BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Di era digital yang semakin berkembang pesat, ketergantungan perusahaan terhadap teknologi informasi menjadi semakin tinggi. Hampir seluruh aktivitas bisnis kini bergantung pada sistem digital, mulai dari pengelolaan data pelanggan, transaksi keuangan, hingga komunikasi internal dan eksternal perusahaan. Namun, seiring dengan meningkatnya pemanfaatan teknologi, ancaman terhadap keamanan siber juga mengalami peningkatan yang signifikan. Serangan siber tidak hanya menyasar perusahaan berskala besar, tetapi juga menargetkan organisasi menengah hingga kecil yang memiliki sistem keamanan kurang optimal.

Serangan siber dapat berdampak serius terhadap aset digital yang dimiliki oleh suatu perusahaan, seperti kebocoran data, kerugian finansial, hingga menurunnya reputasi perusahaan. Serangan ini dapat terjadi dikarenakan lemahnya sistem keamanan dan kurangnya kesadaran manusia terhadap pentingnya keamanan siber. Oleh karena itu, diperlukan sebuah sistem yang dapat mendeteksi dan merespons setiap serangan siber dengan cepat dan efektif.

Stellar merupakan sebuah platform berbasis *Open XDR (Extended Detection Response)* yang dikenal memiliki fitur keamanan yang efektif dan efisien. Stellar menawarkan berbagai keunggulan dalam konteks keamanan siber, termasuk enkripsi data yang kuat, autentikasi pengguna yang ketat, dan kemampuan untuk mendeteksi aktivitas yang mencurigakan secara realtime. Penggunaan Stellar ini dapat meningkatkan tingkat keamanan sistem dari beberapa client PT. Sembilan Pilar Semesta, serta meminimalisir resiko dari serangan siber yang berpotensi merugikan dari suatu client. Selain itu, Stellar ini juga dilengkapi dengan machine learning yang dapat mengidentifikasi pola-pola ancaman yang kompleks, serta memberikan peringatan dini sebelum insideninsiden keamanan terjadi. Dengan demikian Stellar berperan penting dalam mencegah serta mengurangi dampak serangan siber terhadap client perusahaan.

Dalam implementasinya, Stellar digunakan untuk melakukan monitoring keamanan terhadap berbagai *tenant client* dengan karakteristik dan tingkat risiko yang berbeda. *Client* yang ditangani mencakup sektor perbankan, transportasi kereta api, serta beberapa lembaga pemerintahan yang mengelola data dan

sistem bersifat kritis. Sektor-sektor tersebut memiliki kebutuhan keamanan yang tinggi karena berkaitan langsung dengan data sensitif, layanan publik, serta keberlangsungan operasional. Oleh karena itu, proses monitoring, analisis, dan respons insiden dilakukan secara berkelanjutan untuk memastikan bahwa setiap potensi ancaman dapat terdeteksi dan ditangani sejak dini guna meminimalisir dampak terhadap sistem dan kepercayaan publik.

1.2 Maksud dan Tujuan Kerja Magang

Maksud dari pelaksanaan magang ini adalah untuk memenuhi kewajiban program magang yang ditetapkan oleh kampus, sekaligus memberikan kesempatan untuk menambah wawasan serta pengalaman praktis di bidang keamanan siber dan analisis insiden keamanan. Melalui keterlibatan langsung dalam kegiatan monitoring dan analisis sistem keamanan menggunakan platform Stellar di lingkungan PT. Sembilan Pilar Semesta, kegiatan magang ini juga dimaksudkan untuk memperdalam pemahaman mengenai cara kerja sistem deteksi dan respons ancaman serta proses penanganan alert keamanan secara real-time. Selain itu, magang ini juga menjadi sarana untuk melatih kemampuan dalam mengidentifikasi pola serangan, memahami alur eskalasi insiden, serta mengenal lebih dekat dinamika kerja di bidang keamanan informasi pada bidang cyber security.

Tujuan dari pelaksanaan kerja magang ini adalah untuk melakukan analisis dan evaluasi terhadap *alert* serta aktivitas mencurigakan yang terdeteksi oleh Stellar Cyber pada jaringan client PT. Sembilan Pilar Semesta. Kegiatan ini meliputi pemantauan keamanan secara berkala, klasifikasi tingkat keparahan alert, verifikasi potensi ancaman, serta pelaporan hasil analisis kepada tim keamanan siber perusahaan. Dengan adanya kegiatan analisis ini, diharapkan dapat membantu meningkatkan efektivitas sistem deteksi ancaman, meminimalisir risiko serangan siber, serta memperkuat keamanan data dan infrastruktur digital milik client. Selain itu, pelaksanaan magang ini juga bertujuan untuk memberikan pengalaman nyata dalam proses incident monitoring, threat analysis, dan cyber defense operations di lingkungan profesional.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Program magang di PT Sembilan Pilar Semesta (SPS) dilaksanakan selama enam bulan, terhitung sejak 26 Agustus 2025 hingga 25 Februari 2026, yang

berlokasi di Ruang SOC (Security Operation Center), Gedung SOHO Pancoran Suite Noble 1006 Lt.10, Jl. Letjen MT. Haryono Kav. 2-3, Kelurahan Tebet Barat, Kecamatan Tebet, Kota Jakarta Selatan – 12810. Selama periode magang, kegiatan dilaksanakan berdasarkan prosedur yang telah ditetapkan sebagai berikut:

1. Kegiatan magang dilaksanakan secara WFO (Work From Office) selama lima hari kerja dalam seminggu, dengan total waktu kerja sekitar 40 jam per minggu. Jadwal kerja bersifat fleksibel, menyesuaikan dengan kebutuhan perusahaan serta sistem shift kerja yang berlaku di ruang SOC.
2. Setelah setiap akhir shift, dilakukan rekap aktivitas shift yang berisi laporan mengenai kegiatan, hasil pemantauan, serta kendala yang dihadapi selama jam kerja.
3. Perusahaan menyelenggarakan rapat rutin setiap minggu melalui Google Meet untuk membahas perkembangan pekerjaan, evaluasi hasil kerja, serta koordinasi antaranggota tim.
4. Jika ditemukan kebingungan atau keraguan terhadap alert yang muncul, segera dilakukan eskalasi kepada tim senior atau supervisor untuk mendapatkan konfirmasi dan memastikan langkah penanganan yang sesuai.
5. Program magang dapat diperpanjang hingga dua belas bulan atau dilanjutkan ke tahap kerja penuh waktu setelah dilakukan evaluasi terhadap kinerja.