BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring berkembangnya teknologi, ketergantungan organisasi terhadap infrastruktur teknologi informasi sudah menjadi hal yang tidak terlepas lagi. Banyak organisasi yang mengembangkan aplikasi berbasis web maupun mobile baik untuk keperluan organisasi maupun publik. Ini secara langsung meningkatkan resiko terjadinya serangan siber. Karena itulah, bidang keamanan siber bukan lagi sekadar pelengkap, melainkan sebagai fondasi utama dalam menjaga integritas data dan menjamin keberlangsungan operasional organisasi. Namun, fakta di lapangan menunjukkan bahwa masih banyak sistem aplikasi yang memiliki kerentanan fatal. Fakta ini diperkuat berdasarkan data dari [1], yang menunjukkan bahwa serangan seperti Broken Access Control secara konsisten menempati posisi 10 besar dari 2021 hingga 2025. Resiko serangan siber juga diperparah dengan adanya penemuan yang menunjukkan bahwa 62% organisasi masih menggunakan sistem *legacy* [2] dan 71% aset jaringan organisasi berada dalam kondisi *ageing* [3], sehingga meninggalkan celah eksploitasi yang dapat mengancam infrastruktur organisasi.

Karena kondisi tersebut, organisasi perlu menetapkan suatu strategi untuk menjamin agar infrastruktur organisasi tetap aman dari ancaman siber. Strategi-strategi ini bisa berupa strategi ofensif seperti melakukan pengujian penetrasi (*penetration testing*) secara berkala pada sistem/aplikasi perusahaan. Ini memungkinkan tim keamanan organisasi dalam melakukan patching terhadap celah kerentanan tersembunyi sebelum dieksploitasi oleh pihak eksternal [4, 5]. Adapun strategi defensif yang dapat diterapkan dalam organisasi dalam mendeteksi serangan lebih awal sehingga organisasi dapat mencegah *lateral movement* sebelum serangan menyebar lebih luas [5]. Strategi defensif dapat berupa *monitoring and detection* menggunakan tools seperti SIEM, SOAR, dan lain sebagainya. SIEM memungkinkan organisasi dalam memonitoring aktivitas log dari berbagai aset infrastruktur dalam jaringan secara real-time [6], sedangkan SOAR memungkinkan tim keamanan dalam menangani ancaman yang lebih tinggi, dikarenakan ancaman yang lebih rendah akan ditangani otomatis oleh SOAR, sehingga proses insiden respon menjadi lebih cepat [7].

Sebagai salah satu pengembang properti di Indonesia, Agung Sedayu

Group mengandalkan berbagai infrastruktur teknologi informasi, termasuk platform aplikasi berbasis *website* dan *mobile*, untuk menunjang operasional bisnis skala besar serta memberikan pelayanan optimal kepada publik. Dikarenakan tingginya nilai aset digital dan data sensitif yang dikelola, implementasi strategi keamanan siber menjadi hal yang penting untuk mengantisipasi potensi insiden keamanan. Berdasarkan hal tersebut, maka diperlukan aktivitas pada pemantauan lalu lintas jaringan menggunakan SIEM/SOAR serta melakukan pengujian celah keamanan (*penetration testing*) guna mengidentifikasi dan memitigasi risiko kerentanan sedini mungkin.

1.2 Maksud dan Tujuan Kerja Magang

1.2.1 Maksud Kerja Magang

Kegiatan program kerja magang dijalankan dengan beberapa maksud, sebagai berikut:

1. Belajar sekaligus menambah pengalaman dalam bidang cybersecurity melalui praktik langsung di lapangan
2. Mengembangkan kemampuan komunikasi di lingkungan profesional
3. Membangun jaringan (*network*) profesional

1.2.2 Tujuan Kerja Magang

Kegiatan program kerja magang dijalankan dengan beberapa tujuan, sebagai berikut:

1. Monitoring lalu lintas jaringan dengan menggunakan SIEM untuk mendeteksi anomali lebih dini
2. Melakukan *penetration testing* pada aplikasi perusahaan berbasis website dan mobile untuk menemukan kerentanan
3. Melakukan dokumentasi hasil temuan sebagai bahan pembelajaran sekaligus memberikan rekomendasi perbaikan

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Career Acceleration Program (CAP) di Agung Sedayu Group dilaksanakan selama 6 bulan, terhitung mulai dari tanggal 29 Januari 2026 hingga 31 Juli 2026. Pelaksanaan kerja magang ini bertempat di ASG Tower, Jl. Pantai Indah Kapuk No.2, RT.6/RW.2, Kamal Muara, Penjaringan, Jakarta Utara 14470. Selama periode tersebut, sistem kerja yang diterapkan adalah *Work from Office* (WFO) dengan ketentuan hari kerja mulai dari hari Senin sampai Jumat, serta jam kerja operasional yang dimulai pada pukul 08:00 hingga 17:00 WIB.

Adapun beberapa prosedur pelaksanaan kerja magang setelah mendapatkan kesempatan magang di perusahaan Agung Sedayu Group, yaitu:

1. Tahap Persiapan dan Orientasi (*Onboarding*)
   Pada tahapan ini, diperkenalkan dengan lingkungan kerja seperti aturan perusahaan, jam kerja, dan lain sebagainya. Selain itu, diperkenalkan juga dengan tim IT Security dan mendapatkan kesempatan berdiskusi dengan pembimbing lapangan mengenai proyek atau target yang harus dicapai selama masa magang.

2. Proses Presensi Masuk Agung Sedayu Group
   Perusahaan Agung Sedayu Group menerapkan sistem presensi masuk menggunakan aplikasi *GreatDay*. Aplikasi tersebut telah mengintegrasikan sistem GPS (*Global Positioning System*) dan juga kamera, sehingga proses presensi mengharuskan karyawan untuk berada di dalam area gedung Agung Sedayu Group dan melakukan foto selfie sebagai bukti presensi masuk. Jika foto selfie dilakukan saat posisi berada di luar area gedung Agung Sedayu Group, maka sistem secara otomatis tidak mengizinkan dilakukannya presensi.

3. Proses Presensi Pulang Agung Sedayu Group
   Sama seperti pada proses presensi masuk di mana presensi pulang juga menggunakan aplikasi yang sama, yaitu *GreatDay* dan mengharuskan karyawan untuk melakukan foto selfie di dalam area gedung Agung Sedayu Group sebelum pulang sebagai bukti bahwa karyawan bekerja selama 8 jam dari jam masuk kerja dan memastikan karyawan tetap berada di area gedung Agung Sedayu Group.

4. Tahap Pelaksanaan Kerja

Pada tahapan ini, pelaksanaan rapat (*meeting*) resmi belum diizinkan bagi peserta magang. Namun, koordinasi tetap berjalan secara intensif melalui diskusi kelompok bersama tim internal setiap kali terdapat proyek yang perlu dikerjakan. Komunikasi difokuskan pada batasan proyek, seperti dalam melakukan *penetration testing*, di mana ditentukan secara spesifik mengenai jenis serangan yang diperbolehkan dan yang dilarang untuk dieksekusi. Selain itu, diskusi terkait dengan format standar dokumentasi hasil temuan juga didiskusikan agar konsisten dan lebih mudah untuk dipahami.