BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Di era digital saat ini perkembangan teknologi semakin pesat dan terus meningkat hal ini mendorong berbagai perusahaan untuk memanfaatkan system berbasis teknologi. Namun, di balik kemudahan yang diberikan, transformasi digital ini berbanding lurus dengan tingkat risiko keamanan digital berupa ancaman siber yang semakin meningkat. Menurut Laksana dan Mulyani (2024) aset digital merupakan target utama untuk ancaman siber. Kegagalan dalam melindungi aset digital mengakibat kerugian yang sangat fatal, mulai dari segi finansial hingga menurunkan reputasi suatu perusahaan [1]. Maka dari itu, keamanan siber menjadi suatu kebutuhan esensial bagi organisasi yang berguna untuk memastikan bahwa kerahasiaan, integritas, dan ketersediaan data terjaga dengan baik

Suatu organisasi perlu membangun arsitektur pertahanan siber yang komprehensif, dengan mengimplementasikan keamanan proaktif dan reaktif. Secara reaktif, kegiatan *penetration testing* wajib dilakukan di dalamm organisasi guna mengevaluasi sistem keamanan jaringan internal dengan cara melakukan serangan untuk mengidentifikasi dan memperbaiki celah keamanan sebelum di eksploitasi oleh pihak peretas. Dalam sisi pemantauan reaktif dan berkelanjutan, integrasi *Security Information and Event Managemenent* (SIEM) dengan *Security Orchestration, Automation and Response* (SOAR) merupakan peran penting dalam segi pertahanan. SIEM berfungsi sebagai pusat pemantauan dengan mengumpulkan *log* aktivitas secara *real time* guna mendeteksi anomali, sedangkan SOAR berguna untuk mempercepat mitigasi ancaman dengan cara mengotomasikan tanggapan terhadap insiden keamanan [2].

Di dalam ekosistem saat ini harus disadari akan pentingnya kedua aspek tersebut, melaksanakan program magang dengan focus pada *IT Security*. Selama masa magang, fokus pada *monitoring* dengan menggunakan SIEM dan SOAR guna mendeteksi ancaman, serta melaksanakan kegiatan *penetration testing* ke dalam domain internal perusahaan. Diharapkan dapat memberikan kontribusi secara langsung dalam proses membangun sistem keamanan perusahaan, serta memberikan pengalaman yang nyata dalam proses memitigasi risiko keamanan siber.

1.2 Maksud dan Tujuan Kerja Magang

Program kerja magang ini memiliki maksud dan tujuan khusus yang terkait dengan ruang lingkup operasi keamanan siber perusahaan.

1.2.1 Maksud Magang

Maksud dari pelaksanaan program magang ini adalah untuk mengimplementasikan teori-teori keamanan siber yang telah dipelajari secara akademis ke dalam praktik operasional di lingkungan industri nyata.

1.2.2 Tujuan Magang

Adapun tujuan operasional yang ingin dicapai dari kegiatan magang ini adalah sebagai berikut:

1. Mengoperasikan *Monitoring* Keamanan: Mengoperasikan cara kerja *platform* SIEM dan SOAR digunakan untuk melakukan monitoring, triase, dan deteksi ancaman keamanan siber secara *real time*.
2. Mengevaluasi Keamanan Infrastruktur: Melakukan simulasi kegiatan *Penetration Testing* yang terstruktur pada infrastruktur dan domain internal perusahaan guna mengidentifikasi celah keamanan secara proaktif
3. Memberi Solusi Mitigasi: Membuat laporan teknis yang menguraikan hasil identifikasi kerentanan dan saran perbaikan untuk membantu perusahaan memperkuat arsitektur keamanan jaringan internalnya.
4. Meningkatkan Kompetensi Profesional: Meningkatkan kemampuan untuk menganalisis, menyelesaikan masalah, dan memahami standar operasional prosedur (SOP) penanganan insiden keamanan di lingkungan kerja profesional.

1.3 Waktu dan Prosedur Kerja Magang

Magang ini dilakukan secara tatap muka penuh atau dari kantor (*WFO*) di ASG Tower. Program magang akan berlangsung selama sekitar enam bulan, yaitu dari 5 Januari 2026 hingga 30 Juni 2026. Selama masa magang, pekerja akan bekerja dari Senin hingga Jumat dari pukul 08.30 hingga 17.30 WIB.

Proses magang dimulai dengan pengenalan tentang lingkungan kerja, infrastruktur jaringan, dan kebijakan keamanan perusahaan. Selanjutnya, kegiatan operasional biasa dilakukan sesuai jam kerja yang berlaku. Ini termasuk *monitoring* insiden keamanan menggunakan *platform* SIEM dan SOAR serta melakukan tahapan pemeriksaan *penetration testing* pada *domain* internal yang ditugaskan. Seluruh aktivitas pekerjaan, penyebaran temuan anomali keamanan, dan penyusunan laporan dikoordinasikan secara langsung dengan supervisor