BAB 1. PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam tata kelola pemerintahan. Sistem Pemerintahan Berbasis Elektronik (SPBE) menjadi salah satu langkah strategis untuk meningkatkan efisiensi, efektivitas, transparansi, dan akuntabilitas dalam pelayanan publik. Namun, seiring meningkatnya adopsi teknologi ini, ancaman terhadap keamanan siber juga terus berkembang. Ancaman tersebut dapat memengaruhi kerahasiaan, integritas, dan ketersediaan data pemerintahan, sehingga mengganggu operasional sistem secara keseluruhan.

Sebagai lembaga yang bertanggung jawab langsung kepada Presiden, Badan Siber dan Sandi Negara (BSSN) memiliki peran strategis dalam menjaga keamanan informasi dan keamanan siber di Indonesia. Salah satu tugas utama BSSN adalah melaksanakan identifikasi, proteksi, mitigasi, hingga pemulihan dari ancaman siber. Selain itu, BSSN juga berfungsi mengoordinasikan berbagai pemangku kepentingan untuk menciptakan sistem keamanan siber yang komprehensif di lingkungan pemerintahan.

Salah satu unit kerja strategis di BSSN adalah Direktorat Keamanan Siber dan Sandi Pemerintah Pusat (D31). Direktorat ini bertanggung jawab dalam meningkatkan kapasitas keamanan siber di sektor pemerintah pusat, pertahanan, dan penegakan hukum. Dalam pelaksanaannya, Direktorat D31 mengelola berbagai data penting, seperti hasil asistensi keamanan, tingkat kematangan keamanan siber, profil risiko keamanan informasi, serta data terkait sumber daya *Computer Security Incident Response Team* (CSIRT). Data tersebut memiliki klasifikasi terbatas, rahasia, hingga sangat rahasia.

Pengelolaan data yang dilakukan secara manual dan terpisah sering kali menjadi kendala dalam analisis cepat yang dibutuhkan pimpinan untuk pengambilan kebijakan strategis. Pengelolaan manual yang dimaksud melibatkan proses berbagi data antar tim yang masih mengandalkan komunikasi langsung dan saluran yang tidak terintegrasi, seperti melalui *excel* atau pertemuan tatap muka.

Hal ini menyebabkan waktu yang dibutuhkan untuk memperoleh atau mendistribusikan data menjadi lebih lama, sehingga memperlambat kelancaran analisis yang diperlukan. Oleh karena itu, dibutuhkannya optimalisasi pengelolaan dan berbagi data untuk mempercepat proses analisis profil atau anatomi keamanan siber sektor pemerintah pusat. Hal ini bertujuan agar pimpinan dapat menggunakan hasil analisis tersebut untuk pengambilan kebijakan yang tepat, sehingga pembinaan kapasitas keamanan siber dapat lebih efektif bagi *stakeholder* terkait.

Untuk itu, dirancang dan dibangun Sistem Informasi Direktorat 31 (SINDIT31), sebuah aplikasi berbasis *website* yang bertujuan mempermudah pengelolaan dan berbagi data secara optimal di lingkungan Direktorat Keamanan Siber dan Sandi Pemerintah Pusat. Aplikasi ini mencakup fitur pengelolaan hasil asistensi keamanan, tingkat kematangan keamanan siber, profil risiko keamanan informasi, data CSIRT, jadwal kegiatan, pengaturan akses pengguna, catatan aktivitas pengguna, visualisasi data yang terstruktur, serta data lainnya yang bersifat rahasia. Dengan mengutamakan prinsip keamanan siber melalui proses pengujian dan *hardening*, aplikasi ini diharapkan dapat mendukung tugas Direktorat D31 dalam memastikan keamanan sistem pemerintahan berbasis elektronik, sekaligus meningkatkan efektivitas pengelolaan keamanan siber nasional.

1.2 Tujuan dan Manfaat

1.2.1 Tujuan Umum Magang

Adapun tujuan magang secara umum adalah sebagai berikut:

1. Memberikan kesempatan kepada mahasiswa untuk memperoleh pengalaman kerja nyata di lingkungan profesional sesuai dengan bidang studinya.
2. Meningkatkan kompetensi teknis, manajerial, dan interpersonal melalui keterlibatan langsung dalam tugas-tugas di tempat kerja.
3. Menghubungkan teori yang telah dipelajari di bangku perkuliahan dengan praktik nyata di dunia kerja.

4. Meningkatkan pemahaman dan keterampilan mahasiswa dalam perancangan dan pembangunan aplikasi berbasis *website* dengan mengutamakan prinsip keamanan siber.
5. Mendukung tugas Direktorat Keamanan Siber dan Sandi Pemerintahan Pusat (D31) dengan merancang aplikasi Sistem Informasi Direktorat 31 (SINDIT31) untuk mempermudah pengelolaan dan berbagi data secara optimal dan aman.
6. Mengembangkan kemampuan analisis, komunikasi, dan kolaborasi dalam tim untuk menyelesaikan proyek yang diberikan.

1.2.2 Tujuan Khusus Magang

Adapun tujuan khusus magang adalah sebagai berikut:

1. Merancang dan membangun Sistem Informasi Direktorat 31 (SINDIT31) sebagai aplikasi berbasis *website* yang bertujuan untuk mengoptimalkan pengelolaan dan berbagi data secara aman di lingkungan Direktorat Keamanan Siber dan Sandi Pemerintah Pusat (D31).
2. Menerapkan standar teknis dan prosedur keamanan sistem elektronik dalam pembangunan aplikasi untuk memastikan integritas, kerahasiaan, dan ketersediaan data.
3. Memfasilitasi pengelolaan data penting, seperti hasil asistensi keamanan, tingkat kematangan keamanan siber, profil risiko keamanan informasi, data CSIRT, jadwal kegiatan, pengaturan akses pengguna, catatan aktivitas pengguna, serta data lainnya yang bersifat rahasia, melalui sistem yang terintegrasi dan aman.
4. Mengembangkan fitur visualisasi data yang terstruktur dan interaktif, seperti *bar chart*, *radar chart*, dan *donut chart*, untuk mempermudah analisis profil atau anatomi keamanan siber sektor pemerintah pusat.
5. Melakukan pengujian keamanan aplikasi bersama tim BSSN untuk mendeteksi potensi celah keamanan dan melaksanakan proses *hardening* untuk memperkuat sistem sebelum aplikasi digunakan secara resmi.

6. Mendukung tugas Direktorat D31 dalam meningkatkan efektivitas pengelolaan dan analisis data keamanan siber guna mendukung pengambilan kebijakan strategis oleh pimpinan.

1.2.3 Manfaat Magang

a. Manfaat bagi Mahasiswa:
    1. Memberikan pengalaman kerja nyata di lingkungan profesional, khususnya di bidang keamanan siber dan teknologi informasi.
    2. Meningkatkan keterampilan teknis dan kemampuan analisis melalui pelaksanaan tugas-tugas spesifik, seperti perancangan dan pembangunan aplikasi berbasis *website* yang aman.
    3. Mengembangkan kemampuan komunikasi, kolaborasi, dan manajemen waktu dalam menyelesaikan proyek bersama tim profesional.

b. Manfaat bagi Kampus:
    1. Meningkatkan kredibilitas kampus sebagai institusi pendidikan yang mendukung kolaborasi antara dunia akademik dan dunia kerja.
    2. Memberikan peluang bagi kampus untuk mendapatkan masukan mengenai kebutuhan industri atau instansi pemerintah, yang dapat diintegrasikan ke dalam kurikulum pendidikan.
    3. Memperkuat hubungan kerja sama dengan instansi atau perusahaan tempat mahasiswa magang, seperti BSSN, untuk membuka peluang kolaborasi lebih lanjut.

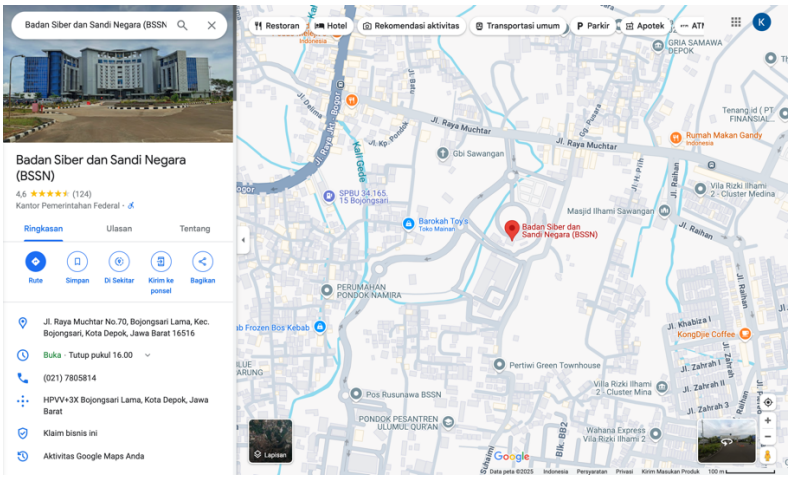
c. Manfaat bagi Instansi atau Perusahaan (Badan Siber dan Sandi Negara):
    1. Mendapatkan kontribusi langsung dari mahasiswa dalam bentuk hasil kerja, seperti aplikasi Sistem Informasi Direktorat 31 (SINDIT31), yang dapat mendukung pengelolaan dan berbagi data secara lebih efektif.

2. Memperoleh perspektif dan ide segar dari mahasiswa untuk meningkatkan efisiensi dan efektivitas dalam pelaksanaan tugas-tugas organisasi.
3. Membuka peluang untuk mengenali potensi sumber daya manusia yang berkualitas dari mahasiswa magang sebagai calon profesional di masa depan.

1.3 Lokasi dan Waktu

1.3.1 Lokasi

Kegiatan magang ini dilaksanakan di Badan Siber dan Sandi Negara (BSSN), tepatnya pada Direktorat Keamanan Siber dan Sandi Pemerintahan Pusat (D31), yang berlokasi di Jl. Raya Muchtar No.70, Bojongsari Lama, Kec. Bojongsari, Kota Depok, Jawa Barat 16516. Berikut adalah gambar lokasi tempat pelaksanaan magang:



Gambar 1. 1 Lokasi Magang di Badan Siber dan Sandi Negara

1.3.2 Waktu

Kegiatan magang ini dilaksanakan selama 4 bulan, dimulai pada tanggal 7 Oktober 2024 hingga 31 Januari 2025, dengan nilai 20 SKS. Jam kerja magang berlangsung dari hari Senin hingga Jumat, dengan jadwal Senin-Kamis pukul 07.30-16.00 WIB, dan khusus hari Jumat pukul 07.30-16.30 WIB.

1.4 Metode Pelaksanaan

Kegiatan magang di Badan Siber dan Sandi Negara (BSSN), khususnya pada Direktorat Keamanan Siber dan Sandi Pemerintahan Pusat (D31), dilaksanakan secara luring (*Work From Office*/WFO). Pelaksanaan kegiatan dilakukan dengan metode sebagai berikut:

1. Pelaksanaan Tugas Perancangan dan Pembangunan Aplikasi

   Tim yang terdiri dari 3 orang bertanggung jawab untuk merancang dan membangun aplikasi Sistem Informasi Direktorat 31 (SINDIT31) dari awal. Peran dalam tim dibagi menjadi *Full Stack Developer* dan *Backend Developer*, dengan masing-masing anggota mengerjakan tugas sesuai pembagian peran. Tim bekerja sama untuk memastikan setiap tahapan proses perancangan hingga pembangunan aplikasi berjalan dengan baik. Diskusi tim dilakukan secara rutin dua kali dalam seminggu untuk membahas progres, kendala yang dihadapi, dan menentukan prioritas pekerjaan berikutnya.

2. Penerapan Metodologi SDLC *Agile*

   Proses perancangan dan pembangunan aplikasi menggunakan metodologi *Software Development Life Cycle* (SDLC) *Agile*. Tahapan dimulai dengan planning, yaitu analisis kebutuhan berdasarkan masukan dari Direktorat D31, dilanjutkan dengan *design* berupa perancangan arsitektur sistem dan antarmuka pengguna (UI), dan *development* untuk membangun fitur-fitur aplikasi secara bertahap. Setelah itu dilakukan *functional testing* untuk memastikan aplikasi berfungsi sesuai desain dan bebas dari *bug*, diikuti dengan *deployment* ke lingkungan pengujian. Tim keamanan BSSN melakukan *security testing* untuk mendeteksi celah keamanan, yang kemudian diperbaiki melalui proses *hardening*. Setelah pengujian ulang memastikan aplikasi aman, sistem diluncurkan untuk digunakan.

3. Sesi Mentoring dan Pembelajaran

   Sesi mentoring diadakan setiap minggu untuk memantau progres pekerjaan dan memberikan arahan kepada peserta. Dalam sesi ini, tim juga diberikan

pembelajaran tambahan seperti product *knowledge*, tanya jawab, dan pembuatan *testcase* untuk pengujian aplikasi.

4. Pencatatan Aktivitas

   Seluruh aktivitas selama magang dicatat dalam *logbook* harian yang disediakan oleh BSSN sebagai dokumentasi kegiata