi kerentanan dalam sistem seperti melakukan rekapitulasi tiket, serta praktikan akan belajar membuat *use case* untuk *dashboard monitoring* yang berguna untuk SOC. Pengalaman tersebut bermanfaat untuk mengembangkan wawasan mengenai proses deteksi dini dan respons cepat terhadap potensi ancaman keamanan siber di SOC.

Praktikan diberikan kesempatan untuk mengikuti program kerja di posisi *Cybersecurity Engineer*. Dalam program ini, praktikan ditugaskan melakukan *dismantle server*, instalasi SIEM Wazuh, simulasi penyerangan ke Wazuh, serta pembuatan *server* dan konfigurasi *firewall*. Pengalaman tersebut memberikan pengalaman praktis yang mendalam di bidang keamanan siber. Praktikan juga diarahkan pada posisi *Vulnerability Assessment Penetration Testing* (VAPT) *and Project Manager* dalam proyek *Pilot Project Technical Security Assessment*. Pada tahap awal dimulai dengan inisiasi kebutuhan pengguna terkait VAPT, mencakup diskusi untuk menentukan area pengujian keamanan dan prioritas risiko. Berdasarkan inisiasi tersebut, Praktikan menetapkan *scope* proyek yang jelas, menyusun *timeline* menggunakan *kanban board* dan *gantt chart*, serta merancang hasil berupa laporan teknis berisi temuan kerentanan, analisis risiko, dan rekomendasi mitigasi. Untuk mendukung pelaksanaan, digunakan *tools* seperti Tenable Nessus untuk pemindaian kerentanan, Canva untuk desain laporan, dan Google Slide untuk presentasi hasil.

Melalui program magang ini, praktikan akan memiliki kesempatan untuk bekerja dalam lingkungan kolaboratif yang mencakup tim profesional berpengalaman. Praktikan akan belajar tentang pentingnya komunikasi dan koordinasi dalam merespons insiden keamanan, serta bagaimana menciptakan budaya keamanan yang kuat di seluruh organisasi. Selain itu, praktikan akan mengembangkan jaringan profesional yang dapat membantu praktikan dalam pencarian pekerjaan di masa depan.

1.2 Maksud dan Tujuan Kerja Profesi

1.2.1 Maksud Kerja Profesi

Maksud dari pelaksanaan kegiatan magang kerja profesi yaitu:

1. Melakukan pemantauan dan analisis keamanan sistem.
2. Mengembangkan dan mengimplementasikan solusi Keamanan.
3. Mendukung tim *cyber security* dalam penanganan insiden

1.2.2 Tujuan Kerja Profesi

Tujuan dari pelaksanaan kegiatan magang kerja profesi yaitu:

1. Meningkatkan pemahaman tentang operasi keamanan siber.
2. Meningkatkan keterampilan teknis dan analis.
3. Menyiapkan diri untuk peran profesional di industri keamanan siber.

1.3 Tempat Kerja Profesi

Praktikan melaksanakan kegiatan Kerja Profesi di PT NOOSC Security Global, yang berlokasi di Gedung Graha Mandiri, 2nd floor Jl. Imam Bonjol No. 61 Jakarta, 10310, Indonesia.

Gambar 1. 1 Gedung Graha Mandiri

1.4 Jadwal Pelaksanaan Kerja Profesi

Kerja Profesi dilaksanakan selama 6 bulan yang dimulai pada tanggal 8 Juli 2024 hingga 7 Januari 2025. Pelaksanaan kegiatan Kerja Profesi pada PT NOOSC Security Global dimulai saat praktikan masuk ke kantor *Office Hour* pada pukul 09.00–18.00 WIB, setelah itu praktikan diarahkan pembimbing ke posisi SOC *Analyst* mengikuti jam kerja *shift* 1 SOC yaitu dimulai pada pukul 07.00–15.00 WIB dan kedua jam kerja tersebut bersifat *on-site* atau datang ke kantor.